On Computer Security

(Edition of 2020)

By the CERN Computer Security Team

This publication is released under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License
Introduction
Introduction

Computer security articles turn 200 (2019)

Recently, we celebrated the 200th *Bulletin* article focusing on various topics relating to computer security. Two hundred hopefully informative articles about the current situation of cyber-security at CERN. About best practices, guidelines and useful tools. About threat scenarios and current attack vectors. About new or established means of mitigation. About the workings of the Computer Security team. About policies and Do’s and Don’ts. Two hundred articles trying to raise your awareness and trying to help you to improve your approach to computer security— the security of your laptops, smartphones, tablets, e-mail accounts, passwords, software and systems – at CERN and at home.

While some articles were published a long time ago – the first ones were released in 2008 – they have never lost their relevance. Sometimes it is useful to crawl into the past and dig out information from them and often these articles also provide guidelines for us when producing advisories for users. So for this 200th anniversary, we have produced a compilation of all the articles published so far. This compilation covers a plethora of topics, sorted into the notorious themes of “Computer Security”, i.e. the literal cyber-security of computers, “Mobile and Cloud Security”, “Network and Data Centre Security”, “Account and Password Security”, “Control Systems and IoT” – the Internet of Things –, “Secure Software Development”, “Data Protection and Privacy”, “Copyrights”, “Rules and Policies” and more. Giving a deeper insight into the computer security landscape, these articles are complementary to our *Monthly Reports*, which usually depict the operational side of what is currently happening at CERN.

You can download the compilation [here](https://home.cern/news/news/computing/computer-security-articles-turn-200). Please feel free to share it with your colleagues, family and friends!
Contents

Introduction ........................................................................................................... 3

Computer security articles turn 200 (2019) ......................................................... 3

Contents ................................................................................................................ 5

Computer Security .............................................................................................. 12

Still on Windows 7? Say “bye bye” to your digital life (2020) ............................. 12
Tele-protect (2020) ............................................................................................. 13
What do apartments and computers have in common? (2019) ......................... 14
When your mike spies on you (2019) ................................................................. 16
The rancid USB box of chocolate (2018) ........................................................... 17
Linux: Windows revisited (2018) ...................................................................... 18
Protect your Family (2018) ............................................................................... 19
An old scam in a new disguise (2018) ................................................................. 20
Stepping up in user education (2018) ................................................................. 21
Malware, ransomware, doxware and the like (2018) ......................................... 22
Another way of making money with ads (2018) ............................................ 24
Enter the next level: Doxware (2017) ................................................................. 25
Why you got a new PDF reader (2017) ............................................................. 26
“WannaCry”? The importance of being patched (2017) ................................ 27
Drive-bye (2016) .............................................................................................. 29
Playing hardball? Unfortunately it’s necessary... (2016) .................................... 30
DNS to the rescue! (2016) ............................................................................... 31
A few Christmas goodies for your security (2016) ............................................ 32
Open door, open screen, open life... (2016) ....................................................... 33
Flash, as bad as bad can be (2016) .................................................................. 33
Ransomware — When it is too late... (2016) ....................................................... 34
Mac security — Nothing for old versions (2016) .............................................. 35
USB sticks — The silent killers (2015) ............................................................... 35
Bye, bye, Windows XP security... Welcome infections! (2014) ...................... 36
Agility for computers (2014) ......................................................................... 37
Don’t put your family at risk (2013) ................................................................. 38
Got a call from "Microsoft"? The social way infecting your PC (2012) .......... 40
Infecting Windows, Linux & Mac in one go (2012) ......................................... 41
Gotcha! Macs lose their innocence (2012) ........................................................ 42
## Contents

### Mobile and Cloud Security

- Found a USB stick? Go and infect your PC! (2012) ........................................ 43
- 25 years — Happy Birthday! (2011) .............................................................. 43
- When apps lead to mishaps (2020) .............................................................. 46
- Un-confidentiality when using external e-mail (2019) ................................. 47
- Trips and travel: Some recommendations (2017) .......................................... 49
- Pokémon GO! Or not? (2016) ...................................................................... 50
- I know where you have been… since forever! (2016) .................................... 51
- Android’s Armageddon… Reloaded (2016) ................................................. 52
- Update on your privacy – or lack of it (2015) .............................................. 53
- Android’s armageddon (2015) .................................................................... 54
- IT or not IT, that is the question (2015) ..................................................... 55
- Enter the cloud, pay with your password (2014) ....................................... 56
- Your iPhone as a key-logger (2014) ............................................................ 57
- Backed up and gone... (2013) ................................................................. 58
- BYOD: Bring Your Own Disaster (2013) .................................................... 59
- Android is the new Windows (2013) .......................................................... 60
- Prison or “Prism”? Your data in custody (2013) ......................................... 61
- … And thank you for your mobile data! (2012) ........................................... 62
- One photo to rule your phone (2012) .......................................................... 63
- Smartphone lost — Privacy gone (2012) .................................................... 64
- When the “Lion” eats your data (2012) ......................................................... 64
- Is your Android running a temperature? (2012) ....................................... 65
- IPhones, Androids, and history repeating (2011) ....................................... 66
- Send your data into the cloud and make it… vaporize (2011) .................... 67

### Network and Data Center Security

- CERN’s new first line of defence (2020) ....................................................... 70
- Scanning for problems (2020) ................................................................. 72
- Videoconferencing pitfalls (2020) ............................................................. 73
- Tunnel Madness (2020) ........................................................................... 74
- Spectre and Meltdown, just the beginning? (2018) ................................. 75
- Scaling out intrusion detection (2018) ....................................................... 76
- Hardball for attackers (2017) ................................................................. 78
- CERN under friendly poking (2017) ......................................................... 79
- An attack for more security (2017) .......................................................... 81
Contents

Transparent monitoring for your protection (2016) ............................................... 82
DirtyCow BBQ — Well done, CERN! (2016) ............................................................ 83
Hacking CERN — A win-win for all (2015) ............................................................. 84
“Heartbleed” — A disaster for privacy (2014) ........................................................ 85
After Prism & Tempora: How much monitoring is OK for CERN? (2013) .......... 86
The lure of wireless encryption (2013) ................................................................. 88
Why I like power cuts... (2012) ............................................................................ 89

Account and Password Security ........................................................................... 90
Password revolutions (2020) ................................................................................ 90
Protecting the accelerator from remote evil (2020) .............................................. 91
A second factor to the rescue (2020) ................................................................. 93
I love you (2019) .................................................................................................. 95
The easy way to lose passwords (2018) ............................................................. 96
CERN secure password competition... NOT! (2018) ........................................... 99
Brain power vs. password managers (2017) ....................................................... 100
Pimp up your password (2016) .......................................................................... 102
The value of your password (2016) ................................................................. 103
What is your identity? (2016) ............................................................................... 104
Your privacy at CERN matters (2015) ............................................................... 105
Oops, there it goes... (2015) .............................................................................. 106
Don’t copy/paste passwords! (2014) ................................................................. 107
When a person leaves — Access rights remain! (2014) ...................................... 109
Maths to the rescue! (2013) ............................................................................... 110
No certificate, no chocolate (2013) ................................................................. 111
Don't tempt me! (2013) ...................................................................................... 113
Don’t let Chrome expose your passwords (2013) .............................................. 114
Creativity@CERN (2013) .................................................................................. 115
Train your brain: Don’t put your password on paper! (2012) ............................ 116
1000 passwords exposed, what about yours? (2011) ........................................ 117
Holidays come — Passwords go (2011) ............................................................. 117
What is a good toothbrush, erm, password? (2011) .......................................... 118
What do passwords and toothbrushes have in common? (2011) .................... 119

Email & Web Security .......................................................................................... 122
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEO fraud (2021)</td>
<td>122</td>
</tr>
<tr>
<td>Telecompromised (2020)</td>
<td>125</td>
</tr>
<tr>
<td>CERN has been phished again (2020)</td>
<td>126</td>
</tr>
<tr>
<td>Don’t answer me (2020)</td>
<td>128</td>
</tr>
<tr>
<td>Click and infect (2020)</td>
<td>129</td>
</tr>
<tr>
<td>Malicious Robots (2020)</td>
<td>130</td>
</tr>
<tr>
<td>Why the Internet is not Christmas (2019)</td>
<td>132</td>
</tr>
<tr>
<td>When CERN.CH is not CERN… (2019)</td>
<td>133</td>
</tr>
<tr>
<td>Click me – NOT! (2019)</td>
<td>134</td>
</tr>
<tr>
<td>Browsing securely and privately (2019)</td>
<td>137</td>
</tr>
<tr>
<td>A free click for your awareness (2018)</td>
<td>138</td>
</tr>
<tr>
<td>Curiosity clicks the link (2018)</td>
<td>139</td>
</tr>
<tr>
<td>The Higgs does not... send mail! (2017)</td>
<td>140</td>
</tr>
<tr>
<td>STOP spam! (2017)</td>
<td>141</td>
</tr>
<tr>
<td>One click and BOOM… (reloaded) (2017)</td>
<td>142</td>
</tr>
<tr>
<td>Protect your click (2017)</td>
<td>144</td>
</tr>
<tr>
<td>E-mail is broken and there is nothing we can do (2016)</td>
<td>145</td>
</tr>
<tr>
<td>WWW censorship? Not at CERN (2016)</td>
<td>147</td>
</tr>
<tr>
<td>“New_invoice.zip” (2015)</td>
<td>148</td>
</tr>
<tr>
<td>Well fought, FP! (2015)</td>
<td>150</td>
</tr>
<tr>
<td>“Conpherencing” — the new phishing (2014)</td>
<td>151</td>
</tr>
<tr>
<td>Jekyll or Hyde? Better browse securely (2013)</td>
<td>152</td>
</tr>
<tr>
<td>Browsing the Internet: Good-bye anonymity! (2012)</td>
<td>152</td>
</tr>
<tr>
<td>Don’t let your mail leak (2012)</td>
<td>153</td>
</tr>
<tr>
<td>Don’t screw up your web (2012)</td>
<td>154</td>
</tr>
<tr>
<td>You’ve received a Hallmark E-Card? Delete it! (2011)</td>
<td>155</td>
</tr>
<tr>
<td>Encryption is useless!? (2011)</td>
<td>156</td>
</tr>
<tr>
<td><strong>Control System &amp; IoT</strong></td>
<td>158</td>
</tr>
<tr>
<td>Smile, you’re on camera… (2018)</td>
<td>158</td>
</tr>
<tr>
<td>The Internet of Things: the walls have ears (2017)</td>
<td>159</td>
</tr>
<tr>
<td>IoTs: The treasure trove of CERN (2017)</td>
<td>160</td>
</tr>
<tr>
<td>Protect your plant: a &quot;serious game&quot; about control system cyber-security (2015)</td>
<td>161</td>
</tr>
<tr>
<td>Your car, my control (2015)</td>
<td>162</td>
</tr>
<tr>
<td>Today’s paranoia, tomorrow’s reality (2014)</td>
<td>163</td>
</tr>
<tr>
<td>Our life in symbiosis (2014)</td>
<td>164</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Cyber-attacks and the risks for CERN (2013)</td>
<td>166</td>
</tr>
<tr>
<td>Hacking control systems, switching lights off! (2013)</td>
<td>167</td>
</tr>
<tr>
<td>Hacking control systems, switching… accelerators off? (2013)</td>
<td>168</td>
</tr>
<tr>
<td><strong>Secure Software Development</strong></td>
<td>172</td>
</tr>
<tr>
<td>A new departmental car service (2020)</td>
<td>172</td>
</tr>
<tr>
<td>A new twist for those who rely on external software (2019)</td>
<td>173</td>
</tr>
<tr>
<td>Go clever! Go central! (2019)</td>
<td>175</td>
</tr>
<tr>
<td>Fatal dependencies (2019)</td>
<td>176</td>
</tr>
<tr>
<td>Improve your code with Gitlab CI (2017)</td>
<td>178</td>
</tr>
<tr>
<td>Do we need more software liability? (2016)</td>
<td>179</td>
</tr>
<tr>
<td>Better code, fewer problems (2016)</td>
<td>180</td>
</tr>
<tr>
<td>SAHARA — Security as high as reasonably achievable (2015)</td>
<td>181</td>
</tr>
<tr>
<td>Professionalism in security, too (2015)</td>
<td>182</td>
</tr>
<tr>
<td>Is your code sane? (2015)</td>
<td>183</td>
</tr>
<tr>
<td>How to succeed in software deployment (2014)</td>
<td>184</td>
</tr>
<tr>
<td>Join the CERN WhiteHat Challenge! (2014)</td>
<td>185</td>
</tr>
<tr>
<td>The security marathon (2014)</td>
<td>186</td>
</tr>
<tr>
<td>The security marathon, part 2 (2014)</td>
<td>187</td>
</tr>
<tr>
<td>Improve software, avoid blunder (2014)</td>
<td>188</td>
</tr>
<tr>
<td>Stop fighting alone, let synergy rule! (2013)</td>
<td>189</td>
</tr>
<tr>
<td>Why can’t I sue my software provider? (2013)</td>
<td>191</td>
</tr>
<tr>
<td>Raise your defence: A baseline for security (2011)</td>
<td>192</td>
</tr>
<tr>
<td>Do you write secure code? (2011)</td>
<td>193</td>
</tr>
<tr>
<td>… An example of flawed code (2011)</td>
<td>195</td>
</tr>
<tr>
<td><strong>Data Protection and Privacy</strong></td>
<td>198</td>
</tr>
<tr>
<td>Computer Security: Don’t print naked (2019)</td>
<td>198</td>
</tr>
<tr>
<td>A “file drop” for confidential data (2019)</td>
<td>200</td>
</tr>
<tr>
<td>Transparency for your privacy (2017)</td>
<td>201</td>
</tr>
<tr>
<td>Confidentiality is everybody’s business (2015)</td>
<td>201</td>
</tr>
<tr>
<td>Printing confidentially (2015)</td>
<td>202</td>
</tr>
<tr>
<td>Thirty years since “1984” — How close was Orwell to today’s interconnected world? (2014)</td>
<td>203</td>
</tr>
<tr>
<td>Working privately in public (2014)</td>
<td>205</td>
</tr>
</tbody>
</table>
Contents

Coming soon, a pragmatic data protection policy for an open organisation (2014) ............................................................. 206
How private is “private”? (2014) .......................................................................................................................... 207
Public PCs: Log out or lose out (2013) .............................................................................................................. 208
Let’s play hide and seek (2012) ...................................................................................................................... 208
Your privacy is paramount! (2012) ................................................................................................................ 209
“Clas-si-fi-ed (ˈklæsəftɪd/)” — What’s that? (2012) ...................................................................................... 210
Data protection for all (2012) ......................................................................................................................... 211
How to get properly rid of confidential data? (2012) ................................................................. 212
Classified (2011) ........................................................................................................................................ 213
Privacy, who cares? (2011) ........................................................................................................................... 214

Copyrights ........................................................................................................................................ 216

Insist to avoid troubles (2020) .................................................................................................................. 216
Presenting images that are not yours… (2020) .............................................................................................. 217
When “free” gets even more restrictive (2019) .............................................................................................. 217
When “free” is not free (2018) ...................................................................................................................... 219
Downloading films is no peccadillo (2015) .................................................................................................... 220
A plea to Santa Claus (2015) ......................................................................................................................... 221
Do you have 30kCHF pocket money? (2015) ............................................................................................... 222
Protect CERN — Respect copyrights (2014) .............................................................................................. 223
Getting a better image from the organization (2014) ..................................................................................... 224
Bad (re)presentations (2013) ......................................................................................................................... 225
Software licenses: Stay honest! (2012) ........................................................................................................ 226

Rules & Policies ........................................................................................................................................ 228

Professional access to private devices (2019) ............................................................................................... 228
Welcome Summer Students ! (2019) .............................................................................................................. 229
Negative legacy when moving on? (2019) ......................................................................................................... 232
The problem with crypto-mining (2018) .......................................................................................................... 233
Computing power for professionals… only! (2018) ............................................................................................ 234
Dear summer students (2018) .................................................................................................................... 235
Rules: What’s allowed and what isn’t (2018) .................................................................................................. 236
Summer students, hold on a minute (2017) .................................................................................................. 238
Virtual misconduct – Real consequences (2017) ............................................................................................ 239
Offensive public browsing (2017) ........................................................................ 240
You’re a summer student? Some tips to get you started (2016) ...................... 241
“Hello World” — Welcome to CERN (2015) ..................................................... 242
In the name of CERN (2015) ........................................................................... 244
Posting and mis-posting (2015) ....................................................................... 245
Social media — Dos and don’ts (2014) ........................................................... 246
The naked blunder (2013) ............................................................................... 246
“Security” is YOU! (2012) ................................................................................ 247
Why “security” is not ME… (2012) ................................................................... 248
Security needs you (2010) .............................................................................. 249

Miscellaneous ................................................................................................... 250

From the digital trenches (2020)...................................................................... 250
Digital stolen goods of CERN? (2020) ............................................................. 251
Blackmailing Academia: Back to pen and paper(?) (2020) .............................. 253
Blackmailing Enterprises: You are Patient Zero (2020) ................................... 256
Serious gaming… for your own good (2019) ................................................... 258
Fun facts: Did you know? (2018) ..................................................................... 259
Meeting your family during the holiday season? (2018) .................................. 260
Digital Broken Windows Theory (2019) ........................................................... 261
Take it seriously (2018) ................................................................................... 262
And in the real world? (2017) .......................................................................... 263
About security incidents & issues (2017) ......................................................... 264
WhiteHats for CERN (2016) ............................................................................ 265
The dilemma of fractal defence (2015) ............................................................ 266
Geneva, Suisse Romande and beyond (2014)................................................ 268
The end of encryption (2014) .......................................................................... 270
A short tale of the black sheep of –ITY (2013) ............................................... 271
CERN: Digitally open, too (2013) ................................................................. 273
Security vs. nations: A lost battle? (2013) ....................................................... 274
Security Bingo (2011) ................................................................................... 275
Security Bingo for the paranoid (2011) ........................................................... 276
Security Bingo for administrators (2011) ......................................................... 278
Review your computer security now and frequently! (2009) ............................ 279
Computer Security

Still on Windows 7? Say “bye bye” to your digital life (2020)

We recently received a request from a concerned citizen as to whether it is OK to continue using his Windows 7 PC to remotely connect into CERN. And he was right to be concerned: running Windows 7 is about as secure as running naked through the quarantine ward and hoping not to contract an infection. Would you dare?

Support for Windows 7 ended in January 2020. Apart from for some customers who are paying an extra fee, Microsoft has stopped providing any assistance and security fixes for that version of their operating system. Auto-updates are idle and do not improve the security anymore. Unless you have put additional measures in place, like having it fully disconnected from receiving e-mails or browsing the Internet, or by channeling all traffic through a tightly controlled gateway, your PC is vulnerable. Unprotected. Unsecure. Ready to be infected. In fact, it’s probably already infected.

And with the infection of your PC, your digital life is also most likely infected. Compromised. Gone. The successful attacker, once he or she has infected your Windows 7 system, has free reign on your computer. He or she can read, copy and extract all your documents, expose your private photos and videos (unless you pay a ransom: “Malware, ransomware, doxware and the like”), encrypt all your data (unless, again, you pay a ransom; ““WannaCry”? The importance of being patched!”), enable your embedded camera and/or microphone to spy on you, send malicious e-mails on your behalf, or just steal your Facebook/Twitter/Instagram/Amazon/online banking/CERN password to abuse your digital identity on those sites. Posting embarrassing messages. Buying goods with your credit card. Redirecting your money. Threatening the integrity and operation of CERN (“Blackmailing Enterprises: You are Patient Zero”).

So, it is of the utmost importance for you and your digital life that your operating system is up-to-date. Windows 7 is dead and should be kept dead. R.I.P. Instead, upgrade to a version that is actively supported by the software vendor. Windows 10 would do. Several Linux distributions are excellent alternatives. In any case, keep your computer up-to-date, enable automatic patching, and install and run decent anti-virus software for additional protection. Furthermore, and more generally, be careful when browsing the web or answering e-mails. STOP – THINK – DON’T CLICK in the event of any doubt. Just like washing your hands regularly, these few simple recommendations will nicely reduce your computer’s risk of infections. Easy, no?
The coronavirus has brought normal life at CERN to a well-justified halt, but it also has the potential to shut down CERN’s digital operations. The only infection vectors a “digital” coronavirus would need is human gossip (creating “FUD” – fear, uncertainty and doubt), fast-clicking users, unpatched computers… and teleworking! And an adversary to give it a try.

In fact, as we outlined in our previous Bulletin article on ransomware (“Blackmailing Enterprises: You are Patient Zero”, with more details on this in the next Bulletin issue), attackers are on the prowl to maliciously infiltrate companies and enterprises, but also universities and academic institutes. Just recently, a Czech hospital was hit in the midst of handling COVID-19 patients. While there are no details of this incident yet, here is a roadmap for how CERN could end up in the emergency ward:

**Step 1 – F-U-D:** Fake messages on the subject of COVID-19 trouble not only our minds, but malicious e-mails, WhatsApp messages or the like on the subject could also threaten the security of your computer. Lots of the embedded links being shared point to allegedly new research results, infection statistics, help pages and advisories, or gossip on how you can best protect yourself. Not all of them are benign: some intentionally target your computer. So coronavirus is a vehicle for infecting your computer too. And given all the fear, uncertainty and doubt around this subject, human curiosity acts quickly… click!

**Step 2 – An unpatched computer:** One click on a malicious link is sufficient to infect your computer. And this is almost guaranteed to happen if your computer is running an outdated operating system like Windows 7 (or earlier!) or an unpatched version of Windows, Linux or MacOS. Less likely, but still possible, your computer might be fully up-to-date but your operating system still exposed to a yet-to-be-published vulnerability. Once your computer is compromised, the adversary has access to all its features: keyboard, hard disk, microphone, camera… infect!

**Step 3 – Teleworking:** The (hopefully short) era of socio-physical distancing to reduce the spread of the coronavirus requires more teleworking than ever before. Teleworking involves using your CERN or home computer to remotely connect to CERN. This means that, at one moment or another, you will have to type your CERN password. And with a compromised computer, the attacker can watch every step you take: which program you execute, which data you manipulate, which system you manage, which maintenance work you perform, which password you type. Enough information to impersonate you. Abuse your computer program. Steal your data. Compromise your system. Sabotage your maintenance work. Steal your passwords… game over!
This is how organisations have been brought to a halt in the past. And this is how coronavirus could bring organisations into the emergency ward too. **You are just patient zero.**

So, what can you do to protect yourself, your computer and CERN?

**Step 1 – STOP – THINK – DON’T CLICK:** Just try to restrain your curiosity and do not fall prey to all the gossip circulating at the moment. Be cautious, and don’t click on links from dubious or not-so-dubious sources. This includes web pages offering “newest statistics” on COVID-19, forwarded malicious WhatsApp messages, mails, etc.

**Step 2 – Patch:** Keep your computer up-to-date. CERN-managed PCs already should be. For your own devices, enable automatic patching if this is not your default. If your operating system or applications are outdated and not supported anymore, stop using them and upgrade to a version that is actively supported by the software vendor. Be ready to scrap it any time.

**Step 3 – Connect securely:** There are several official and secure methods to allow you to **work remotely**, to **connect remotely** and to **tunnel remotely** into CERN. Please do not use any other means! In particular, do not abuse any firewall opening assigned to your dedicated service and do not create web proxies for tunneling through. If this puts the Organization at risk, it will be considered as professional misconduct. Finally, in order to better protect your password, the IT department is still aiming to roll out a [multi-factor authentication solution](https://home.cern/news/news/computing/computer-security-what-do-apartments-and-computers-have-common) for especially exposed CERN staff and users.

For more good advice on how to telework securely, please check out this [fact sheet](https://home.cern/news/news/computing/computer-security-what-do-apartments-and-computers-have-common) and join in the discussion with your CERN peers on the dedicated ”~teleworking” Mattermost channel. Thanks a lot for protecting CERN.

Good luck and the best of health to you, your family and friends!

---

**What do apartments and computers have in common? (2019)**


Assume that you have just bought an apartment. Ground floor with a small garden. Top location. Near a lovely park. Tram stop not too far away. Quiet, but still in reach of supermarkets and restaurants. Perfect, if it wasn’t for the daily and nightly flow of people around your building. Most of them seem nice, but some of them look nasty or even malicious.

So, you have properly equipped your entrance door with a modern lock and dimple keys; protected it additionally with a crossbar and installed a reinforced frame with multiple deadbolts. Your windows and terrace doors are also all reinforced and secured by locks so that nobody from the outside can easily open them, even if they are tilted.
Automatic blinds roll down during the night for further protection. Inside your apartment, all your really important belongings are locked away in a small safe attached to the wall in your wardrobe: jewellery, watches, passports, banking codes and some important family documents. And you consulted a local security company who installed some motion sensors and external cameras to monitor abnormal activities when you are not at home. Of course, all that costs money and time to implement, but you feel secure now, properly protected and safe, since, at home, you are the number one person responsible for security. Your household insurance and the local police might help you and provide some valuable advice, but it is up to you to protect yourself and your family.

Enter your laptop. Smartphone. Tablet. PC. eBook Reader. Smart TV. Livebox. Stereo. Playstation. Wii. Internet-connected thingy. Just as within the privacy of your four walls and the valuables you have at home, such digital devices contain lots of information about your private life and that of your family. With some devices, you are even living in tight symbiosis. But have you consciously thought of protecting your devices as thoroughly as your apartment? Deploying all the necessary dedication, money and time?

For the protection of your digital assets, photos, films, documents, banking access, social media, etc., make sure that you apply cyber-security best practices: have all your connected devices configured so that they update themselves regularly. Note that the less “computer-like” your device is, the harder that will be to do (and you might decide to accept the risk of not patching such devices or just not put them online). Make sure that the entry point in your home network (usually your wireless access point, a “Livebox” or similar) is kept up-to-date and configured in a manner that any connection initiated from the outside is blocked. In fact, that should be the default setting. Only deliberately open incoming connections if you have a good understanding of what you are doing. Educate your family. Tell your kids and partner to watch out when browsing the web. Not everything is what it seems, and one wrong click can compromise your home network and all your digital assets. Once more, you are the number one person responsible for the security of your home devices. It is in your personal interest to keep them secured. The Microsofts, Apples, Googles and Swisscoms of this world might help you with that, but still it is up to you to protect you and your family.


So it is in all of our interests to protect the Organization. Just like at home, at CERN you are the person primarily responsible for the cyber-security of your digital assets. It
is you in the first instance who is supposed to apply the same cyber-security measures you deploy at home to all the devices registered to you at CERN. Your laptop. Smartphone. Tablet. PC. Server. Virtual machine. Container. Website. Database. Control system. Software. Computing account. Keep them up-to-date. Tightly control any remote, virtual or physical access to them. Have monitoring capabilities in place. Provide additional protective measures if the device is just weak and not really secure. The CERN Computer Security Team can help you with that. Training. Auditing. Consulting. We also provide additional monitoring, detection and protective means. And in the event of damage, we do incident response and close-out. Whatever cyber-security issue you have, just drop us a line: Computer.Security@cern.ch. We are here to make your professional life more cyber-secure.

When your mike spies on you (2019)

We have reported on sophisticated attacks via smartphones in the past (see https://cds.cern.ch/journal/CERNBulletin/2014/32/News%20Articles/1696916?ln=en). Here are two new twists – probably still theoretical, but both pointing towards new ways to spy on you by misusing your microphone…

The attack vector in both cases is the same: a local microphone to which the attacker has access. The passive attack is aimed at your desktop computer and just uses your smartphone’s microphone (or any other connected microphone to which an attacker has access). Using a Skype call, Google Hangouts, or any other streaming audio chat (even via a Google Home or Amazon Echo device), the attacker listens to the sound of your screen’s power supply. The way the screen renders the display, “sending signals to each pixel of each line with varying intensity levels for each sub-pixel” creates fluctuations in the power consumption, and hence in the “hum” of the power supply. Intercepted by the microphone, sophisticated machine learning techniques are subsequently employed to deduce from the hum what is being displayed on the screen… The first results show that researchers managed to determine which website out of the Alexa top-10 websites was displayed on the test screen with a 97% accuracy. On-screen keyboard strokes could be identified with an accuracy of 96% and 40% depending on the test set-up. Extended to full words, this can exceed 99% and 70% accuracy. And their results to capture paragraphs with more than 100 words displayed on screen look disturbingly accurate too.

The active attack is aimed at smartphones and uses both the local microphone and the local loudspeaker. Paired together, using the loudspeaker to emit acoustic signals inaudible to humans and recording them again with the microphone, they create a small basic sonar system: “The echo signal can be used to profile user interaction with the device”, i.e. the way your finger swipes over and interacts with the screen.
Interestingly, they’ve shown how this sonar can be employed to help identify the swipe pattern used to unlock an Android phone – reducing the number of trials to be performed by the attacker by 70%. And that is only their proof-of-concept…

Admittedly, both attacks are still rudimentary and theoretical, but with more computing power at hand, better machine learning algorithms and more research, both also show what the sophisticated attackers, snoops and spies of this world might add to their exploitation arsenal in the future… By the way, if you are using an Android smartphone and swipe through the 3x3 pattern to unlock it, check out this paper listing the 20 most used swipe patterns. Using one of these is like using one of the top-10 most used passwords. If yours is listed, maybe it’s time to move to another, more secure pattern?

The rancid USB box of chocolate (2018)

How convenient were USB sticks in the past…? And how convenient they still are today despite the fact that with CERN’s free and versatile CERNbox service or the commercial “Dropbox” solution there are simpler methods for sharing files and documents between devices. And even more secure and compliant ones!

The basic problem with USB sticks is that they are a black box, a box of chocolates: “You never know what you're gonna get” (Forrest Gump, 1994). And, indeed, how can you know if your USB stick, the one you are about to plug into your computer right now, holds any infected files, viruses, illegal software or software subject to copyright or particular licence conditions. You can’t, even if the USB stick is brand new. We have had cases at CERN where USB sticks came already infected from the factory – USB sticks in sealed plastic packaging… The risk for your computer and CERN is non-negligible: depending on the type of infection/virus and how up-to-date your operating system is, your computer might get infected right away. This is a particular risk for devices which cannot be kept up-to-date all times, like some control systems used for running our accelerators, infrastructure or experiments!

Worse, our automatic detection tools regularly detect pirated software or copyrighted material arriving via personal USB sticks used previously at home. Of course, what you do at home is your private business and only subject to your local national laws, but once the USB stick is connected at CERN, the use of pirated software or copyrighted material can have significant consequences for the Organization (see our Bulletin articles on the subject: “Do you have 30kCHF pocket money?” and “Music, videos and the risk for CERN”.

So, help us to protect your devices, CERN’s reputation and the operation of CERN’s accelerators, infrastructure and experiments! Please do not bring your USB sticks from home to CERN (and if you need to, please format them beforehand). Take additional care when plugging in USB sticks from third parties. It is better just to refrain from using USB sticks unless you have a good idea of what is stored on them – in particular for
USB sticks found “on the road” (e.g. USB sticks lost by someone, dropped on the floor, handed to you by some stranger). Instead use CERNbox as an alternative. It has sufficient space for big files, synchronises with your CERN home folders, is remotely accessible (even from mobile devices) and provides anonymous access for sharing material with third parties. And please apply the utmost care when using USB sticks to transfer data to production control systems hosted on the Technical Network (TN) or any experiment networks (EN). The corresponding policy, the CNIC Security Policy for Controls (section 6.2.1), stipulates that the “usage of USB sticks being connected to devices on the TN/EN must be avoided by any means and alternative methods for file transfer […] must be used whenever possible. Failure to adhere to this rule will be considered as professional fault putting a risk to the TN/EN.” And, finally, it goes without a saying that always keeping your operating systems up-to-date and using decent anti-virus software (you can get it for free from CERN: will definitely provide you additional protection.

Linux: Windows revisited (2018)

Linux and MacOS folks: do as the Windows people do. Be diligent when receiving unsolicited e-mails with weird attachments.

In the past, “infections” were usually only a matter for PCs and laptops running Microsoft’s Windows operating systems. Windows users should (and, at CERN, must!) apply due diligence to protect their system by, for example, safe browsing and avoiding opening attachments from dubious sources (“Stop – Think – Don’t click”). Users of Linux or MacOS operating systems were thought to be less prone to such kinds of infections… but that is plain wrong.

Computer viruses usually exploit weaknesses and vulnerabilities in the underlying operating system. As the erstwhile market leader, Windows was the number one choice for cyber-attackers due to its large market share. The success rate in infecting Windows PCs was very high. But this has changed in two ways. First of all, MacOS has become very popular too, and cyber-attackers now also target devices running MacOS and iOS – as well as Android tablets and smartphones. Secondly, attackers are focusing less and less on the weaknesses of the operating system, but are increasingly looking into the vulnerabilities of software applications. The best outcome for hackers is if these applications work on all three major operating systems (Windows, MacOS, Linux), like Adobe Reader or Mozilla Firefox. With one good vulnerability, you can exploit them all… An excellent example is the recent publication of a vulnerability in the beloved “Ghostscript” application (and subsequently in “ImageMagick” and “GraphicsMagick”): with one malicious PDF, XPS, PS or EPS document and one single unsuspecting click by the innocent user, your Linux computer is a goner. The operating system infiltrated. All files exposed. Any communication
tapped. This sort of thing from our *Bulletin* article on “Protect your Family”. Game over, Linux.

So, Linux and MacOS folks: do as the Windows people do. Be diligent when receiving unsolicited e-mails with weird attachments (see our *Bulletin* article on “A free click for your awareness”). Stop and think before clicking on weird-looking web links or URLs stemming from unknown or untrustworthy sources (“Curiosity clicks the link”). And always keep your operating system and all applications up-to-date. “Yum autoupdate” is your best friend.

**Protect your Family (2018)**

How many devices do you have at home? Plenty, no? Our physical life today is deeply entangled with our digital one. Best example: ask yourself where your smart phone is. Do you recall the nervousness and unquietness when you do not find it immediately? Digital devices, i.e. laptops, tablets and smart phones, have become fundamental part of our life. We communicate with our friends and family, we take and store pictures and videos, we do Internet banking and shopping. Have you ever thought about the consequences if one or more of those devices are getting lost? Or stolen? Or compromised?

Our digital life today is centred on the laptops, tablets and smart phones we own. But have you ever thought about the consequences when those devices are getting stolen or compromised? Depending on the protective measures you have put in place, an attacker might be able to extract all data from your device. All personal documents. Bank statements. Confidential letters. Your private photos. Your family videos. Your music and videos. The attacker might use this material to blackmail you and exfiltrate money (see our Bulletin articles on “Old Scam in New Disguise”, “WannaCry”? The importance of being patched” and “Ransomware - when it is too late...”). If your device is compromised and remotely accessed by the attacker, your private life becomes public. The attacker can follow online any activity you do on your device: registering every keystroke you do and waiting for you typing a password; taking films or screenshots of your digital desktop, of all open windows, of your browser sessions and monitoring how you do Internet banking; enabling your web camera and your microphone for watching and listening to you while you believe to be safe in your intimate environment “home”. All this gives an attacker ways for more crime. Going for the web services you have accessed, tweeting or posting in your name, buying on your costs, stealing money from your bank account, blackmailing you once more with the material recorded from your webcam and microphone...

Hence, protect yourself and your family! Protect your private life! And once you have done, protect your professional life and your CERN devices, too!
1. Make sure that all your computers, laptops, smartphones and tablets are up to date. Have your operating system's update mechanism enabled and ensure that it is automatically applying any new security patches. If possible, run some decent antivirus software on it, and remember that CERN’s antivirus software for Windows computers and Macs is free to you, even for home use (see here).

2. Do not click on links or attachments sent to you in unsolicited e-mails (recall “Curiosity clicks the link”?). Rather, check the context first: Is the e-mail addressed to you? Is it relevant to you? Does it look legitimate? If in doubt, contact us at Computer.Security@cern.ch. The same is true of browsing web pages. Watch your click. If in doubt, better to Stop – Think – Don’t click! Again, if in doubt, contact us;

3. Finally, back up your important data. CERN data should be backed up on AFS, DFS or EOS – services that are designed not to lose data. At home, back up to an external hard disk (but don’t keep it permanently connected!) or buy a network-attached storage (NAS) device. If you are blackmailed, it’s unfortunate, but do not pay any ransom.

… and check out our good practices (see here).

An old scam in a new disguise (2018)

Money has always been a catalyst for greed and malice. Blackmail is one way to extort money from the innocent and has existed since ancient times. In the digital world, blackmail is not unknown and there are many ways to go about it. We have discussed some of them in previous Bulletin articles (“Malware, ransomware, doxware and the like”). Recently, there has been a clever new twist on an old e-mail scam that might make the con far more believable.

A message received at CERN or elsewhere claims that your computer has been compromised and the attacker has full access to your device. This is not beyond the realms of possibility as computers always have some vulnerabilities that haven’t been fixed yet (by you or the developer of the operating system). And “full access” really implies full access: to the documents stored on that device like photos, videos, bank statements; to the buffer of its keyboard so that every keystroke – including any passwords being typed – can be logged and stolen; to its screen and whatever is displayed on it snapshotted by the attacker; and to the attached microphone and web camera. In the last case, this allows the attacker to spy on any activity committed in the vicinity of that computer (see also our Bulletin article “Curiosity clicks the link”). And the attacker can play dirty tricks with that power. By claiming to have a recording of the webcam’s livestream while the computer was accessing webpages with pornographic material, the attacker can threaten to release the video to all locally registered contacts unless a Bitcoin ransom is paid… The new twist? The e-mail does not only include this
threat but also now references a real password previously tied to the recipient's e-mail address, which makes the scam much more believable!!!

How come? Passwords are a necessary token for protecting your data in any web service. CERN INDICO, CERN EDH, Facebook, Twitter, Amazon, etc. Hence, they are usually stored in combination with an identifier (i.e. your e-mail address) for that web service – but not always in a perfectly secure fashion. At CERN, we protect your password in accordance with best practice, converting it into a non-recoverable string (technically a “salted hash”), but some other sites might store your password in clear text. If those websites are infiltrated, all clear text passwords are exposed and the access protection for any other data is completely lost. From that moment, all data can be considered to be involuntarily public. This is happening more often than you might think [https://haveibeenpwned.com/]. Whenever the CERN Computer Security Team learns about newly exposed passwords linked to your CERN e-mail address or any other address registered with CERN, we will let you know!

Thus, if you receive such a scam e-mail blackmailing you, please DON’T PANIC. And for sure, do not pay any ransom money! The only thing you should do is to change the password revealed in the e-mail – if you recognise where it was used. Consider terminating that specific account. To be more proactive, recall these simple principles to keep your digital life secure: keep all your devices always up-to-date by using the operating system’s auto-update feature (“WannaCry”? The importance of being patched); choose complex and/or long passwords and keep them to yourself (“CERN Secure Password Competition…”); have different passwords for different sites and different purposes; and do not click on links in e-mails or on webpages whose origin you don’t trust or which look dodgy (“A free click for your awareness”!)

Stepping up in user education (2018)

Over the years, we have tried and succeeded in using a number of different methods to educate people on computer security problems and issues: posters, videos, courses, presentations, monthly reports, and Bulletin articles. We would now like to step up a level and introduce haptic feedback for unsecure user actions. Enter: the “Digital Feedback Keyboard” (DFK).

Today, using a computer does not come without risks. Browsing to the wrong webpage, opening a malicious attachment or downloading a bad plugin or software can quickly infect your computer, destroy its inherent defences and render you, your work, your data and subsequently CERN completely naked and unprotected (see for example “Drive Bye” or “One click and boom”). An attacker “owning” your computer in such a way also owns your computing account as, usually, such attackers install malware on your computer which will log any keystroke you make (including your account’s password), enable your webcam and microphone to spy on you, search through your
hard disk for juicy documents and, if there is nothing better, try to extort some money from you ("Ransomware - when it is too late...").

It is generally very difficult to spot those risky actions. “Stop, think, do not click!” does not always enter into our minds promptly. Hence, with these new DF keyboards, a user will get direct feedback from unsecure actions through a series of small electrodes integrated into the keys. These electrodes will distribute a short spike of a few volts for potentially dangerous actions like opening an infected attachment, typing your CERN password into a non-CERN-owned webpage or browsing to a malicious webpage. Higher voltages can be expected when opening applications which directly violate CERN’s Computing Rules or are illegal, such as software using pirated licenses (“Do you have 30 kCHF pocket money?”) or violating copyright (“Protect CERN --- Respect Copyrights”). After a while, such electric feedback will help you subconsciously to practice “Stop, think, do not click!” “It is basically like teaching cows not to touch the fence by using electric wires,” says Chris Lloyd from the IT procurement team.

A first pilot phase will start on 1 April, with about 100 users randomly selected from among all members of the personnel. As other CERN services have already expressed their interest for their particular use cases (e.g. for eLearning, MERIT appraisals, expensive purchasing), the pilot might quickly be expanded throughout CERN. The CERN procurement team and IT department are currently investigating how to efficiently roll out and distribute DF keyboards to every single user. If you prefer not to join this pilot phase for now, just start to practice “Stop, think, do not click!” now. Please beware of strange e-mails sent to you – learn how to identify malicious e-mails – and do not click on random links just because you find them appealing. Better think first and refrain from clicking.

Malware, ransomware, doxware and the like (2018)

Computer security was easy in the last century, when malicious infections usually just involved people misusing a computer to spread or, in the worst cases, delete files. But all that has changed. Today, your computer and smartphone are the centre of your life and people with malicious intent are on the prowl, seeking to compromise them and extort money from you!

The world has changed. Today’s attackers are no longer just a few script kiddies hiding away in dark rooms, as Hollywood suggests. “WarGames” is long gone. Instead, they have created illegal enterprises with Mafia-like structures, where management, attacks on end users, computer exploitation, blackmailing and exfiltration of money are separate activities, partially outsourced to “subcontractors” or just bought from third parties:
• Certain despicable experts create malware that exploits as-yet-unknown vulnerabilities in your favourite operating system or application;

• Others provide lists of e-mail addresses and deliver that malware as an attachment (e.g. as an infected PDF or Microsoft Office document). Alternatively, they run e-mail campaigns asking the recipient to click on a malicious link (see our Bulletin article “Protect Your Click”). The website behind that link has already been compromised by other malicious parties, who have managed to install the malware on it (e.g. as rogue advertisements);

• The malware is just the vehicle. Top management decides what happens next: “ransomware”, “doxware” or just creating chaos. If it is about money, the malicious parties provide the infrastructure required to extract it (“pay us $300 in Bitcoins”) and harvest the virtual money;

• Finally, yet more groups convert the virtual money into real dollars – clean dollars, which cannot be traced back…

Attacking the centre of your life has become a serious, but illegal, commercial business. There is a lot of money to be earned and someone will always pay. Don’t let it be you!

• Make sure that all your computers, laptops, smartphones and tablets are up to date. Have your operating system’s update mechanism enabled and ensure that it is automatically applying any new security patches. If possible, run some decent antivirus software on it, and remember that CERN’s antivirus software for Windows computers and Macs is free to you, even for home use. That should prevent some variants of the malware in step 1 above;

• In order to thwart step 2, do not click on links or attachments sent to you in unsolicited e-mails. Rather, check the context first: Is the e-mail addressed to you? Is it relevant to you? Does it look legitimate? If in doubt, contact us at Computer.Security@cern.ch. The same is true of browsing web pages. Watch your click. If in doubt, better to Stop – Think – Don’t click! Again, if in doubt, contact us;

• Finally, back up your important data. CERN data should be backed up on AFS, DFS or EOS – services that are designed not to lose data. At home, back up to an external hard disk (but don’t keep it permanently connected!) or buy a network-attached storage (NAS) device. If you are blackmailed, it’s unfortunate, but do not pay any ransom. This will prevent steps 3 and 4 from happening. The likelihood of getting your data back is very small. If your computer is infected with ransomware, you may be able to recover your files using the tools provided on the following website: https://www.nomoreransom.org/en/index.html (which

1 If you are lost, have a look at this helpful article: http://www.zdnet.com/article/what-is-malware-everything-you-need-to-know-about-viruses-trojans-and-malicious-software
also contains excellent advice on how to avoid becoming a victim of ransomware).

It’s your life. It’s your computing device(s). Don’t let them get you.

Another way of making money with ads (2018)

One major source of revenue on the Internet is advertisements. One view, one hover of your mouse, one click: everything is counted and converted into money paid by the advertisers to the owners of the website where the ad is displayed. This is not bad per se as it provides visitors with “free”\(^1\) content while still maintaining a revenue stream for the content providers. Interestingly, not only honest companies have embarked on online advertising, but the evil side has also discovered advertisements to spread their malware.

As outlined in a previous article (“Malware, Ransomware, Doxware and the like”), attacking end-user computers is a multi-billion dollar business run by professional, but illegal, enterprises. Many different attack vectors are employed, such as phishing e-mails, malicious attachments, or targeted attacks against companies and their employees. Or attackers even try to infiltrate major websites and hide malware within. If an unfortunate user accesses that website, his or her vulnerable computer is compromised and his or her private life is gone (see our article on “Drive-by”).

Alternatively, the malicious evil-doers just buy themselves into one of the big advertisement network distributors (“ad networks”, see https://en.wikipedia.org/wiki/Advertising_network for examples) and hope that their malicious advertisements (“malvertisements”) are properly distributed and shown on major websites. Superficially, their malvertisements promote fake products or services. Behind the scenes, however, the malvertisement tries to exploit vulnerabilities in your web browser, its plugins, or in your operating system.

Although the ad distributors generally do a good job of blocking such malvertisements, it’s a cat and mouse game. Malvertisements might affect major legitimate and popular websites: news outlets, public transport webpages, feeds in Facebook or Twitter, etc. In such cases, our motto “Stop – Think – Don’t click!” can’t be applied. Instead, it is of the utmost importance that you keep your operating system and all applications, in particular your web browser, up-to-date. Make sure that the respective update mechanism is set to “automatic” so that your devices download and apply fixes as soon as possible. If available, install and run antivirus software and remember that CERN’s

---

\(^1\) The “free” has been put in inverted commas as, unfortunately, advertisements nowadays often come with tracking algorithms that monitor your activity and try to gather more information about you and your computer (e.g. your location, keyboard language, operating system type). If you don’t like this, consider using ad blockers or browser extensions for more privacy.
antivirus software for Windows computers and Macs is free for you to also use at home.
Good luck!

Enter the next level: Doxware (2017)

Do you recall “WannaCry”, the nasty malware of early 2017 that tried to infect your computer and encrypt all its contents? It was unfortunate for those whose device got encrypted, as all data was lost unless you dared to pay the ransom requested by the attackers. And even if you’d paid, it was not certain that you would get your data back – that’s why we usually do not suggest paying any ransom… Now attackers have started increasing the pressure. In the past, infections blocked computers, stopping them from working, spreading their infection, or making fun of their owners. Then, networks of devices were misused to spam the world, attack web sites and web services. Staying silent and monitoring owner activity came next: spying on your banking activities, your passwords, etc. “Ransomware” like “WannaCry” holding your data hostage was the last level (“Ransomware - when it is too late…”). And now comes the next level: “Doxware”.

For many of us, our computer, and even more so our laptop, smartphone or tablet, are the central digital focal points of our lives: we store our personal photos and videos on them, as well as lots of private documents, and we use them as a central hub to access our bank accounts, to communicate with our closest friends (on Facebook, Twitter), or to consult our favourite health application to check out our wellbeing. Where is your smartphone now? You recall that panic when you do not know where it is? With a successful attack against our devices, lots is lost. “Ransomware” destroys our local data, malware like “Dridex” extracts banking and transaction details to extort money, other malware aims at harvesting the passwords for your social media accounts, etc. Already bad, isn’t it? “Doxware” is taking this to the next level. The word stems from “Doxing” (where “dox” is an abbreviation for “documents”), which is the Internet-based practice of researching and broadcasting private or identifiable information (especially personally identifiable information) about an individual or organisation. Like “Ransomware”, “Doxware” will encrypt your hard disk and ask you to pay some ransom money to get that data decrypted. But this time, a simple backup won’t help as the attackers will also threaten to expose all your personal and private data on the Internet if you don’t pay… It’s a difficult call to make, isn’t it?

Thus, keeping your devices secure is once more essential for your privacy and the protection of your (digital) belongings. Keeping your computer, smartphone and tablet up-to-date is one of the central paradigms of computer security. Only if they are kept updated can you be sure that at least the known vulnerabilities and weaknesses are fixed and your device cannot be exploited:
If you have a personal computer with your own Windows operating system, check for “Windows Update” in the program listing on the Start button. Switch to the recommended “automatic” update method!

On Linux distributions, make sure that you regularly run “yum update” or even better, enable automatic updates. Don’t forget to reboot your computer when a new kernel is installed, in order to properly apply kernel patches!

For Apple Macs, use the software update mechanism, which is accessible under the Apple menu.

For iOS or Android devices, check out the system settings.

Running antivirus software on your Windows or Mac device is a great plus, giving you additional protection and prevention capabilities. And such software comes for free for CERN personnel. The CERN anti-virus software for Windows and Mac can also be used at home… for free! If you can, get rid of Acrobat Reader, Flash and Java as these applications are regularly exploited to break into computers. If you can’t, make sure that these and any other applications are kept up-to-date. If you are in doubt (and are running a Windows system), you can install and run this fine program from Secunia which checks your computer for outdated software. Take care with your password and only provide it to websites you fully trust. Never put your passwords in e-mails, not even in reply to someone asking for it. And have separate passwords for different web services. Finally, infection vectors are usually either malicious e-mails or websites. Hence, STOP – THINK – DON’T CLICK when considering clicking on a link or opening an attachment. Only proceed if you trust the origin of the attachment/link. Here are some hints on how to identify malicious e-mails. Yes, it is very difficult. But it is this weakness of human nature that attackers try to exploit first...

Why you got a new PDF reader (2017)


Standard best practice in computer security involves always keeping all your devices up-to-date so that malicious evil-doers cannot exploit known vulnerabilities and weaknesses to their advantage. However, the problem is the word “known”. Not all vulnerabilities and weaknesses are immediately reported and published. On one hand, there is a generally accepted grace period for those that practice “responsible disclosure”: software owners usually have about three months to fix reported vulnerabilities before they are made public. Alongside publication, remediation measures are also documented – and applied through the standard update mechanisms. However, some people, organisations or companies prefer a different approach. Instead of “responsible disclosure”, they collect weaknesses and vulnerabilities to allow evil deeds, selling them to the highest bidder (often on the black market), or using them for offensive action like espionage or other cyber-attacks…
So let’s look at another standard best practice in computer security: reduction of the attack surface. The fewer software packages that are installed on a device, the “better” they are programmed, or the less “mainstream” they are on the market, the smaller the attack surface. Software which does not exist or is not running on a device does not pose any potential risk. Software of high quality that is well programmed, with best-practice security principles in mind, is harder to exploit. And software that is not “mainstream” might not be the main target for attackers as it is not prolific enough to create revenue when abused.

Operating systems aside, for standard Windows PCs but also for Mac and Linux computers, some of the applications with the most vulnerabilities reported in 2017 are Microsoft Edge, Apple Safari, Adobe Acrobat and Acrobat Reader, and Oracle Java JDK and JRE. While there are others, those listed have maximum domination of the IT market and are installed on many different devices – most likely including yours. But do you really need them? Or are there similar, less common products that have less chance of being exploited?

For sure there are. And this is the main reason why CERN has chosen “PDF-Xchange” for Windows PCs and “PDF Expert” for Mac systems as its new default readers for PDFs. Together with other security measures (namely CERN’s sophisticated SPAM filtering engine), this new default reader will avoid computer infections coming via malicious PDF documents aimed at exploiting the vulnerabilities of the market leader. While we do not necessarily believe that the software has fewer vulnerabilities, the chances of them being exploited is just much lower, as most malicious evil-doers will concentrate on mainstream products – the list above – and abuse them for their deeds.

Do you want to do more? Review the software installed on your devices, in particular if it is listed here. Remove applications which you do not need or rarely use in order to reduce your personal attack surface. Think also about replacements. There are many good (i.e. more secure) and sometimes free alternatives to your favourite browser or PDF reader. And of course, for the rest: make sure that they are all up-to-date. “Secunia” provides a good tool for you to check (if you want to install another application to rule them all).

“WannaCry”? The importance of being patched (2017)

Mid-May has seen a big weekend for the cyber-threat landscape, as "WannaCry" (also known as "WannaCrypt") came onto the scene with a bang and affected many Microsoft Windows systems worldwide. Using an old exploit developed by the US National Security Agency and published by the ShadowBroker hacker group,
WannaCry tried to infect non-patched PCs. As Microsoft has already provided fixes to this underlying vulnerability, this shows once more the importance of patching...

What if you haven’t patched? WannaCry installs ransomware (“Ransomware - when it is too late...”), i.e. software that encrypts a wide variety of files hosted on the computer, including MS Office documents, photos, films, etc. – hence the alias “WannaCrypt”. It also tries to identify external storage systems connected to the PC in order to encrypt those files, too. Unless you have a recent unaffected back-up, the only way to recover the files is to pay the ransom of 300 USD (see photo). Even if the ransom is paid, there is no guarantee that the attackers will provide the decryption details...

How can we fight WannaCry? Like any other malware, the primary infection vector is e-mail (also see our Bulletin article “One click and BOOM... (Reloaded)”). The motto “Stop - think - don’t click” therefore applies once more. Fortunately, this time, the CERN e-mail system and its anti-spam filtering identified and quarantined potentially malicious incoming e-mails. More importantly, all centrally managed Windows PCs were already patched against any exploitation of that kind. Microsoft made the corresponding updates available in March 2017 (i.e. MS17-010). The early bird catches the worm! So no harm was done to those computers. For non-centrally managed PCs, patching should be done regularly; a little effort today could save you tons of headaches in the future. Hence our recurring plea to you to keep your Windows, Linux or Mac computers, and also your Android and iOS smartphones and tablets, up-to-date using their auto-update features (see for example our Bulletin articles “Agility for computers” and “Android is the new Windows”). Windows Update, Mac’s Software Update and Linux’s YUM auto-update are an essential first line of defence of your computer. Running decent antivirus software adds to this: the native Windows
Defender (and probably all major antivirus software) was able to detect WannaCry from the beginning. CERN’s anti-virus solution is available to you for free [download and use on your home computers](http://cds.cern.ch/journal/CERNBulletin/2016/24/News%20Articles/2159537?ln=en). In fact, the few infected computers this time were sub-optimal private laptops owned by people temporarily visiting CERN. Too bad for them if they didn’t have reasonable recent back-ups of their local files... In the end, as luck would have it, it turned out that the creators of WannaCry had included a “kill switch” inside their code. The kill switch tests successful connection to a certain domain name on the Internet, and, if it exists, WannaCry will not execute. This kill switch was quickly identified by a security researcher, who then ensured that the domain name existed. Connections from inside the CERN network to that domain are redirected to a website maintained by the CERN Computer Security Team thus preventing the devices from being infected and giving us visibility into the affected systems.

**Drive-bye (2016)**

Like a lion waiting to ambush gazelles at a waterhole, malware can catch you by surprise.

As some of you might have noticed, the Computer Security Team had to block the news site “20min.ch” a while ago, as [it was found to be distributing malware](http://cds.cern.ch/journal/CERNBulletin/2016/24/News%20Articles/2159537?ln=en). This block comes after similar incidents at other Swiss organizations. Our blocking is protective in order to safeguard your computers, laptops, tablets and smartphones.

Unfortunately, this is not the first time we have seen these so-called drive-by/waterhole attacks: once you have visited an affected website, embedded third-party malicious code is downloaded to your computer and subsequently infects it (if running Windows or Android as well as, less likely, Mac operating systems). Hence the name “drive-by”. As “20min.ch” is a very frequented website among CERN staff members and users, it makes it a perfect source for attacks against CERN (or other Geneva-based organisations): instead of attacking those organisations directly, which might be difficult as they are likely to be security aware, why not first target an external site with a lower security level, but with high visibility? Like a lion waiting to ambush gazelles at a waterhole, hence the name “waterhole attack”. In the past, other prominent websites in the Geneva area were also susceptible to such attacks. “20min.ch” has already shown up on our radar a few times in the past.

Protection is difficult as the hosted malware is usually based on “zero-day” exploits, i.e. malware that is exploiting vulnerabilities not publicly known at that moment. We usually recommend having your system completely up-to-date – using Windows Update, Mac Update, Yum auto-update, or any other permanent update mechanism for your preferred operating system and applications. We also recommend running an anti-virus solution: check here for [CERN’s free offerings](http://cds.cern.ch/journal/CERNBulletin/2016/24/News%20Articles/2159537?ln=en). However, these won’t help with fighting zero-day exploits, as neither the patching nor the anti-virus software could
know about them. Still, don’t be negligent. If you want to be careful, browse the web from a Linux PC (like LXPLUS) as they are currently less susceptible to that kind of attack. Or just refrain from visiting this type of website. Remember? When in doubt about the link/URL you are about to open: “Stop, think, don’t click!”

Playing hardball? Unfortunately it’s necessary... (2016)


Time and time again, we see PCs and laptops being infected at CERN. While a local anti-virus software solution should provide you with basic protection, no anti-virus software will ever be able to detect all threats in a timely manner, nor will it be able to clean up an infection completely. If the anti-virus software doesn't manage to quarantine the infection immediately, reinstall your infected PC or laptop as soon as possible and change all your passwords afterwards to be on the safe side!

There are a multitude of ways in which your PC can become infected: lack of vigilance when browsing the web (remember: “Stop – Think – Don’t Click”) and consequently arriving at a malicious website; installing software and plugins from dubious locations with unknown side-effects; infected USB sticks making their way into your PC/laptop; opening e-mail attachments with dodgy content... Once you have fallen into such a trap, the infection will nest itself deeply in your Windows/Mac/Linux operating system. It will try to remain silent. It will start to do its thing: stealing data, sniffing passwords, capturing your network traffic, taking snapshots of your desktop, encrypting your hard disk (and subsequently blackmailing you), attacking others, providing a platform for hosting pornographic images or illegal content... and so on.

Anti-virus software is supposed to provide you with a first line of defence. By analysing activity on your computer, it should be able to quarantine malicious actions before they are executed. It should keep malicious behaviour at bay. But not all malicious actions and behaviour are known before they hit: anti-virus software must be provided with up-to-date signatures to spot them. This update process takes time; your computer might be infected before the anti-virus software has a chance to step in. Therefore, we continue to rely on your personal vigilance and common sense. Beware!

Once your computer is infected and the anti-virus cannot quarantine and contain the infection, all is lost! This is the moment when the infection is deeply hidden and nested in your operating system. Game over for your computer and your passwords. This is also the moment when you should strongly consider reinstalling your computer from scratch. If we detect your computer being infected via our detection mechanisms, we will definitely ask for reinstallation and take your computer off the CERN network until it’s done. Also, we strongly recommend that you change all your locally stored passwords and any password typed recently on that computer. The infection might have sniffed it out. Similarly, credit cards whose numbers were entered on that
computer should be closely monitored. Maybe the infection also took your credit card information? Another good argument to be paranoid (if your money matters to you). Thus, hardball in the event of an infection is – unfortunately – necessary…

Just one more point: the CERN anti-virus software is available for free for your Mac or Windows computer if you work at or for CERN. If you want to top up your protection, we recommend you buy “Malwarebytes” and/or “Spybot Search & Destroy”. Finally, we have drafted a dedicated “Security Baseline for Hardening PCs and Laptops”, which can also be applied to your private and home computers.

DNS to the rescue! (2016)


Why you should be grateful to the Domain Name System at CERN.

Incidents involving so-called “drive-by infections” and “ransomware” are on the rise. Whilst an up-to-date and fully patched operating system is essential; whilst running anti-virus software with current virus signature files is a must; whilst “stop --- think --- don’t click” surely helps, we can still go one step further in better protecting your computers: DNS to the rescue.

The DNS, short for Domain Name System, translates the web address you want to visit (like “http://cern.ch”) to a machine-readable format (the IP address, here: “188.184.9.234”). For years, we have automatically monitored the DNS translation requests made by your favourite web browser (actually by your operating system, but that doesn’t matter here), and we have automatically informed you if your computer tried to access a website known to host malicious content that could infect and compromise your computer, your password, your data, and your life. In parallel, we have used and will continue to use the DNS to block certain web addresses that are known to be malicious and that are used for wrongdoing against the Organization. Similarly, we also block some domains resembling the domain name “cern.ch” that - on a closer look - are different, like “cem.ch” or “cern.cn” (did you spot the difference?) in order to protect CERN against typo-squatting.

But the DNS can do more. Thanks to the IT networking team, the DNS infrastructure has been reinforced: the new set-up is more resilient to denial-of-service (“DoS”) attacks. It also has another benefit: the DNS firewall. Our internet service provider “SWITCH” collects and provides lists of well-known and guaranteed malicious domains. The new DNS set-up allows us to incorporate their DNS firewall configuration such that all those domains are automatically blocked, too. Next time you hit on one of our landing pages for phishing (i.e. webpages trying to harvest your password) or
malware, you should be grateful. Your computer might just have been one click away
from getting infected¹.

A few Christmas goodies for your security (2016)

https://home.cern/news/news/computing/computer-security-few-christmas-goodies-
your-security

Securing your laptop, PC and data is difficult? Not necessarily! You might not
have noticed, but the IT department put under the Christmas tree a wide range of tools
which likely improve the security of your data, laptop and PC. Let us present here a
few. It’s for your protection.

1. Antivirus software. The CERN-chosen antivirus software comes for free
installation on your office computer/laptop as well as on your personal Windows
or Mac devices like those at home. Just get it installed. If you prefer “more”
central assistance, join CERN’s Windows management framework (CMF) - or
the Mac Self-Service. Centrally managed Windows PCs come with centrally
managed antivirus software by default.

2. Full disk encryption. CERN provides centrally managed encryption solutions for
Windows PCs (Bitlocker) as well as Macs (Filevault) and Linux CentOS (LUKS).
Advantage of those solutions is that they are completely transparent and you
do n’t need to hassle with back-up or recovery key storage. Just contact the
ServiceDesk to get your hard disk encrypted!

3. PC hardening. The Computer Security Team and the Windows Desktop support
team are currently working on guidelines on how to harden PCs to a maximum
(while keeping them still usable). A draft of such guidelines can be found here.
But beware, this is for the paranoid or for very dedicated use cases!

4. Secure file exchange. Instead of handing out confidential files to Dropbox and
alike, CERN is hosting “CERNbox”, a file synchronization service for Android
and iOS smart phones, tablets, PCs and laptops. While the data resides well
protected within CERN, it is available and sharable through-out the world.

Apart from those four, CERN’s IT department provides you with a wider range of central
services so you don’t need to reinvent the wheel: Database-on-demand, Drupal, Java
or Sharepoint hosted websites, central storages and back-up solutions
(AF S, DFS, CASTOR, and Tivoli, to name a few). Please find a complete list of their
offerings here. In addition, a dedicated webpage presents a comparison between
commercial/off-site solutions and similar solutions provided in-house by the IT
department.

¹Careful here! We can only protect your computers while they are connected to CERN’s networks. From
home, the malware might succeed!
Open door, open screen, open life... (2016)

How entangled is our physical life today with the digital world? Personal mail and documents, private social media postings, family photos and videos, your favourite music and films... Getting a look at the hard disk of your computer might give similar insights to a tour of your house or apartment. So, the basic question is: why would anybody leave an office containing their laptop open and unlocked while nobody would ever leave their house with the door unlocked?

A short walk through any arbitrary CERN office building during lunchtime allows anyone to take an in-depth look into the private lives of our colleagues. Office doors left open. Computer screens unlocked and glowing. Owners out for lunch. Bingo — with a bit of malicious intent and some chutzpah, the curious can now sit down in your living room and marvel at your life. And we are not talking about a few isolated instances, there are plenty. Open days at home! Your full privacy sphere exposed.

Do yourself a favour: protect your privacy, protect your computer. Lock the screen when leaving your laptop unattended — in your office, at a meeting — even if you just walk away to fetch something from the printer, buy a coffee or answer a call of nature. The screen-lock is just one keystroke away: “Windows-L” for Windows PCs, “CTRL-ALT-L” on Linux systems (depending on your favourite Linux flavour), “Control+Shift+Power” on Macbooks. Also, consider protecting your laptop with a chain (a "Kensington"-lock) and locking your office with a key when you leave: it is not unusual for laptops to disappear from offices... forever.

Flash, as bad as bad can be (2016)

Being flashed by a speed camera on the motorway is a nuisance but it’s usually your fault, you were speeding, and it looks like using Adobe Flash on your computer nowadays can cause a similar blunder. This year, the Adobe Flash Player made it to number 1 in the charts of ways your PC or laptop could be compromised.

Just recently, another vulnerability for Flash was reported, affecting all operating systems: Windows, Mac, Linux and Chrome OS. One vulnerability to rule them all – the main reason why Flash topped the charts at number 1. The first exploits abusing this vulnerability have been already reported and it is now up to all of us to fix our operating systems ASAP. As usual, owners of CERN centrally managed Windows PCs don’t need to worry. Their PCs will have this fix automatically deployed.

But more generally, why do we still stick with Flash? Its time has passed and it is being superseded by the more fancy and modern HTML5. The IT department is therefore actively eliminating any requirement for it in central services and considering dropping...
the installation of Flash from all of its centrally managed PCs. And since they are already at it, Adobe’s Acrobat Reader, which is also a prominent member of the Top 10 vulnerabilities, might be phased out too. Of course there will be suitable alternatives offered for both. So, why would you still need Flash for professional purposes?

Ransomware — When it is too late... (2016)

Some forms of ransomware systematically encrypt files on the system's hard drive, which become difficult or impossible to decrypt without paying the ransom for the encryption key, while some may simply lock the system and display messages intended to coax the user into paying...” (Source: https://en.wikipedia.org/wiki/Ransomware)

It is not unusual to see devices falling prey to ransomware. PCs and laptops, in particular those running the Windows operating system, can easily be infected with ransomware if the user is inattentive. For example, if they open an attachment to an unsolicited mail (see some hints to detect bad emails here), or click on the link to a malicious website (see our articles on our clicking campaign).

So what can you do if you have already fallen to ransomware? First of all, turn the infected computer off immediately. Just cut the power. This will stop the malware from attacking more files. Secondly, do not pay. Do not answer. Contact us at Computer.Security@cern.ch. We might have some tools to unlock your computer again. It is already too late for your data, but if you have been careful, you should have a back-up from which we can recover your files. Standard folders on centrally managed Windows PCs are automatically backed up to CERN’s DFS file storage. You can also enable DFS back-up for Macs and Linux systems or, alternatively, use AFS or CERNbox. If all is lost, we can still offer you a hot beverage to ease the pain.

And how can you protect yourself? First of all, maintain permanent back-ups of your files (see above). Keep your operating system up-to-date by running automatic Windows updates, Mac software updates or the Linux “yum auto-update”. Pass the responsibility to CERN’s IT department if you don’t want to do this yourself. For Macs and Windows computers, install a decent antivirus software. Remember, CERN provides a free solution for office and home usage. Apply due diligence: stop – think – don’t click if that email, attachment, link or URL is suspicious, looks weird, or is not really intended for you (see once more our hints to detect bad emails). Finally, refrain from installing software from dubious webpages. “Free” does not always mean free; some “free” software or applications come with integrated ransomware...
Mac security — Nothing for old versions (2016)


Only software which is up-to-date should be free from any known vulnerabilities and thus provide you with a basic level of computer security. Neglecting regular updates is putting your computer at risk – and consequently your account, your password, your data, your photos, your videos and your money. Therefore, prompt and automatic patching is paramount. But the Microsofts, Googles and Apples of this world do not always help…

Software vendors handle their update policy in different ways. While Android is a disaster – not because of Google, but due to the slow adaptation of many smartphone vendors (see “Android's Armageddon”) – Microsoft provides updates for their Windows 7, Windows 8 and Windows 10 operating systems through their “Patch Tuesday” rollouts. All you need to do is have the automatic “Windows Update” feature enabled (it is by default!). While automatic updates are also provided to Apple Macs by default, they have a more restrictive (but undocumented) policy for their Mac OS: Apple provides security fixes mainly for the latest version of OS X (also dubbed “El Capitan”). Any older versions of MacOS either receive no security updates at all, or do so for only a few of the known vulnerabilities!

Thus, don’t just “feel” secure, even if Apple are still providing some security updates for OS X 10.9 and 10.10. They are not resolving many other known security issues for those versions. And worse, the fact that Apple still provides some software updates – but no security updates – for even older versions of the OS does not mean that these OS versions are still supported. They are not. Hence, any versions of OS X other than 10.11.3 are vulnerable today to any kind of cyber-attack (e.g. when browsing malicious webpages, when installing malicious software or reading malicious e-mails, etc.). If your Mac happens to run another version than the latest, “El Capitan”, (you can check under the Apple Menu and choose “About This Mac”), we strongly recommend that you upgrade it as soon as possible. Just visit this page. However, please note that “El Capitan” might be incompatible with certain, mainly older, software packages. You can find known issues here. Still, upgrading is always the best course of action.

USB sticks — The silent killers (2015)


You've just found a USB stick in Restaurant 1. You'd like to return it … but who is the owner? Maybe the contents can tell you? Connect it to your laptop, and you might figure it out. But hold on, what if its content is dangerous…?

USB sticks are an excellent vehicle for infecting countless PCs and laptops. Years ago, several dozen laptops were infected during a conference when someone passed around a USB stick with flight departure information. Unfortunately, this stick was
infected. Similarly, we have seen a domino effect of infections in the FP and EN departments after some USB sticks made the rounds, infecting one PC after another. In the end, a massive number of PCs had to be reinstalled.

Some USB sticks are even worse. They pretend to be “just a keyboard” (named “RubberDucky”) and, once inserted, they execute a pre-programmed sequence of keystrokes intended to extract information from your computer or take it over. Others have malware compiled into the USB’s hardware chips and not into its storage area, for example e-cigarettes that are charged by a USB cable. Even worse, the next generation of fake USB keys might be able to destroy part of your computer (see here)! No technical solution can protect your computer from that!

So what can you do? First of all, don’t use USB sticks if you don’t trust their provenance. If you’ve found a USB stick, hand it over to Computer.Security@cern.ch. We have means of dealing with infected sticks. Secondly, use good antivirus software, which should be able to detect known threats stored on a USB stick. Give the software the time to run a full scan. The CERN antivirus software is available here for Windows and here for Mac, and can also be used to protect your computers at home. Thirdly, in order to help your antivirus software, keep your laptop, PC, tablet or smartphone up-to-date with all the recent software upgrades and patches. Have the “Windows Upgrade” or Mac “Software Update” set to “automatically download and install”. For Linux use, for example, “yum auto-update”. CERN PCs and laptops are centrally kept up-to-date via CMF. Fourth, if you manage your own PC, check the “autorun”/“autostart” settings for USB sticks. If CERN IT manages your PC or laptop, all is fine.

Finally, be vigilant and report suspicious USB sticks to Computer.Security@cern.ch. If you are really paranoid and just want to use your USB port for charging e.g. your mobile phone, buy a USB “umbrella”, which blocks the data connection and only allows power through.

**Bye, bye, Windows XP security... Welcome infections! (2014)**


Rest in peace, Windows XP. Since your birth on 25 October 2001, you have struggled hard to survive this harsh Internet world. You fell prey to “Melissa”, “Sasser” and “Conficker”, and brought CERN its last large-scale infection with “Blaster” in 2004.

After being upgraded to “SP2”, you discovered software development lifecycles, regular “Patch Tuesdays” and a local firewall that rejected everything by default. In the end, you outlived your weird brother “Vista” and survived as the ugly duckling cousin to the beautiful Mr. Mac. But all your ups and downs are over now. On 8 April 2014,
you were given your very last security updates. These life-sustaining measures will be stopped now. Game over.

From now on, you are a zombie: presumed dead, but still kept running by your master/owner/user. They might not even understand that you now pose a risk to them. Viruses and worms are on the prowl, hunting for any Windows XP system still connected to the Internet. Unprotected and naked, you are now an easy target for infections.¹ Web browsing and opening emails becomes Russian roulette with you.

It's best if your master gives you a facelift, and upgrades you to Windows 7 (or to Windows 8.1). Alternatively, your master might disconnect you from the Internet (see http://network.cern.ch, select Upgrade and uncheck “Internet Connectivity” at the bottom of that page), or, even better, from any network at all (just cut the cable). Putting you on a separated and isolated network would do, too. There you can wait for your retirement… along with your friends, Windows 95/98/NT/2000 and Windows server 2003, as well as your arch-enemies CERN Scientific Linux 3 or 4 and MacOS pre-version 10.6 (“Snow Leopard”). They shouldn’t be here anymore either. Go away!

Agility for computers (2014)

I have just made an inventory of all the digital gadgets connected to my wireless network at home: two Windows laptops, two tablets of different generations, my two kids’ iPods, one iPhone, an Apple TV, an old iMac, the Wii U, a Sony TV, a Sony stereo, the Wi-Fi router (of course!), a Network Attached Storage and two IP telephones. I’m sure other people have many more...

In the future, I could even have an internet-connected car or coffee-machine or a smart meter (see “Hacking control systems, switching lights off!”), and I could eventually even connect my solar panels to my Wi-Fi network. That’s quite some phase-space for vulnerabilities waiting to be exploited by attackers!

Therefore, locking down my Wi-Fi router and blocking all incoming access was essential, but my kids randomly browsing the web still posed an insider threat… Thus, patching and keeping all systems up to date became important, too. But given the number of devices, how could anyone expect me to spend all of “Patch Tuesday” – the day each month when Microsoft publishes its newest updates – running around and keeping all our operating systems, firmware and applications up to date? I am already fed up with keeping my iPhone and its apps up-to-date – every second day, so it seems, I am forced to apply new updates to some apps… How would this scale up to a cacophony of devices at home? In short: it doesn’t, and it also doesn’t work well in a large computer centre like CERN’s. This month, Microsoft issued two critical patches:

---
¹ Even if many anti-virus vendors, including Microsoft, will continue to provide anti-virus signature files, you’ll still be a zombie. Only you’ll be a zombie wearing body-armour with some weak spots.
“MS14-066” and “MS14-068”. You can imagine how extra-busy many system administrators were (twice)!

So we need a change of paradigm. Enter: “agility”. In the near future, I expect security updates to sneak into my devices clandestinely (if I opt in) in order to keep them up to date and provide protection against exploitation. Patching must become “agile”, meaning that updates are automatically pushed and applied once ready\(^1\). And they have to be applied to everything: PCs, laptops, smartphones, embedded systems, control devices, and so on – fully independent of criticality. No need to wait for “Patch Tuesday”, no more hassle running around pushing buttons, and no more reboots that stop me from working.

We’re not there yet, but we should still at least try to become more agile. A good start is enabling services like “Windows Update”, Mac’s “Software Update” and Linux’s “yum auto-update” wherever possible. That means not only on office PCs, laptops and tablets, but also on control devices, SCADA systems, computing nodes, computer centre servers, etc. The more critical a system is, the more we should worry about it not being patched and the more we should invest in enabling prompt and agile patching. In certain, justifiable circumstances, other security protections could be used. We should talk to the vendors of those systems and deploy frameworks to make upgrade management easier. Using Puppet, as we do in CERN’s “Agile Infrastructure” for managing the Meyrin and Wigner computer centres, is a good start. Upgrade cycles have become shorter. However, there is still room for improvement as the security incidents connected with “Heartbleed”, “Shellshock” and “Poodle” have shown: while most of the servers used in the computer centre and for control systems were fixed quickly, many fringe systems remained vulnerable for another month! Better (and quicker) configuration management is important to prevent those systems from becoming insecure.

So, how agile are your systems? How quickly could you apply a security fix if you had to do it NOW? If the answer is “within a day”, congratulations! If the answer is “next summer”, we should talk.

Don’t put your family at risk (2013)

How easy is it to fall into the trap of cyber-criminals? Get one’s online banking password stolen? Lose photos to third parties? It's easier than you think. One single click to open a malicious attachment or a malicious web page is sufficient to put your family at risk.

\(^1\) Normal updates for new features etc., however, would still need the consent of the user in order to prevent unwanted functions from being installed.
Sometimes adversaries even call you in order to get their malicious job done. Once their malware is installed on your home computer, it records all your activity, monitors your online banking activities, steals your passwords, activates your computer’s microphone and camera, and sends all that data back to the adversary. This person can now do whatever they want: take money from your bank account, order books with your Amazon password, deface your Facebook profiles, send strange messages to your peers, or post the captured images of your daughter in front of the computer on dodgy web sites. Not only can you lose (lots of!) money, but having strange messages sent on your behalf and your private images made public can also be very embarrassing.

So don’t put your family at risk! Think of the security of your computers at home! Our advice for protecting networks and computers at CERN also holds for usage at home: restrict access, patch and run anti-virus software, keep your password to yourself, and stop – think – click before accessing untrustworthy websites. Here are a few helpful hints to make your family’s life more secure.

If you run your own wireless access point (a hardware box connected to your telephone line), ensure that communication is encrypted using at least the WPA2 protocol and a strong password. This will protect you and your family from someone piggy-backing on your network connection. Wireless security protocols like “WPA” or “WEP” can easily be broken. Also make sure that the hardware’s firmware is always up-to-date. Usually you can do both from the configuration menu of your wireless access point.

For patching:

- If you have a personal computer with your own Windows operating system, check for “Windows Update” in the programme listing of the Start button. Switch to the recommended “automatic” updating method!
- On Linux distributions, make sure that you regularly run “yum update”, or even better, enable automatic updates. Don’t forget to reboot your computer when a new kernel is installed, in order to properly apply kernel patches!
- For Apple Macs, use the software update mechanism which is accessible under the Apple menu.

The CERN anti-virus software for Windows and Mac can also be used at home - for free! Also, ensure that you also regularly update your Acrobat Reader, Adobe Flash, Java and all the others. If you are in doubt (and are running a Windows system), you can install and run this fine programme from Secunia which checks your computer for outdated software.

Concerning your password, choose it with care and do not use the same password for different sites including CERN. Have a look at CERN’s password rules, which also apply to your home usage. Take particular care of your online banking password! For better protection, banks usually employ an additional hardware token for online
banking (which is why you have a small USB pocket calculator). Eventually, you might want to use similar techniques for your Google+ (called “GAuth”) or Facebook account. Did we mention it before? Stop – think – click when browsing the web. Visit only the sites you deem trustworthy!

Finally, share this information with your spouse and kids. Tell them all! Make them aware of the risks of using a computer connected to the Internet, and remember that “computer security” is like road safety education, looking left-right-left when crossing a road. If you would like to learn more, click here for some easy online courses that delve deeper into this subject.

Got a call from "Microsoft"? The social way infecting your PC (2012)


Still love bashing on Windows as you believe it is an insecure operating system? Hold on a second! Just recently, a vulnerability has been published for Java 7.

Have you recently been called by “Microsoft Security”? At home!? Then beware: these are fake calls trying to make you install malicious software on your (home) PC!

This scam is currently prevalent throughout the Geneva area, targeting many different international organizations and companies. If you receive such a call, just ignore it and hang up. If you have fallen for this scam and followed their pleas, please contact us at Computer.Security@cern.ch.

This kind of scam is called “Social Engineering”. Some “Microsoft” call-centre agent informs you that your PC is infected and will try to convince you to download some software from the web. If you do – BANG – your PC is compromised and your local data is at stake. In other Social Engineering scams, the attackers try to convince you to give them your password or sensitive documents. Thus, recall that the real Microsoft will never call you – and definitely not on your home number. Nor will Apple, the CERN Computer Security or the CERN Service Desk (unless you have asked them to). If someone does, just ignore them and hang up, and let us know at Computer.Security@cern.ch. In particular, if someone was asking for your password.

Better be aware and proactive! Recall that your passwords are yours – and only yours. No legitimate person will ever ask for it: not the CERN Service Desk, the Computer Security nor your supervisor. Also, PayPal, Facebook, Google, Apple, Microsoft, UBS, etc. will never ever ask you for your passwords. Regularly patching your Windows or Linux PCs, as well as Apple Macs, is mandatory and the best line defense your PC/Mac can have – at home as well as at CERN. For Windows and Macs it is even strongly recommended to run anti-virus software. The CERN anti-virus is also available for free.
for your home PC or Mac. Finally, taking care (STOP – THINK – CLICK!) when browsing the web or opening emails is a good habit to protect your assets.

Follow those easy hints for a basic level of computer security awareness… at CERN as well as at home!

**Infecting Windows, Linux & Mac in one go (2012)**


Still love bashing on Windows as you believe it is an insecure operating system? Hold on a second! Just recently, a vulnerability has been published for Java 7.

It affects Windows/Linux PCs and Macs, Internet Explorer, Safari and Firefox. In fact, it affects all computers that have enabled the Java 7 plug-in in their browser (Java 6 and earlier is not affected). Once you visit a malicious website (and there are plenty already out in the wild), your computer is infected… That's "Game Over" for you.

And this is not the first time. For a while now, attackers have not been targeting the operating system itself, but rather aiming at vulnerabilities inherent in e.g. your Acrobat Reader, Adobe Flash or Java programmes. All these are standard plug-ins added into your favourite web browser which make your web-surfing comfortable (or impossible when you un-install them). A single compromised web-site, however, is sufficient to probe your browser’s plug-ins for vulnerabilities, and eventually infect your PC. You are not even safe if you are using Mozilla’s Firefox or Google’s Chrome instead of Internet Explorer: if you neglect to update your Acrobat Reader, Adobe Flash or Java, your PC or Mac will become infected. Full stop. Even worse, these plug-ins are also a standard part of your browser on Linux PCs or Macs - and so the vulnerabilities and the risk of infection might become a part of them too!

Remember that, at CERN, every infected PC must be reinstalled from scratch! Thus, do yourself a favour. Take care of all installed software and apply patches in a timely manner:

- If you run a centrally or locally managed Windows computer, give that small orange blinking “CMF” icon in the taskbar a chance in the evening to apply all the pending patches. Also, let it initiate a reboot at the end!
- If you have a personal computer with your own Windows operating system, check for “Windows Update” in the programme listing of the Start button. Switch to the recommended “automatic” updating method!
- On Linux distributions, make sure that you regularly run “yum update”. Or even better, enable automatic updates. Don’t forget to reboot your computer when a new kernel is installed, in order to properly apply kernel patches!
- For Apple Macs, use the software update mechanism which is accessible under the Apple menu.
Also, ensure that you also regularly update your Acrobat Reader, Adobe Flash, Java and all the others. Usually, they notify you when you should do so. If your application is supported centrally by CERN's IT Department, they will take care of it. However, if this is a programme you have downloaded and installed from the Internet it is up to you to ensure it is up-to-date and patched… If you are in doubt (and run a Windows system), you can install and run this fine programme from Secunia which checks your computer for outdated software.

Gotcha! Macs lose their innocence (2012)  
https://cdsweb.cern.ch/journal/CERNBulletin/2012/18/News%20Articles/1443480?ln=en

Still believe your Mac is secure because Microsoft PCs fall prey to viruses and worms but Macs don’t? Time to wake up! This year has seen the first major compromise of Macs worldwide¹. How is yours doing?

The “Flashback” Trojan is affecting Apple’s own variant of Java and compromises Macs via so-called drive-by infections, i.e. when you visit an appropriately prepared (infected!) website - and this might not necessarily be a site with questionable contents, but could well be a popular, reputable one. Security Companies worldwide have been monitoring this particular Trojan for a while and have estimated that more than half a million Macs were compromised. Connected to a few central command and control servers, the compromised Macs were then supporting the malicious activity of the bad guys! Fortunately, the security companies have now been able to take over those command and control servers and stop their destructive drive.

So, Mac users, face the fact that timely patching and running of anti-virus software is also good for the well-being of your Mac (and your nerves). Keep your operating system up to date and use the “Software Update” mechanism which is accessible under the Apple menu. If you run an older Mac OS version, upgrade to MacOS 10.6 or 10.7 by following the instructions provided by the CERN Mac Support Team. You can find out which version of the operating system your Mac is running by clicking on the “About This Mac” item in the Apple menu.

PLEASE NOTE that running “Software Update” does NOT update to newer major versions of the operating system! In order to move to a newer major version (e.g. 10.6 or 10.7) you have to explicitly install that major version.

In addition, you can get free anti-virus software from CERN. Finally, only move up to "administrator" rights where it is strictly necessary, and elsewhere stick to restricted “user” rights.

¹ Interestingly, the very first ever virus (called “Elk Cloner) targeted Macs in 1981, five years before the first IBM/DOS virus (see here).
Found a USB stick? Go and infect your PC! (2012)

Err. Wait. Please no! USB sticks are not innocent little things. They can quickly mutate into malicious nasty beasts! Just in the recent past, at least two physics experiments were suffering as their control and data acquisition PCs, respectively, were infected by USB sticks holding malicious code. A bit longer ago, a series of laptops were infected at a 2008 computing conference as an infected USB stick made its tour around. Bad luck for those who ran a Windows operating system and inserted that stick…

So, you found a USB stick in the cafeteria? Take care. If this were a lollipop, you wouldn’t just pick it up and lick it, would you? So beware of USB sticks whose origin or previous usage you don’t know. They might infect your PC once plugged in. In order to be on the safe side, accept and share only USB sticks whose owner you trust. Run up-to-date anti-virus software on your PC, make sure that its operating system is patched regularly, and turn off the “auto-play” feature (which should already be off by default on recent systems).

If you are involved in the maintenance or development of control systems for accelerators or experiments, please note that the use of USB sticks on such systems is strictly restricted. Any violation (and a subsequent infection of a control PC) is considered to be a professional fault.

25 years — Happy Birthday! (2011)
http://cds.cern.ch/record/1324840/?ln=en

The nasty PC virus turned twenty-five years this month. The very first computer virus ever was created in January 1986. Dubbed "©Brain", this virus was aiming to infect DOS-based PCs. While this instance was relatively harmless and their creators claim sincere intentions, the world has changed since then. Today’s viruses and worms are malign and aim for making profit. They attack now everything connected to a network: Windows PCs, but also Linux PCs and Macs; iPhones and other mobile devices; directly the operating system, but also applications like Adobe Reader (PDF), Firefox. Thus, protect your computers from viruses and malware. Any unprotected computer connected to the Internet is likely to be infected within minutes! Keep your system up to date.

- Enable the regular automatic installation of updates/patches. If you can, use operating systems managed by CERN’s IT department;
- Use anti-virus software. The CERN anti-virus solution is even free for your home and private usage;
- Do not install untrusted software or plug-ins. Indeed, software from untrusted sources may infect or compromise your computer...;
- Do not open unexpected or suspicious e-mails or attachments. Delete them if they do not concern you or if they appear weird. If in doubt, contact Computer.Security@cern.ch;
- Stop-think-click. Do not click on suspicious links, but only click if you trust their origin. More recommendations can be found on the Security Team’s web site.

Your Computer Security Team

P.S.: The very first virus warning at CERN we are aware of dates from October 1989: Computer Virus Warning to all users of IBM Compatible PCs. It is still valid: “Do not panic … Cross your fingers” :-)

Interestingly, the first virus targeting Macs (called “Elk Cloner”) came out five years earlier in 1981! The first ever virus, “Creeper”, was detected as early as the 1970s.
An open market is a fine thing. Anyone can offer anything for sale. You have a broad variety of products, you can pick and choose. The only drawback is quality. Unfortunately, it is your responsibility to check whether you are getting acceptable quality for the price you pay. While this is more-or-less easy in the supermarket, it gets very complicated when talking about apps for your smartphone from the app market. And the malicious evil-doers are taking advantage of that…

Usually, you just enter “Google Play” or Apple’s “App Store”, make your pick and install the app of your choice. Easy. But how can you be sure that the app does not do more than you expect? A recent analysis of the devices of almost 700 million customers of 31 mobile network operators in 20 countries showed that about 6% of the devices were infected. Given the fact that Android devices account for around 75-85% of all smartphone sales worldwide, they are clearly under targeted attack. More than 98 000 malicious apps were detected, 51% of them available through Google Play, the rest only downloadable through third-party app stores. Thanks to Google’s efforts (“Google Protect” and the “App Defense Alliance”), 18% were removed.

So 32% remain which were not. The remaining 32% which, when installed, are used to abuse your phone. Top of the list is malware to conduct “advertisement fraud”, i.e. downloading hidden ads, automatically generating clicks on advertisements (so-called “Clickbots” like “emoji keyboard” or “Snaptube”), or tricking you into clicking on them without being aware (“Click-Jackers”). Different malware is using different techniques to avoid being spotted by the advertisement companies so that every click generates revenue for the app’s company, leading to a multi-million dollar loss for the advertiser. Other malware is misusing the smartphone’s CPU resources to generate cryptocurrency (“Bitcoin mining”), initiating fake calls to expensive phone numbers or sending premium SMSs at your expense (“subscription fraud”). In fact, there is a mafia-like industry selling your smartphone’s resources to the highest (evil) bidder.

Once more, the responsibility is in your hands: always keep your smartphone up-to-date with the most recent version of your operating system (and if this is not possible as the smartphone hardware is too old and not supported anymore, consider replacing it completely). When downloading apps, “STOP – THINK – DON’T CLICK” (“Don’t install!”) is your best protection. A high number of downloads does NOT indicate that the app is clean. Check out the comments for the app you’re interested in. Take special care when installing apps from third-party stores. The security mechanisms put in place by such stores to avoid fraudulent abuse might be mediocre. Better to just refrain from downloading (trivial) apps you don’t really need produced by unknown (small)
companies. One recent example discussed here is the problem of apps providing fraudulent VPN tunnels (see our Bulletin article on “Tunnel Madness”). Finally, it is a good idea to check your privacy settings regularly: do only those apps with a justified need have access to your camera, microphone, location, contacts? Some apps might reset these when they are updated.

**Un-confidentiality when using external e-mail (2019)**


Using the CERN e-mail service gives you some flexibility. Maybe a bit too much, as some current practices are problematic under CERN’s Computing Rules ([CERN Operational Circular No. 5](https://home.cern/news/news/computing/computer-security-un-confidentiality-when-using-external-e-mail)) since they can have severe implications for password secrecy and the confidentiality of certain documents sent by e-mail!

E-mails are like unsealed envelopes. Everyone who has physical access to that envelope can read the letter inside. In the digital world, this means that everyone with access to your mailbox can potentially read all your e-mails. This is why the CERN e-mail service is hosted within CERN and its managers are subject to strict confidentiality rules. E-mail communication within CERN is encrypted, but easily gets lost once e-mails leave the Organization. So let’s take a look at just how easily...

To take one example, configuring a forward for all e-mails sent to your @cern.ch address towards an external e-mail provider like Gmail, Yahoo, Mail.ru, GMX.de or Outlook.com, exposes all forwarded e-mails to that third party. CERN confidentiality is left to be “just” governed by the third party’s commitment to maintain confidentiality and hence is subject to any business interest they might have. No guarantees, but plenty of terms and conditions. The confidentiality of CERN’s internal information, documents and attachments exchanged by e-mail is lost. And the original sender might not even realise this! In addition, forwarding e-mails to third parties poses a risk to CERN’s privileges and immunities as an intergovernmental organisation (as also stated on the e-mail service’s configuration page). They become void when confidential information is forwarded by e-mail, leaving the Organization unprotected (see our very old Bulletin article entitled “Don’t let your mail leak”).
Secondly, giving an external e-mail provider such as Gmail full access to fetch or delete e-mails from CERN’s mail servers and write e-mails on behalf of CERN defeats password secrecy. Your CERN password is yours and only yours. It must not be shared with anyone else. However, for the aforementioned full access the third party has to store original, plain text CERN passwords, and use them directly on behalf of the CERN user, to connect to CERN’s e-mail service and let Gmail fetch data from your CERN mailbox. This is different from configuring your local (local!) mail client to fetch these e-mails as your local mail client resides on your local laptop, smartphone or tablet, and is not handed out willingly to any third party.

Thirdly, e-mails with confidential content leaving the Organization require special care. Encryption of the confidential contents is the usual (but difficult) remedy. Better is to avoid e-mail as a communication channel for such data at all. For personal data, CERN’s Office for Data Privacy (ODP) recommends avoiding wherever possible the use of e-mail to communicate personal data. In any case, secure collaboration workspaces are the preferred mechanism (see our Bulletin article entitled “A ‘file drop’ for confidential data”).

What next? Help us to protect CERN’s data, operations, and privileges and immunities. Reconsider your working principles:

- Avoid forwarding e-mails to a third party e-mail provider. If you are employed by CERN, the CERN e-mail service should be most appropriate for your professional needs;
- Do not allow a third party e-mail provider to automatically fetch and process your CERN e-mails. Keep your password and access to CERN protected;

1 Interestingly, Google has started doing exactly the same: restricting remote API access calls to its Gmail service. Until now, for instance, you could configure any third-party e-mail app to access your Gmail account in order to send, read and delete e-mails remotely. But that has ceased due to Google’s privacy concerns.
Refrain from sending confidential documents, in particular those containing personal data, via e-mail. Instead, use CERNbox as a secure alternative.

The CERN Computer Security Team, in collaboration with the CERN account management service, the e-mail services and the CERNbox team are always actively looking into providing you with the best ways to keep your communications secure.

Trips and travel: Some recommendations (2017)

Autumn conference season is fast approaching. Have you ever thought about how best to secure your laptop and smartphone — and with it your data and documents or your (private?) photos and videos — while travelling? See below for some recommendations…

Of course, the best option is just to leave your laptop at home. Take a break from Facebook, WhatsApp, e-mail, etc. for a few days, relax and enjoy your conference. Remember that Internet kiosks or terminals in the hotel lobby are not an option as these computers might already be compromised and able to sniff your password. If you can’t be without your laptop — and there are plenty of reasons why — the second best option is to bring along a “disposable” laptop which does not hold any important data and which you can completely reinstall once you are back. Any work-related data can be kept at CERN and remotely accessed through CERN DFS or CERNBox. This might be particularly useful if you travel frequently and run a higher risk of theft. Using a disposable laptop might not be an option either, but there is a third option: encrypt your laptop so that all data is properly protected. CERN provides centrally managed full disk encryption solutions for Windows laptops (“Bitlocker”) as well as for Macbooks (“Filevault”) and Linux CentOS (“LUKS”). Taking a backup just before your trip is beneficial too. Just in case…

Similarly for your smartphone, the best option is to leave it at home and get a dumb brick-type mobile phone. That way you will remain available for emergency phone calls but cannot lose any data. And once again, if this doesn’t work for you, leave your phone completely switched off when not in use and make sure that it requires you to type a strong passcode (more than 4 digits!) every time you switch it on! Never connect your phone to a docking station that is not yours. An adversary might just suck up all your data via this means. Better to use your own charger and USB adapter. Alternatively, buy a so-called “Umbrella” stick which allows you to charge your phone from any USB port but physically blocks data exchange.
Finally, if you are on duty travel and carry a CERN device (laptop, iPad, smartphone), do not forget to put the “PROPRIÉTÉ CERN” sticker, which is a means to show that your device is a CERN property enjoying, as such, the inviolability (solely available for CERN devices at the CERN Stores Urgency Window). The latter applies on the territory of the CERN Member and Associate Member States only. This does not imply that the customs or police officials are aware of CERN’s international status. As a precaution, we recommend to completely shut down your CERN device before passing through customs. If you are requested to switch it on, we recommend that you state calmly that it is protected by the inviolability granted to CERN property and that you disagree with any search. If you are obliged to disclose your password or PIN code, please inform the Computer.Security@cern.ch of this unauthorized access ASAP. Please also note that we need to be informed if your device has been taken away, even for a few minutes, or connected to another device. We will take the necessary measures to prevent any potential remote access and, if necessary, replace your CERN device.

Pokémon GO! Or not? (2016)
http://cds.cern.ch/journal/CERNBulletin/2016/33/News%20Articles/2207052?ln=en

Have you already joined the hype surrounding the No. 1 iOS and Android app “Pokémon GO” and started hunting for wild virtual Pokémon while walking through the real world? Have fun and catch them all!!! But also take some physical and digital care!

If you haven’t heard of “Pokémon GO”, it is an iOS and Android game in which your virtual avatar has to hunt for cute and sometimes less cute little monsters, so-called Pokémon (if you are as old as me or have kids, yes, those GameBoy, TV Series, card-game Pokémon!). The ultimate goal is to find and collect all 150 different Pokémon species. Your smartphone’s location information displayed on a Google map lookalike provides you with hints as to where to find them. Augmented reality is employed to project virtual Pokémon in your vicinity onto your smartphone’s camera picture so that
you can catch them by throwing “Poké Balls” at them. These items can be found at other locations, known as “Poké Stops”. The more Pokémon you collect, the more powerful you become (see here for details). No harm in that, eh?

True, from a health perspective, “Pokémon GO” is great as it encourages you to walk around, which is good for all of us. But there is a snag: the app does not know about places you must not go! Walking around while staring at your smartphone’s screen already poses a safety risk. So watch where you are going! Roads. Stairs. Ditches. Open manholes. Ponds! Playing the app while riding a bike or driving (!) is stupid: it goes without saying. In addition, the app just embeds Pokémon where its algorithm deems them best suited. Arlington Cemetery, close to Washington D.C., has already asked players to refrain from playing the game on its premises. The same might be true for hospital wards. And, of course, for CERN: some buildings, caverns, tunnels and other locations on the CERN sites are definitely off limits for gaming. Don’t hunt Pokémon in these locations as it might be dangerous to your health. Some other locations might be off limits as they are private property... Worse, some criminals have used the game to lure people to deserted places, to rob them of their belongings. Think of your safety first! Watch your surroundings, be sensible and don’t get too immersed.

Digitally, there are also risks: “Pokémon GO” has not been made available in all countries, so you might think of downloading the app from dubious sources... But “dubious” already implies that you might get more than you asked for: a full compromise of your smartphone due to the app you downloaded being malicious (see “Android’s Armageddon” for examples). Better to wait to download it from the legitimate and official iOS app store or Google Play! Furthermore, as with many other apps, the “Pokémon GO” app is constantly recording your location, which has an impact on your privacy. Finally, some particularly nefarious people have also jumped on the bandwagon. Malicious e-mails are flooding the Internet all the time and now the first “phishing” e-mails have appeared, luring players to click on fraudulent links (learn here how to identify “bad” e-mails).

I know where you have been... since forever! (2016)

OK, the “forever” has to be taken with a pinch of salt. But generally speaking, if you were to pass near my office carrying your smartphone, I would be able to find out. It’s all thanks to the wireless communication capabilities of your phone...

So how is it done? Every wireless network has a name (SSID: Service Set Identifier). At CERN, for example, you can find “eduroam”, “CERN” or “CERNn” (any other SSIDs are rogue and should not be used). Whenever you connect to a wireless network, your phone keeps a record of the SSID it has connected to for future use. If your phone detects a wireless network, it tries every SSID it has in its list until a wireless access point answers positively, in order to establish a connection. And the longer you have
your smartphone, the more SSIDs it has connected to around the world and the more it “knows” about where it has been. This is the information I can tap into.

A specialised rogue wireless access point, like the HAK5 “PineApple”, can pretend to be any wireless network. It just sends out a wireless beacon that your smartphone picks up and answers. The rogue wireless access point then records any SSID request your phone tries out from its internal list: “CERN”, “StefanWLAN”, “GVAairport”, “Swisscom”, “SBB-FREE”, “HyattAtlantaGuest”, “AmsterdamRoaming”, “ITUwifi”… And, obviously, very often, the SSID name provides sufficient information about where you or I have been. Voilà.

So, how should you protect yourself? First, disable the option to join wireless networks automatically. If you do this, you will see the SSIDs you can connect to and confirm as required. Alternatively, you can disable your smartphone’s wireless capabilities completely and just enable them in places you know and trust. Resetting the network settings would be an even harsher step, but you would need to reconfigure those networks you regularly use… Finally, you could delete the SSID from your iCloud or Google account and reinstall the phone’s operating system to get rid of it once and for all. But you would have to be really paranoid to do that, don’t you think?

Android’s Armageddon… Reloaded (2016)

About 1 billion Android smartphones are facing their Armageddon. Again.

Android could be facing another Armageddon, just as we saw with the “Stagefright” vulnerability last summer (see “Android’s Armageddon”). But while that “Mother of all Android Vulnerabilities” targeted Android’s Multimedia Messaging Service, this time the driver for Qualcomm’s LTE chipset is in the firing line… And as before, while a fix for this vulnerability has been quickly made available, the big problem has been getting this fix to your Android device: mobile phone manufacturers and providers are incredibly slow at passing it along…

What can you do to get this fix? Basically, there’s nothing you can do but wait. For certain smartphone models (e.g. HTC One M9 and HTC 10; LG G4, G5, and V10; Samsung Galaxy S7 and S7 Edge; and others), you are completely exposed. This four-fold vulnerability, dubbed “QuadRooter”, in the driver for the LTE mobile communication chipset of Android smartphones can be exploited by just one malicious app… Once installed, it becomes “root”, the master and commander-in-chief of that smartphone. Luckily, so far, no public exploitation of that vulnerability has been reported! Potential defences? Usually we would recommend applying the corresponding fix made by Google. However, this requires your preferred smartphone

1 Of course, the deployment of such a rogue wireless access point at CERN would violate the CERN Computing Rules.
manufacturer to adapt that patch to your hardware. And, as experience has shown, this can take a while or might never happen. Alternatively, you can try to re-compile your Android device’s operating system yourself – but this is an approach recommended only for experts.

So, interesting times lie ahead. Not only for Androids but also for many other devices. Vulnerability disclosure cycles are getting faster and faster, and patching, i.e. fixing those vulnerabilities, must be done more promptly. With a world full of smartphones, the Internet-of-Things, inter-connected fridges and cars (see the article “Our life in symbiosis”), and SmartMeters, a new patching paradigm is needed... Today, our patching methods are too slow and inflexible (see the article “Agility for computers”). Android’s Armageddon is just another example.

P.S.: If you believe that Apple’s iOS is better... Er, no, as the recent “Pegasus” exploit showed. However, at least Apple controls the update chain, so security fixes are always rolled out quickly (for iOS versions 9 and above).

Update on your privacy – or lack of it (2015)
http://cds.cern.ch/journal/CERNBulletin/2015/10/News%20Articles/1994237?ln=en

While we have reported on our privacy concerns when using smartphones or cloud services in past issues of the Bulletin (e.g. “Enter the Cloud, pay with your password”, “... and thank you for your mobile data!”, and “Prison or ‘Prism’? Your data in custody”), recent news has once again given us a reason to rant: even after the Snowden revelations, things are not getting better!

Let me start with Microsoft and its initiative to bring the “Outlook” mail client onto Android and iOS smartphones. This app can act as an email inbox for Exchange, Outlook, iCloud, Google and Yahoo mail accounts, just like, for example, the iOS mail client. However, instead of aggregating and storing all emails locally on the smartphone, the user’s email and/or calendar data is aggregated on servers operated by Microsoft. For this, the credentials (i.e. passwords) for the corresponding Exchange/iCloud/Gmail/etc. accounts are uploaded to the same Microsoft servers that subsequently fetch all relevant data, emails and calendar entries. Thus, if you use this app to read your CERN emails, your CERN password will already have been transferred to Microsoft. The European Parliament considered this dangerous enough to warrant banning this app from all its devices and forced all its users at that time to change their passwords. Time for you to reconsider using that Outlook app and to change your CERN password...

In this respect, Microsoft is significantly different from Apple’s iCloud or Gmail if you synchronise your CERN mailbox with them. Apple iCloud holds an encrypted copy of your CERN password through your iOS back-up, but not a clear text one. Gmail doesn’t hold it at all if you just forward the emails sent to your CERN email address to it (but if you are CERN staff, please refrain from doing this as it has implications for CERN’s
privileges and immunities as an intergovernmental organisation; see “Don’t let your mail leak”).

From a different angle, however, Apple has also failed to provide proper privacy (if you believe that this even exists): the Apple mail client provides the capability to block the tracking of emails explicitly, i.e. prevent senders from learning when you’ve read or looked at their emails. Technically, such tracking is done via a unique token (e.g. an image embedded in your email) being downloaded from the sender’s side. Once you look at that email, this download is sufficient to indicate to the sender that you’ve seen it. But you’re not the only one who could be looking at it: the Apple Spotlight search indexes your emails, and, thus, needs to “look” at them, too. This is where Apple failed: Spotlight triggers the download even if it should be blocked, so the sender at least knows that you’ve properly received the email...

In short, watch out: protect your privacy and your CERN password. Some apps and programs might gather more information than you expect. Also, keep your emails with the CERN email service and do not forward them to a third-party email provider.

Android’s armageddon (2015)


“The mobile world’s equivalent to Heartbleed” and “Mother of all Android Vulnerabilities” - just two quotes from the media about the new vulnerability (see here) affecting all Android devices. While Google has been quick to fix this vulnerability, the big problem has been getting this fix to your Android devices: mobile phone manufacturers and providers are incredibly slow at passing it along…

What can you do to get this fix? Basically, there's nothing to do but wait. If you run a recent Android operating system (version 2.2 or newer), you are completely exposed. This vulnerability in Android’s “Stagefright” media playback engine can be exploited by just one MMS (Multimedia Messaging Service) message and you won’t even be able to tell: the exploitation of your Android phone happens during the pre-processing of that message, i.e. in the “door-knocking”-phase. No warning. Nada. Worse, the people who found this vulnerability plan to disclose all details in the upcoming BlackHat conference in August, so we can expect the attacker community to jump on the wagon and misuse the vulnerability for their deeds. All they need is your mobile phone number…

Potential defences? Usually we recommend applying the corresponding fix made by Google. However, this requires your preferred mobile phone provider to adapt that patch to your hardware. And this, as experience has shown, can take a while or might never happen. Alternatively, you can try to re-compile your Android’s operating system yourself - but this is a feat recommended only for experts. As a stop gap measure, however, you can disable the MMS service on your phone. Some recommendations along these lines are at the end of this article.
Thus, interesting times lie ahead. Not only for Androids but also for many other devices. Vulnerability disclosure cycles are getting faster and faster, and patching, i.e. fixing those vulnerabilities, must be done more promptly. With a world full of smartphones, the Internet-of-Things, inter-connected fridges and cars (see our Bulletin article on “Our life in symbiosis”), and SmartMeters, a new patching paradigm is needed… Today, our patching methods are too slow and inflexible (see our Bulletin article on “Agility for computers”). Android’s Armageddon is just another example.

IT or not IT, that is the question (2015)

Following on from our recent Bulletin article on “How to succeed in software deployment” (see here), we repeatedly face the problem that “standard” IT services are replicated within CERN or even outsourced to external companies.

Past experience has shown that such non-centrally managed systems are more prone to security risks and, in the long run, are less well managed – that is, if they’re not eventually orphaned completely. If hosted outside CERN, there is also the risk that sensitive data from the Organization could be leaked and that CERN would not be able to intervene in the event of a security problem.

Imagine, for example, a slide show created by an external consultant and hosted in the cloud… While this might have been convenient for the consultant, a regular user of that cloud service, the content was lost once the consultant’s job was done and nobody at CERN took responsibility for the slide show. Or imagine a web page developed by a summer student using an external web-hosting company. It turned out that the website was flawed and leaked data but neither the student nor the web host were able or motivated to get this fixed. Or a questionnaire sent to colleagues asking personal questions, only for their answers to be disclosed to the general public. Or the development of a web application by an ex-colleague, who was later reimbursed by CERN.

CERN is in the comfortable situation of having many different centres of expertise: the medical service for our health, the fire brigade for safety, the RP group for radiation issues, the FP department for contracts and purchasing, the cooling, ventilation and electricity groups, the metrology section for measurements, technical groups knowledgeable in PCB design, the legal service, the HR department for personnel matters, etc.

Luckily, the same applies to IT matters, and the IT department is there to support you in this. Of course, the commodities of modern life – Facebook, Twitter, smartphones and so on – have brought us closer to IT, but this doesn’t mean that we are all IT experts. While today it is easy enough to open another Dropbox folder, create a SurveyMonkey questionnaire or set up a Wordpress or Joomla webpage, this is not always to the overall benefit of CERN.
So, just as you would consult the FP or HR departments, the medical or legal services or the radiation protection group for their respective expertise, shouldn’t we draw on the expertise and knowledge of our colleagues in the IT department?

If you plan to start a project employing IT technologies (websites, standalone servers, disk storage, external cloud services, etc.) or are already in the development process, may we propose that you consult either us at Computer.Security@cern.ch or our colleagues in the IT department?

This would allow you to focus on the core of your project while we ensure that the IT technologies employed are fully supported and secured, kept up-to-date and fully backed up, and that the CERN Data Protection Policy is properly respected.

In the long run, you can (and should) benefit! Some examples can be found here.

Enter the cloud, pay with your password (2014)

Let me tell you a story that recently happened to a colleague of mine. She was looking for a nice e-mail client for her brand new Android smartphone. She found several apps suiting her needs, installed all of them on her phone, configured them with her CERN password so that they could access her CERN e-mails and tested them thoroughly. In the end, she was happy with one and deleted the other apps.

But she wasn’t happy for long: over the following days, she realized that many new e-mails in her CERN mailbox were mysteriously marked as “read” despite her never having accessed them. A dedicated analysis of the CERN e-mail logs showed that one of the e-mail app providers was still downloading her emails - even though she had uninstalled the corresponding app from her smartphone. In fact, her CERN password had ended up in the Cloud, continuing to allow access to her inbox (similar to what Google does when you let Gmail pull your e-mails from your CERN mailbox). Neither that mail provider’s Terms of Usage nor its Privacy Policy listed this feature, nor were her e-mails destroyed once she purged the app… In the end, she had to change her CERN password to block access.

So pay attention to where your CERN password ends up. Certain apps promise to “unite all your e-mails, contacts and calendars into one single application”. So long as your password remains on your smart-phone, you still retain a bit of control (unless it is stolen or compromised). iOS’ and Android’s native e-mail clients work like this. But once your password is configured with your preferred Cloud provider (e.g. Gmail) or transmitted to a Cloud provider (e.g. mail.ru), you have to trust them to keep that password protected, secret and not to misuse it… If you are dealing with sensitive issues at CERN, regularly share sensitive data (like our colleagues in the FP and HR departments or DG and HSE units), that might be a bit too much trust, don’t you think?
Think twice. CERN's sensitive documents should never be made accessible to third parties unless there is a professional need. Losing sensitive data - both intentionally and accidentally - to third parties is in violation of the CERN Data Protection Policy (draft) and is considered to be professional misconduct.

Please avoid forwarding your professional e-mails to external e-mail providers, as there are implications for CERN’s privileges and immunities as an intergovernmental organisation (see also our article on “Don’t let your mail leak”). The CERN e-mail system provides largely similar functionality. Also avoid sharing sensitive or restricted data on external storage systems like Pastebin, Dropbox or Google Drive. In most cases, CERN DFS web access (CERN Webday), CERNbox, CERN’s OneDrive (you need to be registered with http://social.cern.ch), or CERN’s “Paste” are perfectly acceptable alternatives!

Your iPhone as a key-logger (2014)

In the past, we have repeatedly elaborated on the computer security risk of using smartphones. Today, something new for the paranoid: did you know your smart phone can be used to spy on your PC’s keyboard?!

In fact, the tiny accelerometer, gyroscope and orientation sensors that your smartphone uses to determine its tilt and movements can also determine the letters you type on your computer. Thus, it acts as a hardware “key-logger”! It only requires your smartphone to be put close to your computer keyboard and to run a corresponding, malicious app. The rest is done by the highly precise sensors which can record keyboard vibrations and subsequently the letters you type. In a dedicated study, students of the Georgia Tech College of Computing were able to decipher complete sentences with up to 80 percent accuracy using an iPhone\(^1\). In a nice twist, the same feature can also be used to “infer the occurrence of tap events on the touchscreen as well as the tapped positions on the touchscreen”.

But don’t worry yet! So far these highly targeted attacks have never been used against CERN. However, this does not mean that your iPhone (or your Android phone) is an innocent little gadget. On the contrary: It is a full-blown pocket PC which needs to be taken care of properly. Update it regularly and be careful when installing additional apps, as some malicious apps are known to infect smart phones (see our articles “iPhones, Androids, and history repeating” and “Is your Android running a temperature?”). Other apps are quite greedy and forward much too much of your personal information stored on your phone - for example, your location, address book and local data - to their data centre for further aggregation, analysis and, presumably, future marketing (more in “Smartphone lost - Privacy gone”).

\(^1\) Alternatively, wireless keyboards emit sufficient information to reconstruct your key strokes...
Backed up and gone... (2013)


Remember how easy it is to lose your passwords for web applications ("Don’t let Chrome expose your passwords")? This time we go bigger and discuss how easy it is to lose the passwords for every wireless access point you’ve visited. You just need to be running Android on your smartphone...

Apparantly, Google was already capturing wireless access points during its Streetview campaign but was forced to stop this after complaints from data protection advocates. It was done “mistakenly”.

With Google’s Android now dominating the smartphone market, they’re back to their old tricks. As a useful feature, Android (version 2.2 and higher) stores the identifiers (“SSIDs”) of wireless access points and credentials by default, so that you do not have to reissue them on every connection. The interesting part happens when the smartphone is automatically backed up to Google’s data centres: the SSIDs and the associated passwords are not encrypted once they are there. Thus, Google has full access to them and could, potentially, produce a “free access map” to many wireless access points worldwide. Of course, this would help some anonymous government agencies. Along with Wi-Fi passwords, your keychain is also automatically synced; presumably this includes your CERN passwords as well as your private ones. Not to mention all your other data (photos, emails, videos, apps, etc.) that “vaporizes” once it is backed up in the Google cloud (see our Bulletin article on this subject: "Send your data into the cloud and make it… vaporize").

However, this does not make an Apple Mac or iPhone safer. Once iCloud has been enabled, your device is regularly mirroring all information to Apple’s computer centres: Apps, Music and Films might be fine as you most likely have bought them via the iTunes store. But what about your calendar entries, e-mails, photos and films? It is up to Apple’s discretion whether to analyse this data and use it for advertising purposes (or send it to the aforementioned agencies). Worse, while today you can still disable “iCloud” functionality (iOS -> Settings -> General -> Usage), in the future this might not be possible. Discussions have emerged about whether on “OS X Mavericks” there is no longer a way to sync any i-device except through the cloud”.

In more blunt terms, this would imply that iOS users are forced to provide all their data (or give up on iPhone). Furthermore, Apple is not the only one targeting your data. LinkedIn recently published an app that diverts all your emails through their central servers for data mining. With the NSA and GCHQ spying on us from one side, and big companies like Apple and Google doing the same from the other, what’s left but to sigh, give up and let it happen? Smash your phone and go back to the communication stone age? Rally and hope that politicians tackle the problem? Be less paranoid than the security guys at CERN? We are very curious about your opinion!
BYOD: Bring Your Own Disaster (2013)

Have you ever heard of “BYOD”? No, it is not a pop band. Try again. It is short for “Bring Your Own Device” (the French use “AVEC” - “Apporter Votre Equipement personnel de Communication”) and describes an option long since offered at CERN: the possibility to bring along your personal laptop, smartphone or PDA, use it on CERN premises and connect it to the CERN office network. But hold on. As practical as it is, there is also a dark side.

The primary advantage, of course, is having a digital work environment tuned to your needs and preferences. It allows you to continue working at home. Similarly, you always have your music, address books and bookmarks with you. However, as valuable as this is, it is also a responsibility. Laptop theft is happening - outside CERN but also on site. In France, 30% of stolen laptops were stolen out of cars or homes, and 10% during travel. At CERN, on average one laptop per month is reported stolen to the Computer Security Team. This can become a fully-fledged disaster: with the loss of your laptop, your music is gone, your photos, videos, doctoral thesis... but probably also your private documents, e-mails, bank statements (in your browser’s cache) and stored passwords (e.g. for your wireless access point at home). Worse still, depending on what your role at CERN is, sensitive Organization data might be lost too: contracts, preliminary physics results, MARS assessments, legal proceedings, medical files, job applications, etc.

Only 15% of the aforementioned stolen laptops were encrypted. What about yours? Protect your life and avoid thieves putting your photos onto the Internet! Also protect sensitive Organization data. Use the built-in “Bitlocker” and “FileVault” features on Windows PCs and Apple Macs respectively in order to encrypt your hard disk. For Linux, many software solutions like “Truecrypt” can provide the means to protect your local data. However, take care with the corresponding password: once lost your encrypted data is also lost. Also note that there is currently no centrally supported solution for CERN. In addition, regularly back-up so that you don’t lose your “life” if your laptop disappears. Synchronise your professional laptop with CERN DFS or AFS, back-up your private laptop or Android device to an external USB disk, and use Time Capsule for Macs or iTunes for iOS devices. Finally, if your CERN laptop is stolen, file a report with the CERN Fire Brigade.

As for smartphones... On average, one mobile phone is stolen every 30 seconds in France. You might be able to perform a remote wipe to remove the contents, but if the thief removes the SIM card quickly enough, you’re screwed. Standard 4-digit PIN numbers can be cracked within minutes - you had better choose more digits. And no,

---

1 This reminds me of a case of a young woman whose photos - taken by her boyfriend with her smartphone - were posted on a popular porn site by the thieves who stole her phone (recall our Bulletin article on Smartphone lost --- privacy gone).
there is no really good encryption software to protect your contents. In short, you had best keep both eyes on your smartphone all time.

Android is the new Windows (2013)

Do you recall the early virus attacks in the early 2000s? “Blaster”, “I love you” and “Slammer” were attacking the pretty much unprotected Microsoft Windows operating system.

While Microsoft has been hit hard in the past, they have tried to improve and are now on a par with other software vendors. Today, they can even be happy that Android is taking over the baton - at least on mobile platforms.

According to the Sophos 2013 Security Threat Report “Android [is] today’s the biggest target” and Android devices in Australia and the U.S. experienced even more malware attacks, whether successful or unsuccessful, than PCs during the past three months. The Kaspersky security company recently added that 99% of all mobile threats target Android. Lucky you if you use an iPhone, or a good old Nokia with no Internet connectivity at all.

But why is that? It is partly down to the same factor that affected Microsoft in the past: market share. More than 50% of all mobile devices run the Android operating system. In addition, the Android app market is heterogeneous and uncontrolled – the complete opposite of Apple's central iTunes app store. This heterogeneity makes it easy for attackers to publish and distribute their malicious apps. However, one of the main reasons, according to Katja Locker of SWITCHcert, is that only 10% of all devices are running the newest version of Android called “Jelly Bean”. “Gingerbread”, which is two years old, still powers over 47% of all devices. She quotes IT expert Michael Kroker saying that this isn’t the users’ fault though – over the past 24 months, Google has “failed to hold manufacturers and providers accountable and get them to convince their customers to update.” In comparison, Apple’s iOS6 had a 60% conversion rate just one month after release.

So how can you improve? Obviously, running or updating to the latest version of Android (“Jelly Bean”, version 4.2) helps. If you can’t do that, be careful when installing apps. Only download apps from a location or store that you trust. Beware of malicious URLs and QR codes (see our Bulletin article “One photo to rule you phone”) – STOP, THINK, CLICK can also help you here. Finally, you might want to consider installing dedicated anti-malware detection apps like those offered by Avast or ESET.
Prison or “Prism”? Your data in custody (2013)

http://cds.cern.ch/journal/CERNBulletin/2013/2/News%20Articles/?ln=en

"Send your data into the cloud and make it... vaporize" was the title of one of our Bulletin articles in 2011. We were not precise enough. We should have entitled it “Send your data into the cloud and make it... available to a national security agency”.

What has long been feared has just been confirmed by whistle blower Edward Snowden: with ties into Microsoft, Google, Facebook, Apple, Skype, AOL and Yahoo, the NSA (U.S. National Security Agency) “Prism” surveillance programme has been monitoring e-mails, chats, videos, photos, stored or transmitted data and video conferences primarily made by foreigners using those services. So our data is trapped there now... and analysed.

But it is not only trapped with the NSA. If you’ve synchronized your files, music and photos with Apple’s iCloud, Microsoft’s SkyDrive, or with Dropbox; received phone calls or messages via Skype¹; managed your e-mails with Gmail or Hotmail; or installed third-party apps on your smart phone; be assured that your data has already been analysed. This is the primary business model of Google, Facebook or Dropbox: they take apart your private data in order to profile you and your interests, identify your consumer preferences, and strip your digital being into a statistical pattern of zeros and ones. Scientia potentia est (“knowledge is power”) – but only for those companies.

So let us encourage you once more to review the implications of using cloud services for work purposes and in your private life. Data privacy is our own responsibility – particularly when dealing with data in the possession of the Organization. Make sure that you do not leak sensitive documents or personal files to those services. This includes data provided to convenience applications such as URL-shortening services (i.e. TinyURL.com) or online questionnaire tools (i.e. SurveyMonkey). Avoid installing programs on your PC that synchronize with cloud storage (like the “Dropbox” plugin), and do not use peer-to-peer applications that export the contents of certain local folders onto the Internet. “Don’t let your mail leak”, especially when automatically forwarding e-mails from your CERN address to an external mail provider like Hotmail or Gmail.

Instead, remember that CERN provides similar services too (admittedly, not always with the same level of convenience, but therefore much better controlled). Your CERN mailbox is also available from the Internet, as are your files stored on DFS or AFS. CERN GO and Sharepoint services provide URL-shortening tools and tools to create questionnaires, respectively. Remote log-in is possible through the LXPLUS cluster or the CERN Windows terminal service. So why not use a service you can trust and which complies with CERN’s rules (such as the CERN Security Baselines) and the

¹ Microsoft, the new owner of Skype, was recently caught when users “sending HTTPS URLs over the instant messaging service, those URLs receive an unannounced visit from Microsoft HQ in Redmond”. Microsoft claimed that this is to filter out spam and phishing websites, but this argument has not convinced security experts.
upcoming CERN Data Protection Policy)? Check the different ways of connecting to CERN from the Internet here.

Finally, be aware that browsing the Internet is not an anonymous activity. Depending on which browser you use, it already exposes lots of information: the local language, time zone, screen size, installed plugins, available system fonts, etc. As these settings can vary significantly, it means that the probability of you and I having exactly the same settings is very low. Ergo, this information can be used to pinpoint your browser and uniquely identify you when browsing the web… If you don’t believe it, check out Panopticlick and note that some browser plug-ins (i.e. “Stealthier”) or security settings (i.e. “In Private” browsing) might change the odds in your favour. Also note that, if you are logged in with your Google or Facebook account, they can profile your activity even outside their domains. This is mainly due to the wide use of Google Ads/Analytics and Facebook’s “Like”-button: the embedded code directly feeds back into your Google and Facebook profile… For a bit more privacy here, log out whenever you don’t need to be logged in and consider installing something like the “Ghostery” plug-in in your browser.

... And thank you for your mobile data! (2012)

Do you recall our Bulletin articles “Smartphone lost - Privacy gone” and “Your privacy is paramount”? In an interesting twist, we recently learned of a senior CERN staff member who returned his old smartphone to the CERN Telecom Service in exchange for a new phone. Guess what came with it? All his e-mails and plenty of personal data. Privacy, anyone?

Indeed, today’s smartphones clone your personality into the digital world. Like a personal digital butler, it stores all the e-mails and messages between you and your family, friends, peers and colleagues; it contains photos and videos of the top moments of your life; and it holds your favourite music, movies and zillions of other bits of personal information stored in the apps of your choice (like GPS information on your jogging routes, a vault of your passwords, access to your Facebook or Twitter profiles, bank access information, and flight and hotel bookings). Your phone might also be used for making payments in shops.

But what about when your phone becomes obsolete? Physical destruction is of course the most obvious choice (and we encourage you to have a look at the CERN Data Destruction Policy). But still, “obsolete” for you does not mean “worthless” for someone else. Thus, you might wish to pass it on to a colleague or to the CERN Telecom Service. If it is your personal smartphone, you might give it to your family or friends or sell it on eBay. But before you do, think twice!
Remember to wipe your phone beforehand! Reset it to the factory settings, and remove its SIM card. The CERN Telecom Service provides details on how to do this with all major CERN phone brands. Also note that there is a possibility to wipe your mobile phone remotely if it gets lost or stolen. It’s even better if you always protect your smartphone against unauthorised access by locking it with a PIN code or swiping pattern. And while you’re at it: what about your laptop(s)?

One photo to rule your phone (2012)

Have you ever seen those black-wide squares (picture below) called “Quick Response Codes”? Such QR tags are the two-dimensional forms of EAN codes (International Article Number, the black-white bars scanned at Migros’ check-outs) encoding a web address. Scanning those codes with your smart phone can lead you to a webpage, send an SMS or an e-mail depending on the contents of the tag. Beautiful, isn’t it? But wait. Can you trust that QR tag? What if the QR tag leads to something malicious? Just to add more fun, we have recently heard about a vulnerability for Android devices prior to version 4.1.1 on its so-called “USSD code handling”.

The USSD code allows a phone to be reset or a SIM card to be blocked. Combined with clicking on a malicious link or tagging a malicious QR tag, this is a lethal combination that can convert your phone into a useless brick.

In the past, we’ve suggested to “Stop - Think - Click!” before browsing webpages, clicking on strange links or opening email attachments. In this respect, QR tags are not very different from web-links provided by URL shortening services like “bit.ly” or “tinyurl.com”. You are blind to where those links lead you to. Thus, using a QR tag might compromise your mobile phone like a bad link might infect your PC. So beware! Just as you should take care what links you click, only tag QRs from sources you trust! Take advantage of your mobile’s preview feature to understand what the QR tag contains, and only continue when you are comfortable (click here to learn how to do this for URL shortening services). Many mobile phones provide you with a pop-up window with the QR tag’s content which you have to approve.

In fact, this is where the aforementioned Android vulnerability comes in… Please test whether you are affected at this site. A confirmation window should pop up if all is fine and you should just click on “Cancel”. Otherwise, your “IMEI” code will be displayed immediately: your Android phone is affected. We recommend you update to version 4.1.1, if possible, or STOP - THINK - CLICK.

1 If you would like to shorten a CERN URL, check out IT’s newest service. Take a look!
Smartphone lost — Privacy gone (2012)

Who doesn't own an iPhone, Android or Blackberry mobile phone today? Lucky you if you don't! In previous issues (Issue 06/07, 2012 and Issue 32/33/34, 2011) we have pointed out their lack of security. But what happens if you lose your smartphone or it gets stolen?

Today, a smartphone clones your personality into the digital world. Your phone archives all your emails and messaging communications with your family, friends, peers and colleagues; contains photos and videos of the top moments of your life; holds your favourite music and movies and zillions of other bits of personal information stored in the apps of your choice (like GPS information of your jogging paths, a vault of your passwords, access to your Facebook or Twitter profiles, bank access information, flight and hotel bookings). In the future, your phone might also be used for making payments in shops.

Have you ever thought of how you would feel if you lost your smartphone or it got stolen? Naked? As I now know everything about your friends and your secrets. Ashamed? When I make your private photos public. Embarrassed? As I scoff at your weird taste in music. Helpless? Once I use your SIM card to call my friends in Australia.

There is no silver bullet for mitigation. The most easy prevention is of course disabling unused features and refraining from storing too much information on your smartphone. Back up its contents regularly and purge unnecessary data and photos. Also reduce the retention depth of your local mail box so that older mails get purged automatically. Note that there is a possibility to wipe your mobile phone remotely if it gets lost or stolen\(^1\). Finally protect your mobile phone against unauthorised access by locking it with a PIN code or swiping pattern.

And while you are at it: What about your laptop(s)?

When the “Lion” eats your data (2012)

Welcome to “Mountain Lion” - Apple’s most recent operating system for Macs. More than 200 new and useful functions come with this version\(^2\). But hold on! New and

---

\(^1\) The CERN Mail Service provides a possibility to wipe your phone remotely. The option is available from the CERN webmail interface and you can get more information [here](http://cdsweb.cern.ch/journal/CERNBulletin/2012/26/News%20Articles/1456530?ln=en). Note that on recent smartphone devices (iPhone, Android, etc) the “wiping process” can remove all data (pictures, music, applications etc) and restore factory settings.

\(^2\) This new version is available on [CERN DFS](http://cdsweb.cern.ch/journal/CERNBulletin/2012/35/News%20Articles/1473672?ln=en).
useful? With this Lion comes the full integration into Apple’s “iCloud”, the same iCloud already used for iPhones and iPads.

While iCloud might be pretty smart if you want to synchronize or back up all your data, it is a black hole for privacy and confidential documents. iCloud not only synchronizes your photos, music and videos, but also your e-mails, calendar entries, passwords (in encrypted form) and fully backs up your device. With “Mountain Lion” even your Microsoft Word documents locally stored on your Mac might be pushed over to the Apple computer centres. It is still unclear what Apple intends to do with these masses of data. Of course they don’t just do it because they are kind people. They have a business to run and money to earn. So maybe they will follow the Google/Facebook route and profile you and analyse your activities…

And this is where the problem starts. If you enable iCloud on your Mac (or iPhone/iPad), sensitive CERN information might leak out of the Organization. This could have serious consequences as external providers do not necessarily guarantee the same level of data privacy as that provided by CERN, as they are subject to national legislations which are less protective. Furthermore, once CERN documents are transferred, there are implications for CERN’s privileges and immunities as an intergovernmental organisation. We have just lost control over our sensitive assets…

Of course, this is not a Mac-only issue. If you forward your CERN e-mails to any external mail provider like Gmail.com and, thus, “let your mail leak” or if you “send your data into the cloud and make it… vaporize” at Dropbox or Rapidshare, for example, proper protection of this data can no longer be guaranteed. Worse, this cannot be reversed: once the documents are out of CERN, they are totally beyond control. Just recently, Dropbox lost a list of e-mail addresses of some its customers to an attacker.

Therefore, think twice if you enable “iCloud” on your Mac, iPhone or iPad, or use Dropbox, Gmail & co. For professional data, remember that CERN is also a cloud service provider. Your CERN mailbox is available, too, over the Internet, along with your files stored on DFS or AFS. Remote log-in is possible through the LXPLUS cluster or the CERN Windows terminal service. So why not use a service which you can trust? Check the different means to connect to CERN over the Internet here.

If you have any questions, suggestions or comments, please contact the Computer Security Team or visit our website.

Is your Android running a temperature? (2012)
http://cdsweb.cern.ch/journal/CERNBulletin/2012/06/News%20Articles/1421243?ln=en

You might have heard about Botnets, i.e. networks of infected (Windows) computers which are unwittingly under control by a malicious party. Public examples of botnets-in-action are attacks against the FBI, the U.S. Department of Justice, or against
Universal and Warner Music as a retaliation for the shutdown of Megaupload.com. But have you ever heard of a Botnet made of Android phones?

Some apps available from your favorite app store are malicious and try to steal your private data once installed or auto-dial expensive premium phone numbers.

Unfortunately, the open model for Android apps employs neither quality control nor an approval process. Several Android apps, e.g. wallpaper apps and sound clips, have already been identified as being malicious. Symantec recently reported at least 13 different malicious apps which are suspected to span up a Botnet of thousands of mobile phone. If you run apps from “iApps7 Inc.” (e.g. “Counter Elite Force” or “Heart Live Wallpaper”), from “Ogre Games” (e.g. “Balloon Game”, “Deal & Be Millionaire”, or “Wild Man”), or from “redmicapps”, then beware as your phone might have been compromised.

For further details and mitigations, please check the corresponding advice from Symantec. iPhones, iPads etc. are less affected since Apple tightly controls their app store. But the risk remains high for those who have jail-broken their iOS devices. Generally, be aware that mobile phones must be protected like normal computers: keep your system up-to-date, enable the regular automatic installation of updates/patches, and do not install untrusted software from untrusted sources. Check out our guidelines for protecting you PC here. There is lots which can be directly applied to your mobile phone, too.

IPhones, Androids, and history repeating (2011)

Remember when everyone was bashing Bill Gates because his operating system was insecure and a primary target for malicious software? While Microsoft has (tried to) improved on this, the IT world keeps on turning and the new target is your mobile phone. The Android and iPhone market is still growing. Can you live without your mobile phone today? Probably not. Mobile phones have become part of our identity.

They are with us all the time and record every step we take (see the iPhoneTracker application). Do you worry that your iPhone sends a unique token to every app company who wants to pin-point you and your activity? 15 years ago there was a rebellion and legal measures against Intel’s Pentium II/III unique serial number intended to do the same (see this CNN article). Also, think about how much confidential or sensitive stuff you already store on your phone (e.g. your mail, music, photos, and credentials). In the future, you might even be able to pay with your phone - initial plans have already surfaced from all major Internet companies. This will make your mobile phone an even more valuable target for attackers - cyber attackers or just old-fashioned thieves!
We don’t want to “cry wolf” here, but you should be aware that the shiny world of iPhones and Androids has a dark side, too. Thus, beware! Some apps available from your favourite app store are malicious and try to steal your private data once installed or auto-dial expensive phone numbers. Unfortunately, the open model for Android apps employs neither quality control nor an approval process. Several Android apps, e.g. wallpaper apps or sound clips, have already been identified as being malicious. For the iPhone, things look a bit better since Apple tightly controls their app store. But the risk remains high for those who have “unlocked” their iPhone.

Finally, if you want to roam around incognito, switch off the geo-localization services on your mobile phone, and recall that a unique token might still identify you to your app company. Use common sense before installing a new app or sound clip. Check what permissions the application asks for. If you just want, for example, a compass and it asks for your address book and Internet connection, don't install the app. If in doubt, don’t install. In order to protect your mobile phone against theft, lock it with a PIN code, back it up regularly, and familiarize yourself with ways to wipe your mobile phone remotely if it gets lost or stolen¹.

Send your data into the cloud and make it... vaporize (2011)

“Cloud computing” --- the term is as nebulous as real clouds.

Basically, it means storing data somewhere on the Internet. This certainly has advantages, since this data will be available anytime from anywhere. For example, the Google mailbox is available from everywhere; “Dropbox” provides a central storage for any type of files; “ZAPR” and “TeamViewer”, once installed, allow you to share your local files by just sending around links, or give third parties full remote access to your PC, respectively. In addition, there is a growing number of cloud synchronisation services (e.g. “iCloud”/“MobileMe”, “Firefox Sync”, “Dropbox”) which provide (semi-)automatic back-ups of all local files of a laptop, PC or mobile phone.

But hold on. What actually is transferred into the cloud? Personal files like bank statements? Passwords, especially CERN passwords, too? “Back up” usually encompasses everything, including those passwords and bank statements. Furthermore, is this data properly protected? The actual degree of security provided by a cloud services is often extremely difficult for random users to find. Just recently, “Dropbox” confirmed that “a programmer’s error caused a temporary security breach

¹ The CERN Mail Service provides a possibility to remotely wipe your phone's Inbox: Log into CERN webmail (http://cern.ch/owa), select “Options” and “See All Options” and click then on “phone”. The “Wipe Device” option can then be used to clear all Exchange information.
that allowed any password to be used to access any user account” and, thus, any user’s data. There the passwords and the bank statements vaporize…

Thus, be careful when using cloud services. Make sure that you do not leak sensitive or personal files to those services. In particular, avoid installing programs on your PC which synchronize with cloud storages (like the “Dropbox” plugin), or, worse, open up your computer for remote access from anywhere (like “TeamViewer”). Do not use peer-to-peer applications that export the contents of certain local folders onto the Internet. Finally, do not register your CERN account and password with external cloud services (e.g. Google mail). You have committed to protect your CERN password against disclosure…

Also recall that CERN is a cloud service provider, too. Your CERN mailbox is available, too, from the Internet as well as your files stored on DFS or on AFS. Remote log-in is possible through the LXPLUS cluster or the CERN Windows terminal service. So why not use a service which you can trust? Check the different means to connect to CERN from the Internet here.
CERN’s new first line of defence (2020)

Christmas has come early this year for the Computer Security team and the Communication and Network group (IT-CS) in the form of hardware for a new outer perimeter firewall. This next-generation firewall is intended to boost performance and bandwidth as well as being a sophisticated means to better identify and protect against cyberattacks.

CERN’s new outer perimeter firewall. (Image: CERN)

CERN’s outer perimeter firewall is the first line of defence protecting the Organization from any malicious or otherwise unwanted network traffic entering its general-purpose network. The firewall exposes to the internet selected computing services that need to be accessible from outside CERN, controls internet traffic from and to all user devices,
and blocks malicious traffic. Due to an increasingly aggressive global cyberthreat landscape, it is imperative to strengthen our firewall’s cybersecurity protection and detection capabilities using modern and sophisticated prevention tools. Unfortunately, the firewall currently installed at CERN, with its protective features and its limited throughput, has become insufficient to support the Organization’s networking and protection needs.

Enter our Christmas present! CERN’s new outer perimeter firewall will correct these two drawbacks – limited bandwidth and limited protection capabilities – and provide a sustainable solution for the next seven plus years.

On the hardware side, it will be able to digest, filter and control up to 200 Gb per second in uplink (i.e. leaving CERN) and downlink (i.e. entering CERN) traffic without any performance penalty. Its set-up is flexible, meaning that this total bandwidth can be adapted to CERN’s current and future needs and ramped up whenever necessary. Of course, hardware redundancy will guarantee high availability and spare CERN from connection problems in the event of one of the hardware chassis or their network connections failing. And the whole functionality will be integrated into the network automation software developed and used by IT-CS, to ensure that configurations are properly managed and can be changed easily and consistently.

On the computer security side, this new firewall benefits from advanced threat intelligence, which offers enhanced capabilities compared to traditional threat prevention services. Such threat intelligence services rely on security researchers to track down specific threat groups, ranging from cybercriminals to nation-state attackers, in order to produce detailed, up-to-date, specific indicators for detecting malicious attacks. Combined with the threat intelligence already available to CERN’s Computer Security team, this means sophisticated potential attacks will be automatically identified and malicious content automatically filtered before it can cause harm.

These advanced services also make it possible to enforce certain CERN Computing Rules (OC5) by blocking internet content that is considered to be inappropriate (e.g. pornographic or sexually explicit material, or sites that promote the abuse of both legal and illegal drugs) or offensive (e.g. websites promoting terrorism, racism, fascism or other extremist views that discriminate against people or groups of different ethnic backgrounds, religions or other beliefs, but not websites discussing controversial political or religious views) or violates applicable laws (e.g. sites that infringe copyright by illegally offering music, movies or other media for download). We still need to determine the extent to which such content should be blocked without overly restricting our academic liberties and freedom of communication. We would like to hear your thoughts on this – write to us at Computer.Security@cern.ch.

In the next few months, the IT-CS experts and the Computer Security team will put this lovely Christmas gift of a new firewall into production – for a better first line of defence.
And we want to spread the Christmas spirit by wishing you all a happy and healthy holiday season. Enjoy your time off, take care of yourself and your family, and stay safe and secure!

Scanning for problems (2020)

At CERN, the responsibility for keeping your digital house in order lies in the first instance with you. Keeping your digital house in order is sometimes very difficult. And it's even more difficult when looking at it from the security perspective. There are just too many possibilities as to what might go wrong. Too many areas with potential weaknesses. And too many components with potential vulnerabilities.

Just think of a common webserver. The various web components and frameworks used (Apache, PHP, Drupal, Joomla!, WordPress, etc.) need to be kept secure and up-to-date to avoid them being directly compromised. Up-to-date versions. Up-to-date libraries. Up-to-date software packages. Ditto for the security of the underlying operating system, be it Linux or Windows. Up-to-date everything. With access control to the host on every layer. And individual passwords changed from their documented defaults. The same holds for the protection of hardware. BIOS. IPMI interfaces. Always kept updated – often a particularly difficult feat! With access control. And, of course, the securing of all hosted webpages. Access control for sensitive content. And if some webpages serve dynamic content, filtering and sanitisation of any input on the server side. To avoid cross-site scripting (XSS), SQL injection or similar (see the OWASP top 10 on that subject). It's a difficult endeavour. So many layers. So many components.

In a dynamic, agile and fast-changing environment.

At CERN, the responsibility for keeping your digital house in order – that aforementioned webserver, but also your computer, your Internet-of-Things gadgets, your control system, your computing services – lies in the first instance with you. It is your responsibility to ensure that your hardware and your software stack are kept up-to-date and as secure as possible. We try to help you wherever possible with security advisories in the event of critical vulnerabilities, detailed recommendations and guidelines, in-depth training or broader-view Bulletin articles. But we can do more.

The Computer Security Team has therefore recently revamped its vulnerability scanning infrastructure with a view to better and earlier detection of weaknesses, vulnerabilities and sub-optimal configurations of devices and services hosted on CERN’s office and data centre networks. The new infrastructure is supposed to scan every device on those networks about once a month and will be able to detect more than 1500 different types of problems: still existing and valid default passwords; the use of ancient SSL or SMB versions or of FTP or Telnet (R.I.P!); expired certificates; disclosed vulnerabilities; or simply outdated and supposed-to-be-dead operating systems. And more types will be added when they appear. When a problem is
discovered, the owner of the corresponding device or service is notified directly, with the hope that these problems are quickly resolved for the sake of improving the Organization’s protection and security stance. Remember, the primary responsibility for the computer security of your computing resources lies with you. The Computer Security Team is standing by to help you improve the security and protection of your assets. Just contact us at Computer.Security@cern.ch.

**Videoconferencing pitfalls (2020)**

After two months of teleworking, videoconferencing has become the ultimate tool for staying in touch with colleagues, friends and family. Skype. WhatsApp. WebEx. Teams. Hangouts. Vidyo. Zoom. There is a plethora of potential tools and a plethora of pitfalls to catch us out. Let’s review a few of them.

The privacy and security of your meeting are essential of course. Generally, the use of a web/browser-based client should be favoured over client installations, which can be more invasive of your privacy and can pose problems with the security of the device where they are installed. Admittedly, web clients usually come with less functionality and reduced quality of service, so if a client installation cannot be avoided, make sure that the software comes from a trusted source like [https://vidyoportal.cern.ch](https://vidyoportal.cern.ch), CMF (for Skype for Business) or [https://cern.zoom.us/](https://cern.zoom.us/), or directly from the Google or iTunes app stores. Avoid sources that look dubious or check with us at Computer.Security@cern.ch if in doubt. And, as for any other software, make sure that your client is kept up-to-date!

When on a call, stick to the appropriate netiquette. Remember that the meeting might be public or recorded. So do not say something you might regret later. Muting your microphone protects you against any blunder when you are not the focus (think of your kids hopping around, or offline discussions on, for example, what to eat for dinner). This is particularly valid if you use a built-in microphone rather than a headset, as it might pick up sounds from your surroundings, such as traffic or construction site noise. Also remember your web camera. It records more than just you. So ensure that your background is content free or, at least, does not show compromising or offending items. Consider switching off your webcam if it’s not really essential, in particular to reduce bandwidth consumption if the overall videoconference quality is mediocre.

If you are organising online/videoconferencing meetings, please make sure, whether you’re using Vidyo or Zoom, that you protect your meeting with an access code and ensure that this code is not publicly visible (e.g. posted on a public webpage, Twitter or a public INDICO event page)! In recent weeks, mischievous people have looked out for such unprotected meetings and spoiled the proceedings in multiple (funny and not so funny) ways: including at CERN. It also helps, if possible, to centrally disable microphones and webcams of participants by default and tightly control when screens
are shared. Furthermore, record sessions only when needed and make this explicit to everyone on the call prior to starting the recording!

Finally, what is CERN’s pick for videoconferencing tools? Skype for Business and Vidyo are already established tools, which were recently joined by a CERN pilot of the popular Zoom software. The Computer Security Team has performed an assessment of Zoom using public information on the software’s security and privacy posture as well as on CERN's Zoom configuration. Based on this assessment, the Zoom@CERN pilot instance has been configured in the most privacy-preserving and secure manner possible. The recommended video-conferencing tools for the CERN community are currently:

- Skype for Business for meetings of a confidential nature and up to 10 people;
- Vidyo for meetings of a confidential nature and up to 100 people; and
- the Zoom@CERN pilot (under evaluation) for any public or quasi-public meeting with up to 500 people and meeting organisers willing to participate in the pilot programme.

Tunnel Madness (2020)

A series of users of the CERN network recently received a warning about using a particular VPN tunneling plug-in (named here as "Allo VPN" for the sake of brevity) with their favourite browser. VPN tunneling is a perfectly legitimate way to preserve the anonymity of your communications, and to make your remoteness seem local. But using this particular plug-in comes with a risk. For CERN. And for you, when using it at home.

While the use of Virtual Private Networks (VPNs for short) out of CERN provides lots of advantages with regards to privacy and security, for example, and while this does not pose a problem to the overall cyber-protection of the Organization, the "Allo VPN" service is different. It is a peer-to-peer VPN service, allowing other people to access the Internet through your Internet connection. Its business model is based on the underlying VPN technology, "Luminati SDK", selling CERN’s or your home’s network bandwidth for re-use by other users.

This means that with any usage of "Allo VPN", any third party can have unfiltered direct access into CERN's internal office network (the so-called "General Purpose Network") as any PC or laptop running this particular VPN plug-in becomes part of their worldwide peer-to-peer overlay network. And, consequently, this increases our liability if illegal activities are tunnelled through this network… It’s the same if you use this plug-in at home on your home Wi-Fi: If someone commits crimes through your – now shared – connection, the police are likely to come knocking on YOUR door, take away your hardware for forensic examination, and you may be subject to investigations related to
whatever crime was committed (copyright violation, hacking, propaganda or sexual abuse material)...

Worse still, the "Allo Unblocker" Windows client, Firefox add-on, Chrome extension and Android application have been found to contain multiple vulnerabilities that allow a remote or local attacker to execute code and potentially take control of your computer. Additional design flaws allow any user to be tracked across the Internet via a persistent ID. And, as such users – wittingly or otherwise – act as exit nodes for the overlay network, each is capable of acting as a middleman for other users of the free or premium peer-to-peer network, or its commercial "bandwidth" service ("Luminati"), thereby compromising the privacy and anonymity of their browsing and exposing them to further attacks...

Consequently, the "Allo Unblocker", "Allo Better Internet" and "Allo VPN" plug-ins have been explicitly banned from being used at CERN. Violations are supposed to be detected and the owners of the corresponding devices are informed and asked to refrain from that activity. In parallel, we have blocked the associated commercial "bandwidth" service ("Luminati"). If you use these plug-ins at home, time to re-consider. Apologies for the inconvenience, but we hope we can count on your understanding.

Spectre and Meltdown, just the beginning? (2018)

The beginning of the year has been dominated by two security vulnerabilities, known as Meltdown and Spectre. Both, in their own way, allow any local user to access a system's memory and misuse the contents for malicious purposes. Let's see why this is bad and why it may become worse in the future...

In technical terms, Meltdown breaks down the boundary that prevents user applications from accessing privileged system memory space. This vulnerability has been confirmed to exist in all Intel processors produced since 1995, except for Intel Itanium and Intel Atom before 2013. This includes computers by popular vendors such as Apple, Microsoft, Dell, HP and Lenovo. Spectre is similar, but allows an attacker to use a CPU's cache channel to read arbitrary memory from a running process. Unlike Meltdown, Spectre is known to affect Intel, AMD and ARM processors. This includes computers, tablets and smartphones made by Apple, Microsoft, Dell, HP, Google and Lenovo, among others. Spectre is much more difficult to successfully exploit than Meltdown, as its attack surface is limited to user space processes, such as web browsers and desktop applications.

Technicalities apart, abusing Spectre or Meltdown allows an attacker to download the contents of the memory from your device and dissect it offline to extract your passwords, private SSH keys or certificates, or any other juicy information. Fortunately, the memory does not come with a big sign saying “Password here!” Therefore, any
extraction process would be slow, cumbersome and not straightforward. Hence, while proofs of concept do exist, no systematic exploitation of either Spectre or Meltdown has yet been reported.

So far, so good, no? Not quite. First of all, and most problematic so far, the fixes greatly depend on your computer’s hardware, i.e. the chip set. While the most recent and popular chip sets will receive fixes in a timely manner, other hardware might not: think of your computer’s BIOS, or your Internet-of-things device (see our Bulletin article “IoTs: The treasure trove of CERN”). So we may end up with many embedded devices that will never receive a fix for Spectre or Meltdown. Secondly, there are fears that applying the current fixes will naturally slow down any computer: depending on what your computer is used for, reported performance drops vary between a few per cent and up to 30%. But there is no need to panic (yet), as newer fixes might correct that, too. Thirdly, Intel and probably others have allegedly known about these vulnerabilities for a while. This may mean that people with malicious intent were already exploiting these vulnerabilities long before they became public knowledge. However, so far no reports have confirmed whether or not this has actually happened. And, as a result of all these things, this may be just the beginning. As with past scares of this nature, the focus of security research and the way in which the vulnerabilities are exploited will change! Think of the POODLE SSLv3 vulnerability found in the aftermath of the Heartbleed OpenSSL vulnerability: Spectre and Meltdown are probably just the first known vulnerabilities linked to exploiting hardware weaknesses. The next generations of Spectre and Meltdown may be more intrusive and easier to exploit, and may not quickly become public knowledge. A feast for security agencies and criminals, a pain for those of us responsible for defending our IT systems…

So, this is just the beginning. Be prepared for more to come. Raise the bar! Make sure that all your systems are automatically updated when your hardware or operating system provider issues new fixes. Use the standard (automatic) update mechanisms of Windows, Linux, Mac, Android or iOS devices. And keep an eye on your embedded devices. Try to keep them up-to-date, too. Or, if you can’t, don’t connect them to the Internet or allow just anyone to access them.

You can find more details on CERN’s strategy regarding Spectre and Meltdown here.

Scaling out intrusion detection (2018)


Automatically and autonomously monitoring digital activities on CERN’s network and its firewalls between CERN and the Internet, activities on CERN’s computing clusters and related with CERNs web services is an essential part for guaranteeing the protection of the operation and reputation of the Organization. It allows us to detect – attempted or successful – break-ins (“An attack for more security”) or preventive scans
for vulnerabilities of our computing infrastructure ("CERN under friendly poking"), and, of course, the abuse of our computing facilities for malicious deeds ("Virtual Misconduct – Real Consequences"). Therefore, the new CERN Security Operations Centre (SOC) was deployed recently to cope with CERN’s ever growing networking and computing resources. It shall automatically check for malicious activities, alert in such cases the Computer Security Team and end-users, and provide all necessary information to conduct and conclude incident forensics (of present or past incidents).

At the core of this new SOC lies threat intelligence data, i.e. structured information on various ongoing and past computer security events. This includes “Indicators of Compromise” (IoC), e.g. malicious IP addresses or domains as well as signatures (“file hashes”) of various malware samples. IoC are constructed from the results of investigations of computer security incidents discovered at CERN, but also received from partner organisations. Through participation in vetted trust groups the CERN Computer Security Team is automatically exchanging threat intelligence information with peer organisations. This data exchange is managed by a dedicated open-source tool dubbed “MISP” ("Malware Information Sharing Platform") and covers not only IoC but also tactics, techniques and procedures used by the various threat actors or groups of threat actors. Seeing any CERN computing activity linked to such threat intelligence data indicates a problem: CERN computing resources might have been attacked, abused or compromised...

Hence, different Intrusion Detection Systems (IDS) have been deployed at CERN. On the network level, i.e. at CERN’s outer perimeter firewall but also at the boundaries between internal networks – so-called “gates” –, one network-based IDS ("Snort") is simply looking for different patterns of malicious activity in the flow of data. The second, more sophisticated one ("BroIDS") extracts source and destination IP addresses and port numbers, transferred data volumes as well as some high level application metadata. Similarly, host-based IDSees gather information from CERN’s computing clusters in the data centre (e.g. “LXPLUS”, “LXBATCH”), from CERN’s Single Sign On portal, from the LDAP and Active Directory services, from the centrally managed web servers, from the Domain Name Server, and from several other sources (see our Privacy Statement for the full list). All this security data is being processed in real time and enriched with missing information such as the hostname linked to an IP address (in those cases where the source of data only contains IP addresses) or adding geographic ("GeoIP") information. All data gets stored in two different systems (“Elastic Search" and “HDFS"), one allowing the data to be easily queried and visualised via web dashboards, the other one for longer term storage where we keep data for one year maximum.

The SOC automatically compares any security data against known IoC and raises an alert every time such an IoC is being seen. Advanced intrusion detection methods employ complex rules and correlation among multiple sources of data. Subsequently, raised alerts undergo a further step of aggregation by correlating similar alerts (for
example multiple CERN devices being targeted by the same malware) in order to identify common root causes. Incorporating additional context around the detected activity also allows us to easily reject false alerts. Once a security incident is detected and confirmed, incident response kicks in. At CERN, due to its unique academic environment and the associated academic freedom, computer security is highly democratic and all computing users are responsible for it. As such, for most security incidents affected end users will receive an automatic notification informing them of the problem. The CERN Computer Security portal provides additional guidance on how to resolve the different classes of security incidents (with or without the help of the Computer Security Team). When the situation asks for it, the CERN Computer Security Team has dedicated tools for the handling of large scale security incidents (i.e. “FIR” and “the Hive”). But, hopefully, thanks to this new SOC, that should be rare: We should be able to follow the upscaling of CERN’s data centre and the ever increasing traffic towards and from the Internet: Monitoring and intrusion detection for the protection of the operation and reputation of CERN.

Hardball for attackers (2017)

Successful cyberattacks always start with the compromise of a PC. Once the attacker “owns” that PC, he or she can install additional software to spy on the user, extract data and passwords, enable the microphone and webcam, and manipulate any software, application or transaction by the user. Hence it is reasonable to try to prevent this initial compromise as thoroughly as possible. And while Windows PCs remain the most susceptible, here is what CERN is doing to “harden” the Windows PCs and laptops managed by CERN’s IT department.

Of course, not only Windows PCs are under attack. Linux, MacBook, Android and iOS devices are also vulnerable. But Windows still has a big market share and many attack vectors are aimed at it. In addition, Windows is used widely in CERN’s administrative sector, which manages lots of sensitive data. And, finally, a large fraction of Windows systems are still centrally managed by CERN’s IT department. They can easily help to protect end users from cyber threats but, due to CERN’s academic environment, for most other platforms the paradigm is “bring your own device” (BYOD) – and with your freedom to do so, you also inherit the responsibility to deploy adequate protection measures. At CERN, in the first instance you are responsible for the security of your own devices...

But if you run a centrally managed Windows PC or laptop, the IT department is ready to help you with that responsibility – in particular if you are working in an environment dealing with lots of sensitive data or are often required to access “random” webpages or open unsolicited e-mails and attachments (like our colleagues in the administrative sector, in procurement, in senior management, or in the secretariats). Our “hardened
Windows PC" configuration provides you with a more secure and protected Windows PC.

The first rule for a hardened PC is the use of Windows 10 instead of Windows 7. Windows 10 comes with enhanced and state-of-the-art security (and, admittedly, a few privacy concerns still to be resolved), as well as additional protective measures. Full hard disk encryption is enabled by default (but don’t worry, at no performance cost!). Dedicated anti-exploit tools protect against malicious links and the (hidden) download of malware from infected websites. The local firewall is configured so that some malicious payloads using Windows Powershell are inhibited, and we have enabled additional logging and traceability options just in case an attacker makes it through.

Furthermore, we are locking down program execution rights to prevent the execution of malicious macros so that, for example, malicious Word or Excel files cannot create havoc. Using an alternative PDF reader and limiting (or even disabling!) Adobe Flash will remove two often used attack vectors, as vulnerabilities in Adobe Reader and Adobe Flash are often used by adversaries to gain unauthorised access to Windows systems (as well as to MacOS devices). We are even considering introducing some “fake” processes to make malware think the PC is a security researcher’s “honeypot”: a lot of malware avoids such honeypots in order not to reveal its internal workings...

On the user side, administrator rights for regular users will be removed and execution of software from the user profile will be restricted (no software usually needs to run from this location and it is often abused by malware). For browsing the Internet, reading unsolicited e-mails and opening unknown attachments, it is also possible to use a hardened PC configuration in an additional – virtual – environment so that neither browsing nor opening e-mails can be a vector for infecting the primary PC.

Of course, we are trying to make these PCs as convenient and transparent as possible for you and your everyday work. The more “standard” your usage is, the easier it will be for you to have a “hardened PC”. Some of these measures will certainly also make it into the configuration of normal Windows PCs managed by the IT department. Some other measures might also be deployed, to our Mac community for example. So, please stay tuned. If you want to participate in our pilot programme, please contact us at Computer.Security@cern.ch.

CERN under friendly poking (2017)

At the beginning of September, CERN’s computing systems came under attack. Adversaries tried to find their way into CERN’s Windows infrastructure with the aim of taking over the essential central Domain Controllers. And the experts from the University of Toronto did a great job!
Reviewing CERN’s computer security defences is part of our catalogue of best practices, as it is naturally better to identify suboptimal configurations under friendly fire than to succumb to evil BlackHats exploiting them for their malicious deeds. Therefore, CERN’s Computer Security Team repeatedly reviews and audits the various computing services, control systems, web applications, and software implemented and deployed at CERN.

But having an independent review can shed light from a different angle and highlight weaknesses and vulnerabilities missed by our audits. Enter the University of Toronto, where Allan Stojanovic and his team of professional hackers took up the challenge of trying to break into CERN, namely its Windows computing infrastructure.

During the first weekend of September 2017, Allan and his colleagues scanned CERN’s computing infrastructure as it is visible from the Internet – the “reconnaissance” phase. Having identified potential areas of interest, they then tried to take over servers and websites belonging to the Windows computing infrastructure – i.e. they tried to penetrate computing facilities that are usually protected behind CERN’s outer perimeter firewall.

Once inside, their mandate would have allowed them to continue as far as they could to show that they could have taken over administrator rights on the so-called central Domain Controllers, the core systems of the Windows infrastructure. Becoming administrators of those servers would have provided them with full access to any other centrally managed Windows system at CERN. In order to avoid any accidental damage, every step taken by them was coordinated and authorised by CERN’s Computing Security Officer. After three days of heavy poking, some frustration, and lots of pizza and coffee, the exercise ended and Allan provided CERN with a detailed report of significant, less significant and collateral areas for improvement. Thank you very much, Allan and colleagues!!! All of those weaknesses have now been addressed.

And we have not finished yet. The IT department and the Computer Security team are considering teaming up with other professional companies and teams to further poke around for areas for improvement under the umbrella of CERN’s WhiteHat Challenge. Given the complexity and vastness of CERN’s computing facilities, there must be more weaknesses!

And you can join in: if you also want to become a penetration tester and learn how to detect vulnerabilities, poke for weaknesses and identify potential areas for improving CERN’s computer security in general – or the security of your computing service, control system, web application or software in particular – sign up to the WhiteHat Challenge. Roughly 140 people plus six universities have done so far, constantly improving CERN’s computer security defences!
An attack for more security (2017)

CERN found itself under heavy attack in summer 2015 with cybercriminals trying to take over PCs and computing accounts and aiming to extract some of our public documents. While the attack only lasted a few days and was visibly not successful in the end, it laid the foundation for an initiative to strengthen CERN's protective measures further.

CERN, with its open, academic culture, has always been susceptible to cyberattacks of many different kinds, as are all companies and institutes worldwide. Thanks to you being vigilant, attacks are usually fought off. Training sessions and awareness-raising campaigns have shown to be fruitful on many occasions. Still, there is room for improvement (see our Bulletin article on “One click and BOOM... (Reloaded)”). Computer security is a moving target and defensive measures need continual adaptations and adjustments. The aforementioned attack in summer 2015 and the 2016 Crisis Management Exercise by CERN’s senior management triggered increased efforts to raise our defences. Thanks to the support of the CERN Management, four important security initiatives were launched:

The mail service, in collaboration with the Computer Security team, has deployed a dedicated appliance that automatically analyses all our e-mails for malicious content (see also “Protect your click”). Our FireEye EX device even simulates user activity trying to trigger any malicious activity in the e-mails sent to us. It is now in full operation and many waves of malware such as the Dridex banking malware have been prevented from arriving in your inbox.

- For those mails that still make it through, the IT department’s Windows team has started deploying specially hardened Windows PCs for those colleagues who have to open unsolicited attachments regularly, in particular PDF files. If infected, those PDFs will certainly compromise the PC and the local computing accounts. Hardened Windows PCs are less susceptible to infection thanks to a suite of additional protective measures (e.g. administrator rights removed, an alternative PDF reader installed, phasing-out of Flash, execution restrictions for macros and local commands). A pilot is already running with our colleagues in the Finance and Human Resources sector. A big thank you to all participants!

- Thanks to a collaboration between the Accelerator and Technology sector and the IT department, additional access protections are on the horizon: multi-factor authentication (the use of a hardware token in addition to your password) is currently being investigated so that it can be deployed on dedicated Windows and Linux Bastion hosts (see also our article “Pimp up your password”). Those Bastion hosts (bastions indeed!) will become gateways for any interactive remote access into CERN’s accelerator network (i.e. the “Technical Network”) as well as for administrator access to CERN’s Data Centre.
Finally, in line with a new strategy defined by the Beams department and the CNIC (Computing and Networking Infrastructure for Controls) working group, our colleagues from the OpenStack virtualisation service have started looking into ways to provide dedicated virtual machines for the control system development on the accelerator network. While those virtual machines are currently located on CERN’s office network, they should virtually move closer to the control system devices to ease development and testing.

Of course, we are trying to make all these extra measures as convenient and transparent as possible for you and your daily work. Still, we are counting on your support to ensure that CERN’s operations proceed in the most secure fashion.

**Transparent monitoring for your protection (2016)**


Computer security can be handled in one of two ways: in secrecy, behind a black curtain; or out in the open, subject to scrutiny and with full transparency. We believe that the latter is the only right way for CERN, and have always put that belief into practice. In keeping with this spirit, here is a reminder of how we monitor (your) CERN activities in order to guarantee timely responses to computer security incidents.

We monitor all network traffic coming into and going out of CERN. Automatic tools look for suspicious patterns like connections to known malicious IP addresses, web pages or domains. They check for malicious files being downloaded and make statistical analyses of connections in order to identify unusual behaviour. The automatic analysis of the logs from the CERN Domain Name Servers complements this and provides a redundant means of detection.

We also constantly scan the CERN office network and keep an inventory of the individual network services running on each device: web servers, SSH clients, etc. The antivirus software installed on centrally-managed Windows computers provides our virus experts with alerts in the event of malicious or suspicious activity being discovered. For similar purposes, all e-mails into or out of CERN are automatically scanned by the Microsoft spam filters. Statistical tools identify mail accounts that send spam – it is only in very rare cases that people manage to send more than 3000 legitimate e-mails a day…

We monitor your logins, whether they are using SSH or the CERN Single Sign-On portal ([login.cern.ch](http://login.cern.ch)). If the origin of the login is unusual in our eyes (and bear with us if it is not unusual for you!), we automatically notify you and ask you to check. We also automatically inspect all activities on our central computing clusters, including commands and parameters typed, network traffic and connections, manipulations to the kernel or installed software, etc. Finally, we monitor external feeds which, depending on their nature, report on compromised or vulnerable webpages, publish stolen password files, etc. Google Alerts helps us with that, too.
Most of these data sources are fed into a single analysis framework. Our new analysis infrastructure will be able to cope with the automatic live analysis of about one terabyte of data every day. If your account/webpage/device appears to be compromised or negatively affected, you will get an automatic notification. Let’s hope that you never do! For later use (e.g. for forensics purposes), all this data is stored for one year and then purged. Access is restricted to the CERN Computer Security Team only.

However, rest assured that the Computer Security Team has no right to “just” look at your activities for fun. Our accesses are governed by the CERN Computing Rules (OC5). Direct access to your mailbox or to your private files stored on CERN’s file systems is strongly regulated by the CERN Data Protection Policy (in draft) and its subsidiary policy and requires official authorisation by the Director-General. Any violation is considered to be professional misconduct and will result in dismissal.

DirtyCow BBQ — Well done, CERN! (2016)

I had a big smile on my face on the evening of Friday, 21 October 2016, when I saw how quickly the CERN IT department, the LHC experiments, teams in the accelerator sector and many more individuals were rushing to secure their Linux systems against a new and highly critical vulnerability dubbed “DirtyCow” (i.e. CVE-2016-5195). ArsTechnica labelled this bug the "most serious Linux privilege-escalation bug ever", which stresses its severity nicely, and it was too risky to go into the weekend unprotected!

It seems that computer security problems tend to occur at weekends. “DirtyCow” was a particularly nasty one that, when exploited, allows any local user to inherit administrator privileges and, subsequently, become master of the corresponding Linux system. Although CERN’s SLC5 and 6 were said to be unaffected, a few brave members of the IT department spent the Thursday evening analysing the exploitation vector in depth and finally disproved this initial statement: it turned out that SLC5 and 6, as well as CentOS7, were very much affected… Unfortunately, a prompt patch was not immediately available, so the security risk was uncomfortably high for the CERN Data Centre, its interactive computing clusters – namely LXPLUS and LXBATCH – and many other interactive Linux services in the experiments and the accelerator sector. The risk was especially high as the weekend lay ahead.

Fortunately, however, the IT department was able to propose a mitigating workaround as a temporary protective measure. Intense hours were spent on Friday preparing new Linux “system-tap kernel modules” and proving that the impact on Linux systems was minimal (in fact, only debugging functions would be affected). Finally, at around 3 p.m., the green light was given for the massive roll-out to thousands of Linux LXBATCH servers and hundreds of LXPLUS servers in the CERN Data Centre. An official warning
was sent out to all relevant stakeholders at CERN, including SWAN, ATLAS, CMS and others, who promptly applied the workaround to their systems. By late night, all critical services had been secured and were ready to run through the weekend. Great job, CERN! Congratulations to you all!

Addendum: The workaround is no longer needed. CVE-2016-5195 can be fixed by deploying the most recent kernel version available from CERN Puppet or the YUM repositories. Time to bring your system up to date!

**Hacking CERN — A win-win for all (2015)**


The first round of the CERN WhiteHat Challenge has finished (see here). At the end of March, CERN was "attacked" by a dozen students from the St. Pölten University of Applied Sciences, Austria.

These attacks were part of their Master's degree in computer science and computer security, where they study penetration testing and vulnerability scanning, i.e. finding weaknesses in computing systems: techniques, tools, approaches and ethics. Usually, such studies are done against mock-ups like "Google Gruyere", the "Damn Vulnerable Web Application" or OWASP’s “WebGoat” and “Hackademic”. However, while those mock-ups are in principle useful, they rarely resemble the operational reality of the Internet.

CERN has offered computer security professors an alternative: the opportunity to use CERN’s web-ecosystem and all other systems open to the Internet as their playground. Their students can learn how to perform penetration tests and vulnerability scans against real, operational targets.

This is a win-win-win situation for all. Students win as they learn to develop strategies in a real-life environment - this brings with it both advantages and disadvantages, as real-life is not as easy as mock-ups and there is a chance that students will find nothing. In such a case, they “just” learn that the security level of the system they’ve tested is higher than their skills and expertise. For professors, this is also a win, as they don’t need to set up mock-ups and can concentrate instead on educating their students.

And CERN wins, too. CERN is under permanent attack anyhow - but the "evil" side never tells us what they’ve found. The students will have to. Formally, there is a Memorandum of Understanding (MoU) signed between the participating university, the supervising professor and CERN. Part of this MoU is a “Code of Ethics” providing the ground rules for performing tests against CERN. “Ethics” are also part of the classes taught before the penetration tests are performed.

About ten students from the University of Rotterdam also carried out penetration testing exercises earlier this month. HEIG VD in Yverdon-les-Bains is also preparing its students, and four more universities worldwide are currently in the process of
signing the MoU. In parallel, 57 CERN staff and users have successfully passed the two half-day WhiteHat training courses, signed the same “Code of Ethics” and are now ready to poke around CERN’s computing services. In-depth training sessions have also started. For more information, visit the CERN WhiteHat Challenge website or sign up to the WhiteHat candidate e-group.

If your service or system fails to withstand such a hack, it may be time to understand why it was not robust and resilient enough to survive. Any malicious person may take advantage of the vulnerability, but either didn’t bother or just didn’t spot it. Take advantage of the situation and talk to us about how to better secure and protect your service: Computer.Security@cern.ch.

“Heartbleed” — A disaster for privacy (2014)

"On a scale of 1 to 10, this is an 11," claimed the famous security expert Bruce Schneier (see here). Indeed, the serious vulnerability dubbed “Heartbleed” affects everyone who relies on secure and private Internet communication. You cannot avoid it, so let’s see how it affects you.

“Heartbleed” is the name that’s been given to a vulnerability for OpenSSL (CVE-2014-0160). This software implements “the Secure Socket Layer (SSL v2/v3) and Transport Layer Security (TLS) protocols as well as a full-strength general purpose cryptography library”. SSL and TLS protocols are used to encrypt any communication between a client and a server, and to ensure that your communication is safe from eavesdropping or spying - that is, until 2012, when this bug was introduced. It allows the extraction of the first 64 kB from the memory of a server or client using OpenSSL (not necessarily web servers), and can potentially be used to reveal not only the content of a secured message, such as passwords over HTTPS, but the SSL keys themselves (see e.g. this for details).

This has become a catastrophe as OpenSSL is widely used in many different applications, including Linux distributions, Netapp storage systems, Cisco or Juniper VPN appliances, HP management software… It comes as no surprise that Facebook, Yahoo and even Google were concerned. CERN is no exception and, as CERN takes security very seriously, it is taking all the necessary measures to prevent potential exploitations of the “Heartbleed” vulnerability. Fortunately, LXPLUS, CERN Eduroam, the CERN mail service, the CERN Single Sign-On portal, most of the centrally managed web servers and all major CERN web applications (e.g. EDMS, EDH) were not affected. Similarly, EGI and OSG have launched their own emergency response procedures to ensure that the Grid infrastructure is kept safe.

So what can you do?
Thanks to many of our colleagues at CERN - in the IT Department, in technical departments and in the LHC experiments - our server infrastructure is fine;

As a preventive measure, you will have been asked to change the password of all your CERN accounts (you can do this at https://cern.ch/account);

If you run your own web/file/etc. server using a Linux operating system like CERN Scientific Linux 6, make sure you apply all pending patches as soon as possible (e.g. through “yum update”; SLC5 and Windows Server are OK);

If you run Microsoft Windows, Apple MacOS X/iOS or Linux on your office PC/laptop/tablet, and use a web browser like Chrome, Firefox or Internet Explorer, you should be fine on the client side. This also holds for your computers at home;

If you are customer of external web services like Facebook, Google, Yahoo or others, check for their messages and consider changing your password with them. They all should have fixed any potential vulnerability by now.

After Prism & Tempora: How much monitoring is OK for CERN? (2013)
http://cds.cern.ch/journal/CERNBulletin/2013/33/News%20Articles/1566881?ln=en

Edward Snowden’s revelations about the “Prism” and “Tempora” surveillance operations, run by the NSA in the US and GCHQ in the UK respectively, created quite a stir! Why has the witch hunt of a whistle-blower dominated newspaper headlines when there appears to have been no outcry over the fact that two countries have deeply penetrated our digital lives for so long?!

With echoes of George Orwell’s 1984, the two agencies collected a huge amount of Internet traffic, tapping into as much data per day as the LHC produces per year (see here). How much privacy are we willing to give up in order to protect ourselves against terrorist attacks? How much monitoring of our Internet activity is justified in order to feel safer? And how much monitoring is OK in the academic environment of CERN?

As the world’s largest high-energy physics research lab and the home of the LHC, CERN is a target for hacktivists and cyber-attackers. CERN must pro-actively protect its assets in order to safeguard its operations and its good reputation. While this protection (and incident prevention) is mainly in your hands, since at CERN you are responsible for securing your computers, networks, data, systems and services in the first instance, the Computer Security Team is ready to help you assume this responsibility (see our Bulletin articles on ““Security” is YOU!” and “Why “Security” is not ME…”).

And protection is just one important facet: detection of abuse, attacks and infiltration is another. Therefore, the Computer Security Team also uses a series of automatic intrusion detection tools. Network-based intrusion detection systems such as “Snort”
inspect all network traffic to and from the Internet in real time for malicious patterns. In particular, all web traffic is analysed live and logged for one year in order to facilitate retrospective incident forensics. Further real-time intrusion detection is based on statistical analysis of aggregated network traffic, so-called flows, which are also kept for one year. In parallel, DNS resolution calls, i.e. the process which converts domain names like “www.cern.ch” into machine-readable IP addresses, are compared to a list of malicious domains and, if they match, resolution is blocked automatically.

Aside from network monitoring, host-based intrusion detection tools run on all public Linux clusters, monitoring for suspicious activities like brute-force attempts, strange login patterns, or unusual or dangerous system calls and commands. Centrally provided anti-virus software is used to detect malicious files and programmes on centrally managed Windows PCs¹. Finally, we constantly scan web pages and web servers for basic vulnerabilities (e.g. those on the “OWASP” list of the ten most critical web application security risks), file systems for unprotected credentials like unprotected private SSH keys or passwords stored in publicly readable files, and all devices connected to our networks for an up-to-date inventory of running computing services.

Although this monitoring gives the Computer Security Team lots of sensitive data, it does not imply that we constantly spy on you and your activities. We never have and never will. First of all, we highly value CERN’s Digital Privacy Statement and CERN’s planned Data Protection Policy. In addition, the CERN Computing Rules (OC5) strictly define the scope of our work. The aforementioned monitoring tools run completely autonomously and automatically inform the parties concerned. Only upon an initial trigger – a suspicious activity reported to us – will the Computer Security Team take up the baton and try to understand the details of an incident, assess its impact and start incident response procedures. Similarly, we only get involved if there are legitimate requests for access to mailboxes and private files stored on AFS or DFS. The corresponding procedures for accessing such data are precisely defined in a subsidiary rule to OC5.

Thus, we believe we have a good balance between the academic freedom at CERN and our protective monitoring measures. Still, we are interested in your opinion: how much monitoring is OK for CERN? Please write to us at Computer.Security@cern.ch, and check our website for further information, answers to your questions or help. If you want to learn more about computer security incidents and issues at CERN, just follow our Monthly Report.

¹ You can get your personal copy for home use for Windows PCs here and for Macs here.
The lure of wireless encryption (2013)

Following our article entitled “Jekyll or Hyde? Better browse securely” in the last issue of the Bulletin, some people wondered why the CERN wireless network is not encrypted...

There are many arguments why it is not. The simplest is usability: the communication and management of the corresponding access keys would be challenging given the sheer number of wireless devices the CERN network hosts. Keys would quickly become public, e.g. at conferences, and might be shared, written on whiteboards, etc. Then there are all the devices which cannot be easily configured to use encryption protocols - a fact which would create plenty of calls to the CERN Service Desk… But our main argument is that wireless encryption is DECEPTIVE.

Wireless encryption is deceptive as it only protects the wireless network against unauthorised access (and the CERN network already has other means to protect against that). Wireless encryption however, does not really help you. You might get a false sense of security as your traffic is encrypted between your device and the wireless hub, but further down the wire it is not. In reality, your traffic transits the Internet in clear text apart from the first few wireless metres - unless you take additional protective measures.

Therefore, don’t let yourself be lured by wireless encryption! If you are serious about privacy and encryption, ensure that your traffic is encrypted on the whole path from your local application to the remote service you are using. Check for the “S” (“secure”) in your communication protocol:

- “HTTPS” for secure web browsing, as displayed in your browser’s address bar;
- “IMAPS”/“POPS” for secure e-mail transfer; the default for accessing your CERN mailbox;
- “SSH” and “SCP” for secure remote access and data transfer, mainly on Linux PCs. “SSH” can even be used to encrypt other protocols, a technique called “tunnelling”;
- On Windows PCs, there is also “RDP”, the Remote Desktop Protocol, which is encrypted too.

Of course, there is more to encryption than this. In order to protect your privacy and undermine surveillance, take advantage of so-called “Anonymize” services like http://www.anonymizer.com or the Tor network. These hide your IP address and channel your traffic through a proxy network, making the determination of traffic partners very difficult.

If you host sensitive or confidential data (see the new CERN Data Protection Policy), access protection and data encryption are a must! This is particularly true if you keep this kind of data on a USB stick or laptop, both of which can easily be lost or stolen.
while you're travelling... TrueCrypt is a good open-source on-the-fly encryption tool for data stored on Windows, Mac and Linux PCs.

**Why I like power cuts... (2012)**


Accidental power cuts - a permanent nuisance when running accelerators or computing services, since it takes a lot of time to recover from them. While I feel very sorry for those who are under pressure to get their service running again and deeply regret the loss of down-time and availability, I must admit that I like power cuts: power cuts make computers reboot! And rebooting computers at CERN means all the pending software patches are automatically applied.

But don't think I am egotistic enough to endorse power cuts. Not necessarily! I am already happy if you regularly patch your computer(s) yourself, where regularly means at least once a month:

- If you run a centrally or locally managed Windows computer, give that small orange blinking “CMF” icon in the taskbar a chance in the evening to apply all the pending patches. Also, let it initiate a reboot at the end!
- If you have a personal computer with your own Windows operating system, check for “Windows Update” in the program listing of the Start button. Switch to the recommended “automatic” updating method!
- On Linux distributions, make sure that you regularly run “yum update”. Or even better, enable automatic updates. Don’t forget to reboot your computer when a new kernel is installed, in order to properly apply kernel patches!
- For Apple Macs, use the software update mechanism accessible from the Apple menu.
- Finally, familiarize yourself on how to update your mobile devices, e.g. iPhones, iPads or Android phones.

Of course, there's more to patch than just the operating system. Pay attention to notification messages issued when running your favourite applications. If your application is supported centrally by CERN’s IT Department, it will make the necessary adjustments. However, if this is a program you have downloaded and installed from the Internet it is up to you to ensure it is up-to-date and patched... If you are in doubt (and use a Windows system), you can install and run this fine program from Secunia which checks your computer for outdated software.

Thus, help us eliminate the need for power cuts: patch your computer in a timely manner.
Account and Password Security

Password revolutions (2020)

With the new Single Sign-On portal (“New CERN Single Sign-On (SSO) Portal”) and the upcoming deployment of a multi-factor authentication solution for CERN (“A second factor to the rescue”), the Identity Management and Computer Security teams have also started reviewing the use of passwords at CERN. Expect some small revolutions ahead.

Your CERN account password is the primary token for accessing CERN computing resources: CERN e-mail, INDICO, EDH, EDMS, LXPLUS, etc. One password to rule them all. And one password, if you were to lose it, that would put your work, your data and CERN at serious risk (“Protect your family”). On the underground market, similar passwords are traded with a value of $50 each, as malicious actors can misuse a CERN account, e.g. for sending SPAM, running unauthorised computing tasks on our computing clusters (like crypto-currency mining; “Computing power for professionals… only!”), or downloading CERN-licensed software or publications from our digital libraries for “free”. Worse, a stolen password might allow a targeted attacker to take over computing services or even try to manipulate the operations of accelerators or experiments. Hence our push towards a central multi-factor authentication solution for critical services (“A second factor to the rescue”).

But how are passwords lost today? The main vector is lack of user diligence, where a user is convinced to send his or her password to an attacker (so-called “Phishing”) or where the user is lulled into clicking a link, leading to the full infection of his or her computer and thus allowing an attacker to extract passwords and do more harm (“Click me – NOT!”). Brute-forcing, i.e. trying to sign in with any kind of potential password and hoping for a successful match, is a second vector. And stealing CERN’s central database of hashed and salted passwords is a remote third possibility. The IT department is following standard IT practices to protect all secrets from unauthorised access, and to protect CERN users from falling victim to phishing or their computer being infected (“Protect your click”). Dedicated security campaigns (“I love you”) are supposed to train users to STOP – THINK – DON’T CLICK in order to protect their digital assets. But we can do better.

This is where the small revolution enters. With the new authentication and authorisation system, we will drop the requirement for annual password changes. Instead, you will select a strong and unique password once and for all. This better password can be either very complex, as today consisting of capital and small letters, symbols and numbers, or a very long passphrase (i.e. more than 24 characters) without such a sophisticated mixture of letters/numbers/symbols. It is your choice: compact &
complex or long & light. Of course, your password must not contain just words that can be found in dictionaries or variations of such words (like “C3RN”). In addition, it is important that you do not reuse your CERN password for computing services external to CERN. The Instagrams, Amazons and Facebooks of this world deserve their own, dedicated passwords. Automatic checks at CERN will regularly verify whether a password identical to your CERN one has been exposed and disclosed, using the “HaveIBeenPwned” database (“The easy way to lose passwords”) and similar databases of exposed passwords. If there’s a hit, you will be asked to change your password to something better. And finally, remember that your password is like a toothbrush: you don’t share it. Not with your colleagues. Not with your supervisor. Not with us or the Service Desk.

Last but not least, we will ramp up our brute-force protection: if logging into your account fails 30 times within a minute, your account will be blocked for another minute. And if the failed attempts continue we will add more minutes (up to blocking any login attempt for 15 minutes). More holistically, if a particular IP address is trying to sign into CERN on one or more accounts and fails 20 or more times within an hour, we will block that particular IP address from any further attempt for another hour (using open source software named “Fail2Ban”).

To recap: with the new authentication system, we will relieve you of the burden of inventing a new password every 12 months. However, in order to keep a high level of protection of your digital assets, we will review the quality of your current password on a regular basis and block your account when we see a risk to it (due to the fact that such a password has been publicly exposed or that someone has failed too many times to sign in to your account). Does this sound like an acceptable deal?

Protecting the accelerator from remote evil (2020)

A typical question when it comes to computer security is “What is your worst nightmare scenario?” Despite the fact that we usually sleep quite well, tranquilly and deeply, one answer would be CERN succumbing to a so-called “ransomware” attack. The second answer would definitely be the loss of the password of one of our data centre system administrators or of one of the engineers or experts running and managing our technical infrastructure and the accelerators. As we have covered ransomware attacks already in detail in past Bulletin issues (“Blackmailing Academia: Back to pen and paper(?)”, “Blackmailing Enterprises: You are Patient Zero”), let’s see why we worry so much about your expert password...

Actually, and more importantly than ever during these days of teleworking, your CERN password is the Holy Grail for access to all your digital possessions at CERN: your CERN mailbox, your CERN storage space, your CERN PC and laptop, your
documents and databases, any CERN websites you manage, the CERN computing services you run, or the accelerator or experiment control systems you operate or develop. One password and you’re in. For an adversary, this is an easy target. One successful discovery of a CERN password, and he or she is in… And depending on who owned that password, the adversary has all sorts of access at hand: access to your mailbox to spam the world, access to your storage space to expose your data publicly on the Internet, access to your PC or laptop to spy on you, access to your data to encrypt it and blackmail you, access to your websites ready to deface them, and access to the computing service you run or the accelerator or experiment control systems you operate or develop. In these last two cases, if the adversary has a targeted plan or is bold enough, he or she might just monitor your activities for a while: when you log in to your computing services, which settings you apply, how you manipulate the control system settings and how everything is interlinked. On day zero, the attacker will strike and abuse your expert power for his or her evil deeds. Kill computing services, delete databases, dump beams, and run control system parameters out of bounds. Nightmare fulfilled. Goodnight, CERN!

In order to protect CERN’s calm sleep, the IT department has started putting more and more privileged access routes to vital configuration services behind multi-factor authentication. You might be familiar with multi-factor authentication from your bank: the smartphone app, the SMS they send you, the pocket calculator device you have to use… The same goes for CERN IT: the use of Puppet, Foreman, Tellme/Pwn/Tbag has recently started to require system administrators to authenticate themselves in a two-pronged way: with their usual CERN password (“something they know”) plus, and this is new, a so-called second factor (“something they have”), e.g. a hardware token or a dedicated token-generating app running on their smartphone. In the next couple of months, more and more essential computing services will be put behind multi-factor authentication.

And we are not done yet, as the nightmare has a second prong: access to our accelerator control systems and technical infrastructure. Discussions have therefore begun with the Beams department on how remote access to that technical infrastructure, namely the so-called Technical Network (TN) that serves it, can be put behind multi-factor authentication, too. A first step has already been taken for IT managers who need to access services hosted on the TN. Next will be an analysis of how the remote development clusters can benefit from multi-factor authentication, and how remote expert access can be better protected… Stay tuned and follow our discussions at the CNIC meetings. And help us rid CERN of nightmare scenarios!
A second factor to the rescue (2020)

Working in the IT department is like working in heaven: many of our IT colleagues have professional god-like powers when managing their corresponding computing services. And nearly all centrally provided computing services are critical for CERN’s operations, for the operation of the accelerators, infrastructure and experiments, and for our local and worldwide user community. New security improvements will ensure this availability even if the gods lose their power.

The CERN IT department provides a plethora of different computing services to run the accelerators and experiments, store and analyse data, and make life easy for our user community. In some way, every activity within CERN relies on IT’s computing services – and in many cases this reliance is critical. Moreover, due to how the IT infrastructure and the CERN data centre are run, many services are inter-linked and depend on (or affect) each other, which increases the overall criticality. Through necessity, more or less every colleague in the IT department is managing and administering one or more computing services, and hence has full access and configuration power for those services. Therefore, due to the aforementioned criticality, it is of utmost importance that only IT professionals access their services and that any unauthorised third party – the evil attacker – is kept out. Otherwise the attacker will be able to wreak havoc: by taking over CERN’s computing services, bringing down or sabotaging operations, deleting or modifying data, stealing and exposing confidential documents, reading personal e-mails, etc. Until now, access protection has only been based on a single factor: “something you know” – also known as your password. Their CERN password, like yours, not only allows our IT colleagues to access their mailboxes and PCs, but is also the single token for managing their computing services. Once lost to an attacker, all their – all your! – digital life is exposed (see our Bulletin article “Protect your family”). And, maybe worse, CERN's operations are at risk.

But this is going to change. The IT department is deploying the use of so-called “two-factor authentication”. In parallel to the password, i.e. “something you know”, IT service managers and administrators now also need to present “something they have” in order to log into the computing services they manage. This “something you have” could be a mobile phone having the “Google Authenticator” app installed which produces one-time passwords (or any other smartphone application supporting that), or a USB-based hardware token from Yubico (known as “Yubikeys”). You might recall two-factor authentication from your bank. The Swiss bank UBS, for example, provides a small “pocket calculator” that acts in exactly the same way (check out Facebook, Instagram, Twitter, Google… for their second factors!). Any hardware token makes the malicious work of an attacker much more difficult: besides stealing the password of our IT colleagues, the attacker now also needs to get his or her hands on the token… And this would imply physical/local presence – which is unlikely. In addition, would you not
notice immediately if your smartphone was stolen? Hence, two-factor authentication is coming to the rescue to make CERN’s computing services more secure and CERN’s operations more robust. And eventually we will have similar protections for access to critical control systems.


One fundamental pillar of the security of CERN and its digital assets is their protection against any unauthorised access. For any web application, this protection has for a long time been centrally controlled by CERN’s Single Sign-On (SSO) webpage, which asks for your one and only CERN password. New Year 2020 brings a new look (and functionality) to the Single Sign-On page. So that you don’t mistake this new page for malicious phishing, please read on.

CERN has made a tremendous effort to centralise all CERN-hosted but also externally provided web applications (like ServiceNOW) to use this central Single Sign-On portal\(^1\): CERN SSO. This avoids you needing to recall any more than just one password for CERN (and we acknowledge that memorising passwords is not that easy, see our Bulletin article entitled “CERN Secure Password Competition”) and provides you with

\(^1\) IT is still trying to incorporate any remaining fringe applications. If your application is not using the central CERN SSO, time to reconsider now. Contact us on Computer.Security@cern.ch for information on how to set it up.
one central portal for all your authentication attempts into CERN. One portal to rule them all.

Unfortunately, there are also many copycat fake webpages circulating on the Internet resembling CERN’s SSO page that aim to steal your CERN password and gain unauthorised access to CERN using your own (stolen) credentials. So, if you are a security aware Internet user – and we bet you are – you might be cautious when you see the new SSO page. Remember: STOP – THINK – DON’T CLICK! In order to avoid confusing the new CERN SSO page with a fake phishing site, have a look, here it is:

The most important security feature, since the look and feel can easily be spoofed, is the URL, so check the bar at the top of your browser. As shown encircled in red in the screenshot, the URL should start with “auth.cern.ch” or, ideally, “https://auth.cern.ch”, and be accompanied by a small lock icon showing that your communication is encrypted and that the corresponding certificate is valid. Any other webpage asking for your CERN password, aside from this new one and the current “old” one, should be treated with caution and be reported to us at Computer.Security@cern.ch. Similarly, if you see any error message popping up before the SSO page displays, please let us know too.

The new SSO portal will also benefit from more login options: external researchers can use their Edugain or similar federated identity, social identities from Google, Facebook and others are recognised for certain CERN applications, and – most importantly for CERN computer security – we will soon start rolling out multi-factor authentication for some critical CERN applications, too. Stay tuned to the CERN Bulletin for more on this.

I love you (2019)

Actually, I don’t. And usually, wouldn’t only a few people address you like that? And what if this article had been an e-mail? With “I love you” as the subject line…? Sent by us, you would have simply ignored it, no? On the other hand, we got your attention – piqued your curiosity – and this is what malicious evil-doers are aiming to do too: get your attention via malicious e-mails. If you open up these e-mails, reply, click on links or open attachments – they have succeeded!

E-mails are one of the two primary vectors for screwing up your digital life (see our Bulletin article entitled “Protect your family”). Like browsing onto the wrong – malicious – webpage, one all-too-quick click on an embedded link, one attachment too many opened, one password sent in reply to an e-mail from a malicious attacker, and your digital life is in jeopardy. Your PC could be compromised; your data could be getting encrypted; your webcam could start to watch you; your microphone could start to spy on you. The attacker is recording every key you strike, every move you make, every word you speak; reading all the documents you host; and following all your posts on Facebook, Instagram, Twitter, etc. Privacy gone. Your digital life exposed. Game over.
Unfortunately, spotting malicious or fraudulent e-mails is getting more and more difficult. While CERN has deployed sophisticated measures in an effort to block malicious e-mails before they even arrive in your inbox, not all of them are filtered out: there might still be some that you can read. And worse, click on or reply to… So, beware: don’t let curiosity overwhelm you. Here are a few hints as to how you can easily spot malicious e-mails. Use common sense. Is this e-mail really addressed to you? Do the contents (or does the context) make sense? Does it relate to you, your life, your job, your interests? Is it in one of the languages in which you normally communicate? An e-mail stating “I love you” but not coming from your loved ones should be treated with care. Message texts written in German, if you don’t speak that language, should be ignored. An attachment from “Dänische Telekom” is almost certainly fraudulent if you do not have a subscription with them. And nude photos from your favourite rock star or actor just don’t exist — so no need to open them!

Similarly, e-mails that threaten or try to blackmail you should not be responded to. In the past, there were malicious e-mail campaigns that included passwords, maybe even a password you recognise, claiming that this is proof enough that the attackers have compromised your computer. But these are just scams. While it is true that your password may have been exposed somewhere (see our Bulletin article entitled “An old scam in a new disguise”), your computer has not been tampered with by those attackers. Even if those e-mails seem to be sent from your own e-mail address, they are still a scam. The e-mail protocol, unfortunately, has its weaknesses, and sender addresses can easily be spoofed. So please don’t think that a valid sender means it’s a valid e-mail! And check the fine print: when using small fonts, “cern.ch”, “cerm.ch”, “cem.ch” or “cen.ch” all look quite alike…

Finally, beware of embedded links. The magic of web links is that what is displayed and where it takes you might be different. Hover your mouse over the link before clicking. A small pop-up box should display and show you the link’s true destination. If this looks different to what is displayed, looks like gibberish, or just doesn’t make sense, don’t click! Better to hold on and let us help you! We can easily check whether this is a fraudulent or legitimate e-mail. If in doubt, send the e-mail to us at Computer.Security@cern.ch. Or check out our recommendations on how to identify malicious e-mails. Or test yourself with this excellent quiz made by Google.

**The easy way to lose passwords (2018)**

Following up on some questions we received concerning our last Bulletin article (“An old scam in a new disguise”), let us expand on the easiest way to lose your CERN password… just reuse it on insecure web services outside CERN!
Passwords are a necessary token for protecting your data in any web service: CERN INDICO, CERN EDH, Facebook, Twitter, Amazon, etc. During registration, passwords are usually stored in combination with an identifier (i.e. your e-mail address) for that web service, and later on requested during the login (“authentication”) process in order to verify your identity. At CERN, this is managed through the CERN identity management system and CERN Single Sign-On (“CERN SSO”). This provides a handy way to get you logged into any CERN web and computing services. And as all CERN computing services are required to use this central solution, all you need to remember is just one password and not a plethora of unique passwords. The CERN SSO portal then protects your password in accordance with best practice and converts it into a non-recoverable string (technically a “salted hash”). Of course, as the access possible with such a CERN password is wide-ranging, a number of due-diligence requirements are applied with respect to password length and complexity as well as expiry date (see our Bulletin article on “Brain Power vs. Password Managers”). In certain circumstances, e.g. when accessing critical services, the CERN SSO might even require you to provide a second authentication factor (besides the password you “know”, a token you “have” – like the “calculator” used for some Internet banking services).

But it is not always guaranteed that other web service providers will apply similar due diligence… “Security” might not be their core business. Passwords might not be given the necessary attention but just be stored weakly encrypted or even in plain text without any further protection. If those websites are infiltrated, all clear text passwords are exposed and the access protection to any other data is completely lost. From that moment, all data can be considered to be involuntarily public. This is happening more often than you might think. The reliable and trusty website provides a long list of compromised websites that have already lost their data. Feel free to enter your private or CERN e-mail address. You might be surprised.

But you shouldn’t be. The CERN Computer Security Team has subscribed to the “;--have i been pwned?” web service as well as to several others. Through them, and through our network of peers from other computer security teams, from academia, industry and security companies, as well as from national authorities and law enforcement agencies, we usually learn in advance of newly published “password dumps” (i.e. lists of e-mail addresses and clear-text passwords linked to a particular web service). Our automatic mechanisms analyse those dumps and identify entries linked to your CERN e-mail address or any e-mail address you have registered with CERN (e.g. with your lightweight account, or an e-mail address used to forward mails to). This allows us to inform you in a timely manner that your external password has been disclosed. Time for you to change that password or to consider terminating that account completely. Similarly, we process those password dumps in order to identify exposed passwords and e-mail addresses linked to sites of the Worldwide LHC Computing Grid (the WLCG), other affiliated universities and institutes, some of the
Geneva-based international organisations, and even some Swiss companies. The corresponding computer security teams are informed of all necessary details. A partnership at its best…

**CERN secure password competition (2018, 2015)**

It’s time for a spring clean at the CERN Single Sign-On portal. We will take this opportunity to review all 20,000+ passwords used with CERN primary, secondary and service accounts. This campaign has three purposes: to identify password duplicates, to extend the password history rule to all CERN accounts, and to reward the “best” passwords used at CERN.

The first aim, identifying password duplicates, involves finding different accounts using the same or similar passwords. As of 1 April, we will prevent the use of a password if it is already in use by someone else. We will notify the affected users well in advance and also provide them with the email addresses of peers using the same or similar passwords - this Facebook-like feature will allow users to form interest groups and share experiences of their password (usage).

In parallel, we will extend the password history rule to all CERN accounts. This history currently prevents you from reusing any passwords that you’ve used before. As of 1 April, this will be extended to include the previous passwords of all users: once a password has been used by one of the 20,000+ CERN accounts, it can never be used again…

Finally, we have formed a joint jury of colleagues from the HR and IT departments who will reward the best, most secure and most complex passwords used at CERN, the longest ones, the most creative or prosaic, the funniest and the most inspiring. The basis will be the CERN password database. The winning passwords and the names of their account owners will be published in the next issue of the CERN Bulletin. If you want to make sure that your password is among those, please point us to your account name (please do NOT send us your password as your password is yours and only yours).

Here are some hints to help you choose good, secure passwords:

- Choose a line or two from your favourite song or poem, and use the first letter of each word. For example, "In Xanadu did Kubla Kahn a stately pleasure dome decree!" becomes "IXdKKaspdd!" Mathematical formulas would also do: “a**2+sqr (b) ==c^2”.
- Use a long passphrase like the sentence "InXanaduDidKublaKahnAStatelyPleasureDomeDecree!" itself.
Account and Password Security

- Alternate between one consonant and one or two vowels with mixed upper/lower case. This provides nonsense words that are usually pronounceable, and thus easily remembered. For example: "Weze-Xupe" or "DediNida3".
- Choose two short words (or a big one that you split) and join them together with one or more punctuation marks. For example: "dogs+F18" or "comP!!UTer".

Remember that your password is like your toothbrush - you do not share it and you change it regularly. Neither your colleagues, your supervisor, the Service Desk nor the Computer Security team have any valid reason to ask for it. They should not and will never do so. The same is valid for any external company: UBS, PayPal, Amazon, Facebook or Google will never ask you for your password! Your password is yours and yours alone.

CERN secure password competition… NOT! (2018)

OK. Apparently, our “Secure Password Competition” announced in the last Bulletin was too easily spotted as an April Fools’ gag… Congratulations to those who didn’t fall for it. And a “keep smiling” message to those who did :) Apologies if you were hoping to meet peers using a similar password…

In fact, an important cornerstone for computer security at CERN (but also elsewhere) is the secrecy of your password. Remember that, as things stand, your password is in many cases your only key to and protection for a computing service (or, in the case of CERN, all computing services through CERN’s Single Sign-On portal). Losing that key means losing any protection for your documents and data. Losing your CERN password to a malicious attacker allows them to misuse CERN’s computing resources: spamming the world with your e-mail address, instantiating virtual machines in the computer centre to illegally generate crypto-coins, downloading digital journals from the CERN Library that are paid for by CERN, spying on your work in order to later attack the computing services or control systems you work on or manage, or misusing your computer to attack others at CERN or outside CERN. At home, losing your computer’s protection puts your personal life at risk: your Facebook profile, your Twitter feeds, your Instagram posts, your Internet banking, but also your photos and videos stored locally. And your privacy in general: with your computer’s password attackers can take it over completely and log every keyboard stroke you make, watch you on your webcam, or listen to you and your surroundings using the built-in microphone.

Hence, your password must be yours alone and must remain yours alone. CERN does not store your password but just a “hash” of it – a mathematical fingerprint properly protected by the CERN IT department’s identity management professionals. The Service Desk and the Computer Security Team do not know your password. And do
not want to know it. There is no need to tell them. If they need to access computing resources protected under your account, there are procedures for this that do not require your password (see the subsidiary rule to the CERN Computing Rules on “Third-party access to users’ accounts and data”). Also, there is no need to share your password with other third parties like your colleagues or supervisor. They should never ask for it. If they do, let us know the reason and we’ll find a solution to avoid it. Remember that your password is like your toothbrush: you don’t share it and you change it regularly.

Hence, too, your password must not be guessable. Make it sufficiently complex by using a mixture of letters, symbols and numbers. The longer, the better. Think of sentences: “In Xanadu did Kubla Khan a stately pleasure dome decree!”. Or, if you are of a mathematical mind-set, use formulas: “\(\Delta x \times \Delta p \geq \hbar/2\pi\)” (for physicists\(^1\)), “\(a^2 + b^2 = \sqrt{c}\)” (for engineers and technicians\(^2\)). In any case, do not reuse your passwords. Have different ones for different services. CERN deserves one; Facebook another. Your bank definitely a third. If you struggle to remember them all, use a password vault like “Keepsass”, Apple’s “Keychain” or even the built-in password managers within Internet Explorer/Edge, Firefox, Safari (i.e. Apple “Keychain”) and Chrome. But before you start using any of them, please consider whether you are fine with putting all your eggs in one basket. Or you could consider creating a few small baskets for different purposes.

Remember what is at stake: at home, nothing less than your private life. At CERN, the Organization’s operations and reputation. Both are worth protecting. Thanks for making the effort.

**Brain power vs. password managers (2017)**


The primary entry point to your digital life is your password. Your Facebook password to meet your friends, your Instagram password for sharing your photos, your Amazon and PayPal passwords for buying stuff, your iCloud password (or similar) for all your photos, music and videos, and your CERN “NICE” password for your professional activities for the Organization. A lost password means full exposure: with your password, an adversary can dig deep into your private (and professional!) life. Imagine someone who’s able to roam through your flat – but much more clandestine. It’s not rocket science that your passwords deserve the same care and attention as your car and house keys, your credit cards or your Smartphone. Their loss can have a significant impact on your life…

---

\(^1\) Please folks, do not all use these examples. We do already. Be creative and invent your own.
A good password is something you can easily remember, is unique for each computing service, has never been shared with someone else, and is sufficiently complex that it cannot be guessed by humans or automatic tools (like so-called dictionary attacks trying out every word in a dictionary and even combinations thereof). Unfortunately, “memorable”, “unique” and “sufficiently complex” seem to contradict each other for the average human brain. Brain power seems to be too limited nowadays to recall several dozens of password/site combinations. What seemed to be easy for my grandma, remembering hundreds of phone numbers and whom they belong to, seems to have become difficult today. And the usual hints of:

- Choosing a line or two from a song or poem, and using the first letter of each word. For example, "In Xanadu did Kubla Khan a stately pleasure dome decree!" becomes "IXdKKaspdd!";
- Using a long passphrase like the sentence "In-Xanadu-Did-Kubla-Khan-A-Stately-Pleasure-Dome-Decree!" itself or mathematical formulas like "\( \sin^2(x) + \cos^2(x) = 1 \)";
- Alternating between one consonant and one or two vowels with mixed upper/lower case. This provides nonsense words that are usually pronounceable, and thus easily remembered. For example: "Weze-Xupe" or "DediNida3";
- Choosing two short words (or a big one that you split) and joining them together with one or more punctuation characters between them. For example: "dogs+F18" or "comP!!UTer" do not work for everyone.

The easiest thing to do, of course, is to reduce the number of passwords: Your Google or Facebook account can already be used for services outside the Facebook and Google realms. And CERN is also actively working on a “federated identity” solution so that you can use your CERN username and password to access computing services at other institutes and universities – and vice versa! In addition, there is nothing to stop you using easy passwords like “123456” for websites on which you do not expose anything personal, have no financial risk, and where an adversary cannot create havoc (e.g. newsletter subscriptions). If you seldom access those pages, you might even forget those passwords and reset them only once needed...

For more important computing services, you might want to consider using a password manager to store all your different passwords and protect them with a very strong, complex and long master password. There are many technical solutions on the market: “Lastpass”, “Keepass”, Apple “Keychain” or even the built-in password managers within Internet Explorer, Firefox, Safari (i.e. Apple “Keychain”) and Chrome. But before you start using any of them, please consider whether you are fine with putting all your eggs in one basket. If the device running your password manager is compromised, all your passwords are potentially compromised and not only the ones you recently typed into that device; if the password manager is ill-conceived or turns out to be vulnerable, all your passwords are at risk, too (see, for example, this slightly biased old article); if
that device is lost, the only hope left is your brain power. Furthermore, what about the risk of loss of control? Some solutions, like “Lastpass”, push your passwords into the cloud. In the end, it is your choice regarding the balance between convenience and risk.

However, whatever you decide, also consider enabling multi-factor authentication solutions where possible. You use this already for your online bank transactions, and Google, Facebook, Twitter, and others offer similar protection! Multi-factor authentication will also soon come to CERN for privileged access to computing services, the Technical Network and for financial transactions (see our Bulletin article on “Pimp up your password”).

Pimp up your password (2016)

In the past, we have repeatedly stated the importance of a well-chosen, complex and unique password, for your account at CERN (see the article “Oops, there it goes…”), but also for your accounts on Facebook, Amazon and all other sites (see the article “The value of your password”). While this is all still valid, it might not be enough anymore…

Of course, making your password complex (with letters, symbols, numbers, using mathematical formulas, song titles or poems; see our recommendations) is still a must. It is still a necessity to avoid using the same password for several sites and essential not to share the password with anyone else (“your password is your toothbrush - you don’t share it and you change it regularly”). But this is not always sufficient. Passwords can be cracked not only through guessing or brute-force dictionary attacks (hence the requirement for a complex password not to be found in any dictionary) but also just by sniffing. An attacker can sniff out a simple password as easily as a complex one just by installing some keyboard logging software on your computer. “Stop, think, don’t click” is the only way to protect ourselves from such attacks and their consequences: do not click on suspicious links, only click if you trust their source. Unfortunately, as our latest clicking campaign has shown (“One click and BOOM…”), far too many of us are still clicking on malicious links, so putting such a keylogger in place would be easier than we would like for an attacker in our environment. The campaign showed that an attacker could easily have taken control of 10 to 20% of all Windows computers at CERN and could have sniffed out a large number of CERN passwords…

The consequences? Severe, if you manage computing services, operate accelerators or experiments, or handle CERN’s finances! Once they own your password and the attached rights, the attackers would just sit and listen. They would take the time to understand how you work. They would observe when and how you access your resources and services. They would gather information. And when the time came, they
would be in a position to impersonate you and strike hard: they could try to bring down your computing service, manipulate your accelerators or experiment, or steal money – to your dismay and to the harm of the Organization.

The silver bullet? Pimping up your password (i.e. something you know)! Then enhancing it by using an additional second token - namely something you have: a piece of hardware like your smartphone, your CERN access card, or a dedicated USB stick. Banks very often ask their customers to use a small card reader to authenticate themselves. In technical jargon, this is called multifactor authentication, and in collaboration with the IT department, the BE department and the FAP/AIS group, we are looking into how to use such authentication methods to better protect access to computing services, financial systems and the accelerator network and its control systems. Of course, this will cause some inconvenience, but we will strive to make it as seamless and simple as possible. A little bit more time at login for much more security while working – is that a fair trade-off? For more details, check out this dedicated webpage or contact us at Computer.Security@cern.ch.

Think also of the value of your passwords at home: those you use for Facebook, Twitter, Google and Amazon, for example. What havoc could attackers create in your private life if they knew your passwords? They could enter your private sphere, post in your name, spend your money, etc. For reasons similar to the ones that drove CERN to turn to multifactor authentication, Google, Facebook and others allow you to opt in to such authentication too. We strongly recommend that you benefit from this, for your own protection.

The value of your password (2016)
http://cds.cern.ch/journal/CERNBulletin/2016/03/News%20Articles/2120676?ln=en

Of course, your passwords have a value to you as they allow you to access your computer and your Facebook page, to buy on Amazon, to create a Twitter feed, and to use a multitude of computing services provided by CERN. But have you ever thought of their value to the malicious people of this world?

With your account password, I can take over your computer. I can install software allowing me to enable your microphone and listen to your communications and what is happening around you as long as your computer is turned on. I can take regular screenshots and monitor you while you work. With that, I can try to determine your working habits, your online behaviour, the way you write e-mails... Useful, if I want to impersonate you believably (e.g. to attack CERN and the systems you are working on at CERN). What’s more, with access to your computer, I can install a key logger to record your every keystroke – including when you type all your other passwords: Amazon, PayPal, Facebook, and Twitter. Of course, with those passwords, I can go on a nice shopping spree with your money...
So, what is the value of your password to those malicious people? A few bucks? A bit more or a bit less, depending on the type of account. There are black market websites where they can buy and sell account names and passwords in bulk. Think of what an attacker could do with your CERN password. For example, they could access your mailbox and send spam to people all over the world, which could earn them some money if people respond. By sending phishing emails, they can harvest even more passwords. They could access CERN’s software repositories or our online journal library; downloading them in bulk and selling them on the black market would definitely create revenue – at CERN’s expense!

They could access your computer and manipulate your work: if you work in finance, the attackers might try to siphon money out of CERN. If you have access to computing resources, the attackers might misuse them, by blackmailing third-party web services and threatening to bring their sites down or by running dedicated computing jobs to mine BitCoins or crack hashed password files. If you have access to control systems, targeted attackers might even misuse your power to grind your system to a halt...

So, is your password already on sale? Hopefully not. Just follow a few simple steps to keep your password yours – both at home and at CERN: keep your PCs and laptops up to date and run antivirus software. Do not install software downloaded from dubious sites. Browse responsibly – stop and think before you click. Make use of browser extensions and plugins that can help you. Keep your password to yourself, do not share it and do not type it into webpages you are not sure of. Do not use the same password for multiple sites. And finally, make your password complex: for example, you could use the title and artist of a song you like (“Money4Nothing---DireStraits”), a mathematical formula (“DeltaX*DeltaP>=h/4pi”), or a poem (“3quarksforMusterMark!”). Recall what is at stake: lose your password and you are digitally naked...

What is your identity? (2016)

In the physical world this is fairly clear; your sense of self is multi-faceted and highly complex but the entity of “you” is well defined. You can prove your identity simply, typically by showing your ID card or by having someone vouch for you. You are a being layered with attributes. Other people may request some of these attributes: your first name at Starbucks or your shoe size at the bowling alley. But only your most trusted contacts are granted access to your entire set of attributes… or maybe you never expose your identity entirely!

Online, your identity is a very different beast. It is fragmented. Each piece of your identity is typically verified by its own username and password. Occasionally pieces are forgotten or lost to the depths of the Internet. The hundreds of accounts that identify “you” present a security problem. Can you keep track of these accounts and is it even realistic to use unique, non-trivial passwords for each of them? Often the answer is no
and multiple pieces of your identity can be chipped away by malicious actors (see [this link](http://cds.cern.ch/journal/CERNBulletin/2015/16/News%20Articles/2001040?ln=en) for a detailed discussion).

What if you could have just one cyber identity? You may have noticed that the option to create new accounts online based on an existing Facebook or Google account is becoming commonplace. Attributes from each of the services with which you authenticate yourself are being added to your social digital presence. The Internet is creating an increasingly complete picture of “you”.

When you next authenticate yourself via CERN Single-Sign-On, scroll to the bottom of the page where you will find the option to sign in via a trusted, alternative organisation, e.g. your home university. CERN has established a trusted relationship with these institutions, allowing them to vouch for you and to assert your identity on your behalf. By allowing logins from reliable organisations, we are limiting the creation of unnecessary accounts and trivial passwords. By using this form of login, known as Federated Login, you are limiting the fragmentation of your identity profile. Whether you choose to separate your social and your research profiles remains up to you.

This idea is called Federated Identity Management. You are already able to access resources worldwide using your CERN account; why not test it and use Foodle to schedule your next meeting or create a survey? CERN has proven itself to be a trusted partner and so this service, based in Norway, allows us to use their app.

**Your privacy at CERN matters (2015)**


Congrats to all those who spotted that our last contribution to the CERN Bulletin (“CERN Secure Password Competition” – see [here](http://cds.cern.ch/journal/CERNBulletin/2015/16/News%20Articles/2001040?ln=en)) was an April Fools’ Day hoax. Of course, there is no review and no jury and there won’t be any competition. Consequently, we are sorry to say that we cannot announce any winners. The extension of the password history rule and the initiative of finding password duplicates are absolute nonsense too.

In fact, the Computer Security team, just like the CERN Account Management service, the Single Sign-On team and the ServiceDesk, does not know and has no need to know your password. Passwords are actually salted and hashed using the SHA256 cryptographic hash function. Thus, there is no literal password database and no way can that anyone apart from you know your password – unless you have given it away intentionally or inadvertently…

Remember, your password is yours and only yours, so please do not share it with anyone. Also, beware of “phishing” emails trying to convince you to hand over your password. Nobody legitimate will ever ask you for your password: neither us, nor the ServiceDesk, nor your supervisor. Not Facebook, Google, Amazon, your bank, any other Internet service. Never type your CERN password into webpages that do not look
like the CERN single sign-on portal (we do our best to have all authentication done there!). Check that the webpage’s address starts with “https://” and is part of the “cern.ch” domain (the authentication portal is accessible via https://login.cern.ch).

In the event that we do need to access your account, mailbox or private data repositories like the “My Documents” folder on DFS (distributed file system) or the “~/private” folder on AFS (Andrew file system), strict procedures apply. For example, if your summer student is on a prolonged holiday in the Amazon, not reachable by phone or e-mail, and you as the supervisor need that one document stored in the student’s private mailbox, the procedure for getting that document is governed by CERN’s policy on “Third party access to users’ accounts and data”. Be prepared to provide exact information. The Computer Security Officer will consider and, if appropriate, approve your request to access the document. Of course, in the interests of full transparency, the initial document owner will be notified, so he or she can object in retrospect. If you need full, unlimited access, however, this would require the additional written consent of the Director-General and would also involve the CERN Legal Service and the IT department head.

Oops, there it goes... (2015)

Do you love riddles, hide and seek or picture puzzles a la “Where’s Wally”? Then take a look at the photo below, and try to spot the error.

It is hard to spot: the yellow sticker on the computer screen shows a password providing access to the web application running on the screen. Surprising! Fortunately, this sticker was quickly removed by the corresponding system owners and the password changed. However, we can all make improvements: passwords must never be written down and definitely not on stickers attached to screens, keyboards, or desks.

Remember: your password is your “toothbrush” - a toothbrush you do not share and you change regularly. Neither your colleagues, your supervisor, the Service Desk or the Computer Security Team have any valid reason to ask for it. They should not and
will never do so. The same is valid for any external company: UBS, PayPal, Amazon, Facebook or Google will never ask you for your password! Your password is yours and yours alone. In this particular case, the password is not a personal one, but used between collaborators to access a shared resource (the web application). Still, we should try to do better!

Wherever possible, shared accounts should not be encouraged. Avoid using them and instead use e-groups listing individual members of your team and limit access to your application or service to the people in the e-group. All CERN web-services easily allow for this through the CERN Single Sign-On portal. If your application is a commercial one and requires a shared password, put this password in an encrypted file on AFS, or use one of these password vaults: KeePass or Password Safe (but note that usage is at your own risk - neither the CERN Security Team nor the IT department support these tools). Do not write the password down in a file stored on a public or restricted webpage! If the password is hardcoded in your software, look for alternatives and take care to check whether your preferred software repository leaks that password. And, of course, do not put it on a sticker and glue it to the monitor, under or on the keyboard, or put a corresponding note in the drawer close-by.

Finally, the password on that tiny yellow sticker was “Administrator”… recall that good security requires creativity (see our Bulletin article on “Creativity@CERN”)! Use complex passwords and different passwords for different sites (“Don’t Copy/Paste Passwords!”). A good password must be private, i.e. known and used by only one person (“Don’t let Chrome expose your passwords”); secret, i.e. it must not appear in clear text in any file or program, or on a piece of paper pinned to the monitor (“Backed up and gone...”); easy to remember, so there is no need to write it down; and at least eight characters long with a mixture of at least three of the following: upper-case letters, lower-case letters, digits and symbols (see also our password hints). It must not be listed in a dictionary of any major language and it must not be guessable by any programme in a reasonable time.

Don’t copy/paste passwords! (2014)  

What do umbrellas, hair, wars and passwords have in common? Over time, they all get lost.

While some losses are inevitable, we can at least help you reduce the impact. Millions of passwords are stolen or lost every year. Partly because of inattentive users falling for “Phishing” traps, where adversaries simply ask people for their passwords; partly due to compromised web sites having had their database of passwords stolen.
For example, over the past few years, eBay recently asked their 145 million users to change their passwords, LinkedIn lost 6.5 million hashed passwords, and the hacking of the CERN HyperNews service rendered 4745 password hashes public. Just recently, 860,000 usernames, e-mail addresses and hashed passwords were stolen from the MacRumors forum, and Adobe lost a record 150 million e-mail/password combinations. So far, not good. At CERN, 746 people were notified when their CERN e-mail address was found among these combinations. Indeed, it was likely that some people used a similar password for their CERN account, as some password hints exposed suggested this: “cern id”, “nice pw dec 2011” and “wie edh” but also “us the year of LHC startup”.

So take up this small challenge. We are creative people! Good security practitioners use complex passwords and different passwords for different sites. A good password must be private (used and known by only one person); secret (it must not appear in clear text in any file or program, or on a piece of paper pinned to the monitor); easily remembered (so there is no need to write it down); at least 8 characters long with a mixture of at least three of the following: upper case letters, lower case letters, digits and symbols. It must not be listed in a dictionary of any major language and it cannot be guessable by any programme in a reasonable time, for instance, less than one week.

A good password is a work of art. Here are some hints to help you choose good passwords:

- Choose a line or two from a song or poem, and use the first letter of each word. For example, "In Xanadu did Kubla Kahn a stately pleasure dome decree!" becomes "IXdKKaspdd!". Mathematical formulas would also do: “a**2+sqr(b)==c^2”.
- Use a long passphrase like the sentence "InXanaduDidKublaKahnASatelyPleasureDomeDecree!" itself.
- Alternate between one consonant and one or two vowels with mixed upper/lower case.
- This provides nonsense words that are usually pronounceable, and thus easily remembered. For example: "Weze-Xupe" or "DediNida3".
- Choose two short words (or a big one that you split) and join them together with one or more punctuation marks. For example: "dogs+F18" or "comP!!UTer".

1 "Hashes" are results of a mathematical one-way functions like MD5 or SHA. Calculating a “hash” of a password is easy; but the inverse is supposed to be difficult. Once you login, the hash value is calculated from your password and compared to what is stored with the web service you intend to use. However, if an attacker gets hold of this list of hashes, they can use so-called “rainbow tables”, i.e. pre-calculated hashes for a wide variety of passwords produced from common dictionaries, and hope that one entry of those pre-calculated hashes matches those in the stolen list of hashes. As a counter measure, random data is now added to hashes as “salt”, so that the size of a rainbow table grows exponentially.
Remember that your password is your “toothbrush” - a toothbrush you do not share and which you change regularly. Neither your colleagues, your supervisor, the ServiceDesk or the Computer Security Team have any valid reason to ask for it. They should not and will never do so. The same is valid for any external company: UBS, PayPal, Amazon, Facebook or Google will never ask you for your password! Your password is yours and yours alone.

If you still struggle to recall all your passwords, use one of these fine password vaults: KeePass or Password Safe (but note that usage is at your own risk - neither the CERN Security Team nor the IT department support these tools). However, refrain from using the password cache offered by your browser, e.g. Chrome, Firefox, or Internet Explorer, as passwords are not always stored in a secure manner (more on this in our Bulletin article “Don’t let Chrome expose your passwords”). In particular if you lose your device, you might also give away the access to your favourite web sites! Another good reason to re-type your password, especially on smart phones, is that a hardcoded password might end up in your devices’ back-up - stored somewhere in the cloud (“Backed up and gone...”).

When a person leaves — Access rights remain!
(2014)

We have been contacted recently by an embarrassed project manager who just figured out that a student who left at the end of 2013 still had access rights to read the whole project folder in February 2014: “How can that be?! In any other company, access rights would be purged at the same time as an employment contract terminates.” Not so at CERN.

CERN has always been an open site with an open community. Physical access to the site is lightweight and you just need to have your CERN access card at hand. Further restrictions have only been put in place where safety or security really require them, and CERN does not require you to keep your access card on display. The same holds for the digital world. Once registered at CERN - either by contract, via your experiment or through the Users’ office - you own a computing account that provides you with access to a wide variety of computing services. For example, last year 9,730 students/technicians/engineers/researchers/staff joined CERN. A similarly large number of people left CERN as their contract with CERN or with their university ended. Eventually, a fraction of those people come back to CERN with a follow-up contract from CERN or their university, or having enlisted with another university. This is not unusual as students often graduate with a MSc degree in one place and continue with a PhD on their favourite research topic at another university.

Had we taken the harsh approach adopted by “normal” companies, we would have immediately closed their computing account, deleted all their data and wished them
“Good Bye”, only to find that they re-join CERN a few weeks later. Not exactly optimal. Therefore, CERN has decided to grant a two month-long grace period: CERN computing accounts will be kept active for two months after the end of the affiliation with CERN. If a person comes back, nothing will have changed for him/her in CERN’s digital world. If not, the account will be automatically blocked after this grace period and all data, e-mails, folders, etc. will be purged after another four months.

The project manager mentioned previously discovered this the hard way. He was worried, as his project dealt with sensitive data that needed to be kept well protected and accessible only on a need-to-know basis. People should not feel tempted to misuse access rights (“Don’t tempt me!”) - not to mention the potential of data leakage or misuse... Thus, if you want to be on the safe side and protect your data, service and folders properly (“How private is “private”?”), keep this article in mind. Usually people are not malicious and, if they were, they would have already had time to express that. Still, if required, you can ask us at Computer.Security@cern.ch to block an account prematurely, provided a written justification from the corresponding supervisor, hierarchy or team leader is given.

Maths to the rescue! (2013)

Do you recall our article on “Creativity@CERN” and the problem of creating good, memorable passwords? Given the feedback we’ve received, it still does not seem to be that easy.

So let’s take another approach – the physicist’s/engineer’s/mathematician’s way. For them, mathematical formulae are bread and butter: binomial expansion formulae, Pythagoras’ Law, integrals or derivatives, Laplace or Fourier transforms – you name it. Furthermore, there are plenty of physics formulae: Maxwell’s equations, the Schrödinger equation, the standard model Lagrangian and so on. So why not use your favourite mathematical or physics formula as your password?

Passwords are supposed to be at least eight characters long with a mixture of at least three of the following: upper-case letters, lower-case letters, digits and symbols. “\(\sin^2(x) + \cos^2(x) = 1\)", “\(e^{i\pi} = -1\)”, “\(\text{Integrate}[x^n,x]=x^{n+1}/(n+1)\)” or “\(i\hbar \frac{d\Psi}{dt} = H\Psi\)” would do the job perfectly! The variety is vast and you already have them memorised ever since your early studies at school or university! What’s more, if you’ve used Latex or Mathematica before, you will even know how to write those formulae without using mathematical symbols…
Thus, using formulae is quite good if you also recall the other basic rules for a good password: it must be private (used and known only by you); secret (it must not appear in clear text in any file or programme or on a piece of paper pinned to the monitor); easily remembered (so there is no need to write it down); not listed in a dictionary of any major language; and not guessable by any programme in a reasonable time. In addition, of course, please do not put all your eggs in one basket – avoid re-using your password for different sites or different purposes. The pool of formulae is big enough to pick (and memorise) a few more to cover all your passwords! Finally, remember that “your password is your toothbrush”: you do not share it and you change it regularly. Neither your colleagues nor your supervisor, the Service Desk or the Computer Security Team have any valid reason to ask for it. They should not and never will. The same is true of external companies: UBS, PayPal, Amazon, Facebook and Google will never ask you for your password!

No certificate, no chocolate (2013)

Are you already ready to use “certificates” to log into CERN or to connect to the global “eduroam” wireless network? No, I am not talking about your birth certificate, medical certificates or academic certificates. I am referring to “certificates” used for authentication where you would usually use a password.
These digital certificates are a valid alternative to cumbersome passwords. Like the aforementioned personal certificates, a digital certificate is an official document that proves who you are or your qualifications. Your personal digital CERN certificate is tied to your digital identity at CERN. In that respect, a digital certificate is like a password. It is a credential that you must not share with anybody else! With your digital certificate, I can impersonate you and take over your mailbox, your web sessions and more...

Digital certificates bind your digital identity to a public/private-key infrastructure (PKI). This is based on a simple mathematical fact: multiplication is easier than division, hence the difficulty of factorising prime numbers (take, for example, “8633=89*97” and now think of prime numbers with thousands of digits). Through a sophisticated algorithm, this difficulty is transferred into a pair of certificates: a “public” one and a “private” one.

The public certificate can be shared, so that others can encrypt e-mails so that only you can read them when you use your private certificate. Similarly, your private certificate can be used to prove that you are you if I know your public certificate. At CERN, your certificate is signed by the CERN Certification Authority as a proof of identity. Of course, this is highly simplified (for details see the X.509 standard), but it might give you an idea of what is happening behind the scenes...

In the High-Energy Physics community and at CERN, certificates are used in many places. For example, to submit analysis tasks to the Worldwide LHC Computing Grid (WLCG), you need a certificate issued by CERN or by your home institute. CERN is part of the International Grid Trust Federation (IGTF/EUGridPMA), which establishes trust at the policy and technical levels within the Grid community. It ensures that your CERN certificate is recognised by all the IGTF partners worldwide — a great example of global trust among peers.

If you want to log into CERN via the CERN Single Sign-On portal, a CERN certificate is a valid means. A second certificate would need to be stored on your CERN access card if you are requested by certain web services to provide a second means of identification (i.e. in addition to something you know (your password), you provide something you have (your CERN access card certificate)).

You can also use your certificate to digitally “sign” your emails and, thus, prove that they are really from you. Last but not least, thanks to the CERN Networking Group, your CERN certificate can be installed on your smart-phone, tablet or laptop. This way you can benefit from a free, easily accessible wireless connection wherever the “eduroam” wireless network is available (click here for a complete list).

In order to benefit from a digital CERN certificate, create your own at the CERN Certification Authority and follow a simple procedure to install it on your PC, laptop, tablet or smart phone. But remember: this certificate is to be treated like your toothbrush (or your password); you must not share it with anyone else. If it, or a device where it is stored, is lost or stolen, please revoke your certificate immediately at the...
CERN Certification Authority in order to avoid misuse of your CERN computing account!

Don't tempt me! (2013)

Over your CERN career, have you ever changed activities, functions or responsibilities, but nevertheless kept the access to your “old” control systems or computing services? Accessing the systems for which you are no longer responsible seems innocent enough, because you just want to help by using your previous work and experience but... Does this sound familiar to you? Let’s think this one through because it may have bad consequences.

In my previous life, I worked as a software developer and system expert for the “Detector Safety System”, a control system used in the LHC experiments. After this system had been deployed and the project moved into maintenance mode, I was assigned new responsibilities which finally led me to the CERN Computer Security Team. My system was now in the care of a new team of excellent people. However, as my experience of the Detector Safety System didn’t just disappear, I was kept on their expert list with all the access permissions needed. I was honoured by this, as I felt valued and needed. But with time, the fact that I still had access was forgotten. Meanwhile, I began to feel more and more uncomfortable: the system changed over time, the software was adapted, and additional requirements and hardware were added. What would have happened if I had called in and screwed up? In the end, I arranged for all of my access rights to be revoked...

But wasn’t it tempting? The more access, the better! I could have used my access to copy (parts of) my code and re-used it in another project; I could have accessed the PCs to conduct tests which can only be run on live systems; I could have been malicious and prevented the LHC experiments from working. Ergo, the more access, the WORSE (1)! If I had misused my access to those systems or software, and if I had screwed up, I am pretty sure that would have been considered a professional fault!

So please, do not tempt me or any of our colleagues! If you manage a service, system or software and want to be on the safe side, make sure that you have procedures in place on how to deal with the access rights of people leaving your team and then apply them! This is less of a question of your trust in them, but rather an act of due diligence: in the end it is you who bears the burden when problems happen. It might be your professional fault!

---

1 Note that this is also the reason why you ought to handle your password like your toothbrush: don’t share it! Otherwise, you might tempt others...
Don’t let Chrome expose your passwords (2013)

Do you still struggle with remembering your password? Is this despite our many attempts to help you: “Train your Brain: Don't put your password on paper!” (article here), “Creativity@CERN” (article here) and “Maths to the rescue!” (article here)? Then you might have considered the “save your password” features in Chrome, Firefox or Internet Explorer… these features remember your Facebook, CERN, Twitter, Amazon and eBay passwords. But be careful: it might be easy for someone to read them!

If enabled, Chrome, Firefox, Internet Explorer and others can remember the password of specific sites after you’ve logged in to those sites the first time. As the passwords are, however, stored in plain text, they can still be read out by anyone with access to that computer. In Chrome, just type “chrome://settings/passwords” and click the password you want to reveal. Or in Firefox, go to “Options->Security->Saved Passwords...” and hit “Show Passwords”. Internet Explorer does not provide such a “simple” option, but there are tools that can access your saved passwords in this browser too1.

If you are security-aware and want to be on the safe side, never ever type your password into a PC that you don’t own or don’t trust. Examples of such public PCs include those in Internet cafes, hotels and conference venues, as well as those available near the CERN Users Office, in the CERN Library or in the CERN training centre. If you have to, use private browsing, e.g. the “incognito window” in Chrome, the “Private Window” in Firefox and “InPrivate Browsing” in Internet Explorer. Also consider changing your password once you’re back on your personal PC. In order to store passwords on your personal PC, protect the password vaults with a master password. In Firefox, you “Use a master password” in “Options->Security”. For Chrome and Internet Explorer, the master password is tied to the logged-in account. Alternatively, you can use generic password vaults like KeePass or Password Safe2.

However, Google has made a strong statement on this issue, stating that the security of your passwords on your own PC strongly depends on who has access to it. And right they are. The ultimate security for all your individual passwords strongly depends on the protection level of the PC you use; whether all of its applications, in particular its operating system and browser(s), are up-to-date and patched; the way you browse the Internet and handle emails (“Jekyll or Hyde? Better browse securely”); and finally how strong and secure your account’s password is. Recommendations on the choice of a good password can be found on our website.

1 Very helpful technical documentation on this can be found here.
2 Note that usage is of your own risk. Neither the CERN Security Team nor the IT department support these tools.
Creativity@CERN (2013)

Aren’t we innovative and creative people? Building complex accelerators and doing sophisticated physics analysis is not easy and requires a lot of excellent brains. Some items of hardware are pure works of art, worthy of a place in an art museum. Some software takes advantage of all the finesse of computer science to optimize every last bit of computing power. So, yes. We are. Innovation and creativity are our middle names.

But I wonder why these splendid characteristics are lost when dealing with passwords? Recent computer security scans have found a series of unprotected passwords and, I hope you agree, “Operator1”, “SamFox” or “Admin123” do not reflect our innovative nature (and might even be taken as an insult). I believe we can do much better than that and encourage you to be Creative@CERN!

So take up this small challenge. I am sure you can do better than your colleagues! Your good password, however, must be private (used and known by only one person); secret (it must not appear in clear text in any file or program, or on a piece of paper pinned to the monitor); easily remembered (so there is no need to write it down); at least 8 characters long with a mixture of at least three of the following: upper case letters, lower case letters, digits and symbols. It must not be listed in a dictionary of any major language; and not guessable by any program in a reasonable time, for instance less than one week.

A good password is a work of art. Here are some hints to help you choose good passwords:

- Choose a line or two from a song or poem, and use the first letter of each word. For example, "In Xanadu did Kubla Kahn a stately pleasure dome decree!" becomes "IXdKKaspdd!"
- Use a long passphrase like the sentence "InXanaduDidKublaKahnAStatelyPleasureDomeDecree!" itself.
- Alternate between one consonant and one or two vowels with mixed upper/lower case. This provides nonsense words that are usually pronounceable, and thus easily remembered. For example: "Weze-Xupe" or "DediNida3".
- Choose two short words (or a big one that you split) and join them together with one or more punctuation marks. For example: "dogs+F18" or "comP!!UTer".

Finally, remember that your "password is your toothbrush": you do not share it and change it regularly. Neither your colleagues, your supervisor, the ServiceDesk or the Computer Security Team have any valid reason to ask for it. They should not and will never do. The same is valid for external companies: UBS, PayPal, Amazon, Facebook, Google will never ask you for your password! Your password is yours and only yours.
Train your brain: Don’t put your password on paper!
(2012)

I completely acknowledge that constructing a good password can be difficult. And
remembering it for some time isn’t easy, either. However, noting it down on a sheet of
paper and hiding it in a drawer in your office (or even attaching a sticky note to your
monitor) isn’t a valid solution. It violates CERN Computing Rules.

You can do better! Train your brain! Here are some hints to help you choose good
passwords:

- Choose a line or two from a song or poem, and use the first letter of each word.
  For example, "In Xanadu did Kubla Kahn a stately pleasure dome decree!" becomes "IXdKKaspdd!";
- Use a long passphrase like the sentence
  "InXanaduDidKublaKahnAStatelyPleasureDomeDecree!" itself;
- Alternate between one consonant and one or two vowels with mixed
  upper/lower case. This provides nonsense words that are usually
  pronounceable, and thus easily remembered. For example: "Weze-Xupe" or
  "DediNida3";
- Choose two short words (or a big one that you split) and join them together
  using one or more punctuation characters. For example: "dogs+F18" or
  "comP!!UTer"

For a series of hints on how to choose a good one, please check out our password
recommendations page.

Also, remember that nobody legitimate will ever, ask you for your password. Never!
So, if you are asked for it by your supervisor or team leader, the ServiceDesk or
somebody else (like these fake phone calls pretending to come from Microsoft), please
turn them down. They must not ask for your password. Your password is yours!
Instead, report this to Computer.Security@cern.ch and we will take the appropriate
action. If you think your password may have been exposed or stolen, then change it
here.

Of course, this is valid for every other password too, e.g. those you use on Amazon,
Twitter, or Facebook. However, please do not use the same password for all those
sites as this can increase the risk of exposure. You can do better and use one distinct
password for every site. Again: Train your brain!
1000 passwords exposed, what about yours? (2011)

In the last three issues of the Bulletin, we have stressed the importance of the secrecy of your password. Remember: Your password should be treated like a toothbrush: do not share it, and change it regularly! And this is not only valid for your CERN password, but also for any other password you use to log into your university or laboratory, Facebook or Twitter portals, or other web sites.

Unfortunately, recent security checks have revealed a huge area for improvement here. Within a period of only one week, more than 1000 different passwords passed through the CERN outer perimeter firewall in clear text. “Clear text” means that the password was readable to any adversary able to intercept the communication.

Make sure your web connection is secure! This can easily be checked in the address bar of your web browser. If the address starts with “HTTPS”, everything is fine. If it is only “HTTP” (without “S”), your password is at risk and can be easily sniffed out by an adversary.

Protect yourself! Never type your password into an “HTTP”-only page unless that password is completely unimportant to you and not used anywhere else. If you have done this, change the password as soon as you can. If you know the owners of those web sites - e.g. the local security team - contact them and inform them of this flaw. They will be happy to make the necessary improvements. Finally, check our passwords recommendations here.

Holidays come — Passwords go (2011)

The holiday season is approaching and with it, the best chance of losing your password!!

If you are keen to access your CERN mailbox or other computing facilities at CERN from the Internet café at your hotel, hold on and think twice. Is that local PC trustworthy? Most likely it is not. It might never have been patched, and, thus, has been infected by plenty of computer viruses long time ago. Worse, nasty people might have installed tools which aim at stealing your password once you type it. Therefore, it is better to use your own laptop or mobile phone for such activities. If you decided to connect to CERN from an untrustworthy computer and had typed in your CERN password there – please seriously consider changing your CERN password at http://cern.ch/account as soon as you have access to a trustworthy computer.
However, also take care when using your own laptop or mobile device: wireless communication can be intercepted. Many wireless access points, e.g. at airports, do not encrypt and protect network traffic by default. When you access sensitive webpages like your CERN mailbox, your bank account, or your Facebook profile, you have to ensure that you use encrypted protocols. For example, look for a “HTTPS” in your browsers address bar (and avoid “HTTP”). If you connect directly to CERN mail servers, however, you are safe: these accept only encrypted connections.

Finally, take care on your laptop. Thousands of laptop get lost per year at international airports, not to speak about those which got stolen. If this is not bad enough, losing a CERN laptop which holds sensitive or confidential documents can become embarrassing to the organization. Either encrypt your data or consider leaving such a laptop at home. Recall, losing a laptop with confidential CERN data might be considered to be a professional fault…

Happy holidays! Enjoy!

What is a good toothbrush, erm, password? (2011)

Do you remember the answer to the question posed in the previous issue of the Bulletin? "Your password should be treated like a toothbrush: do not share it and change it regularly!" After our last article, we received a series of questions on how to choose a good password and remember it easily… Thus, here we go.

Do you remember the answer to the question posed in the previous issue of the Bulletin? "Your password should be treated like a toothbrush: do not share it and change it regularly!" After our last article, we received a series of questions on how to choose a good password and remember it easily… Thus, here we go.

A good password is:

- Private: used and known by one person only;
- Secret: it does not appear in clear text in any file or program or on a piece of paper pinned to the monitor;
- Easily remembered: so there is no need to write it down;
- At least 8 characters long with a mixture of at least 3 of the following: upper case letters, lower case letters, digits and symbols;
- Not to be found in a dictionary of any major language nor guessable by any program in a reasonable time.

Here are some hints to help you choose good passwords:
Choose a line or two from a song or poem, and use the first letter of each word. For example, "In Xanadu did Kubla Kahn a stately pleasure dome decree" becomes "IXdKKaspdd";

Alternate between one consonant and one or two vowels with mixed upper/lower case. This provides nonsense words that are usually pronounceable, and thus easily remembered. For example: "Weze-Xupe" or "DediNida3";

Choose two short words (or a big one that you split) and connect them together with one or more punctuation characters between them. For example: "dogs+F18" or "comP!!UTEr".

If you have to deal with multiple passwords, one for CERN, for Facebook, for eBay or Amazon, please do NOT reuse the same password for all sites. Instead, use different passwords for different purposes. To remember those easily, you might take your favourite music CD and apply the aforementioned rules to its songs. Alternatively, you might use one of these password management tools: KeePass Password Safe, Passwordsafe (note that usage is on your own risk. Neither the Security Team nor the IT department support those tools).

For more on passwords, including a video explaining how good passwords can be chosen, please check the Computer Security team recommandations.

If you think your password may have been exposed or stolen, then change it here and inform us.

What do passwords and toothbrushes have in common? (2011)

Your password is your entry token into the digital world. eBay, Amazon, Facebook, Twitter, FNAL, DESY, and CERN - all ask you for a password to authenticate and prove that you are you. And vice versa. If I know your password, I can impersonate you and use your money to buy from eBay or Amazon, post nasty messages on your Twitter or Facebook profile, or misuse CERN's/DESY's/FNAL's computing facilities in your name!

CERN accounts have been compromised in the past and misused to send spam across the world. Are you keen to delete tens of thousands of return e-mails from your mailbox? It's no fun.

Would you give me your UBS bankcard and its PIN number? Of course not! Please apply the same sensitivity to your digital credentials, i.e. passwords, SSH keys, certificates, CERN card, etc. Beware of attempts to "steal" your password. CERN's computing staff, including the Computer Security Team, will never ask for your password (nor will any other legitimate person at Facebook, FNAL, eBay, etc.). So be
wary of malicious e-mails, or other means requesting your password. Never send it via e-mail, and type it only into web interfaces you know and trust.

Remember: Your password should be treated like a toothbrush: do not share it, and change it regularly!

For more on passwords and hints on how to choose a good one, please check here. If you think your password may have been exposed or stolen, then change it here and inform us.

Finally, remember that your “password is your toothbrush”: you do not share it and change it regularly. Neither your colleagues, your supervisor, the ServiceDesk or the Computer Security Team have any valid reason to ask for it. They should not and will never do. The same is valid for external companies: UBS, PayPal, Amazon, Facebook, Google will never ask you for your password! Your password is yours and only yours.

For further information, questions or help, please check our website or contact us at Computer.Security@cern.ch.
Email & Web Security

CEO fraud (2021)

Have you ever heard of “CEO fraud”? It is a social engineering method to extract money from a company, playing on several psychological techniques to make people stop thinking consciously:

- Fear, guilt and shame, i.e. making a threat to you or your family (“I know what you did last summer and will tell your family if you don’t…”). Under that pressure, you will just comply as your fear adverse consequences if you don’t;
- Flattery, i.e. luring your ego, pride or complacency (and narcissism?) into complying;
- Seniority and respect, i.e. blindly obeying because you are instructed by someone much more senior than you, you are just a little cog in the machine.

The CEO fraud plays the “seniority” card: “I am the CEO and you will do as I wish”. Full stop. And such a targeted CEO fraud attack has been run against CERN by abusing the name of our DG and spoofing her e-mail address. It all happened in the morning of October 19 when several people in the CERN hierarchy or with budget responsibilities received the following message (Image 1):

![Image 1.](image1.jpg)

Note that the “From:” address has been spoofed. The so-called header information of that e-mail – something like the address on the envelope of a letter – indicates that the mail does not come from CERN (but from “XXXXpower.com”) and that all replies would go the e-mail address “boardpresXXXX@gmail.com” (Image 2):

![Image 2.](image2.jpg)

---

1 As detailed in another Bulletin article, there is no simple defence against e-mail address spoofing. E-mail sender addresses, like sender addresses on normal postal envelopes, can easily be faked...
2 In Outlook, you can access this header information by opening the e-mail, clicking on the small arrow to the right of “Tags” and then looking at “Internet headers”. In Thunderbird, open the mail and go to “View > Headers > All”. Similarly for Apple Mail: “View > Message > All Headers”.

---

123 | P a g e
The trap has been set. The attacker just needs someone to reply… Bingo (Image 3):

On Mon, Oct 19, 2020  wrote:
Hi Fabiola,

I am at work. At the moment I am

Cheers

With bi-directional communication established, the attacker can now engage, using their social engineering powers, and try to convince the victim to comply with their wishes (once more, the “From:” address is fake, replies go to the aforementioned Gmail address) (Image 4):

From: Fabiola Gianotti <fabiola.gianotti@cern.ch>
Date: Monday, 19 October 2020 at 10:29
To:
Subject: Re: CERN LOGISTICS SUPPORT REQUEST

Hello,

Thank you for your email reply and I am glad you are well and in good health.

Apologies for the troubles, I need your assistance with a transfer of 2,875 Euros, for CERN logistics support payment.

Our treasurer is not able to process the transfer due to a family emergency, and I'm having some troubles with international transfers without my bank access token while on vacation.

Kindly let me know if you can help with the transfer, and if I can forward you the details to transfer the payment on behalf of CERN?

Rest assured the amount will be fully reimbursed back to you as soon as our treasurer is back in office.

Look forward to your return email for transfer details if you can help.

Regards,

Fabiola.

Unlike in other similar cases, the attacker does not even play the “secrecy”-card and requests 100% confidentiality of this communication (i.e. “This is a highly confidential transaction and should remain between you and me”). Instead, the attacker explains why other alternatives (the treasurer) are not an option. Thanks to the power of the alleged DG, the scam works (Image 5):

On Mon, Oct 19, 2020  wrote:
Hi Fabiola,

No problem. I can transfer the money. Please let me have the details.

Cheers

There we go (Image 6):
Fortunately, this scam was spotted by other people having also received the initial e-mail. Some noticed – as you can too! – that when trying to reply to this fraudulent mail the new recipient is indeed NOT Fabiola (Image 7):

So, the fact that they reported the scam e-mail to Computer.Security@cern.ch enabled CERN to:

- block similar e-mails from entering CERN mailboxes as well as blocking the attacker’s e-mail address;
- identify other people who had received the scam and warn them;
- ensure that the attacker’s IBAN was flagged and blocked from being used at CERN.

This is why vigilance and suspicion are helpful. Please don’t let yourself be impressed (or intimidated!) by seniority. By CEO power. By a strong voice. Similarly, please don’t let yourself be ashamed, harassed or intimidated by e-mails trying to create fear, guilt or shame. These are usually scams too. Instead, in particular in the event of any doubt, involve your hierarchy, the CERN Internal Audit Service or Computer.Security@cern.ch. They are here to support and help you! Your early notification helps protect CERN when other means fail. Better to ask than to be sorry…
Telecompromised (2020)

The number one vector for getting your computer compromised, your password disclosed, your data exposed and your digital life screwed up is social engineering, i.e. manipulating you in a way to make you trust an e-mail, a web URL or attachment, and lure you into clicking on a malicious link. One click and it's game over!

Indeed, we have covered the risk of browsing the web (remember “STOP – THINK – DON’T CLICK”?), malware and drive-by downloads as well as phishing in various recent Bulletin issues. In many cases, the primary attack vector boils down to convincing you to click on a malicious link (or open a malicious attachment). In today’s teleworking world, a nice new evil path opens up: malicious video-conferencing invitations...

Collaboration in teleworking times requires us to use one or more different video conferencing tools. Skype. WebEx. Teams. Vidyo. Zoom. You name it. Scheduling of the corresponding meetings usually proceeds via e-mail and calendar invitations, like the one below. Looks familiar, no?

As with any other e-mail, the ultimate truth of this calendar invitation depends on many factors: the sender’s name, the sender’s e-mail address, whether or not the e-mail has been digitally signed, the message text and contents, typos, language, social hook and level of intimacy, etc. If this overall “package” looks reasonable to you, you will trust its contents and follow up. And if this is a sophistically crafted but evil message, you might fall for the trap and click the malicious link. Check the example above again! The link is indeed malicious and the meeting is not on CERN’s default Zoom instance at cern.zoom.us… Instead, the link leads you to cern.zoom-us.aws-e4dfa2f4.com, which has nothing to do with Zoom nor with CERN, and which might not even host teleconferencing software, but is solely intended to infect and compromise your device. With just a few clicks: game over!

So, once again, hold on a second. Check your e-mail/invitation thoroughly. Did you expect it? Does the subject concern you? Do you know the sender? Is the content in a
language you understand? Hover your mouse pointer over the provided URL: does the tool-tip, the little pop-up box, correspond to the link displayed in the message? Does it point you to CERN’s cern.zoom.us instance (i.e. http://cern.zoom.us/j/NNN) or to an external Zoom instance known to you, to CERN Vidyo (like https://vidyoportal.cern.ch/join/XXXX) or any other valid teleconferencing portal (definitely hard to tell!)? If you have answered “no”, watch out! STOP – THINK – DON’T CLICK! Contact the meeting organiser to cross-check, ideally via another channel than e-mail, or get in touch with Computer.Security@cern.ch. We are here to help you.

CERN has been phished again (2020)
https://home.cern/news/news/computing/computer-security-cern-has-been-phished-again

At the end of June, CERN saw yet another phishing campaign against its staff and users. About 21 000 owners of a CERN mailbox received e-mails from "Sonia Abelona", "Michel Dutoit", "Ralf Brant", "Federico Campesi", "Anne Darenport-Smid" or "Andreu Tomanga", on topics related to "contract amendment", "pension fund balance situation", "confidential covid-19 report" and "new teleworking rules". All e-mails stemmed from either “CERN.COM”, “CEM.CH” or “CERM.CH”. And all of them contained a link, either directly in the body of the message or in an attached PDF or Word document, pointing to a fake CERN login page hosted outside the CERN.CH domain (note the “192.91.245.24” at the top).
Entering a CERN account name and a password into that fake login page would have put the Organization at risk and your private life at peril, giving access credentials to malicious evildoers for their malicious deeds (see our Bulletin articles on “Blackmailing Academia: back to pen and paper(?)” and “What do apartments and computers have in common?”).

In the wild world of evil, there are groups of criminals such as “SilentLibrarian” that do exactly this: targeting universities, companies and organisations with well-crafted, malicious e-mails in order to infiltrate their networks, gain access to their computing resources and extract confidential information. With sufficient preparation and reconnaissance, and given the human nature of being curious, this “social engineering” is easy as pie… unfortunately. Luckily, this time, these malicious e-mails were part of the CERN Computer Security team’s annual phishing campaign. The attachments were benign and the fake login page did not accept passwords at all. CERN passwords were not collected or exposed during this campaign. So no harm done, but lots of disturbing lessons learned.

Disturbing “Game Over” #1: 10%\(^1\) of all recipients did not recognise the fake login page. The wrong web address (URL) at the top. That implies that 10% of CERN accounts would have been compromised. We deem that about 90% of those accesses came from teleworkers. Hence, in nine out of ten cases, there are no means for our computer security detection to spot this… it all happened outside CERN. The ultimate silver bullet to protect CERN against such a loss is the deployment of multi-factor authentication, which will be introduced in the coming months (see our Bulletin articles on “A second factor to the rescue” and “Protecting the accelerator from remote evil”).

Disturbing “Game Over” #2: Even just opening the attachment (18%!\(^1\)) created a risk to the computer used to open it. If the document had been malicious, it could have easily compromised the local computer. Game Over! In particular, in times of teleworking, the security measures deployed at CERN would not have helped… So it is of the utmost importance that your own personal PCs and laptops at home are always automatically updated and run an up-to-date antivirus solution. In the future, the CERN IT department might offer you a sophisticated anti-malware and EDR (Endpoint Detection and Response) solution for enhanced protection.

With those two disturbing facts – if this had been a real attack – CERN accelerator and experiment operations, sensitive HR and financial data and computer centre services would have been put at imminent risk…!

---

\(^1\) In detail: More than 30% of all 21,083 recipients opened the e-mail for further inspection. 18% opened the PDF or Word doc attachment, if present. One quarter followed the embedded link to the fake login page. About 12% did so when that link was hidden within the PDF/Word doc. And an astonishing 50% of those (i.e. 10% of all recipients) tried to log into the fake login page with their CERN account name… The numbers split by department will be made available to the corresponding department heads and our computer security contacts within each department.
Encouraging fact #1: Within the first five minutes of the campaign, the Computer Security team received notifications of this campaign going on. Such quick alerts are essential to raising our defences and protecting, at least, devices and accounts from within CERN. We could have even gone so far as to purge the malicious e-mails from individual inboxes (a task we usually avoid, given privacy implications).

Encouraging fact #2: In total, we received more than 800 SNOW tickets on the subject, which implies that our awareness raising is working for many! 80% didn’t open the attachment or follow the link. 90% didn’t enter their account name. Well done, guys!!!

So how can you help to protect your private life and CERN as an organisation? First, be vigilant. Be hesitant. Be suspicious. STOP – THINK – DON’T CLICK!!!

- Check once more our hints on how to best detect fraudulent e-mails and fake login pages;
- Help us deploy a two-factor authentication solution; and
- Deploy a decent anti-malware solution on your home computers.

Don’t answer me (2020)

Sometimes, occasionally, maybe not very often, it is good to pretend you’re not there. Pretend you haven’t heard. Or ignore what just has been sent. Because you just don’t want to interact. Because you just don’t want to talk. Or because you just don’t want to reply. With regard to e-mails, however, your e-mail client might expose your reluctance against your will…

Last year, the CERN Security Operations Centre detected 27 CERN hosts contacting so-called “tracking domains” used for reconnaissance and associated with national state-sponsored actors. A CERN researcher was using a shady Google Chrome extension (installed from the official Google Chrome Web Store) for e-mail tracking, and sent a number of legitimate e-mails to many people and lists, via Gmail in Chrome. The shady Google Chrome extension silently added malicious HTML code to each of the e-mails sent via Gmail. As a result, the recipients who had not disabled “Remote Content Loading” in their e-mail client inadvertently visited the malicious tracking domains (see our corresponding monthly report). And it is this “Remote Content Loading” which, when enabled, exposes you to the e-mail sender, telling him or her that you at least opened that e-mail (and, subsequently, most likely read it).

If enabled in your e-mail client, the “Remote Content Loading” feature automatically downloads any embedded images, photos or similar content from a remote webpage once you open an e-mail with remotely provided content. Nice for those who like
colourful texts. Or not, as this also implies that the remote site knows to whom to send that remote content, i.e. you, and can link this to the time when the content is loaded. Overall, this allows the remote site to know at which particular time you opened, checked out and read a specific e-mail...

Usually, lots of SPAM but also legitimate e-mail advertising campaigns (those to which you have subscribed) use this feature in order to better track and monitor your e-mailing behaviour, e.g. whether and when you read the e-mail. Even individuals can use that feature to learn quickly whether you read their e-mail even if you were not replying to it (e.g. by using that aforementioned Chrome extension). You can imagine how this can create conflicts: “I sent you that e-mail the other day.” “I haven’t received it…” “You DID actually!”...

Hence, in order to enhance your privacy, we suggest that you turn off the “Remote Content Loading” feature of your preferred e-mail client. Unfortunately, this is not the default for all e-mail clients, so it’s worth checking if you value your privacy: Kopano, Outlook, Thunderbird, MacOS Mail, iOS Mail app, Gmail and while you are at it, check also that the automatic sending of “Read Receipts” is toggled to off.

Click and infect (2020)

Do you recall last year’s e-mails from our dear colleagues S. Abelona, R. Brant, F. Campesi, A. Daren-port-Smid and M. Dutoit, who each shared an attached file with you? Except they aren’t actual colleagues. They’re all fake. As were their e-mails and their attachments. They were just intended to tempt you to open the attached Word document or PDF in order to have your computer infected...

Indeed, this is a standard pattern of attacks against the Organization. Attackers sending fake e-mails, ideally with content very close to the operations of CERN or very close to professional or personal aspects of your life, and sufficiently real that you believe them and open the attachment. This time the subjects were “your contract amendment request”, “new IT security measures”, the “pension fund balance situation”, “your input to [their] results”, and “the confidential design report”. The more targeted these malicious e-mails are, the more likely it is that you believe they are genuine and click. The more sophisticated the attack, the more probable that your computer, PC or laptop gets compromised. With one click, your Windows system, your Macbook or your Linux installation can be gone. Infected. Compromised. Owned by the malicious evil-doers abusing your computing resources, stealing your passwords (e.g. for CERN or for Internet banking), encrypting your documents (in order to blackmail you), sharing your photos and videos (“cyber-mobbing”), or exposing your local webcam images and microphone recordings (“I know what you did last summer”).

The CERN e-mail service and the CERN Computer Security Team are doing their best to protect you. Beside the “standard” SPAM filtering, they run a dedicated e-mail
appliance checking every single attachment entering the Organization and probing it to see whether it contains malware\(^1\). This is a cat-and-mouse game and, while the detection rate is very high, not all malicious e-mails can be caught, as attackers obviously try to evade our detection capabilities. This is where you come in, hopefully running an up-to-date operating system. This is easy nowadays as they should all update themselves automagically. And hopefully having deployed a good anti-virus solution. They don’t cost a fortune and provide a basic second layer of defence. And using an alternative to Adobe Reader, as a lot of malware tries to exploit weaknesses in it. And being vigilant and alert. Some e-mails really are too-good-to-be-true. Sometimes it is better to STOP — THINK — DON’T CLICK. Instead, forward anything suspicious to Computer.Security@cern.ch for additional checks.

Fortunately, this time, these particular e-mails were all fake, as they were part of our annual clicking campaign. Out of about 22 000 e-mails sent by us, around 30% were confirmed as having been opened by an e-mail client. In about 20% of cases, the user made all efforts to also open the attachment and thus ultimately put their computer at risk... Thanks to approval by the Data Privacy Office, we were even able to correlate the clicking rates with anonymised personal data. However, comparing the clicking rates for different age brackets did not reveal significant differences. Also, within statistical errors, the clicking rates of female and male colleagues were the same. When comparing different employment types, i.e. physicists vs. engineers vs. technical staff vs. administrative staff, the variations were also within statistical errors. It seems that the clicking rate just depends on the curiosity of our human nature\(^2\)! Finally, checking the timing, people were quick in reacting. Less than 10 minutes into our campaign, we received the first tickets notifying us that CERN was under (false) attack. That would have been the moment where we would have deployed additional protective measures (e.g. blocking the malware’s access of the Internet in order to download its malicious content). After about half an hour, that wave of attack would have been contained. But don’t count on that. Not every e-mail is part of our annual clicking campaign.

**Malicious Robots (2020)**

“Stop – Think – Don’t Click” is one of the standard pieces of advice when you are asked to click on links to unsolicited, unknown or dubious webpages, or when browsing the web in general. To paraphrase the words of Forrest Gump: "My momma always said, “[browsing the Internet is] like a box of chocolates. You never know what you’re gonna

\(^1\) In technical terms, the appliance is spawning virtual machines of different operating system flavours and e-mail clients, simulating user activity in opening the potentially malicious e-mail and its attachment, and monitoring whether this attachment “detonates”, i.e. starts modifying local system settings or making Internet connections (“call-backs” requesting the real malware).

\(^2\) For more details, check out this Bachelor thesis by T. Betz entitled “Comparing and Analysing the CERN E-mail Security Awareness Campaigns”.
get." Once again he is right. And here is a new twist in the way attackers try to dupe you into clicking on their malicious content… Captchas.

“Captcha" are a kind of online proof that you are a human being with human cognitive capabilities and not an automatic software algorithm (a so-called “bot”). Usually a Captcha verification asks you to copy a series of letters inside a distorted image, sometimes with the addition of an obscured sequence of letters or digits, or to identify a certain subset of photos within an array of many (“Select all pictures displaying cars”). In the age of the rise of artificial intelligence, big data and massive offices full of cheap office labour (in particular in third-world countries), one can start questioning how efficient and effective those Captcha verifications are, but for the attackers that is not the point. They just want you to click…

(Image: https://malwaretips.com/blogs/remove-notification-list-com/)

Their embedded Captcha dialog boxes look a bit different (see second screenshot). Once you click on them, your browser will pop up another window asking you for permission for the current website to be able to send notifications to you. And if you confirm, Captcha Gotcha. From that moment on, you will start seeing spam popups directly on your desktop even if your preferred web browser is closed. These can be ads for adult sites, online web games, fake software updates and unwanted programs...

Fortunately, notification permissions can easily be disabled again in the settings of any browser. In addition, you might want to consider improving your privacy when browsing the web (see our Bulletin article “Browsing securely and privately”). And, best of all: once more “Stop – Think – Don’t Click” when you are not sure where you are going: “Browsing the Internet is like a box of chocolates. You never know what you’re gonna get.”
Why the Internet is not Christmas (2019)

Maybe this is a bit far-fetched, but have you ever thought about the differences between the Internet and Christmas? The distinction between hyperlinks and presents? The contrast between clicking and unwrapping? Basically, in one word, it is trust.

Western-style Christmas has turned into a commercialized religious festival. Presents all over the place. Wrapped boxes. We are not discussing here whether this is good or not, we’re just talking about the love and affection that comes with being given a present. Because usually, the gifts presented to you come with goodwill and the goal of making you happier (apart from some nasty family members who never get it right and just want to annoy you). And in a spirit of trust, curiosity and fun, you open the wrapping in the expectation of more happiness being just around the corner.

Enter the Internet. Isn’t the Internet also a bit like Christmas? Behind every strange webpage, behind every newly received e-mail and attachment, behind every new post, might lurk more pleasure. Funny cat pictures. New music videos. Lovely Instagram stories. And we curiously click our way through post after post, photo after photo, swiping left and swiping right, scrolling, scrolling and scrolling even further down. Because what we get, what we see, can be funny and interesting, enriching and satisfying. Again and again. With our curiosity as a motivator. Hence, we click and click. Unfortunately, this is where the big difference comes in…

While at Christmas the gifts and presents (usually) come from people you like and love, respect and trust, the Internet is not necessarily like that. Trust is the key when opening up gifts and the same is true of browsing the Internet. But the Internet is anonymous. As a famous proverb says, “On the Internet, nobody knows that you are a dog”... And how can you trust a dog, or any other stranger presenting you with an unsolicited post, link, URL, webpage, e-mail or attachment? Instead of increasing your happiness, the malicious dogs of the Internet might want to try to bring you grief and pain: infect your computer, delete your data, steal your money, make fun of your photos, compromise your digital life and that of your family. On the Internet, you must be vigilant and careful when being presented with links, posts, URLs, e-mails, webpages or attachments. The Internet is not Christmas...

So, continue unwrapping your gifts, tear the wrapping into pieces, open your presents innocently and with curiosity, but hold back when it comes to the digital world. STOP – THINK – DON’T CLICK next time you receive an e-mail, next time you are about to open an attachment, next time you plan to download and install software, next time you want to click on that new link. Can you trust its originator? Can you trust its provenance? Can you trust that what you believe you’ll get is harmless and will make you happier? If so, go ahead. If you have a doubt, maybe just skip it this time. Or check
your suspicious e-mail, attachment, link or webpage with us at Computer.Security@cern.ch.

With those words, we wish you a calm and stress-free holiday season and a happy and cyber-secure 2020. Relax and, maybe, discuss with your friends and family why Christmas is much better than the Internet…

**When CERN.CH is not CERN… (2019)**

We recently received an e-mail from a colleague who was astonished to learn that an e-mail that appears to be sent from “CERN.CH” does not necessarily really come from someone at CERN… Indeed, everything is not always what it seems. Therefore, let us explain to you when CERN.CH is CERN and when it isn’t.

For e-mail, the sender address can be anything. Just like on the envelope of a normal hand-written letter, any sender address can be specified. “CERN.CH” can easily be spoofed so that an e-mail looks like it comes from someone at CERN, but actually doesn’t\(^1\). The ancient e-mail protocol cannot do better and any technical means to improve on this break other functions when sending e-mails (like posting to mailing lists…) – see our *Bulletin* article “E-mail is broken and there is nothing we can do”. There is no good protection apart from CERN’s SPAM filters. Once an e-mail has passed those filters, the second line of defence is you… So, just hold on a second and think about whether each e-mail is really intended for you. See our recommendations on how to identify malicious e-mails on the Computer Security Team’s homepage. If you’re really in doubt, just ask us to check by e-mailing Computer.Security@cern.ch.

And since we are already on the subject: no, similar domains with different endings (so-called top-level domains like .CH) are definitely not CERN’s! For example, browsing to CERN.CA gives you “…a non-profit organisation in Canada striving to promote the Francophone culture throughout the country”. CERN.BE points to a neuropsychologist. And CERN.SK is the webpage of a Slovak central register for work-related accidents… Moreover, there are also many other domains that look like CERN’s but aren’t: CERM.CH, CERN.ORG, CERN.CG, XERN.CH, CEM.CH (this one is more difficult to detect in lowercase as “cem.ch” – “r” and “n” look quite like “m”, don’t they?). These are usually called typo-squatting or Doppelgänger domains, i.e. domains whose name is just one character away from CERN’s. Attackers love them as they can be used to trick us into clicking on the wrong link: “cem.ch”, anyone?

\(^1\) For the technically-minded among you: checking the so-called header information does reveal the real origin of an e-mail unless this has also been heavily tampered with. If that information points to the CERN e-mail servers, it is most likely that the mail has been sent from a real CERN e-mail address. Still, there is no guarantee that the sender is the person behind the name in that e-mail address. His or her account might have been compromised. But that’s another story.
For your protection, since adversaries might try to use them for their malicious deeds, we have blocked a series of these typo-squatting domains within CERN’s domain name servers. That means that you should be redirected to a warning page instead of arriving at the adversary’s malicious one. However, this only protects you when browsing to those domains from within CERN. For a more holistic approach, we also tried to buy some of these domains in order to prevent any abuse, but didn’t succeed in all cases...

Therefore, once more, we have to count on you: security is not complete without you! Be vigilant!!! CERN is CERN.CH and dotCERN. Any other domain does not belong to the Organization¹ and should be accessed with care. The best thing is just to ignore these domains and go somewhere else. Or ping us at Computer.Security@cern.ch and we will check for you whether or not a domain is benign.

Click me – NOT! (2019)  

In late June, CERN was subjected to a wave of seemingly targeted e-mails containing a potentially malicious PDF or DOC attachment. Opening those attachments and eventually following the embedded links could lead to your computer being compromised (https://cern.ch/security/recommendations/en/malicious_email.shtml). However, this time, fortunately, these e-mails were part of the annual e-mail awareness campaign...

The e-mails sent by "Anne.Darenport-Smid@cern.ch", "Federico.Campesi@cern.org", "Michel.Dutoit@cern.com", "Ralf.Brant@cern.ch" and "Sonia.Abelona@cern.ch" were based on real malicious attacks against the Organization earlier this year. Back then, the e-mails contained a very short, rather generic text, along with a Word or PDF attachment. Opening that document would have started an unfortunate malicious chain of action against your computer, eventually leading to it being fully compromised. And with that, your professional life and even your and your family’s private life (see also “Protect your family”; https://home.cern/news/news/computing/computer-security-protect-your-family) would have been compromised. Worse, in those real attacks, the attackers were using the e-mail addresses of real CERN group leaders and sending their messages just to members of those leaders’ groups. Easy as pie, as CERN is quite open: many organigrams are public (just search for “organigram site:cern.ch”); as is the CERN phonebook and its advanced search feature, so filtering for members of a particular group is easy. And something else that is easy as pie: the e-mail protocol allows you to spoof any sender (just like you can easily spoof the name on a snail mail envelope, put a stamp on it, and – albeit not very cheaply! – “spam” any recipient). So

¹ For the pettifoggers among you: CERN does indeed own a series of other domains: e.g. CERN.EU, CERN.JOBS and CERN.ORG, but also CiXP.CH, INDICO.GLOBAL, OHWR.COM, REANA.IO, ZENODO.COM. But mentioning all of those would double the length of this article...
there it is, your targeted attack on the group of your choice... Fortunately, then, our e-mail filtering systems detected those malicious attachments in good time and prevented any havoc...

Based on those attacks, the CERN Computer Security Team sent similar e-mails to about 22 000 owners of CERN e-mail addresses, all within the space of 90 minutes. The sender addresses, i.e. "Anne.Darenport-Smid ", "Federico.Campesi", "Michel.Dutoit ", "Ralf.Brant" and "Sonia.Abelona" (all fake, of course), sending domain ("cern.ch", "cern.org", "cern.com", "cerm.ch" and "cem.ch") and the contents ("your input to our results", “report on pension fund balance situation”, “confidential design report”, “new IT security measures”, “your 2019 contract amendment request”) were randomly assigned. In addition, half of the recipients got an e-mail with a Word .DOC attached, the other half one with a PDF. In both cases, the documents were literally empty: the Word document claimed to be “created in a different version of Microsoft Office Word.” and stated: “In order to view this document, please click the “Enable editing” button on the top bar and then click “Enable content”” – a technique to bypass Microsoft Office’s basic protection mechanism. To no avail, as that document also offered the option to “View document online: https://client.microsoft.com/en-us/office365/?id=0e49-f8242b-a3” – leading to a page controlled by the attacker and certainly not hosted by “Microsoft.com”. The PDF just asked users to “Please click the link below to access your PDF document.” – leading to a similar page to the one used for the Word document.

This document was created in a different version of Microsoft Office Word.

In order to view this document, please click the “Enable editing” button on the top bar and then click “Enable content”.

View document online: https://client.microsoft.com/en-us/office365/?id=0e49-f8242b-a3
Empty or not, however, it doesn’t matter. Just by opening the document, you would have put your computer, laptop, tablet or smartphone at risk (“I love you”; https://home.cern/news/news/computing/computer-security-i-love-you) – and, indeed, 17% of all recipients did (21% for the DOC; and more than 14% for the PDF). By clicking on the embedded link, the chances of your device being compromised would increase even more (“Curiosity clicks the link”; https://home.cern/news/news/computing/computer-security-curiosity-clicks-link). In total, 10% of people managed to ignore all the security features (e.g. clicking “enable macros” in Word or following the link in the attachments) and reached our dedicated information page (https://cern.ch/security/malicious_attachment.shtml). By this point, their device would have been compromised. Lucky for them that this was “just” an awareness campaign. Looking in more detail, the attachment on “your 2019 contract amendment request” generated more clicks (i.e. 24% opened it), while the “confidential design report” and the “new IT security measures” were more likely to be ignored (15% each). Also, people spotted the malicious domains “cerm.ch” and “cern.org” easily and refrained from opening the attachments (only 15% and 17% did, respectively), while the “cern.ch” domain of course looked legit and led 20% to open the attachment… And in terms of the different departments? The trophies go to the FAP department and the Pension Fund, whose click rates were way below average. Well done, folks! For everyone else, next time, beat them: STOP – THINK – DON’T CLICK should be your mantra, in particular for e-mails which look weird, come from unknown sources, contain blatant typos, or are just not really relevant to you… Hints on how to spot this kind of
malicious e-mail can be found on our computer security pages (https://cern.ch/security/recommendations/en/malicious_email.shtml). And if you spot such a malicious e-mail, forward it to us. Once we know about them, we can block the malware from being downloaded and thus protect everyone at CERN. In this particular campaign, it took just a few minutes until the first alerts were received by the Computer Security Team. Blocking would have dropped the click-rate to below 2%, unless you happen to click on the link outside the CERN network – a location where we can’t provide any protection…

Browsing securely and privately (2019) 

Besides clicking on links in malicious e-mails or opening dubious attachments, browsing to the wrong webpage is the second major way of getting your laptop, your account and your data compromised. One click on the wrong link, just one malicious URL, and your laptop gets infected, your password exposed, your data encrypted or stolen… Remembering to STOP – THINK – DON’T CLICK prior to opening a link is the conscious, responsible way to protect yourself. And a good choice of well-secured web browser can provide you with a second way of keeping your digital life in your own hands!

Indeed, think of your laptop – leaving aside your smartphone for a moment – as one of the digital centres of your life. If an attacker takes over your laptop (or smartphone), he or she owns your data; can use your embedded webcam to watch you (even at night!); can use the embedded microphone to listen to your conversations; can access all locally stored documents, photos and films; can spy on your keyboard and extract the passwords you type on it – and hence, write your Tweets, make your Facebook posts, buy stuff on Amazon and access your Internet banking. Frightening? Indeed it is (see our Bulletin article entitled “Protect your Family” for more on this).

The best way to protect your web access – your browsing of the World Wide Web – is to use a well-supported and up-to-date web browser like Chrome, Edge or Firefox. From the security perspective, Google’s implementation of Chrome clearly separates every individual website you access and thus follows best security practice. Mozilla’s Firefox Quantum has also started to employ a similar functionality, while Microsoft’s Edge browser does not (and never will). Especially if you have the default auto-update mechanism enabled, both Chrome and Firefox can be considered to be the most secure browsers currently on the market (as well as some variations of them like Brave). Firefox might well have a slight advantage thanks to a feature being added in the upcoming version 67: it will actively block the misuse of your laptop for unauthorised crypto-currency mining as well as stopping services that track your online activity.
So what about the privacy side? Both Chrome and Firefox come with a plethora of plugins making your browsing experience more secure (“HTTPS everywhere”) and more private (“Ghostery”, “uBlock Origin”, “DuckDuckGo Privacy”, “Privacy Badger”, “Privacy Possum”). You just need to install them via “chrome://extensions” or “about:addons” respectively. And, of course, permanently engaging the “Incognito” or “Privacy” mode makes your browsing more stealthy (but beware, not 100% stealthy; you would need to use, for example, TOR’s “Onion” browser for much better anonymity). However, the major difference between Chrome and Firefox is that the former is a closed-source product of one of the world’s biggest data aggregators and the latter is an open-source browser maintained centrally by a community foundation. Out of the box, Mozilla’s Firefox is a much more privacy-preserving alternative to Google’s Chrome browser. Google operates an extensive data-collection ecosystem in which its search engine and a vast array of other products and services are used to build a profile of a person’s interests by tracking users’ online activities. Red pill or blue pill. Take your pick. But choose wisely.

A free click for your awareness (2018)

After our Bulletin article entitled “Curiosity clicks the link” at the end of February, our annual “clicking campaign” followed on one month later. Based on e-mail templates created by students of the University of Rotterdam, using only information they were able to find on CERN’s public webpages, 20937 “suspicious” e-mails were sent, to everyone with a CERN e-mail address. Many reported these malicious mails to us immediately, a few detected them as our awareness campaign, and some recipients clicked…

Are you still curious? Learn from examples of “Phishing mails” provided by a “David.Marquinais @ cerm.ch”; verify your e-mail address for “CERN Lightweight Account verification” (“support @ cern.com”); check out your account for the “Cern Pensions update” sent by “head.office @ cem.ch”; or answer the “CERN Students & Educators evaluation email” from “outreach @ cem.ch” in order to comment on their new website… Yes, many sender addresses do not make sense. “David Marquinais” as “Head of User Support” and “Fabien Delacroix” as “Head of CERN” do not exist at CERN. Neither do “cern.com”, “cem.ch” (which looks like “cern.ch” when displayed in small fonts). CERN only uses “cern.ch” and “.cern” (dotCERN). If you read the corresponding mail bodies, the embedded links look weird and have no apparent ties with CERN. But this is what the malicious evil-doers (in this case the students from Rotterdam) try to do: to lure you in believing the mail is genuine. To make you click. To fall for it. To fail.
Clicking had no negative consequences... this time. But in reality, with real malicious e-mails, with one click, your computer would have been lost. Infected. Compromised. With one click, the malicious evil-doers might be able to install software on your Windows PC/laptop or Macbook (less likely on Linux systems), which register every keystroke you make in order to figure out passwords to your Facebook account, your Twitter feed, to access CERN or for accessing your bank details. Attackers will enable the webcam and the microphone in order to spy on you. They will download your documents, encrypt them in order to obtain money from you, and if you don’t comply make those documents public. Game over.

Luckily it was just a clicking campaign this time, as we would have had a “game over” for 15.2% of the recipients. 15.2% clicked on the embedded links. Their compromised Windows PCs/laptops or Macbooks would now pose a threat to the Organization. Compared to previous years, this is a decrease from 18.7% in 2017 (16.5% in 2016). Other industries have reported similar “click rates”. But in the end, the number doesn’t really count, as the “click rate” scales with the level of sophistication of the e-mail. Targeted and well-engineered e-mails are harder to spot, and the “click rate” would be higher. Also, to be fair, many people informed us immediately after they received a suspicious e-mail. Thanks to them, we would have quickly been able to block any malicious website, URL or e-mail. Thanks to them, we would have been able to warn others. Of course, this time we let it go. But in reality, a quick heads-up send to us at Computer.Security@cern.ch can crucially help to secure CERN and minimise impact.

Hence this awareness campaign, helping you to identify strange e-mails early, be more vigilant, and avoid clicking before you lose your private data. And before you give the malicious evil-doers access to CERN. Just be reasonable. While it is difficult to protect yourself from the more sophisticated and targeted e-mails, protect yourself against the “easy” ones. It is like in the real world. If a stranger offers us, for example, a small bag of white powder and asks us to carry it across the border, we decline and walk away, don’t we? It’s the same in the digital world: if an e-mail, its sender, its context, the language, the way it is phrased, the embedded links and URLs, etc. look weird to you, just do not click. Delete it. Or, if in doubt, send it to us for verification. If it looks malicious, give us a heads-up!

Curiosity clicks the link (2018)

Oh, how wonderful e-mails are. And chats. And the web. All this interconnectivity. Blue lines underneath keywords everywhere. Links. URLs. Redirections. All taking us to more information. More cat photos. More distractions. Awesome. Like Christmas, with presents and yet more presents to open. An infinity of presents. But some presents might result in a rude awakening...
The underlying assumption in the above is that you trust the originator of the e-mail, the chat or the webpage, the creator of the blue line, the links and the URLs ... and Santa Claus for the presents. But what if you shouldn’t? Would you enter a shabby bar in a dark alley downtown (and risk getting beaten up)? Would you dare put your hand in a rabbit hole (and risk getting bitten by a fox hiding inside)? Would you accept a parcel from a stranger (and risk going to jail if it turns out to be a package of drugs)? Would you take the red balloon from Pennywise the clown and follow him around the corner?

Surely not! But why is it that many people still throw this “surely not” over board and click on random links in random e-mails from unknown senders, on random attachments from unknown authors, on random webpages of unknown origin? With one wrong click, your computer might get infected. With one single infection, your digital life gets exposed. For many of us, our computers, and even more so our laptops, smartphones or tablets, are the central digital focal points of our lives: we store our personal photos and videos on them, as well as lots of private documents, and we use them as a central hub to access our bank accounts, to communicate with our closest friends (on Facebook or Twitter, or via video or audio streams) or to consult our favourite health applications to check out our well-being. One single infection and all those photos, videos, documents, bank accounts and communication channels, as well as access to our webcams, microphones and medical information, are in the hands of people with malicious intent. Goodbye data, goodbye privacy, goodbye digital life (see our Bulletin article Enter the next level: Doxware).

So, be sensible! If you’ve just got divorced, a love letter from your ex-spouse doesn’t make sense. Neither does an attachment from Deutsche Telekom if you’ve never lived in Germany, or an e-mail in a language you’ve never spoken. Your favourite celebrity will never send you naked photos and your bank will never ask you to reset your password. And the advert promising you thousands of dollars for no work is a scam, like anything else offered to you “free” on the internet. Read more about identifying malicious e-mails here.

Hence, only the curious click the link – and put their digital assets at risk.

The Higgs does not... send mail! (2017)

“The Higgs boson does not exist!” stated an e-mail recently sent to many of our colleagues within CERN as well as with our global research community. We can definitely enter in a technical discussion about physics results produced by the LHC. But here, this is not the point. As many recipients noticed, this e-mail appeared as having been sent from an e-mail address “Fabiola.Gianotti [at] cern.ch”, i.e. the address of our Director General. However, no worries! The mail has not been sent by
her. And her account has not been compromised. Rather, the issue lies in the technical ways the email protocol is working and – like in this case – can be abused...

Technically, e-mails are delivered like normal “snail mail” letters. In a normal letter, you can put whatever contents or opinion you want. Love letters, or threats. True statements, or fake news. And you can put any sender on its envelope, as well as any purported sending address --- not necessarily yours, but that of someone else, like that of our DG… Finally, but rather obvious, e-mails can be sent to any valid (and invalid) e-mail addresses. Due to our open and academic nature, CERN email addresses are published through the CERN phonebook and are available through many other webpages: conference participation lists, experiment memberships, service manager lists, on-line/shifter duty lists...

Therefore, there is no good technical measure¹ to generally prevent such e-mails if sent from a fake (“spoofed”) e-mail address world-wide. Also, locally for the protection of CERN mailboxes, this is not as easy. While the SPAM filter tries to catch such fake emails, the attacker repeatedly made many modifications in order to bypass those filters (the attacker even expressed his frustration with our filtering when sending a few mails with the subject “[…] you Service Desk”). Thanks to our email service managers, they engaged in that cat-and-mouse game… Mostly with success, but sometimes with mails going through. Apologies for that.

STOP spam! (2017)

Did you know that about 83% of all messages destined for CERN are flagged as spam and rejected? The IT department’s e-mail service works hard to overcome the permanent wave of spam messages trying to pour into CERN… just recently, we deployed a dedicated appliance that automatically analyses our e-mails for malicious content. But in the end, some spam, particularly the most sophisticated messages, makes it though. At this stage, it is up to you to identify it. Here are some ideas to make your lives easier.

Of course, there is our usual advice: “STOP – THINK – DON’T CLICK” (“Protect your click”) and our campaigns for spotting malicious e-mails (“One click and BOOM… (Reloaded)”). On the other hand, why not reduce e-mail traffic in general and make our lives easier when we are trying to identify genuine and valid e-mails?

- First of all, let’s stop spamming ourselves over and over again (see also “Save our inboxes! Use e-mail wisely”). While the “CC” and “BCC” fields leave plenty of space to fill up, do we really need to add everyone and his or her dog?

¹ For the technical people: yes, “SPF”, “DMARC” and “DKIM” might theoretically help, but all those methods come with drawbacks resulting in delivery or compatibility problems, especially with standard mailing lists (see the experience made by Yahoo! in 2014). But that might get better in the future as e.g. mailing list software is trying to adapt (https://wiki.list.org/DEV/DMARC).
Shouldn’t we limit ourselves to sending e-mails to those that have a need-to-see? Do we really need to click “Reply All” just to say “Thank you” to the sender – in particular if you “Reply All” to an e-group with hundreds of members! Also, 100 people in the “To” or “CC” boxes does not make any sense and might be an invasion of privacy. Here, the “BCC” box is better. And, is the e-mail (and any ping-pong e-mail exchange!) necessary at all or wouldn’t it just be nicer to visit the recipient and buy him or her a coffee?

- Signing e-mails using your CERN certificate would help too. On the basis of your digital signature, the CERN recipient can be assured that the e-mail has really been sent from your CERN e-mail address and not been spoofed by a malicious attacker… You can easily enable e-mail signing by following these instructions. The only limitation is that, as CERN certificates are currently not recognised outside CERN, this signature only works for CERN mailboxes…

- Finally, if you manage a system for sending automatic e-mails (on behalf of CERN), don’t make them look like spam! The sender should clearly point to your service (and not be an obscure tag). Ideally, the sender should be listed in CERN’s phonebook; the subject should be clear and precise; the introduction should directly address the recipient by his or her name used at CERN (as listed in the phonebook); the message text should be flawless, contain no typos, and be precise; embedded URLs and web links should be written out in full and should point to websites hosted at CERN (starting with “HTTPS://cern.ch/…”); attachments should also have clear titles and should be introduced in the text; and your e-mail should have a signature that makes it clear from whom and why this e-mail has been sent.

While these steps won’t eradicate external spam, they could reduce internal “spam” and allow us to focus on “real” e-mails. If you still receive spam, please report it to spam-report@cern.ch (or submit a ticket).

One click and BOOM… (reloaded) (2017)

Browsing the World Wide Web is not as easy as it seems… One wrong click and all your passwords (CERN, Facebook, PayPal, Amazon, etc.) could be stolen; all your activities could be clandestinely monitored (mouse movements and clicks, words typed, screenshots, microphone and webcam recordings, etc.); confidential documents could be stolen; and an attack path (a so-called back-door) into CERN could be opened… As a result, you would have to reinstall your computer from scratch and change all your passwords! One of our colleagues learned this the hard way. One wrong click in summer 2015 permitted malicious attackers to infiltrate CERN but, fortunately, no real damage was done. Still, the cost of investigating the incident ran to
several tens of thousands of Swiss francs and a lot of time was wasted trying to understand the attacker’s intent and the extent of the infiltration...

With the goal of increasing more awareness of the risk of clicking on links in unsolicited e-mails, the Computer Security Team recently re-ran the “Clicking Campaign”, sending fake e-mails to you and your (our) colleagues, intended to lure you into clicking on the embedded link. Once an unfortunate, imprudent victim clicks, they are led to an informative webpage explaining “how to identify malicious e-mails” (see the image). Of course, this click rate is proportional to how sophisticated and well-targeted the e-mail is: the more convincing the look and content of the e-mail, the higher the probability of a click (up to a point where a distinction is possible only by experts). Therefore, in order not to be biased (we can easily design e-mails which you will definitely click), we reused the fake e-mails designed for us by students at the University of Rotterdam for last year’s campaign. Then, their boundary condition was to use only information that is publicly available from CERN’s webpages or from their own imaginations. Still, the results were frightening. Some suggestions were so well-designed that more or less everyone at CERN receiving them would have clicked. Experts would call this a sophisticated and targeted attack, a so-called Advanced Persistent Threat (APT). In the end, we selected five fake e-mail suggestions that we deemed to be basic, simple and "easily" identifiable as malicious by the recipients...

The click rates, however, told a different story. Once more, we got an average click rate of 18% (comparable to last year’s number)! One in five recipients clicked on the link... If those e-mails had been real malicious messages, clicking would have meant: computer infected, all local activities monitored, password stolen, data lost and an attack platform into CERN opened. That one click could have had severe operational and financial consequences for CERN... So if you fell for this scam, and our sincerest apologies if you did, let us explain to you how you can better identify such e-mails and
what consequences clicking on such a malicious link might have for you and your
digital assets:

On the positive side, many people identified those fake e-mails for what they were:
malicious. We got hundreds of ServiceNow tickets notifying us of "some malicious
mails going around". Well done, folks! In any case, stay vigilant and take care. Only
click once you are sure. If you are in doubt, contact us at Computer.Security@cern.ch.

And keep in mind: we might run a similar campaign next year with some more
sophisticated e-mail messages…

Protect your click (2017)

Today, "links" are the main threat to your operating system and, consequently, to your
professional and private data. With one single “click”, an attacker can compromise your
device and start snooping on your life. While we still rely on you to click with care
(remember – “Stop – Think –Don’t click”), the CERN IT department is preparing
additional measures for your protection.

Indeed, malicious links or URLs embedded in websites or e-mails, as well as malicious
PDFs (attachments or downloads) can take advantage of the inherent vulnerabilities
in your operating system – most likely if you are running a Microsoft Windows operating
system or have an Android Smartphone, but still possible if you run MacOS, and not
fully impossible with Linux or Apple iOS. Following your innocent click on a malicious
link, URL or PDF, a well-crafted piece of software is executed that anchors itself in
your operating system and clandestinely takes control.

With this unfortunate click, the adversary now has access to all your locally stored data.
Software. Documents. Photos. Videos. Reading your e-mails. Snapshotting your
activities. With your unfortunate click, the adversary might enable your webcam and
your microphone. Watching and listening to you. With this momentous click, you are
naked. Your life is exposed. And the chances are low that you will even detect it…

Last year, a dedicated clicking campaign using untargeted and irrelevant e-mails to all
CERN people resulted in a 20% click-rate. 20%! This means that an attacker would
now own up to 20% of CERN PCs… Fortunately, this was part of a campaign we ran
to help you understand the risks of clicking (One click and BOOM…). In summer 2015,
we weren’t that lucky. A targeted attack, starting with two malicious e-mails, kept the
Computer Security Team busy for two months and caused some non-negligible costs
for the Organization. Fortunately, given the potential risk, damage was very limited.

In either case, “Stop – Think – Don’t click” is your – and CERN’s! – First line of defence.
If you receive e-mails that are not addressed to you, not in a language you usually use,
with weird or unrelated content, full of typos, with a sender whose e-mail address looks
completely different, take care! This might be such a malicious e-mail (for more details
on how to identify malicious emails, click here). But you are not alone. The IT department has recently deployed a dedicated device automatically analysing all our e-mails for such malicious content. The “Fireeye EX” device even simulates user activity trying to trigger any malicious activity in the e-mails sent to us. And since malicious PDFs are one of the main attack routes, plans are currently being made to replace our current solution with a suitable and safe alternative. This would replace a notoriously vulnerable software package with something much less likely to be targeted. Finally, the IT department is currently working on better reinforcing Windows PCs so that they are less susceptible to unfortunate clicks, while making this completely transparent for you. A draft of such guidelines can be found here. But beware, for the moment this is for the experts and for very specific use cases only!

Watch where you “click” to stay secure!

E-mail is broken and there is nothing we can do (2016)

Have you ever received an e-mail from a friend or someone you know and been surprised or appalled by its contents? Or, worse, have you have received a response to an e-mail that wasn’t written by you? Maybe with similarly surprising or appalling contents? If yes, welcome to the insecurity of the mail protocol, where nothing is as it seems...

No, this time we are not talking about “phishing” or malicious attachments but the very basics of the e-mail protocol. “SMTP” aka the “Simple Mail Transfer Protocol” is exactly what it says: very simple! In many respects, e-mails are identical to physical hand-written letters: you cannot deduce from the sender’s address nor from the message text whether it has really been sent by that person. Impersonation has never been as easy as with the SMTP protocol. Due to its simple design, I can pretend to be Mickey Mouse, Harry Potter or anyone else, and send you text messages resembling or contradicting Mickey’s opinion and thinking, deeply offend Hermione, bluntly lie to you, or try to lure you into disclosing secrets to me like your password (“Phishing”, you may recall). But the risk is not only that you are spammed with unwanted messages, the bigger risk is that I can diminish your reputation by sending offensive, weird or embarrassing e-mails in your name...

And there is not much we can do on the mail service or security protection side. E-mail address spoofing is permitted by the protocol. Technically, we cannot block or filter legitimate, but misused, sender addresses – that would deeply affect the free communication of legitimate users with/to/from CERN. For the same reason, we

---

1 The mail industry is trying to solve this issue with new restrictions like the SPF, DKIM and DMARC initiatives. However, as mailing lists can be incompatible with these new security features, none of them have been widely deployed, so far at least...
cannot just block certain mail server addresses. And we shouldn’t, if we value the academic freedom of CERN (see our Bulletin article on “WWW Censorship? Not at CERN”). In order to combat malicious e-mails, we will soon deploy an advanced filtering engine, which will dynamically analyse all e-mails for malicious content and reject any problematic messages. But this will not cover e-mails that arrive with somehow legitimate and valid content – even if this content is wrong, offensive, contradictory, etc.
The Royal Swedish Academy of Sciences is sending this letter to physics departments around the world exposing the fraudulent use of email addresses belonging to Academy members.

This implies that we all have to live with this kind of SPAM. And that we have to live with the fact of someone writing in our name… And hope for the recipients that they contact you to inform you of the nonsense they’ve received so that you can rectify the problem. Conversely, if you really want to be sure that the mail you just received is legitimate and comes from the person who it claims to be coming from, use common sense. Are you expecting such a mail from him/her? Do the content and context make sense? Could you call him/her to cross-check? Or, for the more technophile among you, digitally sign your mails so that the recipient can verify their real origin - you: for Microsoft Outlook, for the Mac OS mail client and for Thunderbird. Dedicated instructions for using S/MIME at CERN can be found here.

WWW censorship? Not at CERN (2016)

Whoops! We received a number of critical responses to our previous article on the upcoming DNS firewall (“DNS to the rescue!” - see here). While they were mostly constructive, the main question was “How dare we censor Internet access?” Let us clarify this.

Computer security at CERN must always find the right balance between CERN’s academic environment, its operations and security itself. Of course we can easily overdo it one way or another, but that would kill our academic freedom and bring the Organization to a halt. That certainly isn’t in our interest. On the other hand, CERN is permanently under attack and we have to do everything possible to ensure that those attacks are kept at bay. Otherwise they could impact CERN’s operations… So, have we found the right balance?

Concerning access to the Internet and in particular to the web, we have not and will not block random websites because of their content unless – and this is crucial – unless the website hosts malicious content that could impact the operation of CERN’s computers or accounts. Malware hosting sites are a good example, as browsing onto such a website might infect a large number of CERN Windows or Mac computers. This is why we blocked the website “20min.ch” a while ago (see our Bulletin article “Drive-bye” on this subject). Sites resembling the CERN Single Sign-On webpage and deliberately created for phishing attacks against CERN are also blocked as a protective measure. And we block Doppelgänger domains, i.e. domain names which resemble those of CERN (like “cem.ch”) or are just one typo away from CERN’s (like “cern.cg”, etc.), in order to protect you against typo-squatting.

But that’s it. We do not block webpages because of other, arguably undesirable content, whatever “undesirable” might mean. For example, we do not filter
pornographic sites. Of course, the consultation of pornographic content violates the CERN Computing Rules and CERN’s Code of Conduct and I doubt there is anyone at CERN with a professional need to consult such material, but we do not block them (just monitor their illicit usage). Hence, in response to the question: “How dare we censor Internet access?” the answer is: “We don’t dare: we do not censor at all. We believe in and value academic freedom at CERN and aim to balance our computer security measures accordingly.”

“New_invoice.zip” (2015)

Thanks for reading this. But I wonder, what do you expect? Why did this generic title catch your interest? Of course, you might read our articles on a regular basis and it is the “Computer Security:” that brought you here. But still, was there anything else? You should stop reading here... unless you believe this text is meant for you. Or if you are curious. Or if you expect to learn something. Actually, that’s it. “New_invoice.zip” taught more than 40 people at CERN a lesson... the hard way.

“New_invoice.zip” was the name of an attachment to a rather blunt e-mail sent directly to many of our dear colleagues. Others received the e-mail via mailing lists like “it-dep”.

![Image of email with attachment](https://example.com/image.png)
The subject of the mail was “invoice” and its message read “Check the document”. The recipient list was vast and full of many different, not necessarily connected names. Clicking on the attachment “New_invoice.zip” revealed another file named “invoice_id25769.exe” (see Image 2) - a file that, if clicked on, infected your Windows computer.

Unusual? Unfortunately not. Sending and receiving invoices is common business in secretariats, in the procurement service, in the hostel and the CERN restaurants... But remember our repeated warnings about phishing e-mails with malicious content. This e-mail is a prime example. Still, more than 40 people clicked thrice in order to get at the juicy contents: first to open the mail, a second time in order to look at the attachment, and then to open (and execute) the “invoice_id25769.exe” programme. Game over: Windows PC infected. User password lost.

What could have prevented those people from clicking? First, many just opened the attachment out of curiosity: “It came from a colleague and I just wanted to know...”, even if it was unusual. Neither were the brevity of the message text and its rather common subject line a hindrance to continue. Nor was the fact that this “invoice” was addressed to dozens of people. Why should all of them have gotten the same invoice? Another red alert missed.

Finally, the “.zip” file contained an “.exe” file. Do you know what an “.exe” is? No? So, why open it? “.pdf”, “.doc”, “.xls”, “.ppt” or “.txt” will do, but never open “.exe”! “.exe” in an e-mail is a synonym for “infect my computer”. And so, this “invoice” created a nice learning opportunity for more than 40 colleagues (and counting!). Their 40+ accounts and their 40+ Windows (office) PCs were blocked after their mail client started spamming the world with similar messages. 40+ Windows PCs were subsequently reinstalled and 40+ new passwords were created. 40+ people got annoyed and lost precious working time. Just because curiosity beat vigilance...

So, be prudent and be aware:

- If you aren’t expecting such an e-mail, if it is none of your business - just ignore it;
- Is the message text reasonable? Does it ring a bell? Does it apply to you? Is it in your native language or a language you usually communicate in? Are there typos or factual mistakes (“Rolf Heuer, CERN President”)?
- Check the recipient list. Was this an e-mail for you or is the mix of recipients weird? Why should you all get the same e-mail?
- Look at the attachments. “.zip” or “.exe” files are highly suspicious as they hide their real, malicious nature. And no, your anti-virus does not always protect you;
- If you are in doubt, contact the sender and cross-check before opening the attachment. Or check with us at Computer.Security@cern.ch;
Be prepared. A malicious e-mail will infect your computer. Make sure that you have proper back-ups so you can easily re-install it from scratch at any time. Just like our poor colleagues were asked to do…

Well fought, FP! (2015)
http://cds.cern.ch/journal/CERNBulletin/2015/06/News%20Articles/1983586?ln=en

We are used to spam and phishing emails. But at the end of last year, a very special email struck one of our colleagues in the FP Department.

An accountant was gently asked in an email from “Rolf.Heuer@cern.ch” to prepare a financial transaction - in the strictest confidence. A phone call from the beneficiary to the accountant was made in an attempt to support this request. Despite being instructed not to talk to anyone, the e-mail, the phone conversation and the circumstances were all so suspicious that our colleague consulted his hierarchy, the internal audit service and us. Well done, FP Department! This is a rare case of an attempt at “social engineering”, i.e. luring someone into doing something detrimental to the Organization.

The e-mail was fake. While it appeared to come from “Rolf.Heuer@cern.ch”, it actually came from an alleged fraudster outside CERN. The e-mail and the phone call showed that he was well prepared and directly focused on this particular accountant. Besides the technical details for the transaction, this scam e-mail also contained every element needed to succeed: complimenting and trust-building (“Nous effectuons en ce moment une opération financière importante sur laquelle je travaille depuis quelques mois. Je vous ai choisi pour votre discrétion et travail irréprochable au sein de notre société car je ne veux aucunes fuites.”) and the requirement for strict confidentiality (“Cette OPA (offre public d'achat) doit rester strictement confidentielle, personne d'autre ne doit être informé pour le moment, y compris vos collègues.”, “Merci de ne faire aucune allusion en interne ou externe sur ce dossier, ni même par téléphone. Je suis en séance toute la journée, je vous le répète veuillez communiquer uniquement par courriel avec [FRAUDSTER] selon la procédure imposée par l'AMF (autorité des marchés financiers).”) But our colleague did not succumb! (“Michelin” seems to have not been so lucky).

So remember, the e-mail protocol does not provide any protections against fake sender addresses. Unless your sender digitally signs his or her emails, you can only tell from the overall package (sender, subject, message, and circumstances) whether it is a legitimate e-mail or a scam. Note that you are the first line of defence in those respects. If you have any doubts, consult a colleague, your supervisor or Computer.Security@cern.ch. This particular case is a prime example of how professional vigilance works!
“Conpherencing” — the new phishing (2014)

CERN is regularly the target of so-called “phishing” attacks, where troublemakers with bad intentions send fake emails to CERN people to try to lure them into disclosing their CERN passwords (or other passwords). Fortunately, few people nowadays fall into such traps. Simply remember to treat your password like your toothbrush: don’t share it and change it regularly (see our Bulletin article “What is a good toothbrush, erm, password?”).

But do you know about “conpherencing” (yes, with “ph” in the middle)!? “Conpherencing”, a term coined by us, is like phishing, but instead of a fake login page, it uses a full-blown conference website resembling that of a popular mainstream conference. Similar to the webpages described in our “Jekyll or Hyde? Better browse securely” article, this evil twin includes a scientific programme, details of a committee, sponsors and abstract submission dates.

For example, the ICNFP2014 conference appeared to exist in duplicate: the real webpage of the conference, which will take place in Crete, is on CERN's Indico site (below, screenshot on the left), while its evil twin (on the right) said that it would be in Istanbul. A closer look revealed that (at least) one sponsor was not aware that they had been named as a supporter of that event and refused to be involved once they found out, and some of the “committee members” listed don’t appear in the phonebooks of the universities with which they were supposedly affiliated. This twin webpage even copied the conference summary text! The same web server also had fake pages for many other conferences: ICN2014 (on nanotechnology), ICECE2014 (electrical and computer engineering), ICC2014 (chemistry), ICM2014/ICSMS2014 (maths), ICP2014 (physics), …
Thus, as with all your activities on the Web, please be vigilant: stop and think before you click! Too often, a website’s real purpose is not what you think it is…

Jekyll or Hyde? Better browse securely (2013)
http://cds.cern.ch/journal/CERNBulletin/2013/21/News%20Articles/1546809?ln=en

Surfing the web is like walking through London in 1886. Usually you meet nice Dr Jekyll, interact with him and everything is fine. But at other times, at night, you might encounter the malicious Mr Hyde. He just wants your money and your secrets, and wants to take advantage of you.

As in the novel by Stevenson, good and bad web pages can be very close together. Most web pages exist to provide information or a service. But one click away, one Google page down, there are malicious web pages that aim to steal your password, infect your computer, or lull you into disclosing personal information.

So remember: “STOP - THINK - CLICK!” should be the standard when browsing the Internet. If you are presented with a link that looks strange or contains gibberish (like http://211.268.156.277/.PayPal/cgi-bin/wbsrcmd_login.php), just ignore it! It is always better to type simple, comprehensible web addresses like “www.paypal.com” than clicking on obscure links. If you are asked for your password, be vigilant and think about whether this is justified (and do not use your CERN password on other sites!). Also, first check whether or not the connection is secure, i.e. that the web address starts with “https” and not just with “http” without the “s”. Otherwise, private correspondence and passwords can be intercepted by a malicious third party.

Also take care when typing a web address. “CERN.CH” is of course not malicious, but just one typo away and you might accidentally enter “CERN.CG”, “ERN.CH” or “XERN.CH”. These are not under our control. Many companies have bought those so-called “Doppelgänger domains” or “typo domains”. At CERN, we have blocked the obvious ones in the CERN domain name server, so you will not be able to visit them from CERN. But at home, be vigilant!

Browsing the Internet: Good-bye anonymity! (2012)
http://cdsweb.cern.ch/journal/CERNBulletin/2012/22/News%20Articles/1450931?ln=en

Do you consider browsing the Internet to be your private business? When visiting random web-sites, how far do you assume you are anonymous? Would it matter to you that Google or Facebook can profile your browsing behaviour in order to better target you with advertisements? Did you notice that you already get targeted ads when you are logged on to Google or Facebook even if you are visiting completely different websites? If matters to you, note that browsing anonymously on the Internet is far from easy.
When you are connected to the Internet, you give away a variety of information: your PC’s IP address, some browser settings like language or screen size, and, probably, your login information. So how private is private?

You might argue that your current IP address has been picked from a pool of addresses and therefore regularly changes, so it does not necessarily always pinpoint you. On the other hand, with the dawn of IPv6 there is no need any more for shared IP addresses as the pool of IPv6 addresses is considered non-exhaustive. With IPv6, you might get a permanent IP address assigned. Privacy... game over. The best chance regarding this will be legislation. Already today, IP addresses are considered to be personally identifiable information (PII) in some European countries, which means that storing IP addresses for profiling purposes is illegal. However, to be sure, your best option is to use so-called “anonymisation services”, but this depends how much you trust them!

Then there is the too talkative browser. Depending on which browser you use, it already exposes lots of information: the local language, time zone, screen size, installed plugins, available system fonts, etc. As these settings can vary a lot, it means that the probability of you and I having exactly the same settings is very low. Ergo, this information can be used to pinpoint your browser and uniquely identify you when browsing the web... If you don't believe it, check out Panopticlick and note that some browser plug-ins like “Stealthier”, or security settings like “In Private” browsing might change the odds in your favour.

Finally, your login. If you are logged in with your Google or Facebook account, they can profile your activity even outside their domains. This is mainly due to the wide usage of Google Ads/Analytics and Facebook’s “Like”-button: the embedded code directly feeds back into your Google and Facebook profile... For a bit more privacy here, log out whenever you don’t need to be logged in, and consider installing something like the “Ghostery” plug-in in your browser.

So what else can you do? Not much, as I am not suggesting that you change your browsing habits. There is no silver bullet. I just wanted to take away the illusion that you browse the Internet anonymously. You don’t and you hardly can.

Don’t let your mail leak (2012)
https://cdsweb.cern.ch/journal/CERNBulletin/2012/18/News%20Articles/1442980?ln=en

At CERN, data privacy is of paramount importance, and we are currently developing a comprehensive data protection policy. For example, your CERN mailbox and your “private” folders on AFS and DFS are considered yours...

You might feel like you have nothing to hide, but we are not only talking about personal e-mail: data privacy also pertains to financial mail (acquisitions, tenders), mail related
to HR (contracts, assessments), medical information, etc. As this is considered “private” even if it is work-related, the data cannot normally be accessed by your supervisor, the AFS/DFS/mail service administrators or even the Computer Security Team. Tight procedures have been established for the rare cases where such access is necessary, and these require the prior approval of the CERN Computer Security Officer or the IT Department Head, the Legal Service and the DG (see here for more details).

Data privacy is not only the responsibility of the Organization, however; you should also treat it with respect. There are members of the personnel who use external e-mail providers like Gmail or Hotmail instead of the central CERN e-mail service; some people send mail messages from their external mail address; and some even forward mails sent to their CERN address to that external provider. This could have serious consequences: an external e-mail provider cannot guarantee the level of data privacy provided by CERN, which is inspired by the European Data Protection Directive (95/46/EC). External providers may be outside Europe and subject to national legislation which is less protective. In addition, once e-mail is passed through these providers, there are implications for CERN’s privileges and immunities as an intergovernmental organisation.

For these reasons, the Computer Security Team and the IT department strongly encourage you to use only your CERN mail account for professional exchanges and not an external mail provider. Similarly, you should avoid having a permanent automated forward of all your CERN mail to an external provider.

The CERN mailbox gives you several features out of the box. By default all mailboxes have a quota of 2 GB, which can easily be increased (find out how here), and you can send and receive messages with an attachment of up to 30 MB. Moreover, the CERN mail system is integrated with the CERN phonebook, the e-groups system, an electronic fax service, a calendar that allows you to easily schedule a meeting, and many other services. The CERN e-mail service supports several e-mail clients on different operating systems, including support for major Internet browsers (see here). At the same time, sending messages from external sources (instead of a CERN mailbox) can have implications. A message can be rejected by the CERN antispam system or by an e-group’s posting restrictions.

Don’t screw up your web (2012)
http://cdsweb.cern.ch/journal/CERNBulletin/2012/12/News%20Articles/1431029?ln=en

Publish or perish. Given the large variety of information which needs to be published, you have the freedom at CERN to deploy your own web-server and put your data online on the Internet. Web content management systems like Joomla! or WordPress
together with dedicated add-ons and modules make it easy to quickly create a posh look-and-feel. But hold on. With this freedom also comes responsibility!

Your responsibility does not stop once you have been granted Internet connectivity. No: It falls to you to ensure that your web server is continually secured. Only information which is meant to be public should be put online. Proper access protections must be put in place to secure other data, preferably using the CERN Single Sign-On portal and definitely using the HTTPS (secure HTTP) protocol when transmitting sensitive information like passwords. “Securing” also implies that the operating system as well as the content management system must be updated regularly.

If you are not familiar with configuring web servers or programming web applications, you can take one of our security courses on this topic. Also, we strongly encourage you to follow our security baselines which give you basic recommendations to secure your web server. If you prefer to pass this responsibility on, the IT department offers a variety of different centrally managed web content management systems, e.g. Drupal and Sharepoint, as well as frameworks for deploying web sites in Java, Perl or Python. Choose one of these, and you don’t need to worry any more about securing the operating system or updating the web framework - it comes for free!

You've received a Hallmark E-Card? Delete it!
(2011)

This might not be your friend sending you a card, but a nasty attacker trying to infect your PC or steal your password. Attackers are always trying to take advantage, particularly during the Christmas season. Faking e-mails is easy. While it is evident that subject and message can be freely manipulated, did you know that the sender’s e-mail address can also be freely set? This way, attackers can disguise themselves as somebody legitimate, for example Santa.Clause@cern.ch.

So if you haven’t been expecting an e-card, or if you don’t know the sender, just delete that e-mail. If the e-mail is asking for your (CERN) password, let us know at Computer.Security@cern.ch, and delete it afterwards. If the e-mail includes an attachment or asks you to click on an embedded link, take care. Both might be misused to infect your PC or to steal your password. If it's an e-mail from a friend or your family, maybe this is just the right moment to call them and say “Thank you” before you open the attachment or click the link.

We wish you a Merry Christmas and a Happy New Year!!!
Encryption is useless!? (2011)


This week FTP (the file transfer protocol) celebrated its 40th birthday - and will hopefully retire soon! While a nice and simple means of transferring files, it is totally insecure: both the transferred contents and the authentication password are transferred unencrypted. FTP is not the only protocol that transfers data unencrypted: standard web traffic (“HTTP”) and e-mail (“SMTP”) are not encrypted either.

Not an issue? Think again! Nowadays, we all use wireless Ethernet from our laptops and mobile phones. This means that your traffic can be intercepted by anyone¹… What if I could your web browsing history, read your last e-mail to your boyfriend/girlfriend, or see which commands you’ve just executed? I could easily intercept your Facebook session…

If this worries you, check for secrecy and encryption. Usually this is shown by an “S” in your communication protocol:

- “HTTPS” for secure web browsing, as displayed in your browser’s address bar;
- IMAPS/POPS for secure e-mail transfer; the default at CERN for sending e-mails to the CERN mail servers;
- “SSH” and “SCP” for secure remote access and data transfer, mainly on Linux PCs. On Windows PCs, there is also “RDP”, the Remote Desktop Protocol, which is encrypted too. “SSH” can even be used to encrypt other protocols, a technique called “tunnelling”.

Of course, there is more to encryption than this. If you host sensitive or confidential data, access protection and data encryption are a must! This is particularly true if you keep this kind of data on a USB stick or a laptop, both of which can easily be lost or stolen while you're travelling… TrueCrypt is a good open source, on-the-fly encryption tool for data stored in Windows, Mac and Linux PCs.

If you are looking for recommendations or need help, check out https://cern.ch/Computer.Security or contact us at Computer.Security@cern.ch. The site gives further information about:

- Securely connecting to CERN
- Encrypting connections with SSH
- Tunnelling through LXPLUS
- Transferring files with SSH, and plenty of other useful tips!

¹ If your wireless access point does not encrypt traffic using e.g. the recommended WPA2 standard. At CERN, all wireless access points have no encryption in order to allow free roaming. Encryption would mean distributing a shared secret among all our users, colleagues and guests, so it would hardly be a “secret” anymore…
What do some webcams, CCTV cameras, video-conferencing cameras, control devices, printers and Internet-of-Things devices connected to CERN networks have in common? They are gaping wide open – in a digital sense: they have no access protection configured and either their password protection is disabled or they are still using the default password set up by the vendor. So, while users might think they are protected, the devices are freely open to people with malicious intent.

A recent survey conducted by a computer security student looked for webpages hosted on devices belonging to the so-called “Internet of Things”. These are devices that do not necessarily look like computers, laptops or smartphones, but have similar functionalities at their core. They run some kind of Windows or Linux operating system, can send e-mails, have a wireless adapter and can be configured and accessed through an integrated web server. All you need to know is the IP address of the device and the corresponding password to sign in. But this is the crux of the problem. Such devices usually come with a default account (e.g. “admin”) and a default password (e.g. “admin”, “user”, “12345”), which the device owner is not necessarily obliged to change on first use … to the advantage of an attacker. Given that these are vendor-default passwords, once you know the model and make, you can look them up on a multitude of different websites…

What is the risk? Think of webcams used at home or in conference rooms, for CCTV monitoring or access control: with the default password, anyone can see what they display. Privacy is gone. Similarly, people with malicious intent can enable the embedded microphone and listen to your discussions. Confidential meetings go public… Default passwords for routers will expose all your network traffic to a third-party attacker, i.e. the webpages you are accessing, including any content if you do not use encrypted communication channels such as SSH, RDP, VPN or HTTPS. Worse, your home router is able to connect to all your devices at home (this is its core purpose) and the attacker can therefore probe them all for vulnerabilities in order to widen the attack. Or think of devices controlling some industrial processes, drilling machines, solar panels, coffee machines, etc. Being able to freely configure their settings might render your machine or product useless. Who would accept a plain black coffee if they’d ordered ristretto?

So, next time you install a brand new device on your network at home or here at CERN, remember to change its default password. The same holds for any other device you inherit and start using: make sure that the configured password is known by you and only you. Select a good, strong password. Make it complex by using letters, symbols
and numbers. Do not use it anywhere else. Keep it to yourself. And if your creativity fails, here are some hints:

- Choose a line or two from a song or poem and use the first letter of each word. For example, "In Xanadu did Kubla Khan a stately pleasure dome decree!" becomes "IXdKKaspdd!"
- Use a long passphrase, such as the sentence "InXanaduDidKublaKahnAStatelyPleasureDomeDecree!" itself, or mathematical formulae, such as "\(\sin^2(x)+\cos^2(x)=1\)"
- Alternate between one consonant and one or two vowels with mixed upper/lower case. This produces nonsense words that are usually pronounceable, and thus easily remembered. For example: "Weze-Xupe" or "DediNida3"
- Choose two short words (or a long one that you split) and join them together with one or more punctuation marks between them. For example: "dogs+F18" or "comP!!UTer"

**The Internet of Things: the walls have ears (2017)**


Having “intelligent” devices at home is nothing really new. Aren't our washing machines, robot vacuum cleaners, coffee machines, etc. all sufficiently smart to serve our needs? Apparently not, as the consumer electronics market is now going full steam towards the “Internet-of-Things” (IoT): home appliances that are fully interconnected and, by using central cloud service computing power, able to help you improve your life. Seriously?

To give you a few examples of what I mean: the thermostats developed by Google build up a complete home automation system to manage the temperature of every room. They learn your daily room usage so that you don't even have to adjust the temperature settings anymore. Some “smart” thermometers easily surpass standard healthcare thermometers, as do smart toasters: control them via a smartphone app, share your settings with friends, upload information to Facebook, etc. The new generation of voice-controlled intelligent personal assistants come with a webcam that allows you to rate your outfit. For the best hairstyle ever, a smart hairbrush can optimise your look, taking weather reports, i.e. humidity and temperature, into account!

So what could go wrong? With the advent of the IoT at home, “privacy” is at stake:

- Some Smart TVs are able to use voice recognition to listen to what is happening in your living room;
- The manufacturer of the most famous doll in the world had a similar idea with its latest doll, but this was badly received by privacy advocates;
Once, a smart voice-controlled smart assistant even created some unwanted online orders when a TV news anchor said “Alexa, buy me a doll house”. The voice-activated assistant Alexa simply complied... Data registered by a smart assistant have even been subject to a legal case where “Alexa” might have been a witness to a murder and recorded everything that happened. Similarly, do not commit a crime if you happen to be wearing a fitness wristband – it might be used against you;

...and this list is not exhaustive.

In addition, from the "security" perspective, readers of the CERN Bulletin might recall "IoTs: The Treasure Trove at CERN", outlining a few security risks related to such devices that are part of the Internet-of-Things, and there are many more examples. In October 2016, the Mirai botnet affected close to a million customers of Deutsche Telekom by misusing poorly secured IoT devices. However, it will be much more difficult to keep all those devices up-to-date, so broader protection, like your wireless access router at home, or CERN's outer perimeter firewall, once again become the last and only line of defence... So, we have interesting times ahead. How much "security" and "privacy" are we prepared to trade for more convenience?

It is up to you to make a conscious choice as to how much "privacy" you want to hand over to companies. Check whether you can control which aspects of your personal data you want to expose. When it comes to "security", don't expect too much. As shown by our treasure trove tests, but also by many other reports like those from the last "BlackHat" conference, IoT devices cannot be expected to be secure. The important thing is that, as much as at CERN, your personal firewall at home (usually part of your wireless access point and router) is fully locked down so that no incoming traffic can try to exploit your devices.

IoTs: The treasure trove of CERN (2017)

IoT at CERN? That's the Internet-of-Things (IoT) here at CERN, e.g. any random device, not necessarily PCs, laptops, tablets or smartphones, connected to CERN's General Purpose Network (GPN) – the GPN-of-Things! And why a treasure trove? The Internet-of-Things is known to be unsecured, unprotected and full of vulnerabilities (see for example "Our life in symbiosis", “Your car, my control”, or “Hacking Control Systems, Switching Lights Off!”). The same goes for the devices connected to the GPN: unsecured and unprotected, a playground for hackers and attackers!

At the end of 2016, we performed an in-depth security scan of the CERN GPN\(^1\). Unlike before, when the targets had been laptops, PCs, tablets and smartphones, this time

\(^1\) No, the CERN Computing Rules do not allow you to run such scans yourself. Thus, please refrain from doing so.
we aimed our scan at the “unusual” devices: embedded controllers, web cameras, control systems and any other box with an Ethernet connection. We found an abundance: voltmeters, television screens, oscilloscopes, programmable logic controllers (PLCs), Ethernet-to-whatever converters and power supplies. In addition to this were many private printers, network switches, wireless access points and VoIP phones, despite the fact that the CERN IT department provides central services for networking, telephony and printing. So far, so interesting. But it got worse: many of these devices were using default passwords (“admin:admin” anyone?). Others were running outdated firmware versions allowing attackers to crack the password easily or even bypass the authentication step completely…

So, if you own an embedded device and if you care that this device is functioning properly, make sure that its security posture is up-to-date: replace any default passwords with your own dedicated passwords. Follow the CERN password rules for this. Also, make sure that the firmware is the most recent version. Some of the devices found by us flagged that their current firmware was outdated and that a more recent version was ready for download! If a device is essential for your experiment or one of CERN’s accelerators, refrain from connecting it to the GPN. Instead, check with your experiment or the Technical Network administrators whether your device is a good candidate to be connected there (or to find out about other alternatives)…

Protect your plant: a "serious game" about control system cyber-security (2015)
http://cds.cern.ch/journal/CERNBulletin/2015/03/News%20Articles/1980920?ln=en

Control system cyber-security is attracting increasing attention: from cybercriminals, from the media and from security researchers.

After the legendary “Stuxnet” attacks of 2010 against an Iranian uranium enrichment plant, the infiltration of Saudi Aramco in 2012, and most recently the hacking of German blast furnaces, we should be prepared. Just imagine what would happen if hackers turned off the lights in Geneva and the Pays-de-Gex for a month? (“Hacking control systems, switching lights off!”). Or if attackers infiltrated CERN’s accelerator or experiment control systems and stopped us from pursuing our core business: delivering beams and recording particle collisions (“Hacking control systems, switching... accelerators off?”).

Now you can test your ability to protect an industrial plant against cyber-threats! The Computer Security Team, in collaboration with Kaspersky Lab, is organising a so-called “serious game”. This game is targeted at control and safety system experts, IT people and line managers, and should increase their awareness of the risks and security problems of running modern control systems. Basically, each of the competing teams of 4-6 people is tasked with running a water purification plant in the most efficient way. This plant consists of two independent filtration lines controlled by PLCs, HMIs,
engineeering stations and a data historian. During the five rounds of the game, these
two filtration lines generate revenues. However, the teams also have to face cyber-
attacks potentially impacting plant performance. In order to defend their plant, each
team has to take strategic, managerial and technical decisions while taking operational
constraints into account and maintaining a high level of revenue.

Of course this game simplifies many aspects of running complex control systems. Still,
having played the game, you should have a better understanding of:

- why fundamental cyber-security awareness is beneficial for fulfilling CERN’s
  mission,
- why we need the technical/experiment networks to be properly separated from
  the CERN office network,
- why protecting PLCs and other embedded devices is a must,
- why regular changes of passwords, in particular those used for service
  accounts, are essential,
- why keeping control PCs up-to-date is important, and
- what the benefits of anti-virus software are (among others).

And of course it is quite fun to play in an informal competition with others: the team
having earned the most revenue and having best secured their plant wins a prize!

This game has been developed by Kaspersky Labs, a renowned security company,
and will be presented by them in an interactive fashion using a board simulating the
plant (see image below) as well as iPads for news announcements and for book-
keeping revenues and expenses (find a teaser commercial here). It will be hosted in
the CERN “Pump Hall” (Building 216) and is scheduled to take place on Tuesday, 3
February 2015, from 4 p.m. to 6 p.m. This is a unique opportunity! Register here. As
places are limited, control and safety system experts, technicians and engineers will
be given priority.

Your car, my control (2015)

We have discussed the Internet of Things (IoT) and its security implications already in
past issues of the CERN Bulletin, for example in “Today’s paranoia, tomorrow’s reality”
(see here). Unfortunately, tomorrow has come. At this year’s Black Hat conference
researchers presented their findings on how easily your car can be hacked and
controlled remotely. Sigh.

While these researchers have just shown that they can wirelessly hijack a Jeep
Cherokee, others have performed similar studies with SmartCars, Fords, a Tesla, a
Corvette, BMWs, Chryslers and Mercedes! With the increasing computerisation of
cars, the engine management system, air conditioning, anti-lock braking system,
electronic stability programme, etc. are linked to the infotainment, navigation and
communication systems, opening the door for these vehicles to be hacked remotely. The now prevalent Bluetooth connection with smartphones is one entry vector to attack your car remotely. A second is the built-in GSM modem, which is even part of a new legal requirement in EU states for cars to be fitted with the ability to make automatic emergency calls (eCalls). The aforementioned researchers found a vulnerability in the Fiat/Jeep “Uconnect” GSM feature that allowed them to connect to a Jeep Cherokee remotely, manipulate its firmware, and, finally, take full control of the radio, the air con, and even the accelerator! Definitely not something you want to experience on the motorway… The other findings concerning Fords, Teslas, and Corvettes are no less worrying…

So, computer security problems that were prevalent in PCs in the 1990s and led to industrial control systems in the 2000s (see our article “Hacking control systems, switching lights off!”) are now entering our daily life (“Our life in symbiosis!”)! And while patching CERN's LHC control systems is already a big and complicated effort, how is your security at home? For your car? For your fridge? For your home entertainment system?

P.S. If you own a Jeep Cherokee, a patch for this flaw is available here. European models are said not to be affected.

Today’s paranoia, tomorrow’s reality (2014)

When the Internet opened its gates to academia in the late 80s and, together with the World Wide Web a few years later, to the general public, computer security was considered somehow irrelevant. People pointing to vulnerabilities and security risks (“hackers”) were labelled as paranoid. But they woke to reality during the outbreak of the “ILOVEYOU” virus in 2000, which caused large scale infections of Windows PCs (including many at CERN).

Similarly, warnings about weaknesses and insecure control systems, issued by CERN and others (see our Bulletin article “Hacking control systems, switching lights off!”), were ignored until the “Stuxnet” attack against control systems in Iran proved them right in 2010. Reality beat 'paranoia' attack again. Last year, the paranoid fear of many security experts that our whole IT infrastructure might have been infiltrated and spied on turned real, if you believe in the revelations of whistle-blower Edward Snowden (see “Security vs. Nations: a lost battle?”). Paranoia vs. Reality: 0-3. And the next strike is approaching…

The Internet is currently transforming away from an instrument for people sharing information to an “Internet of Things” with almost any device able to publish relevant and irrelevant data to all those who listen. Many gaming consoles and even TV sets require Internet connectivity for an “enhanced entertainment experience”. So do cars, as their entertainment systems provide interfaces to communicate with your phone. In
the future, they might even communicate with other cars and the next traffic light to optimise traffic flow. “SmartMeters” will measure your energy consumption at home and share this with your energy provider in real time - using the Internet. “Nest Labs” (recently acquired by Google) does the same with home air conditioning and heating. Espresso machines provide USB ports for you to upload your favourite recipes and make your “coffee experience” even better.

The paranoia? All these devices run some kind of operating system. But compared to computers or laptops, the corresponding hardware vendors do not have a real incentive to provide permanent updates and patches for them. Currently, even some smartphone manufacturers are slow to provide suitable upgrades to the firmware of their older product lines. Why should we expect better from a manufacturer of Internet-ready espresso machines or heating systems controllable from your tablet PC? Indeed, this reality has already caught up with us, as German heating systems were found vulnerable\(^1\) and numerous fridges (!) where found to be sending spam messages into the world...

Conclusion? Being paranoid is not that bad. It might just mean that you’re ahead of your time. At CERN, we should listen more to our intuition. Do we really have sufficient security measures in place? Is our data properly protected? Are our computing services able to fend attackers off? Is the way we do development and testing still adequate given that today everything is interconnected? When will reality enter CERN and create havoc? We’re interested to know where you would invest in computer security at CERN, where to improve, and what to leave out. Just e-mail us at Computer.Security@cern.ch. Be paranoid!

Our life in symbiosis\(^2\) (2014)

Do you recall our Bulletin articles on control system cyber-security (“Hacking control systems, switching lights off!” and “Hacking control systems, switching... accelerators off?”) from early 2013? Let me shed some light on this issue from a completely different perspective.

I was raised in Europe during the 80s. With all the conveniences of a modern city, my environment made me a cyborg - a human entangled with technology - supported but also dependent on software and hardware. Since my childhood, I have eaten food packaged by machines and shipped through a sophisticated network of ships and lorries, keeping it fresh or frozen until it arrives in supermarkets. I heat my house with the magic of nuclear energy provided to me via a complicated electrical network. In fact, many of the amenities and gadgets I use are based on electricity and I just need

---

\(^1\) Subsequently, the corresponding vendor suggested affected households disconnect their Ethernet cable.

\(^2\) To be published in the annual yearbook of the World Federation of Scientists.
to tap a power socket. When on vacation, I travel by taxi, train and airplane. And I enjoy
the beautiful weather outside thanks to the air conditioning system located in the
basement of the CERN IT building.

This air conditioning system, a process control system (PCS), monitors the ambient
room temperature through a distributed network of sensors. A smart central unit - the
Programmable Logic Controller (PLC) - compares the measured temperature values
with a set of thresholds and subsequently calculates a new setting for heating or
cooling. On top of this temperature control loop (monitor - calculate - set), a small
display (a simple SCADA (supervisory controls and data acquisition) system) attached
to the wall allows me to read the current room temperature and to manipulate its set-
points. Depending on the size of the building and the number of processes controlled,
many (different) sensors, PLCs, actuators and SCADA systems can be combined and
inter-connected to build a larger and more complex PCS.

In a similar way, all our commodities and amenities depend on many different, complex
PCSes e.g. a PCS for water and waste management, for electricity production and
transmission, for public and private transport, for communication, for production of oil
and gas but also cars, food, and pharmaceuticals. Today, many people live in
symbiosis with those PCSs which make their lives cozy and comfortable, and industry
depends on them. The variety of PCSs has become a piece of “critical infrastructure”,
providing the fundamental basis for their general survival.

So what would happen if part or all of this critical infrastructure failed? How would your
life change without clean tap water and proper waste disposal, without electricity,
without fresh and frozen food? The cool air in the lecture hall will get hot and become
uncomfortable. On a wider scale, with no drinking water from the tap, we would have
to go back to local wells or collect and heat rain water in order to purify it. Failure of the
electricity system would halt public life: frozen goods in supermarkets would warm up
and become inedible, fuel pumps would not work anymore, life-preservation systems
in hospitals would stop once the local diesel generators ran out of fuel… (this is nicely
depicted in the novel “Blackout” by M. Elsberg).

We rely on our critical infrastructure, we rely on PCS and we rely on the technologies
behind PCSs. In the past, PCSs, PLCs and SCADA systems and their hardware and
software components were proprietary, custom-built, and stand-alone. Expertise was
centralised with a few system engineers who knew their system by heart. That has
changed in recent decades. Pressure for consolidation and cost-effectiveness has
pushed manufacturers to open up. Today, modern PCSs employ the same
technological means that have been used for years in computer centres, in offices and
at home: Microsoft’s Windows operating system to run SCADA systems; web browser
as user interfaces; laptops and tablets replacing paper checklists; emails to
disseminate status information and alerts; the IP protocol to communicate among
different parts of a PCS; the Internet for remote access for support personnel and experts...

Unfortunately, while benefitting from standard information technology, PCSs have also inherited its drawbacks: design flaws in hardware, bugs in software components and applications, and vulnerabilities in communication protocols. Exploiting these drawbacks, malicious cyber-attackers and benign IT researchers have probed many different hardware, software and protocols for many years. Today, computer centres, office systems and home computers are permanently under attack. With their new technological basis, PCSs underwent scrutiny, too. The sophisticated “Stuxnet” attack by the US and Israel against the control system of Iranian uranium enrichment facilities in 2010 is just one of the more publicised cases. New vulnerabilities affecting PCSs are regularly published on certain web pages, and recipes for malicious attacks circulate widely on the Internet. The damage caused may be enormous.

Therefore, “Critical Infrastructure Protection” (CIP) becomes a must. But protecting PCSs like computer centres, patching them, running anti-virus on them, and controlling their access is much more difficult than attacking. PCS are built for use-cases. Malicious abuse is rarely considered during their design and implementation phase. For example, rebooting a SCADA PC will temporarily cease monitoring capabilities while updating PLCs firmware usually requires thorough re-testing and probably even re-certification. Both are non-trivial and costly tasks that cannot be done in-line with the monthly patch cycle releases by firms like Microsoft.

Ergo, a fraction (if not many) of today’s PCSs are vulnerable to common cyber-attacks. Not without reason, the former advisor to the US president, Richard Clarke, said “that the US might be able to blow up a nuclear plant somewhere, or a terrorist training centre somewhere, but a number of countries could strike back with a cyber-attack and the entire [US] economic system could be crashed in retaliation ... because we can’t defend it today.” (AP 2011) We need to raise our cyber-defences now. Without CIP, without protected SCADA systems, our modern symbiotic life is at risk.

Cyber-attacks and the risks for CERN (2013)
http://cds.cern.ch/journal/CERNBulletin/2013/10/News%20Articles/1520152?ln=en

In the previous Bulletin, we discussed the cyber-risks for the accelerator complex. However, looking at the broader picture, the cyber-risks for CERN are much more diverse.

Attacks can not only harm the operation of accelerators or experiments, but also impact negatively on the operation of the Organization as a whole and/or its reputation. This would not only hamper and impede our work while making us looking plain stupid, but might also make funding agencies reconsider whether their money is well invested in CERN... Examples? Sure, let’s be imaginative!
What would be the consequences, if:

- A laptop holding sensitive CERN documents is lost or stolen, and ends up on eBay?
- Your password is compromised and your mail account misused to send nasty messages to thousands of external mail addresses?
- An attacker manages to add photos of naked women/men onto a prominent CERN website, and boasts about this on Twitter?
- Confidential documents like job application forms or password lists accidentally become public?
- A member of the personnel downloads copyrighted material and CERN is subsequently sued by the rights holder?
- An attacker infiltrates our central computing clusters or the LHC Computing Grid, and subsequently attacks - say - the Vatican’s website?
- A large fraction of Windows PCs and laptops connected to the office network is infected by a brand-new breed of virus?

And what is the probability of any of the above happening? It's certainly not zero! Therefore, help the Organization to keep the risks of cyber-attacks to a minimum!

Recall that you are, in the first instance, responsible for the computer security of the laptops, smart phones and PCs you use, the accounts and passwords you own, the files and documents you hold, the programs and applications you have installed or, especially, those you have written, and the computer services and systems you manage. The Computer Security Team is ready to help you assume this responsibility by providing training and awareness, consulting and audits. Alternatively, you can delegate that responsibility to the IT department, which manages a multitude of secured computing services.

Hacking control systems, switching lights off! (2013)

http://cds.cern.ch/journal/CERNBulletin/2013/06/News%20Articles/1510561?ln=en

Have you ever heard about “Stuxnet”? “Stuxnet” was a very sophisticated cyber-attack against the Iranian nuclear programme. Like in a spy movie, the attackers infiltrated the uranium enrichment plant at Natanz, arranged for infected USB sticks to be inserted into local PCs, and then the USB viruses did the rest.

Not only did the virus employ four distinct - so far unknown - weaknesses in the Windows operating system, but each weakness could have been sold on the underground market for up to $250,000 each.

The virus was targeted to disrupt Iran’s uranium production. At first, it scanned the infected PCs for dedicated SCADA (Supervisory Control and Data Acquisition) software from Siemens. Once the virus hit upon that software, it tried to identify any control system components, i.e. so-called PLCs (programmable logic controllers),
attached to that PC. If the PLC matched a certain brand (Siemens S7) and configuration, the virus downloaded additional code sequences into that PLC. Those sequences were lethal: clandestinely and over months, they varied the rotational speed of the uranium enrichment centrifuges. Non-constant rotation deteriorated the uranium enrichment and subsequent wear-out rendered the centrifuges useless. So the attackers achieved their goal…

While this seems to be a far-fetched and unique example, reality is much worse. Standard control systems deployed in power distribution networks and energy generation or employed in almost all production lines worldwide (cars, oil, chemicals, etc.) are completely unprotected. While they use similar techniques as standard PCs – like the Windows operating system, e-mails and www, and connect to similar networks – “security” was never part of their design. Thus, breaking into PLCs is easy and straightforward. Switching off the lights in [put your favourite country here] has never been so easy. Not without reason, Richard A. Clarke, advisor to the U.S. President, stated in 2011 that while the U.S. might be able to blow up a nuclear plant somewhere, a number of countries could strike back with a cyber-attack and “the entire U.S. economic system could be crashed in retaliation… and we can’t defend it today”. Replace “U.S.” with “worldwide” and you get the real picture.

What about CERN? Accelerators, experiments and their technical infrastructure are all based on the same control system technologies with the same drawbacks, vulnerabilities and security risks. Interestingly, colleagues in the former IT/CO group (now EN/ICE) had already created a much less sophisticated variant of “Stuxnet” in 2004. Dedicated tests from 2005 to 2007 showed that one third of the tested control systems could be crashed via a cyber-attack within seconds. Consequently, a strategic working group, the Computing and Networking Infrastructure for Controls (CNIC) group, was mandated to improve the cyber-security of CERN’s control system in 2004. This group brought together representatives from all the LHC experiments, the technical and accelerator sectors, as well as the IT department and the Computer Security Team. The result was a clear control system security policy and actions, e.g. separation of office network (GPN) and control network (TN) and prohibition of USB sticks on the TN. Today, CERN is in direct contact with several vendors and governmental bodies, and collaborates with them to better secure control systems…

Hacking control systems, switching… accelerators off? (2013)


In response to our article in the last Bulletin, we received the following comment: “Wasn’t Stuxnet designed to stop the Iranian nuclear programme? Why then all this noise with regard to CERN accelerators? Don’t you realize that ‘computer security’ is
not the raison d’être of CERN?”. Thank you for this golden opportunity to delve into this issue.

Given the sophistication of Stuxnet, it might have been hard to detect such a targeted attack against CERN, if at all. But this is not the point. There are much simpler risks for our accelerator complex and infrastructure. And, while “‘computer security’ is [indeed] not the raison d’être”, it is our collective responsibility to keep this risk at bay.

Examples? Just think of a simple computer virus infecting Windows-based control PCs connected to the accelerator network (the Technical Network, “TN”) and disrupting their functioning. Windows-based control PCs are rather susceptible as they cannot be patched as timely as office computers - neither at CERN nor in industry. Taking advantage of this window of opportunity, the virus might have come via a compromised development PC connected to the office network; shipped in via a new, but already compromised Supervisory Control And Data Acquisition (SCADA) terminal by a third party control system provider; or it might have been introduced by a maintenance laptop connected temporarily to the TN…

Another example would be an account name/password combination for accessing critical accelerator control systems. This combination was accidentally disclosed on one of our public websites. Spotted by an attacker, it could have been misused to manipulate the system in an adverse way. A final example would be malicious code, introduced by an attacker on a Linux-based control PC with a connection to the TN. As the attacker would not know where they “are”, they would run this code to scan the network. This introduces network delays, and stops other control systems from working correctly.

Impossible? Not at all. Harmless variations of these examples have been seen at CERN recently! If they had been serious, they might have brought months of downtime to our physics programme. Fortunately, they have had zero impact so far.

Will this last? “Computer Security” must become another important ingredient in the accelerator complex (like “functionality”, “availability”, “usability”, “maintainability”; read our article “A Short Tale of the Black Sheep of –ITY”). In 2004, the CERN Management mandated a strategic working group, the CNIC (Computing and Networking Infrastructure for Controls), to improve the cyber-security of CERN’s control system. This group brought together representatives from all the LHC experiments, the technical and accelerator sectors as well as the IT Department and the Computer Security Team. The result was the separation of the office network from the TN, the switch from individual office PCs to Windows Terminal Servers and virtual machines for developing controls applications, the introduction of a Windows installation scheme for control PCs (“CMF”, subsequently used throughout CERN), and the prohibition of USB sticks, laptops and wireless devices on the TN. Unfortunately, those measures had to be deployed in an existing operational environment and, thus, had to cope with a multitude of boundary conditions, exceptions and workarounds. Therefore, none of
those measures are perfect and some impact heavily on usability and convenience, particularly for people developing and maintaining accelerator control systems.

Give us your feedback! With the Long Shutdown 1 now underway, we should work together to see how to improve your situation, while maintaining an acceptable high level of “security”.

Join the CNIC users exchange or send an e-mail to the Technical-Network.Administrator@cern.ch. If you are running control systems, check out the CNIC control system security policy: Is your configuration safe? Do you have proper access control? Do you patch in a timely manner? Do you know “security”?
Secure Software Development

A new departmental car service (2020)

…with the cars painted in the favorite colour of the corresponding department head; an individual restaurant per department with the menu voted on by that department’s staff and users; each group with its own key and lock management system, using different techniques and lock sizes; separate badge systems, one per experiment, incompatible with each other and using different implementations; different power sockets following different national standards for different buildings; and, last but not least, different working hours for every section of CERN.

Indeed, that would all make… no sense! The cacophony of different services providing the same commodity – cars, food, keys, badges, electricity – would just be immense and would provide no overall significant benefit to the Organization. Instead, centralised services are paramount. They enable CERN to benefit from synergies and efficiencies when they are run by a group of specialised professionals with a pool of in-depth knowledge and experience, and hence save money and resources. In addition, centralised services allow the service managers to follow a high standard of implementation, ensuring redundancy, business continuity, compliance with CERN or host state regulations like the data protection rules, and integration with other services run at CERN. They can also benefit from additional (usually costly) features such as 24/7 service and Service Desk support.

This is all reasonable and rational in the physical world and at CERN there’s just one car service, one key and lock service, one access control service, one electricity standard and one restaurant provider. And we usually accept that CERN cars are white, the badges are credit-card sized, the power sockets are Swiss, and the restaurant serves those particular menus. So why do we have “shadow” IT at CERN and a cacophony of different non-centralised IT systems?

Why is it OK to violate CERN’s data protection needs and forward e-mails to external e-mail providers? Or store them on external cloud services? Why do some individuals buy fancy third-party presentation software instead of using whatever is already available at CERN? Why do we have the same application stack being run in different corners by different people? Why do we need Joomla when we have Drupal and WordPress? Why do we have many different (external) solutions for questionnaires? Why do we store meeting minutes and presentations in the “wrong” storage systems? Just as for physical services, centralised services are paramount!

Whenever you need an IT service, please check CERN IT’s software portfolio first. Whether you want to manage your conferences, meetings and minutes, would like to
set up a website or database, need storage space or a virtual machine, the IT department, but also the EP-SFT and FAP-BC groups, provide you with a range of centrally managed IT services run in a professional manner, guaranteeing data preservation, security, business continuity, high availability, data policy compliance, and integration with CERN's Single Sign-On. All central IT services are listed here. In addition, dedicated licences are available for a wide variety of office and engineering software packages and for control software. If these do not suit your needs, please contact the CERN Cloud and Software Licence Officer to check your options and, if needed, agree to make a central purchase.

A new twist for those who rely on external software (2019)


Are you a programmer? Software developer? Someone who codes regularly? Or just from time to time? Then you no doubt take advantage of the plethora of software snippets, code excerpts, libraries and the like circulating on the Internet, on Github, Stack Overflow, SourceForge, or others. Nice, but there’s a risk: is the code safe? Bug-free? Maintained? And free of any malicious components?

A few months ago, we discussed the inherent risk and implications for CERN’s computer security of any use of external libraries (see our Bulletin article on “Fatal dependencies”). In the past, several public and open source libraries were found to contain malicious code for extracting credentials or misusing local computing power for crypto-currency mining or other evil deeds. So, all that glitters is not gold. External software libraries and external code snippets should be used with diligence and care. A variety of static code checkers can help you with this. Or consider using a centralised software repository manager like Sonatype Nexus or Apache Maven. But that is not the only risk.

What if the code you depend on is simply withdrawn from your source? In an interesting new twist, a software developer decided to pull all his code from Github after he learned that it was being used by a US agency whose work he did not appreciate at all. His software, “Chef Sugar”, is a Ruby library for simplifying work with “Chef”, a platform for configuration management. Removing the software from the public domain impacted negatively on several customers of that US agency using “Chef”¹. And they might not be the only ones being affected…

Another example is the recent change of Oracle’s terms and conditions for the usage of Java JRE. While any support for Java as part of a commercial software package is still included in that package, updates and support for in-house development might

¹ The full story can be found on Slashdot.
need a paid subscription. Previously free usage has become restricted behind a paywall… While the OpenJDK toolkit (for Java version 11) provided and supported by RedHat until 2023 might still fit certain use cases, other software might run into nasty dependency issues…

So, what are the chances of something like this happening to you? Do you have a full copy of the software you rely on in source code format? Can you freely and independently compile it? Have you assessed the impact in case the original publication location goes bust? Share your experiences with us via Computer.Security@cern.ch.


Do you know what drugs and proprietary software have in common? You bear the consequences if the product you buy is of mediocre quality. There is no possible recourse. Your investment is lost. The big difference is that buying software is legal. Still, there is no chance that you can hand back software that is buggy, return it to the software manufacturer and ask for it to be fixed (OK, you can ask, but…) or press for financial compensation. Instead, you as an individual, or we as an organisation, have to invest additional money in protecting our software stack and its inherent bugs against abuse… So, how can we create an efficient incentive to improve software quality? Legally enforced Bug Bounty Premiums.

While many big software manufacturers already employ so-called secure software development lifecycles to improve their products, many others just come full of bugs in order to be first on the market. The user is the beta tester. Security comes… later. There is just no incentive to guarantee that at least the obvious blunders are corrected. Very frequently, in particular for devices on the Internet-of-Things, the software stack (operating system, network interface, web server, user interface) is just a hack, as the producing companies have no good knowledge of software design and security. Their business is the device itself: thermometers, cameras, you name it. And they just make them “intelligent” by connecting them to the Internet. The same is true for smaller software development companies, they have a great idea to market, but neither the personnel nor the time to ensure a secure design and a software product with as few bugs as possible. Others just don’t care (enough). There is just no incentive to invest in security, except for one: reputation. And looking at the past record of published software blunders in the media, rarely does a company go bust due to a security bug*.

So, why care?

How to create an incentive for more secure software? Legally enforced Bug Bounty Premiums! A “Bug Bounty” programme today is a voluntary commitment by a company to pay you a certain amount of money if you report a software bug found in its products. Google runs one. Microsoft does. CERN does too (but, as we are taxpayer funded, we
Secure Software Development

can hand out only t-shirts as a reward). Unfortunately, many other software developers don’t. And this is where legally enforced Bug Bounty Premiums would help. National governments, the European Union, or ideally a global organisation, should come up with a defined “price list” for bugs, and legally enforce any software manufacturer to pay that money to the first person that finds one. The infrastructure for recording bugs and keeping track of fixes has already been in place for a while: CVEs (“Common Vulnerabilities and Exposures”). A cross-site scripting bug gets you, say, $100; SQL injection, $200; command line injection, $1000; a root exploit, $10 000; etc. And, by law, software manufacturers would be forced to pay that sum to the first finder.

So here come the incentives: either they pay the Bug Bounty Premium, or they invest in better software development processes in-house, or they engage with third parties to find weaknesses before Bug Bounty hunters do. But there are more advantages! Legally enforced Bug Bounty Premiums open a guaranteed revenue stream for software savvy people. Security researchers. Computer engineers. IT students. Anyone who loves to poke into software and hunt for defects can make some additional decent money. And also those who tended in the past to sell their findings illegally on the dark market – they now have the option to move out of illegality and cash in legally.

Of course, there are some lemmas to take into account, namely “software dissemination” and “open source”. For the former, instead of having fixed premiums ($100, $200, $1000, $10 000), the premium should scale with the dissemination of the buggy software. For that small library I wrote, used just by you and me, and where you found a bug, you make hardly any money. But if you find a vulnerability in a major operating system, a dominant web browser, or a widely used library: bingo for you! And open source? This is where the state comes in. The premium is paid out of a national, European or international pot. Maybe this is the most problematic point, but in the long run, it provides another incentive to software manufactures: instead of maintaining (old) proprietary software and eventually paying out for bugs, they can consider making their source code public and open source – and the liability to pay in the event of bugs is gone. Benefit for the community: more open source code!

So, what if?

Go clever! Go central! (2019)

In times of scarce resources, time pressure, and the increasing complexity of running software applications, why not follow the herd and go clever? It just doesn’t make any sense any more to reinvent the wheel and then just stand back. Running your own computing hardware, installation stack, (web) applications, databases, etc., is just not cost effective and usually you won’t be able to commit the required attention to keeping those systems sufficiently secure. Just recently, CERN “lost” two locally managed "Jenkins" instances because they were not kept up to date (see our Monthly Report for
details). So, wouldn’t it be better to concentrate on the real job and delegate non-core responsibilities to CERN’s professionals?

The CERN IT department provides you with a vast catalogue of centrally managed computing facilities, starting with hardware platforms to run your favourite operating system ("Openstack") or application (e.g. "Apache", "Grafana", "Jenkins", "Nexus", .NET/Perl/PHP/Python/Ruby or "Rundeck" on "Openshift"). They also allow you to choose from a variety of centrally supported software applications for Windows ("CMF"), Linux ("Linuxsoft") and Mac ("Mac Self-Service"). This includes dedicated and sophisticated software packages for engineering, mathematics and mechanical design. If you require your own database ("Database-on-Demand") or need to store vast amounts of data ("EOS"; "CERNbox") central professional IT services are there to help. And if you are running your own local computer cluster, CERN IT would be happy to discuss with you how to integrate your needs into the services provided by CERN’s central computing centre.

This approach may not always provide a 100% match but, if you can compromise, it’s a great way not only to reduce the time you spend maintaining layer upon layer of computing hardware and software, but also to relieve you from the need to check for new updates and worry about patches, and to avoid the hassle of implementing all necessary features in order to keep your application well protected and secured. So, take a look at CERN IT’s full list of central computing services and/or join the next IT User’s Meeting for the most recent news and deployments available to you. And if you need help, you can always contact the CERN IT Consultants to get an opinion on how best to cover your needs with CERN IT solutions.

And the IT department is not the only central entity providing you with professional IT services for free. The Business Computing group in the FAP department provides you with all the financial and HR applications you could possibly need. As does the EP-SFT group for physics computing, simulations and data analysis. And the CO and ICS groups of the BE department, which can provide you with all the necessary control system software you need to run your accelerator or experiment at CERN. Thanks to all of these, you can obtain professionally managed and well secured software, applications and computing services for free, instead of losing time through reinventing the wheel.

Last but not least, we’d also like to say a big thank you to another central service, the CERN Translation and Minutes Service, to whom we are grateful for the English proof-reading and translation into French of all our Computer Security Bulletin articles!

Fatal dependencies (2019)

Are you a hacker? Programmer? Software developer? Coder? Many of us are. And, as intelligent humans, we tend to concentrate on the new and not try to reinvent the
wheel, instead benefitting from what has been already created elsewhere. So we have more time to produce something new, something adapted to our needs, and leave the basics to software packages already produced somewhere else. Standing on the shoulders of other hackers, programmers, developers and coders worldwide, Gitlab at CERN, Github around the world and Stack Overflow, to name just three, provide a vast variety of libraries and code snippets for already existing functionalities. All you need to do is download or copy-paste them. But what if those hackers, programmers, developers and coders turn rogue?

Open source code is great, but does not come without risks. As anyone can write and share code, it is an inherent fact that some code comes with blatant security vulnerabilities. These are not necessarily introduced with malicious intent but the openness of the source code allows anyone to verify the integrity of the code and correct it if needed. However, sometimes even the open source community fails to identify major vulnerabilities like “Heartbleed”. So reusing public libraries comes with a risk. And this risk becomes more severe if malicious third parties intentionally tamper with software libraries and just wait for software developers “driving by”, downloading those malicious libraries and running that code in their software. Code executed and… boom! It would not be the first time that companies have been compromised through malicious libraries or modifications thereof. For example, a backdoor was discovered in the Python module named “ssh-decorator” distributed through “PyPi”, a repository of software for the Python programming language. Any SSH connection credentials were forwarded to a malicious party. Similarly, some malicious libraries have been named to resemble the name of a real, widely used library like, e.g. “crossenv”. But the fake one (“cross-env”) was extorting local environment variables and, potentially, also credentials. Thirty-nine more typo-squatted libraries were identified and deleted from “NCM”, a popular package manager for the JavaScript programming language. And then there are legacy libraries, not maintained by anyone any more, but still in use. In this example, the ownership was naively passed over to a malicious evil-doer who then introduced some malicious code in the otherwise clean library…

So automatic integration of external software libraries e.g. from PyPi or through NCM comes with a risk! Like with surfing the web, STOP – THINK – DON’T CLICK (or rather, don’t import). Only install software libraries from trusted sources. And even then, inspect the code either manually (cumbersome as it is) or run at least a static code analysis tool on top of that. The CERN Computer Security Team provides a variety of static code checkers for that purpose. Also consider using a centralised software repository manager like Sonatype Nexus or Apache Maven. The former is provided by CERN IT department and used for accelerator control system development and in the ATLAS and CMS experiments.
Improve your code with Gitlab CI (2017)

Well-tested code is the cornerstone of a reliable and robust software stack: nothing is more annoying than a crashing, failing or misbehaving application, the loss of time and service (!) as a result of this, and the cumbersome debugging process to find the origin of the flaw. Not to mention the frustration of the user community. Although the production of bug-free code is impossible due to the complexities of software and the limited skills of most human programmers, reducing the number of bugs and flaws early in the development process significantly lowers debugging costs later. For the sake of software quality, the IT department provides you and your clients with a few simple tools to save precious time and cerebral pain.

Writing perfect code is far from easy and requires a deep knowledge of the programming language(s) being used, plus lots of experience. The introduction of flaws and bugs is inevitable, it happens and will continue to happen to even the most skilled coders among us. But these skilled coders – the Gandalfs of coding – know how to turn the odds in their favour. They follow common best practices on modularity, isolation, simplicity and readability; they validate every bit of input data and discard unreasonable input; they limit the execution scope and reduce the necessary privileges; they choose safe defaults; they know how to keep secrets secret; and they pay attention to compiler messages (e.g. gcc –wALL anyone?) as, very often, compiler warnings flag code that is in a suboptimal state. Ideally, code should compile without any complaints at all.

Want to become a software magician yourself? Easy, if you apply the best practices mentioned above. Even easier if you use CERN’s Gitlab instance as your primary software repository. Its Continuous Integration framework, Gitlab-CI, lets you introduce additional, automatic static code analyses, running on top of your code repository in a very simple way, to ensure that your code is clean of known security issues and bad practices. This is especially efficient when working in groups or teams, because it allows you to focus more on your task, rather than on which tools everyone should use and how. Since you will not need to prepare your testing environment for every change, you will save a lot of time.

All these static code analysis tools are also available for download. If you are interested in finding out how to better secure your website – in particular if it is directly exposed to the Internet – see our recommendations and our tools for Oracle/APEX. Remember that one of the basics is simple: consider using CERN its central web service!

And of course there are many other opportunities to improve your software. The Computer Security team, in collaboration with CERN’s Technical Training team, has arranged several different “Secure Coding” courses on web development and good programming practices. For those who want to learn “hacking”, we provide regular
hands-on capture-the-flag courses where you can learn to become a penetration tester. Join our WhiteHat Challenge in September 2017! And if you prefer a book, here is a list of further reading on the subject.

Do we need more software liability? (2016)

The CERN Computer Security Team and our colleagues, as well as external students participating in the CERN WhiteHat Challenge and friendly peers around the world, repeatedly detect weaknesses and vulnerabilities in websites and software applications developed or run at CERN. It is a never-ending race between the good side and the evil-doers who would love to misuse those weaknesses and vulnerabilities to break into CERN and misuse our computing resources for their malicious deeds.

So why is software buggy? Of course, complexity is one argument why there will always be software flaws. But we shouldn’t hide behind that argument. The flaws are introduced by humans. Time pressure, suboptimal programming skills and lack of good practices mean that secure coding is overlooked. And there is no incentive to change that. Besides software, there are barely any other products worldwide where the customer has to bear all the consequences of a bad product: maybe drugs? In other fields that introduce risk for the user, such as engineering and medicine, the professionals creating products are required to be accredited and perform audits and safety checks. Perhaps we need to introduce a government-sponsored liability programme for any software being sold or distributed widely? Legally require software companies and programmers to have a bounty programme and make them pay for any vulnerability found in their software. The sum paid to the first finder might follow a nationwide (or even international?) catalogue. Cross-site scripting: 1000 CHF, SQL injection: 5000 CHF, remote code execution: 10,000 CHF. This payment might even be proportional to the user base of the vulnerable software. For Microsoft software, the payment is higher, for my software which barely anyone uses, the sum is lower. But they would only need to pay if their software is closed source. The bounty costs for open-source code would be covered by the government...

What would be the benefits? First of all, software companies and programmers would be required to pay attention to secure coding. Of course, they can decide that it is more effective for them to pay the bounty instead and get their software improved through external means. Or, even more beneficial to the world, make their software open source and have the government pay. Secondly, there would be an alternative to the black underground market for vulnerabilities and exploits. At least those GreyHats who make their living by selling vulnerabilities could be brought back into legality. For any other IT folks, e.g. computer science students, even you and I, who for ethical reasons never went Grey or BlackHat, can train themselves and earn additional revenue. And
third, this programme would direct many more eyes on each software package. And the more eyes, the more vulnerabilities found and the more secure our software foundations. But we are far away from that. And there might be plenty of other details which would need to be considered, too.

For the moment, we have to count on YOU (!) to make any software that you deploy or develop more secure. At CERN, there are several options for programmers and software developers:

- Follow these general guidelines or the dedicated ones for web applications or password handling
- Read a book
- Use our recommended static code analysers which help you to improve the security of your code. We have even provided a dedicated set of static analysis programmes for integration in the Gitlab Continuous Integration process
- Request a security scan for the websites you manage or invoke the APEX scanning tool if you run an Oracle APEX website
- Join our WhiteHat Challenge and learn to penetration test your software
- Or contact us at Computer.Security@cern.ch to help you!

Better code, fewer problems (2016)

The origin of many security incidents is negligence or unintentional mistakes made by web developers or programmers. In the rush to complete the work, due to skewed priorities, or just to ignorance, basic security principles can be omitted or forgotten.

The resulting vulnerabilities lie dormant until the evil side spots them and decides to hit hard. Computer security incidents in the past have put CERN's reputation at risk due to websites being defaced with negative messages about the Organization, hash files of passwords being extracted, restricted data exposed… And it all started with a little bit of negligence!

If you check out the Top 10 web development blunders, you will see that the most prevalent mistakes are:

1. Not filtering input, e.g. accepting “<“or “>” in input fields even if only a number is expected.
2. Not validating that input: you expect a birth date? So why accept letters?
3. Mistakes in session management, authentication and authorisation, e.g. when dealing with “cookies”, “tokens” or custom encryption.

There are plenty of possibilities to screw up, but there is no need to. Following a small number of quick and easy steps can make your web application watertight and secure. Learn how to prevent security incidents from happening by following a dedicated
hands-on course on “Developing Secure Software”. The next course is scheduled for 14 March and there are still a few places left, so sign up quickly…

Once you have followed that course and are longing for more, the CERN Computer Security team, together with a world-renowned “white hat” from the IT/CS Network Team, are providing in-depth training courses on penetration testing and vulnerability scanning. So far, more than 100 people have joined our hands-on training. Do you want to become a hacker too? Sign up now!

SAHARA — Security as high as reasonably achievable (2015)
http://cds.cern.ch/record/2063015?ln=en

History has shown us time and again that our computer systems, computing services and control systems have digital security deficiencies. Too often we deploy stop-gap solutions and improvised hacks, or we just accept that it is too late to change things.

In my opinion, this blatantly contradicts the professionalism we show in our daily work. Other priorities and time pressure force us to ignore security or to consider it too late to do anything…but we can do better. Just look at how “safety” is dealt with at CERN!

“ALARA” (As Low As Reasonably Achievable) is the objective set by the CERN HSE group when considering our individual radiological exposure. Following this paradigm, and shifting it from CERN safety to CERN computer security, would give us “SAHARA”: “Security As High As Reasonably Achievable”. In other words, all possible computer security measures must be applied, so long as they are feasible and cost-effective. In order to achieve this, the security aspects of a new software application, computing service or control system would need to be reviewed beforehand – in the same way that other aspects, like functionality, availability, maintainability or usability, are defined and agreed upon beforehand.

I am happy that many of our colleagues from several departments, including BE, HR, FP, TE, and the HSE Unit, contacted us very early in their development and procurement process in order to check the corresponding security footprint. Great job guys. I hope that many more will do the same!

Unfortunately, in some cases, the Security team is involved too late in the process. This was the case, once again, with some of this year’s summer students. My fear that we would need to disappoint a few of them at the end of their contracts came true once again… in particular those students who were supposed to set up a web application. Summer students tend to do everything from scratch. Thus, as usual, at the end of their contracts, they ask us to open CERN’s outer perimeter firewall for their web application. But hold on. The application runs on a laptop under the student’s desk? His/her supervisors have no idea how to maintain its “Ubuntu” operating system? The web technology is outdated? It employs “Joomla!” or “Wordpress” instead of CERN’s
Drupal? The application is using a local login or sending login passwords in plain text over the network? The webpages themselves are susceptible to common security flaws like “cross-site scripting” and “SQL injection”? It’s an impressive level-five failure for which we have to decline firewall opening. Result: complete frustration for the student who won’t have achieved a thing, a supervisor who is unhappy, and us unhappy too, for killing off a nice project.

Therefore, if you are supervising such a task, make sure your student contacts us at the very beginning. Let’s talk about good and bad IT practices; let’s talk about the building blocks already provided by the IT department; let’s talk about how to architect a good application and create well-designed software. Please spare both of us an uncomfortable situation where we have to scrap your student’s project because it is completely insecure.

In fact, the “SAHARA” paradigm should be applied to every computing service, control system, software application and web application at CERN. Consider “security” early enough in your process and it will save time, effort and frustration later on. On both sides. And it will make CERN a more secure workplace, for the benefit of the Organization’s operations and reputation!

Professionalism in security, too (2015)

At CERN, we apply a great deal of dedication and professionalism to all the work we do. This is necessary because of the complexity and sophistication of the devices we deal with. However, when it comes to computer security, we can all agree that there is room for improvement.

In some cases, we’ve observed devices that are connected to our Intranet networks without the adequate level of protection. Also, in order to allow it to be disseminated easily with peers, information is often disclosed on public webpages, sometimes without appropriate consideration of important security-related aspects. Program code is lost due to a lack of proper version control or the use of central storage systems. Systems are brought down by “finger trouble”, confusing the right and wrong IP addresses. Software or system development is done directly on production devices, impinging on their proper operation up to the point where the system grinds to a halt. Applications full of useful features lack adequate security reviews and fail simple penetration tests or security scans.

So, what about applying more professionalism to the realm of computer security? Ask yourself! If you think your service or system deserves a security review, your data might be insufficiently protected, your devices might lack resilience or robustness, or your access or development procedures might be sub-optimal and need to be better secured - then let us help you. Also, if there are general principles that require more attention with regards to security, let us know. For example, critical system
configurations and settings, including remote access to essential computing services or control systems should be protected by well-thought-out (and not commonly used) passwords.

If you have any doubts, why not let us help? We can probe your applications and improve access protection for critical or precious devices and systems. We can improve the resilience of software programs, straighten out development processes and reduce the risk of misconfiguration.

Is your code sane? (2015)


How many of us write code? Software? Programs? Scripts? How many of us are properly trained in this and how well do we do it? Do we write functional, clean and correct code, without flaws, bugs and vulnerabilities? In other words: are our codes sane?

Figuring out weaknesses is not that easy (see our quiz in an earlier Bulletin article). Therefore, in order to improve the sanity of your code, prevent common pit-falls, and avoid the bugs and vulnerabilities that can crash your code, or – worse – that can be misused and exploited by attackers, the CERN Computer Security team has reviewed its recommendations for checking the security compliance of your code.

“Static Code Analysers” are stand-alone programs that can be run on top of your software stack, regardless of whether it uses Java, C/C++, Perl, PHP, Python, etc. These analysers identify weaknesses and inconsistencies including: employing undeclared variables; expressions resulting in buffer overflows; the usage of deprecated functions (like the insecure “strcpy” in C); and the lack of input checking, filtering and sanitisation. Of course, these tools cannot beat a “four-eyes” line-by-line code review but should still be standard for software architects, developers and programmers to improve their products. So, if you are serious and professional about your job, just run them prior to compilation or – even better – within your software integration framework (e.g. Atlassian’s “Bamboo” or “Jenkins”).

Of course, we will continue to help you. Once the CERN “Jenkins” service is in production, we will also provide a procedure to run our tools from there. In parallel, we are also aiming to scan automagically all public code in Gitlab repositories for certain obvious weaknesses. Any potential hits will be automatically flagged to the owner of the corresponding repository. You can also engage one of our CERN WhiteHats and allow him/her to carry out penetration tests of your applications. And finally, just contact us if you need a fully-fledged security audit of your code stack and a review of your software architecture!

---

1 Yes! Admittedly, there is no such thing as “bug-free code”. Even `<--?php print "Hello World!"; ?>--` might be flawed. Still, we should aim to minimise bugs and eradicate them wherever we can!
How to succeed in software deployment (2014)

The summer student period has ended and we would like to congratulate all those who successfully accomplished their project! In particular, well done to those who managed to develop and deploy sophisticated web applications in the short summer season. Unfortunately, not all web applications made the final cut, moved into production and became visible on the Internet. We had to reject some... let me explain why.

Making a web application visible on the Internet requires an opening in the CERN outer perimeter firewall. Such a request is usually made through the CERN WebReq web interface. As standard procedure, the CERN Computer Security team reviews every request and performs a security assessment. This is where you, your supervisee and the Computer Security team all start to get frustrated. Many summer students delivered awesome web applications with great new functions and a good “look and feel” following precise use cases, using modern web technologies, dashboards, integrated feeds, dynamic actions in response to clicking or mouse pointing, etc. But in many cases, a deeper look raised some security concerns:

- Web applications providing access to local accounts through a login button: given that the application was intended for CERN people, why wasn’t it integrated with CERN’s Single Sign-On?
- Login pages using “HTTP”- an encrypted protocol (“HTTPS”) should have been used in order to protect passwords.
- Web pages susceptible to the usual web vulnerabilities, allowing protected information to be extracted or commands to be injected: no input validation or sanitisation.
- Web servers running outdated operating system versions or web applications: who will keep them up to date in the future? How?
- Server hardware hidden under office desks or on personal laptops: who will own and maintain them in the future?
- Use of technologies similar to those provided by the IT Department: there is no need to reinvent the wheel...

It is a pity that such projects sometimes (seem to) start without properly consulting with IT experts. The CERN Computer Security team is ready to provide you with such consultation, perform penetration testing, assess the security footprint of new systems and audit existing deployments. We can help you choose the appropriate technologies and assist you in system design (of course, you will still do most of the work). As we said in an earlier Bulletin article (“Stop fighting alone, let synergy rule!”), the IT Department provides a long list of centrally supported applications and services. Instead of managing and patching your server hardware yourself, you can obtain a centrally managed server or virtual machine that is kept up-to-date by the IT Department. They also provide centrally managed Web servers, content management...
systems, databases, file storage systems, and engineering applications that are properly managed, adequately secured and maintained long term. That allows you and your supervisees to delegate your responsibility for security to the IT Department and to avoid the burden of managing it yourselves (and possibly failing). Instead, your supervisees can focus on their core work and deliver a great project that will make it into production to the benefit of users inside and outside CERN!

Finally, dedicated training also helps (“Improve software, avoid blunder”) and the CERN training catalogue offers a variety of dedicated training courses for software developers. All you need to do is to sign up your supervisees!

Join the CERN WhiteHat Challenge! (2014)

Over the past couple of months, several CERN users have reported vulnerabilities they have found in computing services and servers running at CERN. All were relevant, many were interesting and a few even surprising. Spotting weaknesses and areas for improvement before malicious people can exploit them is paramount. It helps protect the operation of our accelerators and experiments as well as the reputation of the Organization. Therefore, we would like to express our gratitude to those people for having reported these weaknesses! Great job and well done!

Seizing the opportunity, we would like to reopen the hunt for bugs, vulnerabilities and insecure configurations of CERN applications, websites and devices. You might recall we ran a similar initiative (“Hide & Seek”) in 2012 where we asked you to sift through CERN’s webpages and send us those that hold sensitive and confidential information. Quite a number of juicy documents were found and subsequently removed. However, if we probe deep, we have to apply due care. Not all our applications are robust and resilient enough to withstand vulnerability scanning and penetration testing. It is of the utmost importance that random testing of CERN applications, websites or devices does not stop them from working, delete their contents or render them broken. Therefore, a bit of training and coordination is needed.

Enlist with us and join the CERN WhiteHat Challenge! In order to prepare you, we are planning to hold a half-day work-shop on vulnerability scanning, penetration testing and proper ethics early in the autumn this year. The only prerequisites are programming skills and/or knowledge of system/service administration. Once you have followed and completed the workshop, you will be eligible to conduct penetration tests on CERN applications, websites and devices of your choice. All you will need to do is suggest your favourite area that you would like to test... We will coordinate with the corresponding service manager in order to get a suitable time window or test instance. Once ready, you are “go” to try your vulnerability assessment and penetration testing skills on real applications and live devices. This setup will make your challenge a win-win for everyone: your engagement as a security tester, and the security and
robustness of the area you’ve tested! If you are interested in becoming an official CERN WhiteHat, sign up by sending an email to Computer.Security@cern.ch with subject “Make me a CERN WhiteHat”.

However, please note: the academic curiosity and the perseverance of a nerd shall be your only motivation for this challenge. As compensation, we offer full kudos, a good book on security matters, a letter of appreciation to be sent to your supervisor, and a mention of your findings in our Monthly Report. Of course, such an activity also looks good in your CV. However, we do not and will not provide financial compensation (and have even turned down such requests in the past). If you want to make some money, it is better to look for bugs and weaknesses in Google (earn $100 to $20,000), Facebook ($500 flat), Microsoft (rewards up to $100,000), or elsewhere. But note that such an activity against third parties is your personal business and must NOT be conducted from the CERN network (as it violates the CERN Computing Rules).

The security marathon (2014)

If you believe that “security” is a sprint, that a quick hack is invulnerable, that quick bug fixing is sufficient, that plugging security measures on top of existing structures is good, that once you are secure your life will be easy... then let me convince you otherwise.

An excellent example of this is when the summer students join us at CERN. As the summer period is short, software projects must be accomplished quickly, like a sprint. Rush, rush! But often, this sprint ends with aching muscles.

Regularly, these summer students approach us to have their project or web server made visible to the Internet. Regularly, quick security reviews of those web servers diagnose severe underperformance with regards to security: the web applications are flawed or use insecure protocols; the employed software tools, databases or web frameworks are sub-optimal and not adequately chosen for that project; the operating system is non-standard and has never been brought up-to-date; and the server hardware is old and no longer supported. So, unfortunately, we often must decline making their project public on the Internet. Their fun sprint ends with them in the hospital. Game Over.

In reality, “security” is a marathon. It requires detailed preparation, proper integration and scheduling. Just as running a marathon becomes a part of life, “security” is a part of software development. Thus, as for every marathon run, you need to prepare well. In software programming, being “well prepared” means having a proper software development lifecycle (SDLC).

A good SDLC extends “programming” to phases on software design and repeated testing. Only with proper functional specifications is it possible to verify whether code works as intended, i.e. fulfilling the specified use cases. “Security” is just another
aspect of checking whether the code can be abused or not. We have compiled a list of hints and tips for the various phases of your SDLC. Good books on that are available by R. Anderson (“Security Engineering”) or G. McGraw (“Software Security”). Automatic tools like “flawfinder” might help you discover the easy bugs. We have produced a long list of such automatic static code analysis tools for many different programming languages. Regular training is another step. The computer security team provides adequate training sessions on web application development and programming, Java, C/C++, Python, PHP and Perl. Just check our training web page.

The security marathon, part 2 (2014)

Do you recall our latest article on the “Security Marathon” (see here) and why it’s wrong to believe that computer security is a sprint, that a quick hack is invulnerable, that quick bug-fixing is sufficient, that plugging security measures on top of existing structures is a good idea, that once you are secure, your life is cosy?

In fact, security is a marathon for us too. Again and again, we have felt comfortable with the security situation at CERN, with dedicated protections deployed on individual hosts, with the security measures deployed by individual service managers, with the attentiveness and vigilance of our users, and with the responsiveness of the Management. Again and again, however, we subsequently detect or receive reports that this is wrong, that protections are incomplete, that security measures are incomplete, that security awareness has dropped. Thus, unfortunately, we often have to go back to square one and address similar issues over and over again with the same people.

So, security is a marathon. Sometimes it is even like a marathon combined with hurdles on a balance beam: you have to dodge obstacles and are doomed if you get the balance wrong. Like every other marathon, security requires lots of external assistance and support. On the other hand, it also demands a high frustration threshold, some stubbornness and a lot of perseverance. And as an excuse to all those whom we have pushed too hard - the balance beam is sometimes very thin, so please have mercy!

Let us continue together protecting CERN’s computing facilities and keeping them secure. Please do not repeat the same mistakes made in the past; there will be plenty of opportunities to make new ones. If you run a computing service or develop software (who doesn’t nowadays?), please:

- Do not reinvent the wheel. Make your life easier and use the central services provided by the IT Department;
- Get the adequate training for your favourite programming language;
- Program properly and deploy a thorough software development life-cycle;
- Use static code analysers to detect basic flaws in your software;
- Follow our Security Baselines in order to get your service properly set up.
Recently, a severe vulnerability has been made public about how Apple devices are wrongly handling encryption. This vulnerability rendered SSL/TLS protection useless, and permitted attackers checking out a wireless network to capture or modify data in encrypted sessions.

In other words, all confidential data like passwords, banking information, etc. could have been siphoned off by a targeted attack. While Apple has been quick in providing adequate security patches for iOS devices and Macs, it is an excellent example of how small mistakes can lead to big security holes. [Here](http://cds.cern.ch/journal/CERNBulletin/2014/20/News%20Articles/1698263?ln=en) is the corresponding code from Apple’s Open Source repository. Can you spot the issue?

```c
static OSStatus
SSLVerifySignedServerKeyExchange(SSLContext *ctx, bool isRsa, SSLBuffer signedParams, uint8_t *signature, UInt16 signatureLen)
{
    ...  
    if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
        goto fail;
    ...  
    fail:
    SSLFreeBuffer(&signedHashes);
    SSLFreeBuffer(&hashCtx);
    return err;
}
```

There you are!

The bug was introduced in line 10 most likely due to one copy/paste too many. While the “goto” in line 9 is executed only if the “if”-statement of line 8 is true, the additional “goto” of line 10 bypasses the subsequent security checks and the SSL connection is unverified. Such bugs are also not uncommon at CERN!

Security is an integral part of software in the same way as availability, functionality, maintainability and usability. More secure code means fewer interventions to fix and patch problems, thus increasing availability and improving maintainability. More secure code also means better control of user interfaces and user input, thus enhancing
usability and functionality. Therefore, we strongly encourage you to perform in-depth testing of your software prior to deployment. Simply enable your compiler’s warning (“gcc –Wall –Wextra -Werror” for C/C++ or “javac –Werror –Xlint:all” for Java) and check the settings of your favourite editor or development environment.

Do not hesitate to use several compilers on your code: “clang” is a good alternative to gcc that may help you to find problems, and has nicely coloured output. Compiler warnings can point you to suboptimal coding practices too. In addition, deploy one of our static code analysis tools. These tools are supposed to review your code quickly, looking for some common potential bugs and vulnerabilities (both security- and non-security-related), thus increasing the reliability and security of your programs. The same webpage also provides recommendations on how to keep “secrets” secret and how to secure web applications, as well as a “Security Checklist”.

In addition, do not hesitate to contact us at Computer.Security@cern.ch for consultancy or a dedicated full-scale security audit, or check out our dedicated training sessions on secure coding, scheduled for Spring/Summer 2014:

- Developing secure software (4 hours)
- Secure coding in C/C++ (1 day)
- Secure coding in Perl (1 day)
- Secure coding in Python (1 day)
- Securing Java Applications (1 day)
- Securing Java and Web Applications (1 day)
- Securing PHP Web Applications (1 day)

Stop fighting alone, let synergy rule! (2013)

Could it be true, as it seems to me, that CERN still has manpower to spare? I thought that now, during LS1, resources were scarce and everybody was very busy. But apparently not. We are getting more requests than ever to open firewalls for stand-alone web servers running local databases and custom web applications.

What we are talking about here are “newly” created software applications with similar functions to existing alternatives. We often encounter computing hardware and network equipment managed in multiple ways by multiple people, and commercial software or cloud services that closely resemble CERN’s existing computing services are bought or rented – for instance, SurveyMonkey vs. SharePoint or tinyurl.com vs. cern.ch/go. Why does CERN run two document stores, CDS and EDMS, that provide similar functions and workflows? Wouldn’t one be sufficient? And four (or more!) JIRA ticketing systems? Why are there so many local Git instances, dozens of servers providing Drupal web content management and several Twikis?
In other words, why do we reinvent the wheel again and again? Why do we devote our resources to duplicating and triplicating activities on similar services? It can be partly explained by the natural drive for the new, for playing, for learning, for striving to achieve better. It is also much more fun to build something yourself and not “just” use existing solutions, and as those existing solutions never exactly match your requirements 100%, this gives a good excuse to start from scratch.

On the other hand, we have on more than one occasion declined to open the CERN outer perimeter firewall for a custom-built service sitting under the desk of a physicist. Not because these services are bad as such; on the contrary, they usually provide great new functions and a good “look and feel”. However, behind the scenes, the set-up is often sub-optimal, long-term maintenance not guaranteed, and security protections lacking. This forces us to deny any opening of the firewall and request that the developer concerned start over. We therefore have to ask ourselves if it’s really in the Organization’s best interests to start from scratch over and over again. Shouldn’t we manage our resources better? Is it really so much more fun to take new roads than to improve existing ones?

Setting up a Drupal web server, a Twiki, a JIRA instance or a database is not rocket science, but maintaining its viability and security in the long run is more difficult. Long-term viability and consistent operation are key for a good service, but this requires more work - hard work that is not necessarily as much fun as setting the system up in the first place. In addition, for us, managing the security of one central service that is provided, maintained and secured by trained and hired professionals is much easier than managing a cacophony of soon-forgotten applications in random locations. So why not just use the central services provided free by the IT Department instead? This is ideal as it saves you time that can be spent on something more important, as long as you accept that the IT Department’s solution has some (probably acceptable) limits and might not always completely match your needs. But let’s not settle for that! Let’s put an end to computing services not being able to offer 100%. Instead of wasting resources on individual standalone solutions, we should team up and help the IT Department to deliver the solutions we want! We should stop fighting alone and instead join forces with the department to provide sustainable computing services for everyone. Let synergy rule and free up your time for the real challenges!

We are interested in your opinion! Please write to us at Computer.Security@cern.ch.

Finally, do you want to know how you can help us to provide a better service? Join our dedicated training sessions on secure coding scheduled for September 2013:

- Secure coding in C/C++ (1 day)
- Secure coding in Perl (1 day)
- Secure coding in Python (1 day)
- Securing Java Applications (1 day)
- Securing Java and Web Applications (1 day)
Secure Software Development

- **Securing PHP Web Applications** (1 day)
- **Developing secure software** (4 hours)

**Why can't I sue my software provider? (2013)**


Imagine buying a new car, fixing its number plates on and driving it off to the autobahn in order to test whether the 250km/h top speed on the speed meter is genuine. However, there's too much traffic, and you have to slow down. You hit the brakes but they don't respond. You break through the crash barrier, enter a field and manage to stop the car. You are not hurt, but the car is a write-off…

Fortunately, you will not lose out. A car's safety is the responsibility of the manufacturer and you can sue them for compensation. Even worse for them, if it turns out to be a design flaw they will need to recall and fix all the cars of that model – at their expense. Thus, legal requirements and pressure from clients and automobile clubs ensure that cars are reliable and safe.

Now, imagine you've just downloaded a new web browser. You install it on your laptop and connect to the Internet. But your new browser is flawed, and malicious attackers quickly exploit its vulnerability. They manage to hack your Amazon, e-bay and PayPal accounts and go off shopping with your money. You might not be the only one concerned: hundreds of thousands of other people may be affected, and millions of dollars of losses may be incurred. But when you notify the corresponding software provider, you get nothing but silence. Only after a few months, after security companies and the media have repeatedly reported the security risks associated with the browser, does the provider issue a short statement and acknowledge the facts.

As I expect my car to be safe, I also expect the software I use to be secure. Unfortunately, the latter seems not to be the case. So who has to do the due diligence when using/providing software applications? Why is it that security is not handled like safety? Why can I sue my car manufacturer but not my software provider?

I believe the roots of this mismatch lie in the fact that many software packages are flawed from design, that many technologies have valid use cases but can at the same time be misused and that many companies just don't care. Money and legislation are the best incentives for making reasonably secure software. But there is no regulation (yet) requiring Adobe, Apple, Microsoft or Siemens to make security a priority.

Microsoft has learned its lesson, having been clobbered in the past due to its insecure pre-Windows XP SP2 operating system, and is actively pushing for a secure software development life cycle. Money was the driving force. Apple seems to do well in providing secure software but its communication when dealing with new vulnerabilities leaves much to be desired. Siemens learned its lesson after the Stuxnet attacks.
against its PLCs and is now reviewing how to thoroughly deploy security as another development criteria.

So, we are still left with the consequences. We are the ones who bear the costs of their vulnerabilities. We are obliged to take protective and detective measures. We have to carry the costs of patching and anti-virus software. We have to do due diligence... Image if you had to do the same for your car! So, do we need regulations and laws to force software vendors to provide better, inherently secure code and protected devices? We are eager to hear your opinions. Write to us at Computer.Security@cern.ch.

By the way, what is a good incentive for you to provide secure code? Remember our Bulletin article on “A Short Tale of the Black Sheep of –ITY” and that security has to form an integral part of the overall picture in the same way as availability, functionality, maintainability and usability. More secure code means fewer interventions to fix and patch problems, thus increasing availability and improving maintainability. More secure code means better control of user interfaces and user inputs, thus enhancing usability and functionality. If you would like to learn how to do better, contact us at Computer.Security@cern.ch for consultancy or a dedicated full-scale security audit, or check out our dedicated training sessions on secure coding scheduled for September 2013:

- Secure coding in C/C++ (1 day)
- Secure coding in Perl (1 day)
- Secure coding in Python (1 day)
- Securing Java Applications (1 day)
- Securing Java and Web Applications (1 day)
- Securing PHP Web Applications (1 day)
- Developing secure software (4 hours)

Raise your defence: A baseline for security (2011)

It is an unfair imbalance: the (computer) security of a system/service is only as strong as the weakest link in the chain of protection. This provides attackers with an incredible advantage: they can choose when to attack, where and with which means. The defence side is permanently under pressure: they must defend at all times all assets against all eventualities. For computer security, this means that every computer system, every account, every web site and every service must be properly protected -- always.

In particular, at CERN, those services visible to the Internet are permanently probed. Web sites and servers are permanently scanned by adversaries for vulnerabilities;
attackers repeatedly try to guess user passwords on our remote access gateways like LXPLUS or CERNTS; computing services, e.g. for Grid computing, are analysed again and again by malicious attackers for weaknesses which can be exploited. Thanks to the vigilance of the corresponding system and service experts, these attackers have not been too successful so far.

However, applying basic security measures is not easy, in particular when you are not familiar with security concepts and protection measures: certain aspects might be overlooked or omitted. This might render a system or service open to attack when the corresponding experts believe their system/service is secure! In order to provide better guidance, the Computer Security Team has published a series of so-called Security Baselines:

- Security Baseline for servers, PCs and laptops (EDMS 1062500)
- Security Baseline for file hosting services (EDMS 1062503)
- Security Baseline for Web hosting services (EDMS 1062502)
- Security Baseline for Industrial Embedded Devices (EDMS 1139163)

These Security Baselines define basic security requirements and are intended to be pragmatic and complete, but do not imply technical solutions. They should serve as guidelines for system/service experts. For all critical systems/services, however, the corresponding owner must produce a so-called “Security Implementation Document” and outline how their system/service meets the corresponding Security Baselines. The system/service must be implemented and deployed in compliance with this Implementation Document. Non-compliance ultimately leads to reduced network connectivity (i.e. closure of any outer perimeter firewall openings, ceased access to other network domains, or complete disconnection).

Do you write secure code? (2011)

At CERN, we are excellent at producing software, such as complex analysis jobs, sophisticated control programs, extensive monitoring tools, interactive web applications, etc. This software is usually highly functional, and fulfils the needs and requirements as defined by its author. However, due to time constraints or unintentional ignorance, security aspects are often neglected. Subsequently, it was even more embarrassing for the author to find out that his code flawed and was used to break into CERN computers, web pages or to steal data…

Thus, if you have the pleasure or task of producing software applications, take some time before and familiarize yourself with good programming practices. They should not only prevent basic security flaws in your code, but also improve its readability, maintainability and efficiency. Basic rules for good programming, as well as essential
books on proper software development, can be found in the section for software developers on our security web page. You can also easily test your software yourself. Check the warnings of your compiler thoroughly, and run one of our suggested static code analysers. In addition, the HR technical training provides an excellent course on secure programming in Java, C++, Python, Perl, and web languages. The next one-day, hands-on courses are on securing PHP, Java, and Web applications (September 27th, 28th, and 29th, respectively), as well as on secure programming in Python (October 28th). There are still places available! Finally, do not hesitate to contact Computer.Security@cern.ch if you prefer an external review of your software!

So, how about your skills in writing secure software?

If you want to win one of three marvellous books on software security, please check the short program below and send in the programming flaws you have identified by 12 September to Computer.Security@cern.ch:

```
/* Safely Exec program: drop privileges to user uid and group
 * gid, and use chroot to restrict file system access to jail
 * directory. Also, don’t allow program to run as a
 * privileged user or group */
void ExecUid(int uid, int gid, char *jailDir, char *prog, char *const argv[])
{
    if (uid == 0 || gid == 0) {
FailExit("ExecUid: root uid or gid not allowed");
    }

chroot(jailDir); /* restrict access to this dir */
setuid(uid); /* drop privs */
setgid(gid);
fprintf(LOGFILE, "Execvp of %s as uid=%d gid=%d\n", prog, uid, gid);
flush(LOGFILE);
execvp(prog, argv);

(Courtesy of Barton Miller, University of Wisconsin, Madison, US)
```

Of course, if you have questions, suggestions or comments, please contact Computer.Security@cern.ch or visit us at http://cern.ch/security.
... An example of flawed code (2011)

Do you recall our small exercise in the last issue of the Bulletin?

We were wondering how well written the following code was:

```c
/* Safely Exec program: drop privileges to user uid and group
   * gid, and use chroot to restrict file system access to jail
   * directory. Also, don’t allow program to run as a
   * privileged user or group */
5 void ExecUid(int uid, int gid, char *jailDir, char *prog, char *const argv[])
6 {
7 if (uid == 0 || gid == 0) {
8 FailExit("ExecUid: root uid or gid not allowed");
9 }
10
11 chroot(jailDir); /* restrict access to this dir */
12
13 setuid(uid); /* drop privs */
14 setgid(gid);
15
16 fprintf(LOGFILE, "Execvp of %s as uid=%d gid=%d\n", prog, uid, gid);
17 fflush(LOGFILE);
18
19 execvp(prog, argv);
20}
(Courtesy of Barton Miller, University of Wisconsin, Madison, US)

Indeed, it was not so well written since it contained at least 13 flaws:

1. Line 1: Incomplete specification: Does it run *arbitrary* commands or just a few selected ones? Who checks for errors? The function or the caller? Does it run on *arbitrary* chroot jails? What about thread-safety? Is this expected to run in a multithreaded environment?
2. Line 5: Depending on the platform, there may be integer-related issues.
3. Line 5: No sanitization of "jailDir". For example "/" will do nothing.
4. Line 11: No check for errors on "chroot". chroot("") or chroot(NULL) would bypass the jail.
5. Line 11: Missing "chdir(jailDir)" before the chroot, or chroot("") after it.
7. Lines 13/14: setuid & setgid run in the wrong order.
8. Lines 13/14: No checks for errors, so the attacker may choose some random number for uid and gid and run the program as root.

9. Line 16: Is LOGFILE actually open? This may crash the program, or may make it exploitable.

10. Line 19: No sanitization of prog, it may cause NULL pointer dereferences, crashes, etc. and make the code exploitable.


12. Line 19: No error handling: if execvp() returns it means there is some error to be handled. The specification is weak in this case.

13. If the program runs in a multithreaded environment, sanitization will have to make private copies of jailDir, prog and argv[] and perform the checks on them.

The winners of the three marvellous books on software security are Bertrand Lefort (BE/OP), Paolo Torelli (extern) and Remi Mommsen (CMS). Congratulations!!!

You think this is not easy? True --- and this is the advantage for any attacker. He just has to find a few flaws to exploit that code and take over the corresponding server. Thus, please check basic rules for good programming as well as essential books on proper software development in the section for software developers on our security web page. Also, you can easily test your software yourself. Thoroughly check the warnings from your compiler and run one of our suggested static code analysers. In addition, HR technical training provides excellent courses on secure programming in Java, C++, Python, Perl and web languages. The next one-day, hands-on courses are on securing PHP, Java and Web applications (September 27th, 28th, and 29th, respectively) as well as for secure programming in Python (October 28th). There are still places available!!!

Finally, do not hesitate to contact Computer.Security@cern.ch if you prefer an external review of your software!
Data Protection and Privacy

Computer Security: Don’t print naked (2019)

If you are interested in what is going on at CERN, about professional projects and plans, or private problems and parties, hanging out at one of CERN’s printers is a very effective approach (but, please… don’t!). Too many people are still printing confidential documents without caring that they might be read by third parties hanging around – see for example the image of a document found on one of CERN’s printers earlier this year…

![Image of a document found on a CERN printer]

This shouldn’t happen. Confidential documents, documents with sensitive content, personal information or private e-mails should be properly protected – even when they are converted to paper format.

The CERN printing infrastructure is capable of ensuring the confidentiality of your documents: you can send a print job in such a way that it will not be printed until you input a PIN code at the machine. So the next time you need to print such a document, go to “Printer Properties” (1) and select the “Secure Print” method (2). Once you hit the “Print” button, you will get another dialog box asking you to provide a PIN number (3). Below, you can see screenshots of the different steps on the Windows platform.
Instructions for other operating systems can be found in this ServiceNow knowledge base article.

After you have provided the PIN, your document will be queued on the printer of your choice. For easy PIN input on the printer, we recommend you use any Canon machine. The printer will hold your document for the next 12 hours (4 hours on some models). Once you are at the printer, hit the “SCAN/PRINT” button, choose “Secure Print” (4), select the jobs you want to print (5), hit “Print”, and punch in your PIN (6) (Note: this sequence may vary between models).

Your document is only printed after you provide the correct PIN. And as you are now standing beside the printer, you can be confident that your confidential document is being handled confidentially. And, even better, you can set this as your default printing preference and ensure none of your printouts go walkabout again! See these knowledge base articles for more details – including short video tutorials.
So, don’t let confidential information leak… use the “secure print” function on your nearest preferred printer. And: respect the environment. Don’t print unless it is necessary. Confidential documents that are never printed are less likely to slip out of your control!

A “file drop” for confidential data (2019)

Do you often find yourself in situations where you would like to share documents with your colleagues, or need to ask people to provide you with documents? Given that many encryption solutions (in particular e-mail encryption) require a certain level of IT skills, such documents invariably end up being requested and sent via e-mail and are therefore unencrypted and hence visible to anyone, as the standard e-mail protocol does not come with any protection. Confidentiality rating: zero. This means only one thing: alternative communication channels are needed…

Rather than using e-mail, why not try CERN IT’s CERNbox service (https://cernbox.cern.ch)? It encrypts the transmission of documents during the sharing process, avoids the proliferation of copies by offering a single place to deposit a file, and allows revocation of access (useful for example in the case of erroneous attachments or recipients). Even better, for receiving documents it allows you to create a unique web address where anyone can deposit a file for you.

This means that it represents the perfect method to allow anyone to upload files intended to be shared with you in a secure and confidential manner. It is a “file drop” functionality where anyone can “drop” any kind of file into a dedicated folder, which is only accessible to you and to those whom you expressly grant access. Using a web browser, and a secured HTTPS connection, the communication is well encrypted using an established web standard. Via this method, files can easily be dropped from any Internet-connected device. All you need to do is to provide your external clients a unique web address (like https://cernbox.cern.ch/index.php/s/LnBpPZymsoFEEW1) where they can upload any file required. Once this is done, no one but you will be able to see it. Overwriting or deleting the information is also impossible.

So if you are working for a service which regularly requests documents from third parties or external collaborators, CERNBox is particularly useful as you can set up a unique web address which can be given to anyone. So, give it a go! Here is the recipe:

1.) Go to https://cernbox.cern.ch and log in;
2.) Create a new folder by left-clicking on the “+” symbol on the middle-top, select “Folder” and give it a name;
3.) Once created, Left-click the “<” (share icon) on the right-hand side of your folder: a menu will open up;
4.) Under “Sharing”, select “Public Links” and click on “Create public link”;
5.) Select “Upload only (File Drop)” and click on “Share” (you can also define a password and an expiration date, but please note that this is not recommended here);
6.) In the right-hand menu, you will then see an entry for your folder and below it a unique link/URL. This is the drop box [MS1] folder you can now securely share with your peers for upload;
7.) Check the folder regularly to see newly uploaded files.


Transparency for your privacy (2017)

The CERN Computer Security Officer and his team are mandated by the Organization to protect its users, the operations and reputation of CERN against cyber threats. In order to fulfil this mandate, prevention, protection and detection are key. The team therefore has the means to monitor any digital activity happening at CERN. We are well aware of the trust the Organization has put in us, and treat it with the highest care and integrity. Still, we would like to reaffirm our opinion that transparency in itself is paramount for any security service (see also our Bulletin article on “Transparent Monitoring for your Protection”).

The Computer Security Team’s Digital Privacy Statement describes under which circumstances and conditions the CERN Computer Security team gathers, accesses, uses and shares information about you or your usage of CERN's computing facilities and how the team protects this information. It lists our detection capabilities and how they concern your privacy. It sets the rules and regulations to which we are bound when accessing our monitoring information or, in very controlled cases, your data. While we acknowledge that such transparency might also play into the hands of attackers targeting CERN, we still believe that our transparency towards you is paramount, and you should be aware of our work.

Confidentiality is everybody’s business (2015)

Unfortunately, this is but one example of such mistakes. We have seen other documents made accessible to a much wider audience than originally intended…

CERN takes serious measures to ensure the confidentiality of data. Confidential or “sensitive” documents (following the nomenclature set out in the CERN Data Protection Policy) deserve professional handling and access protections given only to the people...
who really need to access them. As such, they must not be widely circulated as
attachments in e-mails and, most definitely, must not be stored on random public
websites for the sole purpose of sharing them. Instead, these documents should reside
in their original storage location (like AFS, Alfresco, CDS, DFS, EDMS, INDICO,
Sharepoint) and the corresponding access controls should be adapted so that all
people who need access are granted it and everyone else’s access is blocked.

The level of protection is clearly marked in EDMS (“Public access”, “Restricted
access”) and INDICO (“public”, “restricted” or edit the event and check the “Protection”
tab). For AFS and DFS, instructions for properly protecting files can be found [here](http://cds.cern.ch/journal/CERNBulletin/2015/12/News%20Articles/2000992?ln=en)
and [here](http://cds.cern.ch/journal/CERNBulletin/2015/12/News%20Articles/2000992?ln=en), respectively.

Confidentiality is everybody’s business! Think twice before passing on sensitive
documents. Act professionally and use your judgment. Keep the document in its
original place and just share its link or location.

Alternatively, use CERNbox, which even allows you to share documents with people
who don’t have a CERN computing account. However, still remember to configure the
access protections as restrictively as possible. Remember, members of the personnel
are accountable for maintaining the confidentiality of the data entrusted to them. Any
breach of that trust may lead to administrative or even disciplinary action.

Printing confidentially (2015)

Have you ever hesitated to print a confidential document using CERN printers? Or
perhaps you have rushed quickly to the printer after hitting the “print” button in order to
avoid someone else getting hold of and reading your document? These times are over
now with the new printing infrastructure!
Indeed, many of us regularly print out confidential documents like our salary slips, MARS forms, tendering documents and drafts of preliminary papers. The upcoming CERN data protection policy will require all of us to respect the confidentiality of such documents and, as the word “confidential” implies, access to “confidential” or sensitive documents will be tightly controlled. What can we do about the public printers located in many buildings, floors and shared spaces - accessible not only to CERN staff and users but also to visitors and guests? Some printers are located in the vicinity of restaurants, cafeterias or close to paths taken by visit groups. Of course, this contradicts the need for privacy when printing confidential documents.

Thanks to the CERN Print Service, the new printing infrastructure is now capable of ensuring the confidentiality of your documents: you can send a print job that is not printed until you input a PIN code at the machine. So the next time you have to print such a document, go to “Printer Properties” (1) and select the “Secure Print” method (2). Once you hit the “Print” button, you will get another dialog box asking you to provide a PIN number (3). On the right, you'll find screenshots of the different steps on the Windows platform. Instructions for Linux and Mac OS can be found in this ServiceNow knowledge base article. After you have provided the PIN, your document will be queued for the printer of your choice. For easy PIN input on the printer, we recommend you use any Canon machine. The printer will hold your document for the next 12 hours (4 hours on some models). Once you are at the machine, hit the “SCAN/PRINT” button, choose “Secure Print” (4), select the document you want to print (5), hit “Print”, and punch in your PIN (6) (Note: this sequence may vary between printer models).

Your document is printed only after providing the correct PIN. And as you are now standing beside the printer, you can be confident that your confidential document is being handled confidentially.

Thirty years since "1984" — How close was Orwell to today’s interconnected world? (2014)


This year marks the 30th anniversary of the time depicted in the novel 1984, written by the visionary George Orwell in 1947/8, as well as the 25th anniversary of the World Wide Web being invented at CERN. To mark this occasion, both the Cineglobe Film Festival at CERN and the Latitude Festival in the UK are holding panel discussions on the technological and socio-cultural implications of our infinite connectedness in an age of internet surveillance: “How close is our world to that of Orwell's nightmare?”

The novel 1984 describes the fate of its protagonist Winston Smith and his love interest Julia. The setting is “Oceania”, one of three supra-nations at war with one another, a dictatorship blocking all free will (considered to be “thoughtcrime”), altering inconvenient historical truths (using “Newspeak”) and permanently monitoring its citizens (the origin of the phrase “Big Brother is watching you”). Luckily, neither the
year 1984 nor 2014 has seen world-spanning dictatorships, although many local dictatorships have appeared and disappeared in nations trying to find their way to democracy. The World Wide Web, Twitter and Facebook have actually helped to overthrow dictatorships, at least in the short term. Orwell was wrong on that one. Thank goodness.

However, what about free will? We might believe that it exists, but aren’t the media and the World Wide Web influencing our thoughts, attitudes and opinions more and more? With a flood of information out there, we have to be selective. It is natural to listen to, read and watch what we like and to ignore or suppress what we don’t. Our chosen media outlets, RSS feeds, Tweets and Facebook or Google+ group memberships already lead to biases based on our own preferences. For example, you will notice that web advertisements often refer to things you have recently searched for or bought (thanks to Google AdSense).

A recently published psychological study conducted on Facebook manipulated users’ news feeds so that half of the unwitting participants were presented with more positive content while the other half received more negative content. The study found that the participants’ moods were not significantly altered, but the damage was done: Facebook had exercised the means to manipulate the information that forms the thoughts, attitudes and opinions of its users… In addition, with Google’s profiling capability, which allows it to know what we are interested in, who can guarantee that our searches produce objective results? For example, if I search for “wine Côtes du Rhône”, do I (someone who prefers juice) get exactly the same results as a connoisseur? Google might not use this capability, but the potential is there. Thus, Orwell was quite right on that point.

With the dominance of just a few big search engines and media outlets, this also opens Pandora’s box to alter the past (in fact, powerful stakeholders have rewritten history again and again!). Some nations already block websites with undesirable content, opinions and suchlike. In the future, in addition to showing us only what we like to see, major search engines could also completely delete unwanted information from their archives — possibly including not just information subject to the “right to be forgotten” but also information contradicting their values or opinions. Therefore, Orwell is potentially right one this one, too.

Finally: “Big Brother”. Governments’ permanent monitoring of their citizens has already been discussed in past Bulletin articles (e.g. “Security vs. Nations: a lost battle?”). But instead of “Telescreens” spying on us, many of us willingly deploy the means ourselves: smartphones track us as we roam around; social media aggregates our opinions and feelings; cloud services store our private data; mobile webcams or Google Glass record what we see at a given moment; even our health status can be transmitted to dedicated web portals using smart wristbands; and soon we could all have cute little Jibo robots assisting us in our homes.
Thus, (too?) often we voluntarily give away data in exchange for a few extra amenities. But sometimes it’s against our will: certain LG TV screens were found to be recording and transmitting back information on the viewing habits of their users and Microsoft’s new Xbox One Kinect camera was suspected of doing so too. In the near future, SmartMeters will monitor our energy consumption in detail, enabling energy companies to predict whether we are at home and what we are doing. In summary, Orwell was once more on the right track, but he wildly underestimated the extent of monitoring by governments and ignored the monitoring efforts of private companies and our willingness to comply.

So, how close was Orwell to today’s interconnected world? He wasn’t. We have gone far beyond what George Orwell imagined, and we should start discussing the social implications of this and our personal responsibility. For a start, we could rethink what we expose on Facebook, Google+ and Twitter and we could use, for example, DuckDuckGo or StartPage as alternatives for web searches.

Working privately in public (2014)

Gosh, was he annoyed! I just came back from a long duty trip. Nine hours straight on the plane. As usual plenty of time to get some long awaited emails answered, time to write another document, and to prepare some presentations. The guy sitting next to me was probably thinking the same. So, from time to time I gazed over and looked at his screen following what he was working on. Curiosity is part of my job. Laptop screens are attractive. Discretion is part of my job, too. But given the confined space in the economy class of an Airbus, the screen was just shining at me and he was not able to move away or reposition his screen... He seemed to feel increasingly uncomfortable. Consequently, he gave up and read the newspaper instead. Obviously annoyed. He could have protected himself better...

Has this also happened to you? On the plane? On the train? In a restaurant? Or even in a conference or seminar? Do you care? If you do, what about clipping a “privacy screen” onto your laptop display? Such a privacy screen - technically just a polarisation filter - blocks any view from the side while you still have the full picture (assuming you sit in front of your laptop!). A large variety of privacy screens are available through the CERN stores. Just make a “Material Request” on EDH, click on the “Distrelec” punch-out catalogue and search for “privacy filter”. Make sure that you get the proper size. With it, you will feel more comfortable when working e.g. on the tram, on the train, in the restaurant... or on the plane!

So how much is your privacy worth? If you happen to deal regularly with confidential documents and travel a lot, why not invest a few francs in a privacy screen? Your next flight home for Christmas might already be booked! Also note that the upcoming CERN
Data protection policy will require all of us to respect confidentiality when handling sensitive documents like calls for tenders, MARS forms, personal files...

P.S. Please also note that many conference rooms and some control rooms are equipped with video conferencing cameras. You might be watched when working on your laptop. And it can be quite embarrassing if you are caught on camera when picking your nose or browsing some non-work related web pages. In order to make you aware of this, the CERN Video Conference Support Team is now installing “On Air” signs in all conference rooms.

Coming soon, a pragmatic data protection policy for an open organisation (2014)

Like any other organisation/employer, CERN holds confidential data, e.g. medical records, personnel files, files on harassment cases, NDAs & contracts, credit card information, and even unpublished scientific results. Unfortunately, our current methods of handling such documents are inadequate owing to a lack of clarity with regard to responsibilities and obligations.

So, from time to time, some documents have become public that should not have (such as the premature publication of videos about the 2012 “Higgs” announcement); some of us have accidentally leaked confidential information (such as passwords used to access accelerator and experiment control systems in 2011); other colleagues have lost their laptops or had them stolen (e.g. from a delegation on duty travel in 2013) along with the e-mails and private files saved on them. Fortunately, these times of inadvertent data loss and lack of clarity concerning our obligations should soon be over.

A proposal for the establishment of a CERN-wide Data Protection Policy (DPP), adapted to the open environment of the Organization was presented at the most recent meeting of the Enlarged Directorate. This policy is intended to establish rules on how to classify data systematically, how to subsequently store and handle it, how to control access to it, and how and when to purge data within the Organization.

The policy will be as holistic as possible and as pragmatic as necessary, and will help CERN to comply with international standards on data protection without diminishing its openness or academic character. There will be a particular focus on rules concerning confidentiality and the handling of personal data (currently only partly specified in Administrative Circular No. 10). Handling procedures for other data (e.g. those kept by the HSE Department) will be developed in close collaboration with the relevant departments and experiments.

A draft policy has already been prepared by a small working group with members from the GS, HR and IT Departments, the CERN Legal Service and the Computer Security...
Team. In parallel, this working group is in contact with GS and IT service providers in order to start applying similar data handling guidelines to their computing services to reach consistency in data classification, storage and protection and to provide adequate storage facilities for each data classification level. This working group will also provide data protection awareness training for key people, suggest quick and easy steps to improve data protection in the DG Unit as well as in the FP and HR Departments, e.g. through the deployment of uncomplicated disk encryption tools for laptops (more about this here), assist departments and experiments in reviewing and adapting their internal data handling guidelines in line with the new data protection policy, and help them to establish good practices.

How private is “private”? (2014)

What a surprise it would be for you to discover that everyone at CERN can access your Windows “My Documents” folder or your AFS home-folder? Reading your private letters? Looking at your private photos? Digging through your confidential documents? Would you be embarrassed? You would not be the first.

Unfortunately, if you are not careful when handling the access control settings of your AFS and DFS folders, you can easily make a mistake. The IT Department's AFS and DFS services provide you with all the means to protect your documents, but you are the only one who knows which documents should be made accessible to whom… So be careful!!! Mistakes are easy to make, and have happened in the past! The settings on DFS are complex and usually inherit rights from parent folders, so small slip-ups can quickly spread to every other folder. The settings on AFS require special commands (“fs setacl”) instead of the “chmod”-POSix commands. Currently, automatic tools only ensure that your AFS “~/private” and home folders are not globally readable (see here for details). Similar automatic tools do not yet exist for DFS. However, the DFS service permits access only to CERN people.

So this is as far as we can currently get: it is primarily up to you to regularly check whether your folders are properly protected and not (accidentally) opened. Ask colleagues you trust to try to access your protected documents - if these are not intended for their eyes, they shouldn’t have access. If they do, check out these links on AFS and DFS access control. Ensure that your private documents are properly protected. Remember that your “public” folder really is intended (and required!) to be public. Any document you put in there will be shared with all of CERN…

Also note that your privacy at CERN is paramount. CERN takes great care to protect the personal data entrusted to it. Our colleagues controlling the AFS and DFS file systems have all signed a special clause that their “functions, allowing access to confidential and/or sensitive information, implies strict conformance to the rules laid down in OC5 (i.e. the CERN Computing Rules) and in particular those governing
confidentiality”. In the rare instances where access to your files and folders on AFS and DFS is necessary, these [strict procedures apply].

Public PCs: Log out or lose out (2013)

Do you regularly use one of the public Windows or Linux terminals in the CERN library or in front of the Users’ Office? Or do you often give presentations or run meetings, workshops or conferences? Did you recently attend a training session in the CERN Training Centre? If you answered at least once with “yes”, we have a plea for you: LOG OUT when done in order to protect your data!

You might recall that CERN considers that “Your Privacy is Paramount”. But this does not come for free. In the few past months, we have received several reports from vigilant people who have spotted open user sessions on public PCs at CERN. Those users simply forgot to log out once their work, training or meeting was over. Their session continued without them being present. Worse, with CERN using a central Single Sign-On (SSO) portal, their login credentials would allow a malicious person at CERN to use those credentials to access that user’s mailbox, DFS files or EDH documents. Fortunately, no abuse has been reported so far. The aforementioned vigilant people were all kind enough to just silently log the users out of their sessions.

Remember: log out from your web browser after you have downloaded a presentation from INDICO or EDMS using your CERN password on a conference PC. Log out from your Vidyo session at the end of your conference call. Log out from your PC at the end of your training session or (should the session continue into the next day) lock the screen with a password. Log out from the public PCs in the CERN library or in front of the Users’ Office when you are done with your work. Consider rebooting the PC if you cannot log out for some reason. Finally, log out for your colleagues if you find them still logged in. Please restrain your curiosity: attempting to misuse their credentials constitutes a direct violation of the CERN Computing Rules (OC5 III-15).

Let’s play hide and seek (2012)

This week, we would like you to play a small online game called “Virtual Hide & Seek”. The rules are simple: some of our colleagues have published some sensitive or confidential documents on CERN’s central services like Indico, CDS, EDMS or TWiki, as well as on our many websites. Your mission, should you choose to accept it: find them!

If you provide us with documents marked “confidential”, “classified”, “sensitive”, or containing plain text operational passwords, you can win a book on computer security.
There are only few conditions: these documents must be visible from outside CERN, must not require a CERN account in order to access them, and must not belong to you or have a direct link with your work. Have fun!

But seriously, are you sure that your documents are really properly protected? We regularly find confidential documents stored on one of the CERN central services and which have accidentally been made public. Only our oath of discretion forbids us from giving details. However, you may remember the article on “CERN est une véritable passoire” from the “Le Matin” of November 2009, which will give you an idea about the negative consequences leaking documents can have.

CERN central services like CDS, INDICO, EDMS or TWIKI, as well as the web service, provide means to classify your documents and protect access to them accordingly. While these services are inherently secure, it is up to you to check that you are using their protection correctly! Thus, if you own or manage confidential documents, are these properly classified and have access protections been properly applied (e.g. using e-groups)? Can only the people who need them access them? Have you tried to find them with Google searching for “[YOUR SENSITIVE DOCUMENT TITLE HERE] site:cern.ch”? Should you find out that one of your documents ended up publicly available by accident, do not hesitate to contact the corresponding support team directly, as they can give you help and advice.

Still, our challenge remains. Maybe someone else will find your confidential documents publicly available on a CERN site. Whoever sends link(s)/URL(s) for confidential document(s) to Computer.Security@cern.ch by 14 December 2012 can win one of three books on computer security.¹

Your privacy is paramount! (2012)

May I read your e-mails or join you while you browse the web? What if I access all your personal documents on the DFS or AFS disk spaces? I guess you have nothing to hide and all that information is related to your professional duties… so why would you care?

But hold on! The personal use of CERN computing facilities is tolerated (as long as use of resources and bandwidth is negligible). This includes personal mails, reading online newspapers, browsing the web for leisure purposes, or storing private photos on your laptop. In addition, many people bring their own laptops, pads or mobile phones for convenience, instead of using CERN ones. This is because their life at CERN is rather a mixture of working for CERN and for their university, and leisure activities (such as keeping in touch with their families and friends). This implies working

¹ In the event of more than three credible, correct replies, we will draw from the pool of replies.
hours and leisure time are entangled, and the case is the same for your e-mails and documents.

CERN takes great care to protect the personal data entrusted to it. Your privacy is paramount! Therefore, the GS, HR and IT departments, in collaboration with the Legal Service and the Security Team, have drafted a “CERN Digital Privacy Statement” which is designed to describe how and when CERN collects, uses and shares information when you use CERN's computing facilities, and, how CERN protects personal data stored in CERN's computing facilities.

There can be, and there is, no legitimate reason why the CERN Computer Security Team or the Service Desk - or your colleagues or supervisor/team leader - should have unrestricted access to your e-mails and data. Your CERN mailbox and your “private” folders on AFS and DFS are 100% yours, and strict procedures have been established for the rare cases where such access is necessary. So if you would like to keep things private, put them there. On the other hand, your professional stuff, i.e. software, draft documents, minutes, etc., should never be kept there but rather stored in dedicated project folders on DFS or AFS, or within the CDS or EDMS web services.

Similarly strict rules also apply for accessing automatically recorded logging data (resource usage, IP addresses, visited web sites, interactive commands, physical and digital access information, and telephone records) created by your use of CERN's computing facilities. While such data is essential to provide, measure, customize and improve services, as well as to monitor system security, those rights come with obligations already respected by the corresponding system, specified for many decades, and now explicitly expressed in this new Privacy Statement.

The Privacy Statement and the procedures for accessing private data are part of a more comprehensive Data Protection Policy currently under preparation. Have a look and stay tuned!

“Clas-si-fied (ˈklæsɪfaɪd/)” — What’s that? (2012)

Have you ever thought about what information at CERN should or must be classified as confidential? Or public? What does “confidential” mean anyway? European law, for example, requires proper protection of your medical files. At CERN, for security reasons your passwords are yours and only yours (remember: “Your password is your toothbrush”). And it is in your own interest that your credit card details are kept confidential, too. But what about your office location, your CERN phone number, or your official photo for your CERN card?

CERN is now working on a coherent policy for classifying data, with the upcoming Data Protection Policy (DPP) currently under development by the CERN Legal Service, the
GS, HR and IT Departments, and the Computer Security Team. The essential first step for such a DPP is a clear definition of which data must be kept confidential and which data can be treated as public. The draft Data Classification Policy (DCP) proposes four levels of classification: “Sensitive”, “Restricted”, “Internal” and “Public”:

- “Sensitive Data” is considered to be all data which, if disclosed, would compromise personal data privacy and/or could cause damage to CERN or its reputation or impede its work. It is highly confidential and proper protection, including data encryption or equal security, is paramount;
- “Restricted Data” is confidential, too. Its circulation is required for operational purposes but wide-spread disclosure is unacceptable. Therefore, access is only granted on a need-to-know basis;
- “Internal Data” is not confidential as such, but is intended for an internal audience only. The audience is “CERN”, i.e. all Members of the Personnel;
- Finally, “Public Data” is intended for disclosure, and the audience is unlimited.

We avoided using the term “confidential” as a classification level since it is inconsistently used at CERN and could create confusion.

Complementary to this classification scheme is a list of examples for each of these levels. While it does not claim to be exhaustive, it is intended to give guidance on how certain CERN data should be classified. It is important to have the agreement of stakeholders as CERN is currently in a transitional phase with respect to the handling of data, and the classification system will be a major development.

The full details of this draft policy and the list of examples can be found here. As this policy is currently under development, we eagerly await your feedback, comments and input, in particular on the list of examples. Please contact us at Computer.Security@cern.ch. Once approved, compliance with the DCP will be obligatory. The next step is the definition of policies for storing, accessing and transferring any kind of data, regardless of their format (digital or hard-copy) or on which media they reside. Stay tuned!

Data protection for all (2012)
http://cdsweb.cern.ch/journal/CERNBulletin/2012/16/News%20Articles/1434741?ln=en

What a stir… was caused by two articles in the last issue of the Bulletin, on “New Snail Mail Scanning Service” and “CERN meets Facebook”!

Indeed, respondents were completely correct that opening letters addressed to others and scanning such letters violates basic privacy rules. Also, giving your photo, address, computing accounts, personal files and documents to a third party - especially an external party - is a NO-NO, as CERN considers some of this data to be personal. For example, your CERN mailbox and your “private” folders on AFS and DFS are 100%
yours. Neither your supervisor, the AFS/DFS/mail service administrators nor the Computer Security Team have any right to access this data. Strict procedures have been established for the rare cases where such access is necessary, and these require the approval of the CERN Chief Information Officer (CIO), the Legal Service and the DG.

But did you know that CERN is currently developing a data protection policy and the role of an appointed CIO (currently assumed by a combination of the head of the IT department and the Computer Security Officer)? Apart from Administrative Circular No. 10, data protection currently relies on the awareness and care of the individual. Not one of your problems? Indeed, CERN thrives on an open culture, so it is tempting to assume “we have nothing to hide”. Losing physics data might be a nuisance, but is that all? There are also your personal files, mailbox, financial and contractual data, confidential notes and minutes, passwords and credentials, and your medical records. These have to be protected in a consistent and clear way!

So we are set for change. In collaboration with the Legal Service and the GS, HR and IT departments, the computer security team is drafting a comprehensive data protection policy for storing, accessing and transferring data. Currently, the focus is on the proper definition of classification levels, i.e. “public”, “internal”, “restricted” and “sensitive”, and an exhaustive list of examples for each level (see here). This policy will be supplemented by policies on data storage, transfer and access. The list of examples will help to clarify classification and avoid incorrect classification within a data store. Finally, the data protection policy includes a policy on data destruction that has already been deployed (see here; see also our article in the Bulletin 10-11/2012).

However, the best way to protect data is still by being conscious and cautious! If you think some documents, files or data should be protected, make sure that they are. We are ready to help you with that.

How to get properly rid of confidential data? (2012)
http://cdsweb.cern.ch/journal/CERNBulletin/2012/10/News%20Articles/1428518?ln=en

Have you ever bought a used laptop on eBay? Try it and you might not only get (hopefully) functional hardware, but also a bunch of personal files, intriguing photos, sensitive documents, etc. Not everybody worries enough to clean the local hard disks properly before selling their equipment or giving it away. So the next owner of the hard disk can comfortably crawl through the remaining data, and use it at his or her convenience...

In fact, properly cleaning a hard disk is difficult! Deleting local files or formatting the hard disk usually just purges the files from being listed in the folder, but the actual data remains intact on the hard disk. Freely available tools can easily reconstruct those files
and, thus, expose it. It is better practice to get rid of your files by running tools like "shred" on the Linux platform (try "shred –fuvzn1 [FILENAME]" or check "man shred" for details), or “File Shredder” from CNET for the Windows operating system. Both tools overwrite files with random bytes such that it is close to impossible to reconstruct the data afterwards. However, if you cannot run those tools (for example, because the disk is broken), it is best to destroy the hard disk. At CERN, this is the recommended procedure for (broken) disks containing confidential or sensitive data (see the CERN Data Destruction Policy).

So don’t be negligent if you run a service at CERN that stores confidential data such as financial, medical or personal information. Never allow such hard disks to leave the Organization, e.g. for maintenance reasons. Furthermore, ensure that your hard disks are properly destroyed once you phase out the corresponding PC hardware. The Computer Security Team, in collaboration with the IT Computer Centre Operation Team and the GS Logistics Service, can collect your hard disks and magnet tapes which hold confidential data. These are then stored in a sealed container situated in the Computer Centre (Building 513) and regularly emptied by a company specializing in the safe destruction of hard disks.

Take advantage of this service for the sake of confidentiality – and at zero cost! If you would like to safely get rid of your hard disks and tapes (or laptops or USB sticks), please bring them to the operator's desk in the CERN Computer Centre (building 513).

Classified (2011)


In the last issue of the Bulletin, we have discussed recent implications for privacy on the Internet. But privacy of personal data is just one facet of data protection. Confidentiality is another one. However, confidentiality and data protection are often perceived as not relevant in the academic environment of CERN.

But think twice! At CERN, your personal data, e-mails, medical records, financial and contractual documents, MARS forms, group meeting minutes (and of course your password!) are all considered to be sensitive, restricted or even confidential. And this is not all. Physics results, in particular when being preliminary and pending scrutiny, are sensitive, too. Just recently, an ATLAS collaborator copy/pasted the abstract of an ATLAS note onto an external public blog, despite the fact that this document was clearly marked as an "Internal Note". Such an act was not only embarrassing to the ATLAS collaboration, and had negative impact on CERN’s reputation --- it is also a serious violation of the CERN Computing Rules, and has been followed up with the people concerned.

If you own data, documents, code or web sites which are supposed to be sensitive, confidential or restricted in access, make sure that they are clearly marked as such,
and that access is restricted in a way that only people with a need to read them, can do so. AFS, DFS, and the central web service provide means to properly protect your documents. If you have access to a restricted document, do not violate the rules: only share the documents with those who are eligible. If in doubt, check with the owner of that document, and ask for authorization. Finally, if you are a developer or system administrator, ensure that your code and servers are secured and do not leak data! Follow the appropriate CERN Technical Training courses for designing secure software, when in doubt.

Privacy, who cares? (2011)

In mid-April, the Sony “Playstation” and “Online Entertainment” networks were compromised and the records of nearly 100 million (!) users (names, addresses, dates of birth, e-mail addresses) were stolen. It even seems that the credit card numbers of these users where lost, too.

In a different case, a bug in the job portal of UNESCO allowed any applicant to access addresses, mobile phone numbers and salaries of probably hundreds of thousands of other job seekers dating back to 2006. But data loss is not only an accidental or malicious act: Apple’s iPhone and iPads (and to a lesser extent Android devices) store each position location of their owners since 2008, and it is yet unclear whether this data made it back into Apple’s headquarters. Facebook and Google are already known to harvest gazillions of records of user data with the aim of pin-pointing customer behaviour. It is not the first time that, before committing a crime, thieves have consulted the Facebook and Twitter profiles of their victim in order to figure out whether he/she is currently at home; Google maps is used for checking the property. Last but not least, the company behind the TomTom navigation software sold speed data as measured by individual car navigation appliances to the Dutch police (who will now put speed traps at the appropriate places).

It seems that privacy of personal information is nowadays widely ignored, at least on the Internet. Am I old fashioned if I consider my salary, date of birth, private life and credit card numbers being none of your business?

Please be careful. Giving away too much information means giving away your privacy! Think twice before providing personal data to even well-known web sites like Facebook or LinkedIn. Expose only information that is really necessary, and refrain from using sites which seem to be too “greedy”. Also, do not use the same password for different sites. Finally, if you are a developer of an application asking and/or storing personal data, ensure that your code is secure and does not leak data! Follow the appropriate CERN Technical Training courses for designing secure software, if in doubt.
Insist to avoid troubles (2020)

Recently, CERN was facing again an allegation of a potential abuse of the license conditions of a popular engineering application. While, since ever, CERN does not tolerate any license violations or pirating of software, this case turned out to be astonishing as CERN holds licenses for that particular application. Unfortunately, the student supposed to use that application was not able to get the green light from her hierarchy to request the corresponding license – even after insisting several times. With deadlines approaching, the student got creative and embarked on alternative ways… creating troubles.

While creativity is definitely sought after in our academic environment, following the rules instead is essential when it comes to software licenses. The usage of pirated or otherwise illegal licenses can have detrimental consequences to CERNs reputation as well as trigger financial repercussions. Therefore, CERN will not tolerate any abuse of license conditions nor the pirating of license files. Potential incurring costs will be directly transferred to the person or institute violating those conditions – and such fines can easily be composed of five to six-figures (hence our earlier Bulletin article on “Do you have 30 kCHF pocket money?”).

So our plea to you: Check with CERN’s software portfolio first. CERN is providing you a plethora of licensed software intended to help you in the execution of your professional duties via CMF for Windows PCs, LXSOFT for Linux systems and the CERN/Apple Mac Self-Service. Dedicated licences are available for engineering software and for control software.

Alternatively, you might want to use free open source software (FOSS)… But mind the “free” as open source software (OSS) is not always free. Some OSS might be free for personal usage, but not free when used in a professional environment or in larger teams. “Free” might be free when used at home or at your home institute, but not necessarily at CERN. And what concerns “free” (public) cloud services, you might simply pay with your data, e.g. they may use your data in whatever way they please, assume ownership, or don’t provide means to recuperate your data once you quit their service…

In any case, if these do not suit your needs, or if you are in doubt as to whether the licence conditions of your applications are compliant with usage at CERN, please contact the CERN Software Licence Officer to check your options and, if needed, agree to make a central purchase. If, indeed, your preferred software needs to be purchased, insist to get a green light from your supervisor. Escalate to your hierarchy if you cannot get the consent of your direct supervisor. Do not start getting creative here! We are
sure that no department head will block your needs if those are clearly justified!! They would like to avoid troubles, too!!!

**Presenting images that are not yours… (2020)**


Conference season is coming up again – maybe in a different setting to what we are used to, but still with lots of interesting results to present and share. And with lots of presentations being made, lots of images will be shown to embellish the content and act as a visual aid, since inter-human communication is 20% oral and 80% visual… But beware, not every image is a good choice.

The good ones, of course, are those that you have created yourself. Your plots. Your graphs. Your sketches. Photos taken by you. But once you download a photo from the Internet, a nice image you found through a Google search or on Instagram, beware that it might be subject to copyright. It is not unknown for a researcher to receive a cease-and-desist notification from the copyright holder asking to take down the photo and pay compensation fees. And these can get quite expensive!

As with music, films and videos, images and photos displayed on a webpage can be subject to copyright. So be careful. Make sure that you have the proper rights when using visual content, be it graphics, photos or videos. Whether you are a presenter, webmaster or editor, please ensure you hold the correct rights when using visual content and music in your presentations, webpages or publications… Check whether the image is published under a [Creative Commons licence](https://en.wikipedia.org/wiki/Creative_Commons) (see, for example, [Wikimedia](https://commons.wikimedia.org)) or consider paying a royalty fee to a photo repository such as BigStockPhoto.com or iStockPhoto.com. It takes an investment of just a few francs to be on the safe side. If you are really keen on using a particular photo or graphic, contact its author/owner and ask for permission (and keep written proof!). And, of course, take some time to browse the CERN Document Server (CDS) for images and footage from CERN. If you can’t find what you are looking for, why not roam around the CERN site, take the photo yourself and make it available on CDS?

**When “free” gets even more restrictive (2019)**


In a previous Bulletin article, we discussed the problem of free software and why “free” does not necessarily mean “free of charge” or, in the CERN context, why “free” software should not be used for professional or educational purposes. Here is a new theory as to why the situation might get worse!
First of all, a "free" licence might insist upon "personal usage only". But this does not mean it is a single-user licence allowing you to install the software as an individual for professional purposes. It instead refers to the software’s deployment at home and for completely private projects, not related to your profession, your job or the paid work you do. At most, it might permit professional testing for a (short) evaluation period or for you to "try it out". Care must be applied here, too, as "trying out" is definitely an activity not supposed to last forever.

Other "free" licences might authorise the software to be used by, for example, "small teams", even for professional purposes. While this sounds good, it also has a snag: CERN is a big organisation comprising many entities. While you might have deployed software for your "small CERN team", other teams at CERN might have considered this too (and already done so!). So, the software vendor might register a bigger picture, and conclude that CERN as a whole is contravening its licence conditions. And indeed, some have already pointed such a situation out to us and have pushed for CERN to subscribe to one of their professional licence packages. Are you prepared to contribute to these costs?

Finally, there is the "educational licence" for universities, generally intended for classroom usage. CERN is an academic institution and part of our campus can be fairly considered to be university-like. Our mission statement stipulates that we "enable research at the forefront of human knowledge[,] perform world-class research in fundamental physics[,] and] unite people from all over the world to push the frontiers of science and technology, for the benefit of all" – a purely academic activity. We give lectures to students, and even issue certificates or diplomas through the CERN Accelerator School, CERN School of Computing (even leading to ECTS points), the CERN Teachers Programme and Beamline for Schools, among others. However, our academic environment, our fundamental research, lectures and seminars, as well as those certificates and diplomas, might not be sufficient for CERN to be entitled to an educational licence. Worse, and here is the new theory, licence conditions change. What was allowed for version 1.2.3 might not be the case any more for version 1.2.4. Eligibility changes. Terms change. The scope changes. Figuring all this out can be extremely cumbersome, as software vendors do not necessarily point you directly to the changes to their licence conditions! A formerly valid "free" licence might become a liability for CERN...

So, don't put the Organization at risk! Please check out the licence conditions carefully and read the fine print – not only when considering software for the first time, but also when updating it. If in doubt, please contact the CERN Software Licence Officer or the CERN-IPT Purchasing Service. If you want to stay on the safe side, check out the full portfolio of CERN-provided software via CMF for Windows PCs, LXSOFT for Linux systems and the CERN/Apple Mac Self-Service. Dedicated licences are also available for engineering software and for control software. A register of all centrally purchased licences can be found here: https://slma.cern.ch/slma.
When “free” is not free (2018)

Protect CERN, protect yourself! Using applications without a valid licence will lead to repercussions. “Academic freedom” is one of the values held in high regard by CERN. Freedom in terms of open and unbiased research, free communication, free opinions and free discussions. In the digital world, this also includes the freedom to choose which hardware to buy, which operating system to install, which programming language to employ and which applications to use. However, there are also limits and sometimes it is better to choose a mainstream option: coordinating hardware purchases saves money; deploying centrally provided operating systems enables excellent support; aligning programming languages benefits long-term maintenance and collaboration; and refraining from “free” applications avoids licensing troubles. And we know all about licensing troubles!

Protect CERN, protect yourself! Using applications without a valid licence will lead to repercussions (see our Bulletin article on “Do you have 30 kCHF pocket money?”). Deliberately downloading pirated licences is professional misconduct, and might lead to financial penalties. But the innocent installation of “free” applications can also have unexpected consequences: “free software” or “free version” does not necessarily mean that something is free to use at CERN. For example, “free” might imply that a private individual can use the software at home without charges, or a small team of people can use it together without being billed. In the context of CERN, however, neither applies: applications are supposed to be used in a professional context and, very often – in collaborations with big teams – the term “free” is invalid. It is therefore very important to check the Terms and Conditions prior to the first use of any software and to understand under which circumstances “free” really means “free of charge”.

But the word “free” can also have another connotation: “provided for free by my home institute”. CERN’s academic freedom means that CERN is acting as an Internet Service Provider (ISP), providing network connections to the Internet for many of our users. The corresponding hardware, including laptops etc., is sponsored by their home institute and comes loaded with a stack of applications provided by the institute – not by CERN. While these institutes are expected to have purchased those applications under a valid licensing scheme, this scheme and the associated Terms and Conditions might not permit any usage of those applications abroad. Location is key and licences might be valid only when the applications are used at the home institute’s premises! Care must also be taken here. Once more, it is very important to check the Terms and Conditions prior to the first use of any software. In cases of abuse, CERN will decline any responsibility and refer the matter to the user’s home institute.

Therefore, if you need a specific application for CERN-related professional business, please first check CERN’s portfolio of centrally provided software via CMF for Windows PCs, LXSOFT for Linux systems and the CERN/Apple Mac Self-Service.
licences are also available for engineering software and for control software. If these do not suit your needs, or if you are in doubt as to whether the licence conditions of your applications are compliant with usage at CERN, please contact the CERN Software Licence Officer to check your options and, if needed, agree to make a central purchase. And for your private/personal usage, please refrain from installing such software on CERN-owned PCs and laptops and use your private, non-CERN e-mail address to register. Otherwise, any costs that arise will be billed to you.

http://cds.cern.ch/record/1309543/?ln=en

Do you like listening to music while you work? What about watching videos during your leisure time at CERN? Sure this is fun. Having your colleagues participate in this is even more fun. However, this fun is usually not for free. There are artists and the music and movie companies who earn their living from music and videos.

Thus, if you want to listen to music or watch movies at CERN, make sure that you own the proper rights to do so (and that you have the agreement of your supervisor to do this during working hours). Note that these rights are personal: you usually do not have the right to share music or videos with third parties without violating copyrights.

Therefore, making copyrighted music and videos public, or sharing music and videos as well as other copyrighted material, is forbidden at CERN. It violates the CERN Computing Rules and it contradicts CERN's Code of Conduct, which expects each of us to behave ethically and honestly, and to credit others for their contribution. Copyright violation is also illegal in different ways in different European and other countries, including in CERN's two host states.

Downloading films is no peccadillo (2015)

Dear Summer Students, within the Organization, you have many possibilities to pursue your natural curiosity and acquire as much new knowledge as you can siphon into your brain. CERN provides you with the academic freedom to do so, with almost no limitations. But hold on: “free” and “no limitations” don’t mean that you can do whatever you want…

Please note that, when using CERN’s computing facilities, when sending e-mails from your CERN e-mail address, when using your laptop/smartphone/computer, you must follow a basic framework of rules, the CERN Computing Rules. I would like to focus on one particular aspect of those rules: that of accessing music, videos, films or computer games from popular websites like ThePirateBay or using Bittorrent.
CERN has an awesome connection to the Internet, lots of bandwidth and a high capacity for web downloads. However, this does not mean that downloading music, videos, films or computer games is permitted. It is not - basically for two reasons: the first is that CERN’s network is primarily for professional purposes and such downloads are not usually work-related. More important, however, are the legal aspects of such downloads: the downloading of copyrighted material, or at least the sharing thereof, is against the law in many European countries. Copyright violation is no trivial offence. It is no peccadillo!

In the past, CERN has received cease-and-desist letters from major entertainment labels pointing us to individual users who have violated copyright in this way. This is not only embarrassing for the Organization and damages its reputation but can also have financial consequences for the perpetrator (see our Bulletin article “Do you have 30 kCHF pocket money?”). Hence, copyright violations are not tolerated at all by the Organization and will result in administrative measures as consequences to you (plus the financial liabilities).

In order to spare you and us from that mess, please make sure that your Bittorrent clients are disabled before you connect to CERN’s wired or wireless networks. Please refrain from visiting illegal download portals for music, videos/films and computer games while being connected via CERN. Instead, take advantage of commercial solutions like Steam, iTunes, Netflix, MyVideo… And one final word: please also refrain from browsing porn pages. We usually register such access and a notification to you might make you feel embarrassed and awkward.

A plea to Santa Claus (2015)

Running pirated software or illegal licences, using cracking tools to bypass software activation measures, sharing music and films – these are problems that academic environments unfortunately have to deal with. All violate the copyright of the software/music/film owners, and copyright owners are not Santa Claus...

CERN, like other research organisations and universities, regularly receives allegations from external companies complaining about laptops or PCs running illegal software or sharing their films, videos or music with peers – and thus violating copyright.

Usually, we then contact the owners of the corresponding devices in order to understand whether these allegations are true. Very often such allegations boil down to a laptop whose owner replies “I confirm that a torrent client was left up and running on my device by mistake” or “This is a file that is stored on my personal hard disk.” As if those allegations were “peccadillos” (see our earlier Bulletin article “Downloading films is no peccadillo”) and have no consequences.
So why is it that some of us think we have the right to bend CERN’s rules? Violating copyright, using pirated licences (“Do you have 30 kCHF pocket money?”), outsourcing IT technologies when CERN provides similar technologies (“IT or not IT, that is the question”), speeding on the CERN site, parking where it is not permitted… Aren’t we supposed to apply due diligence and avoid such things in order to protect the reputation of the Organization? Aren’t we all professionals bound by the Organization’s Code of Conduct and its rules?

Of course, we could say ‘no more warnings’ and go straight to the more severe consequences and sanctions, involving hierarchy and supervisors, etc. However, since this is the end of the year, let’s make a wish that we will all act in a more responsible and ethical way in 2016!

We are also keen to get your opinion concerning suitable strategies to apply to this issue. Just send us an e-mail at Computer.Security@cern.ch.

Do you have 30kCHF pocket money? (2015)

I am not kidding. Do you have 30,000 CHF to spare? Give it to me, so that I can lose it. It won’t even be well invested. We will just give it away by mistake. An easy mistake, some think. A “gentlemen’s” blunder. Unimportant and, really, not at all a big deal. But, of course, that's wrong - and expensive. Here is my story.

Recently, a student working at CERN was supposed to make a sophisticated simulation of thermal conductivity within a metallic structure, the resulting mechanic stress and the electromagnetic field variations within it. All of his teammates were using a commercial simulation package named - for the sake of brevity - “AllSIM”. But our student failed to download AllSIM from DFS onto his office PC, since that wasn’t where he wanted to use it. He wanted to install it on his laptop so that he could work on his simulation while travelling. However, the CERN AllSIM installation would not allow for this, as roaming usage is not covered by CERN’s AllSIM licence. The student had a need and was not willing to compromise i.e. by using the Windows Terminal Service. Instead, he used Google and quickly found AllSIM for free on a dubious website. Three clicks later, he was ready to go.

Enter the 30kCHF. AllSIM permanently monitors the usage of its software and is able to identify installations with invalid licence keys. Hence, we, the CERN Computer Security Team, received an e-mail accusing CERN of running their software with a pirated licence – despite the fact that CERN possesses a pool of licences to cover all its needs. Their request: stop the illegal activity immediately, buy official licences from them and make an indemnity payment for “licence infringements”. The price tag, as you might have guessed, was 30kCHF.
Understandably, the student was shocked when we investigated the case and he was forced to acknowledge the facts. The AllSIM licence was pirated and the student had violated CERN’s Computing Rules just for the sake of convenience. As he was affiliated with a university, CERN passed all costs to them who, in turn, passed them on to the student. So, do you have 30kCHF to spare?

Through simple ignorance of the CERN Computing Rules, violating proprietary rights and licence conditions, downloading pirated software, and committing copyright infringement, the student has not only placed the Organization’s reputation at risk, but also created a financial liability for CERN, his university and – in the end – himself. So unless you have 30kCHF to throw away, don’t forget that software vendors make a living by charging for their products. CERN offers a variety of commercial software and has all the corresponding licences you’ll need for your professional use. If you can’t find what you need, please get in touch with the CERN Software Licence Officer, Helge Meinhard (IT/PES).

Protect CERN — Respect copyrights (2014)

Are you a physicist who does complex mathematical calculations? Are you a webmaster who regularly embeds visual contents? Do you regularly present to large audiences? Are you an engineer who does sophisticated simulations of heat transfers, structural stability or electric circuits? Are you a technician who often uses CAD software? Do you like listening to music while being at CERN? Go ahead!

But make sure that you have legitimately obtained the software/images/music/videos you are using and hold valid licenses to run your software. Using illegal or pirated software/images/music/videos is not a trivial offense. It violates the CERN Computing Rules (OC5) and puts the Organization at risk!

Vendors deserve credit and compensation. So make sure to buy your software via legitimate channels and use a valid and honestly obtained license. This also applies to “shareware” and software under open licenses, which might also come with a cost. Usually, only “freeware” is completely free. Of course, software installed from the central CERN repositories (i.e. CMF for Windows PCs and SWrep for Linux) are 100% legal and come with appropriate licenses. Some engineering applications, however, have restricted usage. A list of centrally provided engineering applications is available from the IT department and the EN/ICE group. Ask your supervisor if you are not sure or contact the CERN Service Desk.

In addition, make sure that you have the proper rights when using visual content, be they graphics, photos or videos. Whether you are a presenter, webmaster or editor, please ensure you hold the correct rights when using visual content and music in your presentations, webpages or publications… Check whether the imagery is published under a Creative Commons license (see, for example, Wikimedia or this article) or
consider paying a royalty fee to a photo repository such as BigStockPhoto.com or iStockPhoto.com. It takes just an investment of a few francs to be on the safe side. If you are really keen on using a particular photo or graphic, contact its author/owner and ask for permission (and keep written proof!). And, of course, take your time to browse the CERN Document Server (CDS) for footage from CERN. If you don’t find what you are looking for, why not roam around the CERN site, shoot the photo yourself and make it available on CDS?

If you are listening to music or watching films while at CERN, make sure that you have the proper rights to do so (and, of course, that you have the agreement of your supervisor). Note that these rights are personal and you usually do not have the right to share music or videos with third parties without violating copyright. Nowadays film companies are actively scanning for illegal downloads and sharing. So please keep CERN out of their crosshairs!

Quid pro quo. CERN also produces lots of software (and hardware!). We don’t charge for this, as knowledge sharing and dissemination is in the spirit of the Organization. However, we hope you agree that CERN deserves credit if third parties use our products, and that we ensure that this usage remains within spirit of the Organization (e.g. that CERN ware is not used for dubious purposes). Therefore, all CERN software should be published under one of the recommended Open Source licenses, such as GNU GPL v3. CERN has initiated a similar scheme for hardware - the CERN Open Hardware Licence - in order to facilitate the exchange and reuse of hardware design. There are also dedicated terms of use for CERN audio-visual media.

Getting a better image from the organization (2014)

Do you make regular presentations about CERN or CERN's activities to the public? Do you manage public webpages hosted by CERN? Do you edit or contribute to CERN publications? Besides plenty of text, every good presentation, webpage or publication is usually spruced up with visual content: graphics, photos or even videos. But have you ever thought about whether you actually have the proper rights to use such imagery?

Just recently, a stock photo agency contacted CERN regarding an image published on a web page currently under CERN's responsibility. According to them, this image had been used without the proper rights and thus violated their copyright. As the web page is from 2007 and as is part of an EU funded project which has since ended, it is hard to check the facts. The image has since been removed to comply with the photo agency's conditions. We should take all the possible steps to avoid receiving similar letters, and to uphold the good image of the Organization!

Whether you are a presenter, webmaster or editor, please ensure you hold the proper rights when using photos, graphics, videos and music in your presentations, webpages
or publications… Check whether the imagery is published under a Creative Commons license (see, for example, Wikimedia or this article) or consider paying a royalty fee to a photo repository such as BigStockPhoto.com or iStockPhoto.com. It is just an investment of a few francs to be on the safe side. If you are really keen on using a particular photo or graphic, contact its author/owner and ask for permission (and keep written proof!). And, of course, take your time to browse the CERN Document Server (CDS) for footage from CERN. If you don’t find what you are looking for, why not roam around the site, shoot the photo yourself and make it available on CDS?

Also remember that the violation of image copyright is only one aspect. Please respect the copyrights arising from software applications and programs (“Software licenses: Stay honest!”) as well as when downloading or sharing videos and music (“Music, videos and the risk for CERN”).

Bad (re)presentations (2013)

Just recently, a video produced for CERN and published on YouTube and Facebook used background music from a contemporary popular artist. However, the people responsible failed to obtain the appropriate permission to actually use that music. They thought that having bought it on iTunes was sufficient. But it was not: “buying” means you have the right to listen, but not the right for further distribution or re-publication. As a result, the videos were pulled from YouTube and Facebook.

Similarly, how many of us integrate graphics and images “found” on the Web into our presentations? How many of us enhance our web pages with photos by third parties or use third party fonts? Should we? Graphics, images, photos and music files published on the Web still have an owner who can claim copyright fees when his or her work is re-used. That this material is accessible to you does not mean you have the right to copy and reuse it. This is the case for the aforementioned background music and for “shareware”, which can be used on trial but must eventually be paid for. Only “freeware” is really free. It can be quite embarrassing for you, and for the Organization, to be caught violating copyright. Not to mention the legal consequences which might follow.

In order to be sure, check if you do have the proper rights to use the material. If you do not, there are plenty of photo repositories (such as BigStockPhoto.com or iStockPhoto.com) where you can buy images, graphics and photos. It is just an investment of a few francs to be on the safe side. If you are really keen on using a particular photo, image or graphic, contact its author/owner for permission. At the very least, refer to the URL as the image source and for kudos. Reusing music, however, in web pages or publications is more difficult. We usually suggest avoiding this unless you are sure that the music is in the public domain and can be freely used.
In addition, you are reminded that violating copyrights can put the reputation of the Organization at risk and thus constitutes a violation of the CERN Computing Rules. Please refrain from sharing music or videos purchased for your personal use. You do not usually have the right for further distribution. Respect licence conditions and copyrights of software packages, in particular those of software provided for professional use at CERN. And finally, take care when re-using photos and images “found” on the Web in presentations or on Web pages. There might be a usage fee attached to them.

Software licenses: Stay honest! (2012)

Do you recall our article about copyright violation in the last issue of the CERN Bulletin, “Music, videos and the risk for CERN”? Now let’s be more precise. “Violating copyright” not only means the illegal download of music and videos, it also applies to software packages and applications.

Users must respect proprietary rights in compliance with the CERN Computing Rules (OC5). Not having legitimately obtained a program or the required licenses to run that software is not a minor offense. It violates CERN rules and puts the Organization at risk!

Vendors deserve credit and compensation. Therefore, make sure that you have the right to use their software. In other words, you have bought the software via legitimate channels and use a valid and honestly obtained license. This also applies to “Shareware” and software under open licenses, which might also come with a cost. Usually, only “Freeware” is completely free. Of course, software installed from the central CERN repositories (i.e. CMF for Windows PCs and SWrep for Linux) are 100% legal and come with an appropriate license. Some engineering applications, however, have restricted usage. Please check the corresponding website for details.

Quid pro quo. CERN also produces lots of software (and hardware!). We don’t charge for this, as knowledge sharing, dissemination and ensuring the ware is used outside CERN is in the spirit of the Organization. However, we hope you agree that we deserve credit if third parties use our products, and that we ensure that this usage remains within spirit of the Organization (e.g. they are not used for dubious purposes). Therefore, all CERN software is supposed to be published under one of the recommended Open Source licenses, such as GNU GPL v3. CERN has initiated a similar scheme for hardware, the CERN Open Hardware Licence, in order to facilitate the exchange and reuse hardware design. There are also dedicated terms of use for CERN audio-visual media.
Professional access to private devices (2019)

Today’s buzzword, “bring your own device” (BYOD) – i.e. the possibility of bringing your own tablet, laptop or smartphone to work – has long been established practice at CERN. The nature of our community, the comings and goings, new arrivals and departures on a daily basis, researchers from abroad, students, teachers and lecturers, requires flexibility in device provisioning. While CERN’s IT department supports centrally managed Windows laptops and PCs as well as centrally managed solutions for Linux systems, it is an unsurmountable challenge for them to provide any flavour of operating system for any type of hardware in any kind of language. But BYOD does not mean that you can do whatever you want…

Once you are connected to CERN’s wired or wireless networks, you are bound by CERN’s Computing Rules (also known as CERN’s Operational Circular No. 5) which requires you to always keep your system up-to-date, fully patched and protected against unauthorised access. In addition, the personal use of CERN’s computing facilities, i.e. its network, is regulated, must be limited in terms of resource consumption, and must not be detrimental to your official duties, constitute political, commercial or profit-making activity, or be inappropriate, offensive or illegal. While the CERN Computer Security Team is mandated to enforce the CERN Computing Rules and therefore automatically monitors all activity on its networks (see our Bulletin article on “Transparency for your privacy”), CERN also values your privacy (“Your privacy at CERN matters”) as governed by the office of data privacy protection.

Your personal device is yours and only yours. Neither your supervisor, line management or hierarchy, nor IT desktop support, ServiceDesk or local support personnel have the means to access your computer without your consent. If they do need to access your device, e.g. to help you to resolve computer issues, to install software or for any other reason, they should ask for your consent. The consent requirement also holds true for the CERN Computer Security Team. If this consent cannot be obtained, access is still possible with the explicit authorisation of the DG in accordance with CERN’s policy on “third-party access to users’ accounts and data”. Your collaboration, however, is always appreciated to allow us to resolve and follow up on computer security incidents or to carry out fraud investigations.

Please let us know if you believe that your device has been subject to any unauthorised access by a third party within or outside CERN, in particular during (duty) travel. By the way, during any absence, CERN’s policy on “third party access to users’ accounts and...
data” provides a procedure for a requestor to get access to data or a CERN-owned device – if genuinely needed, and only under very strong scrutiny.

Welcome Summer Students! (2019)

A warm welcome to the summer student class of 2019! On the agenda: challenging lectures in CERN’s main auditorium. Visits to CERN’s experiments and accelerators. Social events at the Residence Schuman (bike safely around the Saint-Genis roundabout!). Interesting projects to tackle with the team you work with. Time to take a great big gulp of CERN’s academic freedom, spirit and creativity! In order to make your digital life as comfortable as possible, however, here are a few useful things to know:

When you join CERN you are given a CERN computing account. Take care of its password as any evil-doer might misuse it to spam the world on your behalf, cryptomine in your name on CERN’s computing clusters, download journals in bulk from CERN’s digital library, or simply compromise your CERN PC and extract your photos, documents or personal data – or just spy on you using your computer’s mic or webcam… Similarly, take good care of your CERN and personal computers, tablets and smartphones. Give them some freedom to update themselves so you benefit from the latest protective measures. “Auto-update” is a good friend, just make sure that it is enabled – as it should be by default.

A particular nasty way to lose your password, at CERN or at home, is to answer so-called “phishing e-mails”, i.e. e-mails asking for your password. No serious person – the CERN Computer Security Team, the CERN Service Desk, your CERN supervisor – would send such an e-mail, only dishonest people or fraudsters. So stay on the look out and do not enter your password into weird webpages. Do not click on links in e-mails obviously not intended for you, for example, e-mails not addressed to you; not written in one of your native languages; or of no relevance to you. Ask us at Computer.Security@cern.ch if you have any doubts. Similarly, do not randomly click on web links, but stop and think first. Otherwise you might infect your computer in no time – and the sole remedy will be a full reinstallation of your device (easier if you have backups!).

CERN has awesome network connectivity to the world. But it is for professional purposes. While private usage is tolerated, please do not abuse this. Keep your bandwidth low. In particular, refrain from bulk downloading movies or software. Remember “copyright”? It also applies at CERN. Any violation of copyright reported to CERN will be followed up and any infringement costs will be passed on to the perpetrator. The same holds for pirated software. If you have stored pirated licence keys on your device, it’s time to delete them. Companies are monitoring for abuse of
their software and infringement costs can quickly reach five to six figures. If you need particular software, have a look at CERN’s central software repositories.

Finally, you might be working on a project requiring digital resources. Setting up a webpage. Writing some code. Developing hardware. Please do not reinvent the wheel if you need a database. Or a webserver. Or some software. The CERN IT department can provide a wide variety of centrally managed and secure services for your digital convenience. Just put yourself on their shoulders and build on top. Free your time and brain up for creativity and let CERN IT provide the tools. Moreover, make sure that all your development work, software, design drawings, documentation, etc. are made available to your supervisor for the time after you have left. This will ensure your heritage and your legacy at CERN. If you keep them to yourself, they will get purged and deleted – and your time at CERN will be forgotten.

Computer Security vs Academic Freedom (2019)

The mandate of the CERN Computer Security Team is simple: to protect the reputation and operations of the Organization from cyber risks. But this simple sentence can quickly become complex: what is the risk? What risk must be controlled and what can be accepted? What are good and reasonable protective measures? What is appropriate? What is overdoing it? In particular, in the academic environment of CERN, the academic freedom of research, with CERN’s reputation as an open laboratory welcoming people from all around the world, an acceptable equilibrium needs to be found between “security” and the aforementioned academic freedom, as well as the operation of accelerators and experiments.

The right balance is highly important. CERN is not a bank with money to protect. CERN is definitely not a military site nor engaged in military research. Tilting the balance too much towards bank- or military-style computer security might block academic freedom and the creativity behind it, as well as rendering the operations of the accelerators and experiments much more difficult. The mindsets of our people are accustomed to openness, communication, creativity and freedom of thinking. Too much unreasonable security raises questions and suspicions, and leads to creative ideas as to how to bypass the measures implemented. Rules without enforcement are not taken seriously. On the other hand, being soft on computer security means that evil-doers can sabotage or bring to a halt CERN’s operations or negatively impact its reputation. The right balance is therefore key. The right balance must be able to mitigate real risks, not perceived ones, and not just be a sort of security theatre. And the right balance needs to be transparently communicated and opened to discussion. So here goes:

The “cyber risk” is proportional to the threat scenarios, the vulnerabilities and weaknesses inherent to computing systems, and the consequences of losing those systems and the data stored on them. Like any other organisation, institute or
enterprise, CERN is permanently under threat. Our webpages are probed for vulnerabilities, attempts are made to crack passwords, users are approached to click on malicious links in order to get their laptops and PCs infected. The corresponding attackers stem from many different areas: script-kiddies trying out their skills to deface CERN webpages, cyber-criminals trying to extort money or blackmail individuals, attackers interested in misusing our computing power or that of the Worldwide LHC Computing Grid, for example for crypto-currency mining, jealous insiders trying to sabotage the scientific work of others, potentially even nation states, as CERN is a melting pot of people from all over the world, so why not attack people while they are in an open environment (instead of in a cyber-locked down country)? The threats are therefore not negligible and are real (and all incidents of the past are well documented in our Monthly Report).

Secondly, as is the case for any other user of information technologies, CERN’s hardware and software stack is prone to vulnerabilities and weaknesses. This is an inherent problem of IT. More particular for CERN is the freedom to choose. Within the scope of their work, staff and users can use, test, develop and deploy any kind of application and technology they deem relevant – on the condition that they assume full responsibility for the related computer security. The CERN IT department provides the relevant software platforms for this: centrally managed software packages, virtualisation platforms (“Openstack”), databases-on-demand, web application frameworks (“Drupal”, “Twiki”, “Sharepoint”), but their usage is up to the full discretion of the end user. Similarly, the office network is open to accommodating any kind of (vulnerable) devices, through the so-called principle of bring-your-own-device (“BYOD”). Hence, the phase space of potentially vulnerable and weak devices, applications and webpages, etc. is immense.

Finally, there are many consequences. Reputational. Operational. Financial. And legal. Finding a naked teddy bear posted on one of our home pages will lead to negative publicity; malicious mass deletion of physics data or cyber-sabotage of experiments or accelerators can bring our research programmes to a complete halt; theft of money (“CEO Fraud”) or confidential information has financial implications; and the abuse of computing power to attack external bodies can trigger legal actions against CERN.

In summary, CERN is under attack. CERN’s hardware and software are vulnerable. The consequences for CERN can be immense. The risk is not zero nor negligible. If you are a regular reader of our Bulletin articles, this should not come as a surprise. The CERN Computer Security Team is committed to controlling and mitigating any risk where it is financially and technologically reasonable to do so and leads to an improvement (and avoids any security theatre). Certain risks have been acknowledged and accepted by the CERN Management not to be mitigated (as mitigation would be too intrusive to our academic nature or the benefits do not justify the costs). Implemented measures are well documented on the Computer Security Team’s homepage and in our Privacy Statement, and are discussed at the IT users forum, the CNIC
meeting or here in the CERN Bulletin. Just recently, CERN’s computer security stance has been audited and was largely found to be sound, adapted to CERN’s academic environment, and well-balanced with our operational needs. But you might think differently, so we are interested in your feedback. Where are more cyber-security measures needed? Where are we doing too much, making it too restrictive? Where do you need help? Write to us via Computer.Security@cern.ch.

Negative legacy when moving on? (2019)

CERN’s academic environment is highly volatile. Thousands of people join CERN every year. Thousands more leave during the same time span. Lots of comings and goings. Changes in contract. Affiliation. Home institute. Function. Great successes and accomplishments while at CERN lead to thrilling new challenges outside. The very idea of people moving on even forms part of CERN’s educational mandate. But please, before you embark on your future journey, take care of your digital legacy at CERN.

As a staff member or user working for CERN or at CERN, you are eligible for a multitude of computing resources: a mailbox, disk space, registered devices, databases, websites, virtual machines and more. Usually, these resources are categorised as “professional” or “personal”. “Professional” resources are usually deployed for the operations of the Organization, for its research programmes, to serve our community, for science, for controlling accelerators and experiments, for data-taking, for physics analysis. While one individual always has full responsibility for each resource, they are often used by many, such as computing clusters pledged to separate collaborations, disk space assigned to dedicated experiments, or software repositories managed by individual projects. On the other hand, “personal” resources are usually directly registered under your name, and may hold private or personal information like your personal laptop or smartphone registered with CERN; your mailbox; private documents you store in your home folder on AFS, DFS, EOS or CERNbox; or your personal website hosting your CV, papers and other achievements. The CERN Computing Rules (OC5) explicitly tolerate personal use (OC5, Annex on “Rules for personal use”) as long as its duration is limited, the resources used are negligible, and the activity is not illegal or inappropriate – among other requirements¹. That split between “professional” and “personal” is particularly important once your affiliation with CERN ends and you leave the Organization: Unless you request otherwise, “personal” resources are automatically reassigned to your supervisor, while “personal” resources are purged and lost forever after a short grace period of six

¹ Where that fails, see our Bulletin articles on “Computing power for professionals… only!”, “Rules: what’s allowed and what isn’t” and “Virtual Misconduct – Real Consequence”.
months (some “test” resources are purged after a much shorter, but still defined time span).

This is where “negative legacy” might kick in: unfortunately it is a common occurrence for professional stuff to be stored under the “private” label – and purged after the aforementioned grace period. Software written by a summer student, stored in a local home folder, irretrievably lost. Personal virtual machines running an important control system, terminally purged. Project databases permanently deleted. Experiment websites gone forever… What about your legacy? And what about the legacy of your supervisees? If you are a resource owner, take a moment to review the usage of the computing resources registered under your name. If you are a supervisor, it is your responsibility and in your interest to guarantee a smooth handover when your supervisees or students leave! Check for example the [CERN Resource Portal](https://home.cern/resources), the [network database](https://network.cern.ch), or the [OpenStack cloud service](https://openstack.cern.ch). Are there resources, e.g. webpages or virtual machines, which are labelled “personal”, but are technically “professional”? Is there software and code (snippets) which should be committed to your project’s central software repository like [CERN Gitlab](https://gitlab.cern.ch)? Are all essential papers and presentations archived on the [CERN Document Server](https://docdb.cern.ch)? What about technical documentation which should go to [EDMS](https://edms.cern.ch)? Better to have this sorted out now than to be surprised (and sorry!) once those resources are gone… Plan ahead for a positive legacy!

The problem with crypto-mining (2018)


Following on from Java, app programming, Raspberry Pi, cloud computing and machine learning, the latest trend for computer engineering students is blockchains. One particular application of blockchains is “crypto-currencies”, i.e. virtual money. The past year has seen the birth of a plethora of crypto-currencies. Bitcoin is the best known, but there are also Ethereum, Litecoin, Dogecoin and many more (see [Wikipedia](https://en.wikipedia.org/wiki/List_of_bcryptocurrency_projects) for an even longer list). Even some famous football players are considering [creating their own currencies](https://www.cryptoknight.uk/). All these currencies have one thing in common; in order to obtain coins, there are just two legal methods: you buy them or you “mine” them. The latter is based on a complex mathematical calculation, which eventually results in more coins being added to the total pool and to your digital purse. So here is the problem: what about crypto-mining at CERN?

---

1 If you encounter orphaned resources that might become the victim of a “negative legacy”, please contact Computer.Security@cern.ch, who will be able to recover these resources in accordance with CERN’s policy on “[Third party access to users’ accounts and data](https://cern.ch/Third-party-access-to-users-accounts-and-data)”.
In order to answer that question, one has to distinguish between crypto mining for professional or private purposes, and whether you’re using a CERN-owned computer or a private computer. CERN’s Operational Circular No. 5 (OC5) on the “Use of CERN Computing Facilities” stipulates that the private or personal use of those facilities is tolerated or allowed as long as “it does not constitute [...] profit-making activity” (OC5 “Rules for personal usage” 3c). However, the fundamental nature of crypto-mining is exactly this: making money. Hence, OC5 and its “Rules for personal usage” do NOT allow any kind of crypto-currency mining. Any violation could have serious consequences (see our Bulletin article on “Computing power for professionals… only!”).

When using CERN resources (computers, laptops, servers or virtual machines), mining for professional purposes lacks any reasonable professional justification. While the potential additional demand for electricity is debatable, crypto-mining blocks CERN resources from performing their professional tasks as it takes away CPU cycles, storage memory and network bandwidth. Given that, for Run 3 of the LHC, CERN’s computing needs will grow exponentially, our computing resources should be invested wisely and not wasted. Hence, as the “CERN computing facilities are intended for the attainment of the Organization's aims” (OC5 II 6.), crypto-currency mining on CERN owned hardware is completely forbidden. Exemptions are possible under the authorisation of CERN’s Computer Security Officer, e.g. for stress testing computing hardware or computing power benchmarking. However, experts would need to justify why globally-recognised tools like those provided by the HEPix benchmarking working group are not suitable. And in any event, any money generated in this way belongs to CERN and should be transferred to the appropriate CERN budget code.

Computing power for professionals… only! (2018)

CERN’s OpenStack service provides you with enormous computing and storage resources to achieve your professional goals: if you need CPU power for your analyses, alternative operating systems to test your software, or if you want to run a reliable, high-performance and scalable service… OpenStack is the best choice. In fact, today all LHC experiments, the accelerators sector and the IT department rely heavily on OpenStack to run their analysis clusters and computing services. OpenStack: computing power for professionals… only!

It is the “only” which is important! CERN’s Computing Rules tolerate the personal use of CERN’s computing facilities as long as that activity is legal, non-political and non-commercial, and its resource consumption of computing power, networking bandwidth, storage capacity, etc. is minimal. And this is the crux. Deploying a hundred-odd virtual machines without a professional mandate from your experiment or your department is
definitely not covered by “tolerated”. Unfortunately, this was spotted recently when one user ran a large cluster of VMs for a personal code-improvement project. In the past, we have seen similar abuses where people tried to mine crypto-currencies (“Bitcoins”, “Litcoins”, “Ethereum”) on OpenStack, using BOINC or the worldwide LHC computing grid (WLCG). All immediately attracted the attention of the service managers and led to disciplinary action. Indeed, it is hard to argue that mining crypto-currencies is a professional task. And since it involves money generated at CERN’s (or the WLCG’s) expense, this might trigger legal action by the latter. Even more worrying is that, at least once, the OpenStack service was subject to a targeted attack: an attacker misused the identity of one of our colleagues in order to request 5000 VMs in the OpenStack cluster for some abusive deeds. But such a large request already triggered some tripwires…

So, be reasonable. All these activities violate the CERN Computing Rules (and the WLCG’s security policies) as they stop CERN’s scarce resources from being used more efficiently, consume power at CERN’s expense, and benefit from a service intended for professional use only. Tolerating a bit of personal usage is to the benefit of us all. Exaggerating is not. Deploying dozens of personal VMs is overdoing it. Massive downloading of music and videos (apart from the implications on copyright), the storage of zillions of private photos (whose privacy protection is not necessarily guaranteed by the CERN Computing Rules), constant browsing of the web (diminishing your productivity), the creation of websites with commercial or political content are also a bit much.

Dear summer students (2018)

Welcome to CERN! For the next couple of weeks, you will be able to breathe in the free academic world of CERN. You will have the chance to learn thanks to in-depth lectures, enjoy the freedom of exploring your preferred or assigned research topic, and form your own network of peers during your evening hours. However, “academic freedom” does not imply that there are no boundaries. At CERN, academic freedom also comes with responsibility. Below are some hints on how best to assume that responsibility securely.

You are the primary person responsible for the security of your laptop, smartphone and computer; for your account and your password; for your data; and for the programs, computing systems and services you are developing, so stop and think before acting. If you are working on a project developing code, get the appropriate training first so that your software is “free” of bugs and vulnerabilities that may spoil the functionality of your code and your program. If you have been asked to set up a database or a webserver, consider the offerings of CERN’s IT department first¹: they provide virtual

¹ The full catalogue is available here.
machines, Dropbox-like functionality, databases-on-demand as well as different web publishing frameworks for free. No need to mess around with hardware, operating systems, web servers and the like – simply create your webpages! Also note that employing external services (i.e. web services outside CERN) is not recommended from a computer security perspective. If you are in doubt or need help designing and structuring the computing part of your project, get in touch with the IT consultants. For those of you who are engaged in mathematical simulations, engineering tasks or designing control systems: CERN provides a portfolio of engineering applications for free. There is no need to download additional software from the Internet. If you do need to, contact Software.Licences@cern.ch first as that software might come with license costs or may violate copyrights of third parties.

Talking about rules and copyright violation… Although listening to music or watching videos is subject to the agreement between you and your supervisor, note that sharing videos, music or software packages via torrents or other means usually violates copyrights of third parties and hence is not permitted. CERN regularly gets complaints from those companies and if you are not ready to pay their infringement fees, you’d better make sure now that you legitimately own that video/music/software, and that any sharing applications (e.g. Bittorrent) are disabled. You must also comply with CERN’s Code of Conduct and the CERN Computing Rules. The latter stipulates that the personal use of CERN’s computing infrastructure is tolerated as long as impact is kept minimal and all activity is legal, not offensive and not of commercial nature. And gentlemen, ladies: the browsing of porn sites is considered inappropriate. If you want to spare yourself an embarrassing conversation with us, just don’t do it.

Finally, think of your laptop and PC here at CERN and at home: make sure that it is happy and healthy. Allow it to update itself by enabling “Windows Update”, Mac “Software Update” or Linux’s “yum auto-update”, and get decent free anti-virus software for your Windows computer or Mac! Take care when browsing the web – not everything is as it seems, and a bad infection of your computer might require a full reinstallation. So, if in doubt, STOP - THINK - DON’T CLICK. Good luck, and have a fun summer!!!

Rules: What’s allowed and what isn’t (2018)

CERN has always valued its academic freedom, its international character and its openness, welcoming people from all over the world, giving them the opportunity to think outside the box and try something new, fostering creativity and avoiding placing hurdles in their way. It is this open and free environment that allows us to tackle the riddles of nature, to endeavour to understand the universe and its rules, and to advance
fundamental research and technology. While such an open academic environment is paramount to the operation of CERN, it cannot be completely free of rules…

Rules are (maybe?) an annoying but necessary part of running an Organization like CERN. Rules are imposed on CERN by the Host States, e.g. for safety or radiation-related matters, and are also an essential ingredient in preserving the Organization’s independence. Rules are also enacted by CERN itself in order to enable peaceful and friendly coexistence inside the research community and, like anywhere else in the world, between people. At CERN, the Staff Rules and Regulations, its subsidiary Administrative and Operational Circulars, and the CERN Code of Conduct provide the official and “legal” framework for the proper and efficient functioning of the Organization: employment conditions and working hours; salaries and benefits; working conditions and safety precautions; access rights and control; as well as how to deal with alcohol problems, harassment and fraud.

The CERN Computing Rules, i.e. CERN’s Operational Circular No. 5 (OC5), govern the usage of CERN’s computing facilities, CERN’s wired and wireless networks including all devices connected to them, any computer centre service and the systems, data and applications running therein, any computing nodes and storage clusters for any kind of data processing, as well as any digital and connected device that is part of the accelerator complex or the experiments. Here too, academic freedom prevails and OC5 tolerates the personal use of CERN’s computing facilities as long as this use “is in compliance with [OC5] and not detrimental to official duties, including those of other users; the frequency and duration is limited and there is a negligible use of CERN resources; it does not constitute a political, commercial and/or profit-making activity; it is not inappropriate or offensive; it does not violate applicable laws.” As you can see, online as elsewhere at CERN, you are expected to respect the fact that this is a professional environment and to behave accordingly. The mandate of the CERN Computer Security Officer is to protect the operations and the reputation of the Organization against any cyber-threat; this includes verifying that the corresponding rules are being followed.

As outlined in the Bulletin article entitled “Transparent Monitoring for your Protection”, measures have been implemented to automatically validate the conformity of personal and professional activity with OC5 and its “Rules for personal usage”. Usually, this forms part of our logging and monitoring systems for the detection of intrusions, attacks and malicious deeds against CERN’s computing facilities from both outside and within CERN, as described in some depth in our Digital Privacy Statement. But besides our automatic tools, the Computer Security Team follows up any suspicious activity reported to them by CERN staff, users or third parties from outside the Organization (e.g. affiliated universities, security companies, individuals who are part of our computer “security” network, law enforcement agencies and the police). While we seek to maintain open access to the Internet (including for personal usage), we may in some rare cases block access to, for example, websites hosting malicious content (e.g. drive-
by infections, CERN-like phishing pages) or other kinds of clearly illegal material. Please note, however, that you are always responsible for your own web browsing; the fact that you are able to access a website does not mean that it is legal or otherwise acceptable under OC5.

**Summer students, hold on a minute (2017)**


Summer has arrived. And with it, 2017’s summer students. Welcome to CERN! Ahead of you are two months of great lectures, challenging projects, the possibility to expand your network of peers… and lots of fun! In order to make sure that the fun lasts to the end, here is a small plea from the CERN Computer Security team to you and your supervisor.

CERN runs an open IT environment like you might be used to at your university. You can bring your own computers/tablets/smartphones and hook them up to our Intranet. A CERN e-mail address will be assigned to you. You can launch your own personal homepage hosted by CERN. You can instantiate virtual machines and play around with your pet IT project. Lots of freedom, lots of flexibility. But this does not imply that CERN is the Wild West. Please note that CERN has a set of **Computing Rules**, which define the extent of your freedom and flexibility. They usually stop where the operations and reputation of the Organization are at stake. So the browsing or downloading of illegal, unethical or offensive web content is not permitted. This includes pornographic material of any kind. Running software illegally or using pirated licence keys for software installed on your computer or a computer used by you is also not allowed. CERN has encountered some problems with this in the past (see our article “Do you have 30 kCHF pocket money?”. Furthermore, please refrain from sharing music, videos, films, games or software with your peers, friends and families while using CERN’s networks. Generally speaking, such file sharing is considered to be a copyright violation in various ways in different European countries, including in the two CERN host states, and can affect our reputation in a negative way (see “Music, Videos and the Risk for CERN”). Last, but not least, any political, commercial or profit-making activity, if not related to your CERN duties, should be managed from outside the CERN network and should not use any CERN resources (e-mail addresses, websites, etc.). Just be reasonable!

Finally, if you happen to be working on a project linked to IT, like developing software, designing a webpage, deploying a database… please do not try to reinvent the wheel. We have seen too many brilliant developments fail after the originator left CERN and the project was left in limbo. So if you are working on a project developing code, get the appropriate training first so that your software is “free” of bugs and vulnerabilities that **may spoil the functionality of your code and your program**. If you have been asked
to set up a database or a web server, consider the solutions offered by CERN’s IT department first (the full catalogue is available here: they provide a database-on-demand service as well as various web services for free. No need to mess around with hardware, operating systems, web servers and the like – simply create your webpages! Also note that the use of external services (i.e. web services outside CERN) is not recommended from a computer security perspective. If you have any doubts or need help designing and structuring the computing part of your project, get in touch with us at Computer.Security@cern.ch. For those of you who are engaged in mathematical simulations, engineering tasks or the design of control systems: CERN provides a portfolio of engineering applications for free. There is no need to download additional software from the Internet. If you do need to, contact Software.Licences@cern.ch first, as that software might come with licence costs or may violate the copyright of third parties.

With those few reasonable basics in mind: enjoy your time at CERN!

Virtual misconduct – Real consequences (2017)

In the academic environment of CERN, given the freedom it provides to undertake research and development, it is sometimes forgotten that “academic” and “freedom” do not imply “devoid of rules”, and also do not mean that there are no consequences for inappropriate or illegal behaviour.

The CERN Computing Rules – as set out in Operational Circular No. 5 (OC5) – are based on common sense and apply to everyone using CERN’s computing facilities: staff, users, students, sub-contractors, visitors... In terms of content, it is easy. Anything you would not normally do outside the privacy of your own home, or anything that obviously violates the law or is offensive, inappropriate or immoral, should not be done at CERN. The browsing of pornographic material is one such example. Whether in your office or on a dedicated public screen, it is simply not appropriate in a workplace context such as CERN and has led to the termination of contracts or persons no longer being welcome on the site. (See also our Bulletin article “Offensive Public Browsing”).

Equally inappropriate is the dissemination of material which sheds a negative light on the Organization (or, as the Staff Rules say, creates moral or material prejudice for CERN). An example is the uploading to social media of inappropriate content to do with CERN or filmed on site, which can create a negative reaction in the media and thus impact CERN’s reputation adversely. On one occasion, for example, such activity required the mobilisation of significant resources by the Organization to address the media consequences, as well as for the internal follow-up procedures that were necessary. In that case, disciplinary action was taken in collaboration with the home institutions of the individuals concerned.
Copyright violation and licence infringements are also taken seriously: one university student found herself in a very tricky situation after she downloaded software from a dubious web portal, ran the software without a valid licence key, filed a support request using her university professor's CERN account, and was caught by the company in question. The bill for licence infringement, which was initially sent to CERN, was passed on to her university.

As far as the use of CERN's computing resources is concerned, common sense prevails once more. The CERN computing facilities are intended for professional use exclusively. While some personal activity is tolerated (like privately browsing the web, hosting personal webpages, or use for the benefit of CERN's clubs), extensive misuse is not. An obvious CERN exit strategy? Bitcoin mining! While it might be tempting for a user to run Bitcoin mining on the Worldwide LHC Computing Grid, there are strict rules and extensive security monitoring in place. All violations are systematically escalated and followed up... At least one person once tried to benefit from these resources to generate Bitcoins – to print virtual money for free, while the community paid the costs. The consequence for that person: a formal investigation.

Perhaps most serious of all, and something nobody can pretend to have thought was permissible, is sabotage. Hacking into the computer of a colleague, manipulating his analysis and deleting data is definitely outside common sense and is morally unacceptable. Planting back doors into CERN computing services for usage following your departure from CERN is too. In these cases, the perpetrators were dismissed by CERN or their new employer, respectively...

These examples are not intended to scare you. We just want to remind you that your work at CERN is subject to a set of rules: primarily, the Staff Rules and Regulations and the Organization's Administrative and Operational Circulars, as well as the CERN Code of Conduct. They are there to protect you and ensure a respectful workplace. In particular, your use of CERN's computing facilities is governed by OC5, which is intended to protect the Organization, and therefore you, your data and your work, from any reputational or operational difficulties. So, please familiarise yourself with these rules if you have not already done so, and respect them!

Offensive public browsing (2017)

For the convenience of everyone at CERN, public PC terminals are provided in many different locations so that people can access CERN's websites, as well as CERN's other computing services, even if they do not have a computer/tablet/smartphone to hand. PC terminals are available in the CERN library, in front of the Users' Office, and also for dedicated purposes in conference rooms and the training centre. However, note what they are: public PCs, located in public places.
In the past few months, we have received several complaints about inappropriate use of some of these public PCs, namely the browsing of pornographic material. To our knowledge, there is no professional need to access such websites, and therefore the browsing of pornographic images and films is in violation of the CERN Computing Rules and the personal use policy. Worse, these activities took place in public places where others, by-standers and passers-by, including school pupils and young children, might accidentally notice it – and feel embarrassed or seriously offended! This is why we got the complaints in the first instance.

So, if you happen to use one of CERN’s public PCs, please stick to the rules. Spare yourself the embarrassment of a third party seeing what you are doing (and spare yourself the embarrassment of getting a notification from us). This not only applies to browsing pornographic material, but also doing other private things: internet banking, following your friends on Facebook, reading your e-mails. Of course, this is also true for laptops and tablets used in public places like the restaurants and cafeterias. Browsing pornographic material on an office PC is also in violation of the CERN Computing Rules and we would appreciate it if private activities could remain in the private sphere: at home.

You’re a summer student? Some tips to get you started (2016)

Welcome to CERN. For the next couple of weeks, you will be able to breathe in the free academic world of CERN. You will have the chance to learn thanks to in-depth lectures, enjoy the freedom of exploring your preferred or assigned research topic, and form your own network of peers during your evening hours. However, “academic freedom” does not imply that there are no boundaries. At CERN, academic freedom also comes with responsibility. Below are some hints on how best to assume that responsibility securely.

You are the primary person responsible for the security of your laptop, smartphone and computer; for your account and your password; for your data; and for the programs, computing systems and services you are developing, so stop and think before acting. If you are working on a project developing code, get the appropriate training first so that your software is “free” of bugs and vulnerabilities that may spoil the functionality of your code and your program. If you have been asked to set up a database or a webservice, consider the offerings of CERN’s IT department first: they provide a database-on-demand service as well as different web services for free. No need to mess around with hardware, operating systems, web servers and the like – simply create your webpages! Also note that employing external services (i.e. web services

---

1 The full catalogue is available here.
outside CERN) is not recommended from a computer security perspective. If you are in doubt or need help designing and structuring the computing part of your project, get in touch with us at Computer.Security@cern.ch. For those of you who are engaged in mathematical simulations, engineering tasks or designing control systems: CERN provides a portfolio of engineering applications for free. There is no need to download additional software from the Internet. If you do need to, contact Software.Licences@cern.ch first as that software might come with license costs or may violate copyrights of third parties.

Talking about rules and copyright violation… although listening to music or watching videos is subject to the agreement between you and your supervisor, note that sharing videos, music or software packages via torrents or other means usually violates copyrights of third parties and hence is not permitted. CERN regularly gets complaints from those companies and if you are not ready to pay their infringement fees, you’d better make sure now that you legitimately own that video/music/software, and that any sharing applications (e.g. Bittorrent) are disabled. You must also comply with CERN’s Code of Conduct and the CERN Computing Rules. The latter stipulates that the personal use of CERN’s computing infrastructure is tolerated as long as impact is kept minimal and all activity is legal, not offensive and not of commercial nature. And gentlemen, ladies: the browsing of porn sites is considered inappropriate. If you want to spare yourself an embarrassing conversation with us, just don’t do it.

Finally, think of your laptop and PC here at CERN and at home: make sure that it is happy and healthy. Allow it to update itself by enabling “Windows Update”, Mac “Software Update” or Linux’s “yum auto-update”, and get decent free anti-virus software for your Windows computer or Mac! Take care when browsing the web – not everything is as it seems, and a bad infection of your computer might require a full reinstalltion. So, if in doubt, STOP - THINK - DON’T CLICK. Good luck, and have a fun summer!!!

“Hello World” — Welcome to CERN (2015)
http://cds.cern.ch/journal/CERNBulletin/2015/30/News%20Articles/2034021?ln=en

Welcome to the open, liberal and free academic computing environment at CERN. Thanks to your new (or long-established!) affiliation with CERN, you are eligible for a CERN computing account, which enables you to register your devices: computers, laptops, smartphones, tablets, etc. It provides you with plenty of disk space and an e-mail address. It allows you to create websites, virtual machines and databases on demand.

You can now access most of the computing services provided by the GS and IT departments: Indico, for organising meetings and conferences; EDMS, for the approval of your engineering specifications; TWiki, for collaboration with others; and the WLCG computing grid.
“Open, liberal, and free”, however, does not mean that you can do whatever you like. While we try to make your access to CERN's computing facilities as convenient and easy as possible, there are a few limits and boundaries to respect. These boundaries protect both the Organization's reputation and CERN's computing facilities - including your computing account, your devices, and your data and documents.

Along with your CERN computing account comes responsibility. You are, in the first instance, responsible for securing and protecting your account, your devices, your data, your services and the systems you run. You must also follow the CERN computing rules. These are supposed to be permissive enough not to inhibit your professional work but general enough for us to be able to fulfil our mandate to protect the Organization’s operations and reputation.

Let us recall your main duties:

- Protect your computers. Use them in a responsible fashion and always keep them all up-to-date. “Windows Update”, “Apple Update”, and “yum autoupdate” are your friends. Enable them and let them run in the background. For the “Windows” and “MacOS” operating systems, you can even get CERN’s antivirus solution for free - both at CERN and at home! For more details, see here.

- Be careful with e-mail and the web. Not everything you see is what it seems. “Stop and Think” before you click on random web links. If you don’t know or trust its origin, your computer might end up being infected. This is also the case when installing random “programs”, “add-ons” or “plugins” downloaded from the Internet. You need to trust their sources - and even then, you might compromise your operating system. Also refrain from opening attachments to e-mails that do not seem to be for you (addressed to someone else, you don’t know the sender, etc.) or look suspicious (not in your language, typos, factual errors, does not come from the usual address or domain, etc.).

- Protect your password. Your password is yours and yours alone. Please do not share it with anyone, not even your supervisor, the ServiceDesk, or the Computer Security Team. Treat it secretly, like your bank account’s PIN. And be inventive: make your password complex so that it cannot be easily guessed. Dictionary words in any language fail. Mathematical formulas are great! Some hints can be found here.

- Protect your files and data. The world is watching CERN. If you work on sensitive or restricted documents, make sure that only people who “need to know” can access them. If you value your privacy, also make sure that your personal documents are properly protected! All major CERN storage systems (AFS, Alfresco, CDS, DFS, EDMS, INDICO, Sharepoint, etc.) have facilities for restricting and controlling access. Some documents, e.g. those on the AFS Workspaces, might be “public” by default! Check the CERN Data Protection Policy for details.
• Respect copyright. The violation of licences and copyright is a major offence, and also threatens CERN’s excellent reputation and integrity. Make sure you have the valid rights to run the software installed on your devices. If you inherited the device from someone else, the time to check is now. Note that any financial liability for copyright violation might be passed on to you, and such a liability might easily be as much as the price of a car!
• Follow the CERN Computing Rules. Just be reasonable - do not be aggressive, racist, discriminating or unfair! Note that CERN tolerates your use of its computing facilities for private activities, so long as these are not political or commercial and do not violate any laws. And, ladies and gentlemen, please refrain from browsing pornographic websites. Besides the reputational impact on the Organization, it is awkward if somebody discovers you doing this or if you receive an e-mail from us asking you to justify your porn browsing habits...

Finally, please recall that these simple duties will enable you to work safely with your computers, both at CERN and at home. Just as you care for your safety in the physical world (when talking to people, crossing the road or driving your car), take care in the digital world when chatting and browsing on the Internet or using software applications!

In the name of CERN (2015)

This summer, the American/Canadian dating website Ashley Madison was successfully compromised by a group of hackers (see here) who subsequently published tons of confidential information: addresses, dates of birth, e-mail addresses, ethnicities, genders, names, passwords, payment histories, phone numbers, security questions, sexual preferences, usernames and website activity.

Initially, these attackers blackmailed Ashley Madison and requested that the service be shut down. Later, however, they just made their stolen data public on the Internet. More than 30 million unique e-mail addresses – a hallelujah for miscreants.

What can they do with this data? One possibility is blackmailing the people whose e-mail addresses were exposed by threatening to tell their spouses (“Pay me X bitcoins or I will tell your spouse that you are looking for a date!”). Another is targeting those people who have registered with their company e-mail address, e.g. the many e-mail addresses linked to governmental organisations (“Hand over document X, give me access to Y, or I will tell Z that you are looking for a date!”). Interestingly, that list also included the e-mail addresses of six of our colleagues, three of which were still valid.

Radio Télévision Suisse also reported (in French) on the Ashley Madison story (see especially at 1’19”).

And this wasn’t the first time something like this has happened! Adobe had data for 153 million accounts stolen, including encrypted passwords (which were quickly decrypted). Four million records from Adult Friend Finder were leaked after an attack
in May 2015. The list of customers of Domino’s Pizza in France and Belgium was released in 2014 after a failed blackmail attempt. The Forbes news network fell to attackers in 2014, with more than one million user account details leaked. YouPorn also had 26,000 e-mail addresses plus passwords stolen.

And neither was this the first time that we’ve found CERN e-mail addresses in those compromised lists\(^1\). We have to wonder why people sign up with their CERN e-mail address to personal services not at all related to CERN’s core business… While CERN tolerates the private usage of its computing resources, this is overstretching our tolerance. Thus, if you happen to register with websites and web services that are not related to your CERN work, please use a private e-mail address from your favourite provider (e.g. Gmail, Yahoo, etc.)!

**Posting and mis-posting (2015)**


This is what can happen at CERN if you don’t lock your computer screen...

“Hi, I am looking for a partner either male or female to attend salsa lessons. I have a great body and enjoy rubbing it against other people on the dance floor. I would consider dinner after with the right person. If you think you can keep up with me and enjoy getting sweaty send me a reply. Stay sexy…”

This is the original text of a recent posting on the CERN Market webpage. Some people might find this appealing, some people think this is funny. Personally, I couldn’t care less. But professionally, we had to follow up as this text can be perceived as inappropriate and, thus, in violation of the Terms of Usage of the CERN Market as well as the CERN Computing Rules and its annex on private usage of the CERN computing facilities. We remind you that the CERN Market is a public website that can be used by people within but also outside CERN. All posts are visible worldwide. While this post might be borderline, we have had posts in the past which could have impacted negatively on the reputation of the Organization if spotted by, for example, journalists looking for a story.

If you regularly advertise on the CERN Market, if you host one or more webpages at CERN or about CERN, if you regularly post information about your work at CERN or your opinion on issues happening at CERN on Twitter, Facebook, etc., please use common sense. Publish in a positive and constructive way, respecting CERN's Code of Conduct and the values contained therein. For more details, please consult the CERN Social Media Guidelines. And, finally, please also note that the CERN Market is meant for private sales and services only. Professional offers (dentists, removal services, etc.) are not permitted and will be promptly deleted.

---

\(^1\) If you want to figure out whether your (private) e-mail address (es) have been compromised, we recommend to you this trustworthy website: https://haveibeenpwned.com.
P.S. This example was even worse than it first appeared. The post finally turned out to be a “joke” published under the name of one of our CERN colleagues by members of their team. They neglected the basic rule of locking their computer screen with a password when leaving the office. (Did you spot it? Two more violations of the CERN Computing Rules. Sigh.) Their colleagues took advantage of that, ignoring any adverse effects on the reputation and the moral well-being of the victim.

Social media — Dos and don’ts (2014)

Do you blog frequently? Send tweets about what you’ve done? Keep a lively Facebook profile? Comment regularly on interactive forums? Many of us do.

"Social media", i.e. Twitter, Facebook, public blogs, interactive forums and public commenting functions on websites, are widely used for sharing information, outreach and contact with the world. While you can make use of social media for many different purposes, the lines between private and public, personal and professional are often blurred.

Consequently, it is often difficult to get the balance right. As a social animal, you want to be frank, open and communicative and share your knowledge, experiences, opinions, feelings and life with your peers. On the other hand, while working at or for CERN, you cannot act in the void but have to respect CERN’s Code of Conduct, CERN’s Computing Rules and, for CERN personnel, the Staff Rules and Regulations. Therefore, if your posts include mention of or make reference to CERN, it is worth reflecting on whether your subject, message and choice of words are appropriate.

In order to guide you, the CERN Communications Group, HR Department, Legal Service and Computer Security Team have developed some guidelines on how best to use social media, for your benefit and that of the Organization. These guidelines apply to all CERN contributors (i.e. staff members, fellows, apprentices, associates, users and students) who comment professionally or privately about their activities at CERN using Social Media. Of course, there are no surprises for anyone sensible. These guidelines cover how to post responsibly, correctly, clearly, reasonably and, of course, as yourself. They ask you to be cautious with external sources or products, and require you to respect CERN’s rules and its reputation, as well as privacy, confidentiality and intellectual property. All this, in an easy to follow and understandable way. Take a look and enjoy your online communication activities!

The naked blunder (2013)

In the past, we have published many different articles on a multitude of aspects of computer security and on the risk to CERN and to you when you use your computer at
CERN or at home. Some were relevant to all of us, others only to a minority. This time, we would like to raise a rather delicate and fortunately rare issue: the consultation of pornographic websites and why it is forbidden at CERN.

With 10,000 people at CERN of different cultural and professional backgrounds, some working outside traditional working hours and some staying in one of the three CERN hostels, it is a natural fact that behaviours, interests, perceptions and attitudes vary significantly. CERN highly values the diversity of its personnel and users and the interaction between them. In this respect, the CERN campus is comparable to a small city and, as in every small city, some citizens are attracted to pornography.

It is not easy to find a common definition of pornography. It depends on our cultural roots, our values and the environment we live in. Having said that, if you are in doubt as to whether certain webpages or materials contain pornography, it’s better to assume that they do and to act accordingly.

The browsing of pornographic websites and the downloading or capture and storage of pornographic videos and photos violates CERN’s values and its Code of Conduct and is prohibited under the CERN Computing Rules. The consultation of “adult” pages is never a professional activity; colleagues who encounter this might be irritated, offended or shocked and feel harassed (see Operational Circular No. 9 on harassment). Furthermore, visiting such sites and downloading pornographic material endangers your computer, as the corresponding webpages and files may contain viruses or other malware. It could even violate the copyright of the content owner. Finally, it puts the Organization at risk, as such activities may be monitored by the site owner or third parties (including, potentially, national authorities). It is definitely not good for CERN’s reputation if such parties publish the names of visitors to their pages and “CERN” is listed.

For the same reasons, incitement to violence, discrimination or racism, as well as inappropriate or offensive activities, are not tolerated at all. Spare yourself the embarrassment of getting a notification from us asking you to justify (and cease) any prohibited activity or worse, the possibility of disciplinary action. Instead, refrain from the consultation of porn and other illegal content while connected to the CERN networks, even if you are using your own device!

“Security” is YOU! (2012)
http://cdsweb.cern.ch/journal/CERNBulletin/2012/49/News%20Articles/1496408?ln=e n

Usually, people consider “Computer Security” a technical problem: firewalls, intrusion detection, anti-virus software, encryption… but I don’t. I consider “Computer Security” being like swimming or crossing a road.
You usually don’t actively think about your safety at all, you just do it. You just move your arms and legs or look “left-right-left” (“right-left-right” in countries of the British commonwealth or Japan). This was imprinted on us during our childhood… and I believe we should achieve the same for “Computer Security”!

So, like swimming or crossing traffic, I would like to see a similar culture evolve for “Computer Security”. We need a new mind set. “Computer Security” starts with the human body sitting in front of the screen - the guy who configures a device, the lady who programs an application. “Computer Security” is a people problem, and it can only be solved by people, not by technique. It depends on us ensuring that our Windows/Linux/Mac/iOS/Android operating system is regularly patched. We should remember that passwords are personal and should never be shared. We should protect files and documents appropriately, and we should first take suitable training before writing software or configuring computing services. All this, of course, is independent to CERN. It applies to your life at home too.

Thus, make “Computer Security” a small part of your daily life - like swimming or crossing the road. I’m not asking for a big investment. Just you subconsciously thinking of doing IT the secure way whenever you touch a keyboard, mouse or touchscreen. Also recall that in the free academic environment of CERN, “Computer Security” has been delegated to you. You are, in first instance, responsible for the computer security of the laptops, smart phones and PCs you use, the accounts and passwords you own, the files and document you hold, the programs and applications you have installed or, in particular, you have written, and the computer services and systems you manage. The Computer Security Team is ready to help you assume this responsibility. Alternatively, you can delegate that responsibility to the IT Department who provides a multitude of secured computing services.

Why “security” is not ME… (2012)

Thank you all for your feedback on our latest Bulletin article on “Security is YOU!”. Indeed, I can confirm that at CERN you are, in the first instance, responsible for: the computer security of the laptops, smart phones and PCs you use; the computing accounts and passwords you own; the files and documents you hold; the programs and applications you have installed or, in particular, written; and the computer services and systems you manage. In the free and liberal academic environment of CERN, I, as Computer Security Officer, decline that general responsibility.

How can one take responsibility for something one does not control? Currently, I do not control the operating system you run, the programs and applications you install, the webpages you browse, the software you write, the files and documents you create, and the computing services you deploy. Dictating and restricting you to controlled...
solutions would contradict that freedom and liberty of academic working. Of course, we can change that, but I love CERN’s academic freedom too. So this is probably not the right way to go.

Rather, I see my role as finding a good balance between that academic freedom, the operational needs of the Organization and computer security - and in enabling YOU to assume your share of this balance. “Computer Security” has been delegated to you, but you are not alone. The Computer Security Team is ready to help you. We provide training and awareness, consulting and audits, general protection and detection services, as well as a central Computer Emergency Response Team (CERT). And there is the IT Department! You can delegate your responsibility to the IT Department, which provides a multitude of secured computing services.

In this respect, take this as an offer for 2013. Enjoy the end of the year and have a safe new year!

**Security needs you (2010)**


Academic freedom is a valuable thing, but like any kind of freedom, it comes with responsibility.

Here at CERN, and in the global particle physics community as a whole, we enjoy an open academic environment, which gives us freedom of choice and freedom of expression. It is a strong tradition at CERN, but it’s not something we can ever take for granted. This is particularly true in the area of IT, where our openness and our global visibility make us an attractive target. Attacks on our IT infrastructure in the past have had a negative impact on our reputation, and have even led to changes in the way we operate computing services.

It is the responsibility of all of us, not just the experts in the IT Department, to protect our IT infrastructure while striking the right balance between security, academic freedom and the unfettered operation of our facilities. Everyone using CERN’s IT infrastructure is responsible for the security and protection of the computers they use, the operating systems they run, the applications they install, the programs they write and the data they store. For those of us who manage computing services and systems, that responsibility clearly extends to them as well.

In assuming your responsibility, you are not alone: the IT Department and the Computer Security Team are there to help, and you’ll learn more about how in this issue of the Bulletin. We all have an essential role to play in protecting our academic freedom. Let’s make sure that maintaining vigilance when using IT facilities, and proactively protecting computers & data remains an essential part of that responsibility. At CERN, security is not complete without you.
During a recent audit of CERN’s computer security, the question was raised of how many attacks CERN is subjected to each day. It was a difficult question as there is no good metric for what constitutes an attack and how you quantify it. Does one connection to CERN constitute one attack? Or many connections to CERN from the same source? Or all connections linked to the same attack pattern or theme? Or from the same group of adversaries? Does one brute-force attempt to log into one CERN account count as an attack? Or many different attempts to break into one account at CERN via a so-called dictionary attack? Or is it one attack when one adversary brute forces their way into many CERN accounts via such a dictionary attack?

As you can see, answering that initial question is difficult, and other entities outside CERN answered it with “300-500 million a day”. Apparently, they count every connection, every attempt. The basic fact, as measured with our intrusion detection mechanisms, is that CERN is under constant attack. Always. Even right now. There are few moments when we do not see brute force attacks against CERN accounts. Few moments when public CERN webpages and Internet-facing computing services are not being probed for vulnerabilities. Few moments when CERN mailboxes are not receiving SPAM or so-called phishing e-mails. And few moments when CERN computers are not subjected to viruses, worms and other malware... And that number is not even the most interesting one...

Delving deeper into the numbers from our digital trenches:

- Every day, CERN’s Security Operations Centre (SOC) digests about 3-5 TB of log data, *sifting through for suspicious or malicious activities*;
- CERN’s firewall monitors a stream of 40 Gbps of incoming and outgoing traffic and tries to reject any unwanted or unauthorised packets. In the near future, the CERN Network Team will replace this firewall with a more powerful solution allowing the filtering of up to 200 Gbps of traffic in each direction and the blocking of advanced, sophisticated or targeted attacks;
- The CERN SPAM filters usually reject about 70% of the 2 million e-mails CERN receives each day. For those that pass through, the subsequent advanced malware detection filters quarantine about 50 *phishing campaigns* and 20 campaigns using malicious attachments to target CERN per day;
- The SOC sends dozens of notifications per month to colleagues whose CERN e-mail address or external e-mail address – together with external passwords and other personal data – has been disclosed in *data breaches* from Internet-based cloud services. Much more widely, our automatic tools also regularly
inform hundreds of peer organisations, institutes and universities about thousands of their e-mail addresses and passwords potentially being exposed;

- Members of the Computer Security Team run dozens of dedicated campaigns per year, informing users and those managing CERN’s computing services about newly reported vulnerabilities (e.g. TeamViewer, RDP, SMBv1, WordPress, iOS, Flash) and ensuring, when needed, that these vulnerabilities are closed as fast as possible before the corresponding systems, devices or accounts are compromised by adversaries;

- Similarly, we receive dozens of external reports a year from friendly people and students of our CERN WhiteHat Challenge programme pointing us to sub-optimal configurations or weak set-ups, which are all well deserving of follow-up for improvement;

- On the proactive side, the IT department is running a series of projects (PC hardening, a new identity management system including multifactor authentication, deploying a new anti-virus solution, and providing better tools for programmers...) to improve CERN’s cyber-security posture.

Despite those numbers, what matters more is the – hopefully low – number of successful attacks. In these more severe cases, the Computer Security Team engages five to ten times a year in direct incident response, figuring out how adversaries (like the RockeGroup but also nation-state sponsored actors) might have managed to infiltrate CERN, along with their motives and attack vectors. Due to severe violations of the CERN Computing Rules, three people were dismissed from CERN last year. Furthermore, we also assist several other HEP and HPC sites as well as the WLCG and EGI/EOSChub in incident response. Indeed, our academic community has suffered in recent months from Ransomware attacks. And, finally, we actively help Swiss health institutions protect their assets against attacks using “Covid-19”-related themes as a pretext.

Digital stolen goods of CERN? (2020)

Have you ever had your purse or wallet stolen? Or your laptop? Your smartphone? Did someone break into your apartment or house and leave it in a mess? Or smash a window of your car and remove your valuables? Or did your bike just disappear? Have your credit cards ever been abused? Maybe you just don’t know yet – so wouldn’t you be interested to find out?

The same applies in the digital world. Passwords are getting phished or stolen from unprotected storage and regularly exposed (“The easy way to lose passwords”). Credit card numbers, expiry dates and CVVs (the three-digit security code on the back) are
getting stolen. Computers are getting compromised and all their local data lost (“Malware, ransomware, doxware and the like”). Wouldn’t you be interested to learn if your passwords for CERN or any other external web service have been stolen and exposed by thieves? Wouldn’t you be keen to know whether details of your credit card have been secretly shared among fraudsters? Wouldn’t you like to find out whether your computer has ever been compromised and whether your personal data has been sold among criminals? And wouldn’t you love to acquire information as to whether you or your family have ever been, are or will be the target of cyber-criminals? While, of course, this is your private business\(^1\), it is best practice – in industry and as part of CERN’s due diligence responsibilities – to figure out what information the evil-doers have already gathered about the Organization, its operations, its staff and its users.

So, just as many other organisations and companies do for themselves, the Computer Security team has contracted an external company specialising in intelligence about the underground markets for stolen digital goods (sometimes labelled as the underground economy or the so-called “Deep & Dark Web” (DDW)). This company, like many of its competitors, has expert staff who have gained access to the hidden forums and vetted circles used by cyber-criminals to share, discuss and execute attack vectors and plans, and to sell or buy stolen digital goods, or even vulnerabilities and weaknesses. Consequently, this company collects any interesting data about many different stakeholders, similar to the way that the Google or Shodan search engines index and cache “normal” visible webpages. Our subscription with this external company permits us to query their vulnerability, password and attack vector database using a maximum of 500 keywords related to CERN, e.g. “cern.ch”, “INDICO”, “Large Hadron Collider”, “Medipix”, “Geant4”, “openlab”, “PasseportBigBang”. Based on our past experience, past incidents, past reports from our peers in the security community and past password dumps, such queries are intended to give more insight about the vulnerabilities and weaknesses that evil-doers have already gathered regarding CERN, its computing services and webpages; to discover any weak or disclosed CERN passwords or credit card information; and to find out the aims attackers have when targeting CERN, and which attack vector they plan to use (or, if already too late, have chosen in the past).

After one month of continuous queries, the company came back to us. Fortunately, their report has not revealed any critical or direct threats to the Organization, but provided only a series of minor findings which have been acted upon by the CERN Computer Security Team following its standard procedures and practices. A big thank you to those who swiftly repaired the affected computing resources and services! You can find some details in our Monthly Report once those issues have been fixed.

\(^1\) If you want to figure out whether one of your passwords has been exposed, we suggest this fine and trustworthy site here: [https://haveibeenpwned.com/](https://haveibeenpwned.com/).
The Bulletin article entitled “Blackmailing Enterprises: You are Patient Zero” raised a series of questions: “What is the problem for CERN?”, “We are academia!”, “Why should we worry?”. Some answers can be found below.

Ransomware attacks usually consist of tricking the victim into installing software that will eventually encrypt the victim’s computer (and any remote share or backup that the user has access to) and asking for money – the ransom – in order to unlock (decrypt) the files. Such attacks have been happening for years. However, in recent months, a worrying trend has been emerging fast: targeted organisation-wide ransomware attacks. These attacks are carried out by well-organised and well-funded criminal groups.

Ransomware attacks typically start via traditional infection vectors like phishing e-mails (“You are Patient Zero”). For targeted attacks against an entire organisation, it is also common for the attacker to focus on exposed services, like unpatched Web applications exposed to the public Internet. Once access has been gained on a single device inside the network, the attacker then focuses on silently spreading the intrusion internally in order to gain access to privileged accounts or central services. After gaining access, the attacker explores the network, reading e-mails, finding data troves, and once they know the organisation in depth, they craft a plan to cause the most panic, pain and operational disruption. It can take an average of two to three weeks for the attacker to be in a position to enter the final stage of the attack. With the right level of access and control, the attacker only has to effectively deploy the ransomware payload in a single damaging wave to as many machines as possible, covering end-user machines, central services (e-mail, web servers, etc.), shared file systems and of course, backups. This may sound complicated and costly, but automated tools increasingly perform most of the work and ransomware is currently an incredibly profitable business, allowing attacking groups to source the appropriate expertise and staffing.

As soon as the targeted organisation realises it has been attacked, a ransom note is issued. The goal is very simple: inflict maximum damage on the daily operations of the victim organisation, so that it sees no other option but to pay the ransom. Very often, the damage is total: no IT. At all. Back to pen and paper. And it works extremely well. When Carleton University was affected, it was quoted as saying “Our research is halted right now because all our computers are either shut down or infected”. Sadly, when confronted with such a situation, some victims feel the only effective option is to pay the ransom. This happened at the University of Calgary: “The decision was made to pay the ransom because we do world-class research here […] and we did not want to
be in a position that we had exhausted the option to get people's potential life work back in the future if they came today and said, "I'm encrypted, I can't get my files," said Dalgetty [vice-president of finances and services].

This was in 2016. The academic and research sector is clearly perceived as a viable market for attackers, and their tactics and malicious frameworks have drastically evolved since then. More than half of today's ransomware victims end up paying the ransom. Criminal organisations are taking the time to research their victims in order to maximise the potential damage to the organisation and their payoff. The amount for the ransom demanded is "just right", basically the maximum amount that the organisation can afford to pay. The University of Maastricht was one of the rare victims to expose the attack publicly and even shared a detailed technical report. In 2016, the University of Calgary paid about 20 kCHF. But in 2019, the stakes are higher and the University of Maastricht agreed to pay around 230 kCHF in the hope of unlocking its systems. The attacker completely annihilated the University's computing and network infrastructure on 23 December, and the timing made the attack even more difficult to handle.

This is the one phishing e-mail it took to bring the entire computing infrastructure of University of Maastricht down.

That said, a number of organisations seem to elect not to pay. They may acknowledge that it makes us all less safe, but most importantly that there is no guarantee the files will be unlocked by the criminals. Not all victims agree to share the figures, but ransomware attacks have such a profound impact on the core technical infrastructure of the victim that they are immensely costly, no matter the strategy. The City of Baltimore also did not pay and “has put more than 18 million into the attack. The hackers originally demanded 76,000.”

There are also massive hidden costs: the attacker has access to all of the organisation’s data and information, including personal data about employees, customers, business partners and technologies. And it is hardly possible to hide or continue to operate during a successful ransomware attack, which itself brings additional, significant reputational damage. A ransomware infection must be considered a data breach until investigation proves otherwise. More and more of the ransomware operators are now leaking data belonging to victims who fail to pay up. This recent development means that organisations are increasingly likely to pay the ransom. The cyber insurance industry has also adapted to the new reality. It's getting
more and more expensive to transfer the risk of ransomware, as underwriters are raising premiums for their coverage.

Over the course of the last months and even weeks, the number of victims in the academic sector has kept increasing, with a worrying trend of academic institutions paying ransoms, like Regis University in Denver. It would be too easy to blame the more open “academic environment” in which we operate our services. Our sector is not the only one affected: some serious industry actors are victims as well. One example is Travelex, whose entire banking system was taken down globally after an attack on New Year’s Eve. “Travelex cashiers have been resorting to using pen and paper to keep money moving at cash desks in airports and on the high street.” Beside the attack’s operational costs, the damage to Travelex’s business and reputation is of course gigantic, forcing its CEO to read a public statement regarding the attack. In another attack in December 2019, a US Coast Guard base was taken offline for 30 hours as “ransomware interrupted cameras, door-access control systems and critical monitoring systems at the site”.

Recently, ransomware started adding other functionality to target Industrial Control Systems operations. If such ransomware were to make its way into the CERN Technical Network, that could pose significant risks for the operation of the accelerator complex and the experiments. Even if the malware does not spread to actual programmable logic controllers (PLCs), it can still halt the operations of complex industrial equipment: “[The] natural gas facility shut down operations for two days after sustaining a ransomware infection”, as “A cyber threat actor used a Spearphishing Link to obtain initial access to the organisation’s information technology (IT) network before pivoting to its OT network. The threat actor then deployed commodity ransomware to encrypt data for impact on both networks.” The situation is certainly not new, but the number of victims is rapidly increasing. And most importantly, the fact that the attackers take the time needed and have the capabilities to deploy ransomware so deeply in the victims’ computing and network infrastructure is a new development.

On behalf of the Swiss Government, MELANI has issued multiple advisories and repeated warnings specifically on this issue, as “several well-known Swiss companies have been affected by this kind of attack”. In the same vein, the French ANSSI also produced a detailed report, and explicitly warn that organisation-wide ransomware is currently the most serious computing threat for institutions and companies. ANSSI add that such attacks are sometimes as sophisticated as nation-state sponsored espionage operations. As a result, the question is not whether well-funded organised groups will target CERN with an organisation-wide ransomware attack, but when. But the most important question is: what do we do about it?

- Phishing detection: Our anti-malware filtering appliances detect most phishing e-mails, in particular those containing attachments. But this does not provide complete protection as, currently, it does not follow embedded links to
their origin to verify whether the webpage or file behind the links is legit or malicious. Due to this configuration, it is easy to insert a malicious download link in an e-mail, and it remains reasonably simple to successfully send a malicious attachment.

- **Security patching of exposed services:** It is absolutely crucial to keep all exposed services fully patched. More and more malware carries out scans of the local network even after the initial infection in order to propagate inside the organisation. An example is Emotet, which often delivers the Trickbot ransomware as a second stage. A leading university was affected by an organisation-wide ransomware attack after the attacker “manually” compromised an unpatched Web application after scanning and exploring their exposed services. It is common to have delayed security patching on non-critical services – these make easy targets for attacking groups.

- **End-point protection:** The current signature-based protection unfortunately has a low malware detection rate. Efforts towards better “Endpoint Detection and Response” are ongoing by IT-CDA, although there is no defined timeline or budget.

- **Threat intelligence / SOC:** The CERN Computer Security Team takes great care to collect known ransomware “command and control” servers from hundreds of partners, including MELANI and other government agencies. Very often this provides after-the-fact response capabilities, and does not guarantee all ransomware attacks will be detected.

After the attack, the University of Maastricht produced a number of recommendations based on the lessons it learnt, most of which are relevant to CERN as well. Basically, resilience is the key. It is absolutely crucial to keep all exposed services fully patched. You can help the Organization with that by keeping your computer, laptop, smartphone and, if you manage one, computing service up-to-date. Make sure that you have appropriate back-ups that are not susceptible to unintentional modification or deletion. Secure your computing account appropriately, do not disclose your password to third parties, and segregate the power of service accounts so that the exposure of one does not compromise all the systems you manage. Finally, STOP – THINK – DON’T CLICK on unknown attachments or weblinks, so you don’t become the patient zero compromising CERN (see our Bulletin article entitled “Blackmailing Enterprises: You are Patient Zero”).

**Blackmailing Enterprises: You are Patient Zero (2020)**
Lots has been written in the past about the importance of being vigilant when browsing the web, opening e-mails and their attachments, or when installing third-party software. Remember to “Protect your family” against “An old scam in a new disguise” i.e. “Malware, ransomware, doxware and the like”? But we never spoke specifically about CERN…

In the past, attackers were targeting end-users. You. Me. Our families. Everyone. Trying to get hold of your PC, your laptop or your smartphone. Obtaining illicit access. Sniffing out all your passwords. Reading your personal documents. Watching you via the embedded webcam. Listening to you using the embedded microphones. And eventually encrypting your hard disk. Once that’s done, they will blackmail you by asking for money in exchange for the decryption key. And threatening that, if no money is provided, all data will be purged (“Ransomware - when it is too late...”). With this threat becoming less successful, attackers have started threatening instead to expose your data. Mobbing you. Shaming you. Exposing your intimate details (“Enter the next level: Doxware”). This is why, assuming that you value your privacy and prefer to avoid problems, it is essential to be vigilant when browsing the web, to STOP – THINK – DON’T CLICK on links and URLs received from unknown people, and to pay additional attention when answering e-mails, clicking the links therein, or opening any attached documents (“Click me – NOT!”).

So what about CERN? While CERN has many protective measures in place to avoid large scale infections of CERN-hosted PCs, laptops and smartphones, and while CERN’s central storage system should provide sufficiently secure and independent back-up solutions for you and your professional data, the ultimate security of the Organization depends also on you: Security is not complete without “u”! In particular, attackers have now started to deliberately target companies, enterprises and organisations, and blackmail them by threatening not only to encrypt their (confidential) business data, but to expose that data on public webpages if the affected company does not pay the requested ransom... Admittedly, if they want to expose our physics data, we might even want to help them, but CERN also holds some confidential business data (contracts, NDAs), personal data and the like (“Coming soon: A pragmatic Data Protection Policy for an open Organisation”) that is worth protecting.

So, just like at home please do the same at CERN: be vigilant when browsing the web, STOP – THINK – DON’T CLICK on links and URLs received from unknown people, and pay additional attention when answering e-mails, clicking the links therein, or opening any attached documents. Let us know if you spot something malicious, suspicious or dodgy. And let us know if you have fallen victim to an attack so we can remedy the problem together. Just ping us at Computer.Security@cern.ch.
“Serious gaming” is the gamification of training for professional purposes. When you play a serious game, you are actually also improving your knowledge on a particular subject. For example, in 2015, the CERN Computer Security Team ran, in collaboration with an external security provider, the “Kaspersky Interactive Protection Simulation” (KIPS). Attended by about 80 control and safety system experts, technicians and engineers, the goal of the game was to instruct our control system experts how best to secure their installations. In the game, teams of four to six people had to secure a water purification plant round-by-round, by buying new security features and making sure that attackers did not bring the water treatment process to a halt. The team that generated the most revenue and had the least losses won (see details on this in our Bulletin article “Protect your Plant: A “Serious Game” about Control System Cyber-Security”).

Nowadays, other online security games permit better in-depth training on a multitude of subjects. Take the CERN computer security course, for example, which you are supposed to complete to ensure you know the basics of computer security, password protection and CERN’s rules. But there are more fancy ones:

- Google has produced an interesting quiz, challenging you to identify malicious e-mails;
- Radio Télévision Suisse’s serious game aims to raise public awareness of the implications of data protection and Big Data;
Less related to “computer security”, but great for aspiring programmers: why not learn through **playing** how to **develop code** with JavaScript, Python and other languages.

Give these a try and enhance your skills in protecting your mailbox, your data and CERN!

**Fun facts: Did you know? (2018)**


Like any other organisation, institute or enterprise, CERN is under permanent attack by evildoers. Attackers try to break into our data centres, misuse the computing power of the Worldwide LHC Computing Grid and attempt to steal your CERN password or compromise your laptop or PC. 2018 was no different from the years before. As 2019 begins, we would like to share a few fun facts on CERN computer security and our activities in 2018.

Cybersecurity is a marathon and, as in previous years, CERN computing resources were challenged by many different parties. Thanks to your awareness and care, the proactiveness of our colleagues in keeping the data centres and their computing services up to date, the quick responses when incidents have happened and the willingness of the CERN Management to embark on new protective measures, CERN has been spared from major cyber-disasters. Still, we have not been idle! All our computer security interventions are documented in our Monthly Report and some of them have been discussed in previous Bulletin articles. Here are a few fun facts:

- 116 computer security interventions were performed by the CERN Computer Security team in 2018;
- 2TB of data per day was analysed in CERN's Security Operations Centre;
- This data is compared online with about 17 000 suspicious IP addresses, domain names or known malicious files (so-called indicators of compromise, IoC);
- The most serious computer security incident so far (back in 2016) required 30 person-weeks of in-depth studies before it was finally concluded;
- 3 Macbooks were found to have been infected in 2018;
- 2670 CERN e-mail addresses (and local passwords!) associated with an external web service were exposed in a single data breach of that service;
- In the last “clicking campaign”, 15.2% of the email recipients clicked and would potentially have rendered their device compromised;
- 516 878 EUR in compensation has been demanded following an alleged licence violation;
- 126 CERN staff and users have so far been trained to become White Hats;
26% of non-computer devices, e.g. control systems, webcams, printers, coffee machines, smart meters, oscilloscopes, Raspberry Pis and Arduinos – devices of the so-called Internet of Things – connected to CERN’s office network have been found to be vulnerable;

2766 Service Now tickets were handled in 2018.

Will 2019 be calmer? That would be unexpected and against worldwide trends. Instead, 2019 will doubtless be as interesting as the past! So we continue to count on your help: with a sufficient amount of awareness, sensitivity and caution – STOP – THINK – DON’T CLICK – you can protect your own computers, tablets and smart phones, documents, photos and data, bank accounts and online accounts – and contribute significantly to protecting CERN!!! We wish you, your friends and your families a safe and secure 2019!

Meeting your family during the holiday season? (2018)

Help keep them secure. Discuss “security” with them. Tell them how to protect their digital life, their documents and data, their photos and videos, their Facebook and Instagram accounts, and their online banking access. Start with your family. And then move on to your friends. Here are some ideas of how to do it.

Let’s start with the people you know. And those you don’t. Would you ever invite a random person from the street into your home? Would you accept a parcel from someone unknown and open it up? Would you follow a stranger into his car? (and what about your kids?) And how would that translate into the digital world? Chatting with some avatars on the other side of the world (who might happen to be “a dog”)? Or opening up an attachment to an unsolicited and unexpected e-mail with no return address nor reference to you; unrelated to you, your job or your interests; written in a foreign language; full of typos? What about clicking on random links in similar e-mails, Facebook posts, WhatsApp messages, or on dodgy webpages? Encourage them to be more suspicious. Common sense in the real world also applies to the digital world. Or else your digital life is in jeopardy.

Have a fun discussion about passwords. Secure long ones. Breakable short ones. Stupidly obvious ones. Nice complex ones. Without, of course, disclosing the passwords you use, talk about what kinds of passwords work for you and what kinds don’t. How do you memorise them (how did your grandma remember phone numbers in the last century)? What strategy do you employ for different applications and websites? Do you use a verse from your favourite poem? Or the chorus of your most cherished song? What about a good mathematical formula? Or the recipe of your preferred dish? The contents of a CD you bought 20 years ago? Or a combination of
them all? Remember that good passwords should never be shared with anyone, be sufficiently complex that they cannot be found in any dictionary, and be different for different important websites and devices.

Also show them how they can keep their devices up-to-date: their Windows PCs (search for “Updates”), their Macbooks (Apple logo, then System Preferences, then App Store) but also their iOS (Settings, then Software Update and Settings, then Apple ID, then iTunes & App Store, then enable Updates) and Android (Google Play Store, then Menu Settings and enable Auto-update) smartphones and tablets. Also consider any other networked device, like their wireless access points, webcams, smart TVs, gaming consoles… If you feel comfortable doing so, check whether these are running the most recent firmware version. Usually, somewhere they will provide a “check-for-recent-update” button. Your family and friends will be grateful!

Finally, note that all our Bulletin articles are publicly available on the CERN Bulletin’s home page. In addition, we have collated them into a nice Christmas read. Maybe your friends and family will be interested to learn more about computer security best practice and protective measures…

Digital Broken Windows Theory (2019)

Have you ever heard about the “Broken Windows Theory”? It was introduced in 1982 by social scientists and suggests that serious crime and anti-social behaviour is more likely in environments where small crimes such as vandalism, public drinking and turnstile-jumping have already created an atmosphere of lawlessness. The city of New York adopted the theory, with the hope of reducing crime by creating a more positive urban environment, leading to order and lawfulness. We should try to apply the same theory to running computing services visible to the Internet.

Computing services at CERN are run by a large variety of people, but primarily by our colleagues from the IT department. On top of their service offerings, users can create web services with openings to the Internet. In parallel, our research community, the experiments and the accelerator sector independently run computing services, which themselves have openings to the Internet. While the Computer Security Team controls the openings in CERN’s outer perimeter firewall and performs an assessment on the level of security before any new opening is permitted, it is currently quite tiresome to maintain that security level for all open services. On the one hand, “computer security” is a highly dynamic subject and what was secure yesterday might become insecure tomorrow (think of the “Shellshock” or “POODLE” vulnerabilities of the past). On the other hand, thanks to the motto “don’t touch a running system”, negligence leads to a deteriorated state of open services.
Recent computer security scans have shed some sinister light on those CERN computer services exposed to the Internet. Not all of them are perfectly secure anymore. Certificates have expired or are just “random” (e.g. self-signed or without chain-of-trust), encrypted channels use methods that are now deemed to be insecure, landing pages are missing or software is not up-to-date anymore. All owners of the affected services have, of course, been notified!

But still, like in New York, deteriorated services might attract malicious evil-doers to carry out their malicious deeds. Let’s keep our Internet presence secure and professional! Let’s apply New York City methods! We already scan for vulnerable websites and outdated configurations, we already check whether current firewall openings are still needed and we notify the owners of affected services, but we need to do more! On the one hand, we should look into adapting the defaults for centrally managed services in order to have an elevated and more secure base configuration. On the other hand, we would like to ask all owners of computing services, in particular where running that service is not your primary occupation, to keep a closer eye on them. Don’t let them deteriorate! Keep them up-to-date and verify regularly that all versions are the most recent ones. Check your certificates and renew them in time. Have a landing page or, if not possible, redirect to “home.cern”. And, finally, review all firewall openings and ask us to close them if they are not needed anymore. Let’s keep our Digital Broken Windows under control.

**Take it seriously (2018)**


When it comes to personal health or safety, we usually apply best practices to protect us from adverse events, illnesses or harm. This is more than logical, since our physical life depends on it. But how come in the virtual world, many best practices are simply ignored: “I have nothing to hide”, “Nothing will happen anyhow”?

In the physical world, we apply many safety measures automatically and repeatedly. We look left-right-left when crossing a road; we learn to swim early in childhood; we put on a coat when it is getting cold; we use a helmet when cycling; and even put on safety shoes and a harness when working in construction areas (and are required to do so when working in such areas at CERN!). We avoid dark alleys at night and do not accept gifts from strangers (chocolate, anyone?). We even lock our flat and car when leaving them, and keep our PIN codes and credit card numbers secret. And if asked if we would like a new car with an enhanced airbag system that improves personal safety by, say, just 30%, who would decline?

How come we are more relaxed in the virtual world? Are we? As we have written in previous issues of the Bulletin, our virtual life is deeply entangled with our physical world: Your smartphone and your laptop hold many more photos, documents and data about you and your family than you would ever disclose to your most intimate friends...
(Open door, open screen, open life...). If we lose either our smartphone or laptop to an attacker, we stand naked: (Smartphone lost - Privacy gone). On a bigger scale, our life in general is deeply tied to digital and computerised control systems and the failure of those control systems would transport us back to the stone age (Our life in symbiosis).

So, try to follow a few simple best practices for digital security:

- **Choose a secure password.** Yes, password rules are annoying. But they are the best solution we have. And in the end, we are CERN: we have brains! (Brain Power vs. Password Managers);

- Keep your computer and your smartphone up to date. This is a no-brainer. Auto-updates come with any operating system nowadays. Just don’t turn them off. And use an anti-virus software for additional protection. They don’t provide 100% more security, but the aforementioned 30% airbag enhancement would help too, wouldn’t it? (WannaCry? The importance of being patched!);

- Encrypt your hard disks. Laptops get lost (or stolen). Encryption at least ensures that the data stored on them cannot be extracted (Trips and Travel: some Recommendations);

- **Stop – think – don’t click.** If you doubt the provenance of a web address, link or URL, just don’t click on them. If an unsolicited e-mail comes with an attachment, beware. Only go ahead if you trust the sender and were expecting the e-mail (One click and BOOM…);

And finally: you are not alone. Let us help you! If you have any questions or suggestions, check our website or contact us at Computer.Security@cern.ch.

Protect your life. In the physical world and in the digital. Have a safe and secure 2018!

And in the real world? (2017)

Why do computers remain unpatched? Why are passwords lost even today? Why do people still open malicious attachments? Why encryption not always is embraced? Is the major problem with understanding cybersecurity that it is not tangible? You can’t touch it. You can’t smell it. You can’t hear it. While computers and smartphones can be touched/smelled/heard, their apps and your data can’t. That makes cybersecurity abstract and easy to ignore, forgotten as soon as the mind focuses elsewhere.

In the real world, we have become accustomed to acting securely. We lock our houses and shut the windows when going on holiday. If the lock or window is broken, we get it fixed. If some stranger asks us for our credit card PIN, we tell them to get lost. The same applies if a stranger offers us, for example, a small bag of white powder and asks us to carry it across the border: we (should) decline and leave. And, for sure, we do not shout out intimate details about recent family problems, illnesses, affairs and so on.
On the other hand, we usually also store lots of (digital) valuables in our computers: bank information, private correspondence, family photos and videos. For some of us, our whole life is accessible through our computer (see our Bulletin article “Open door, open screen, open life...”), but we struggle to keep our computers up to date such that basic digital protections are in place. Some people reply if they receive an e-mail from a stranger, in an unusual context, possibly even in a foreign language, asking for their Apple ID, Office 365 account details or CERN password. Sure, they won’t have given away their PIN. But such e-mails are like any other unverified communications in the open with strangers. Only the context transforms the stranger and the conversation into something tangible and trustworthy (or not). The same holds for web links: every blue, underlined text pointing to another webpage is nothing other than a potential “small bag of white powder” offered to us by a stranger. Only the context makes it trustworthy (or malicious). Also, if you do not use encrypted channels (e.g. HTTPS, SSH or VPN), your digital communication with the world is public – whether you’re browsing the web, posting on Facebook or accessing your inbox. All unencrypted communication is shouted out aloud to those who want to listen…

So, please think a bit more about the real world. Think about the protection of your valuables at home. Think of your PIN. Of small bags offered in dark places. About the way you talk about family business. Then do the same in the virtual world: keep your computer, laptop and smartphone up to date, protect your password, STOP --- THINK --- DON'T CLICK, and make sure that you use “HTTPS” when browsing (check for the “https://” in your browser’s URL address bar --- the “s” is important).

About security incidents & issues (2017)

“Stefan, stop being paranoid. There is nothing severe happening with regards to CERN and cyber-security. Let us do our job and stop putting hurdles in the way…” I felt pity when I heard that message as daily business teaches me and my team differently…

The plain truth is: CERN is under attack. Permanently. Even right now. Web servers. Mail systems. Interactive gateways. Databases. File stores. Office PCs & laptops. Passwords & accounts. In parallel, CERN runs a vast and heterogeneous diversity of computing services. Several computer centres. Dozens of control systems. Hundreds of developers. Thousands of users. Millions of web pages. Tens of millions of lines of code. Many of those assets are attackable. Some of them are vulnerable, weakly protected or lack any inherent security posture. This is naturally human. And this is normal for any digital system. But it also makes CERN as a whole vulnerable to aforementioned attacks. And it is only a question of time that such an attack turns out to be successful. Actually, some attacks have been successful in the past. As in any
other enterprise running vast IT systems. And if we extrapolate from the past, there is no reason to believe that we are now safe for all future…

So maybe we just lack some kind of transparency. Transparency, in particular in security matters, is very important in order not to give the impression that we just create “FUD” (fear, uncertainty and doubt) to justify our roles, provide you’re with snake-oil as mitigative means, and monitor everything and all as we love playing policemen. On the contrary, transparency is important to create trust in our work, give you oversight of our doings, let you judge the reasonability of our decisions and provide means to question our strategies. For us, transparency towards our users, clients, and community is essential.

The regular CERN Bulletin articles are one example expressing what keeps us currently awake at night. But if you really want to learn what goes on on a daily basis, we also issue monthly computer security reports which list every computer security incident & issue, important vulnerabilities & weaknesses found as well as mishaps & problems encountered. These are fairly complete and fully reflect the current security problems related with CERN, CERN’s computing services, and CERN’s community. Recently, we delivered the 125th Bulletin article and soon we will produce our 100th Monthly Report! Therefore, if you want to learn more about computer security incidents & issues at CERN, feel free to follow our report and you will understand why I felt pity with the initial quote.

With that, we wish you a very secure 2017!

WhiteHats for CERN (2016)

CERN is under attack. Permanently. Even right now. In particular, the CERN web environment, with its thousands of websites and millions of webpages, is a popular target for evil-doers as well as for security researchers.

Usually, their attacks are unsuccessful and fade away over time. Sometimes, however, they are successful and manage to break into a CERN website or web server… It is imperative that we learn about our weaknesses before others do – and fix them!

Hackers with bad intentions are usually named “black hats” as they misuse their power to cause destruction or downtime via any weakness they can find. “Grey hats” are more moderate and might just have some fun with the weaknesses they find, for example by putting naked teddy bears or a personal message (such as “I hacked U”) on the compromised website. Last but not least, “white hats” report their findings directly to us and suggest that we take action (see here for a few examples) – and we quickly comply! We want more white hats, so in 2015 we teamed up with a number of universities worldwide and created the CERN WhiteHat Challenge. Following dedicated lectures on ethics and security assessment techniques, students of those
universities studying cyber security are entitled to perform penetration tests on CERN’s websites. It is a triple win as the students get to practise on live production systems, their professors don’t need to create an artificial testing environment, and CERN learns early on about vulnerabilities and weaknesses in its webpages. This has worked out well so far: students from the Universities of Rotterdam, Kent and FH St. Pölten have already reported their findings to us. Other universities are preparing for their students to take part this semester.

You might be wondering why we limit this programme to external people. We don’t! The CERN WhiteHat Challenge is also open to CERN employees and users who want to develop their penetration testing and vulnerability scanning skills. No in-depth technical expertise is needed – all you need is motivation. However, it is mandatory to take dedicated training courses covering ethics, web technologies, and an introduction to penetration testing and exploitation. This initial training cycle is complemented by in-depth courses on different subjects (e.g. cross-site scripting, command line injection) given at regular intervals.

If you are a member of CERN’s personnel and want to help us secure our web environment by becoming an official CERN white hat, please subscribe to this e-group and we will invite you to one of the next white hat courses in autumn 2016.

The dilemma of fractal defence (2015)

Aren’t mathematical fractals just beautiful? The Mandelbrot set and the Julia set, the Sierpinski gasket, the Menger sponge, the Koch curve (see here)... Based on very simple mathematical rules, they quickly develop into a mosaic of facets slightly different from each other. More and more features appear the closer you zoom into a fractal and expose similar but not identical features of the overall picture.

Computer security is like these fractals, only much less pretty: simple at first glance, but increasingly complex and complicated when you look more closely at the details. The deeper you dig, the more and more possibilities open up for malicious people as the attack surface grows, just like that of “Koch’s snowflakes”, where the border length grows exponentially.

Consequently, the defensive perimeter also increases when we follow the bits and bytes layer by layer from their processing in the CPU, trickling up the software stack through the operating system via (network) protocols and APIs to user-friendly applications, up to the human “wetware” with his/her initial “Eureka”-type moment.
While this abstraction helps us make our life easier and hides the complexities of computer hardware and hardware-close computing languages, each layer adds up to form our defensive perimeter and makes any defence more difficult. The “higher” we move, the more difficult defence becomes, and the easier it is for an attacker to break in.

At the innermost layer, the CPU and RAM level, complexity makes the detection of sophisticated attacks impossible. Researchers for Google have shown recently how to manipulate RAM information by repeatedly flipping bits. Dissecting the chips in order to identify hardware manipulations doesn’t help us. We just have to assume that nobody has tampered with our hardware… (or have they?).

Moving up, software is known to be vulnerable! At the application and operating system layers, defence is even more difficult, as the number of lines of code (LOC) is huge. An early study stated that in each 1000 LOC, there are on average 10 to 20 defects (Steve McConnell in "Code Complete", 1993). Thus, bugs are discovered regularly; vulnerabilities are reported repeatedly. “Open source” software might be better in that respect, but still, who can scrutinise millions of lines of code? How do we ensure that the compiler doesn’t screw up (as exposed by Ken Thompson in “Reflections on Trusting Trust”)?

Interfaces (APIs) and protocols, the next layer of defence, are no better. Their code base is already enormous and prevalent everywhere. The Internet Protocol (IP) is just one example. The initial implementations of IPv4 were flawed, but at least many of its weaknesses were known and subsequently corrected. Now upcoming is IPv6 with no additional defences, unknown vulnerabilities, and the unfortunate guarantee that new bugs are introduced as old code is ported to IPv6.

And finally, attackers targeting us humans or our devices easily get through. Our human “defence” can be broken, either through persuasion, deception or assault on
the victim. Being generally kind and sometimes naïve and convincing yourself to do what the attacker wants (“social engineering”) makes it easy to get past our defences. Attackers target the multiple devices we own nowadays, i.e. laptops, smartphones, tablets, by stealing or manipulating them...

Thus, welcome to the dilemma of fractal defence. We need you to help protect CERN! We should at least get the basic defences right:

- Protect your computers: any unprotected computer connected to the Internet is likely to be infected within minutes. Keep your system up-to-date, use anti-virus software (provided for free by CERN), do not install untrusted software and lock your screen with a password when you leave your office.
- Be careful with e-mail and the web as cybercriminals are trying to trick you. Stop - think - click: do not open unexpected or suspicious e-mails or attachments and do not install untrusted plug-ins.
- Protect your passwords: exposing them might lead to abuse of your computing account. Never share your passwords with anybody. A good password should be hard to guess and not found in any dictionary. Do not reuse old passwords and have different ones for different purposes or for different sites. Change them all regularly as they might have been exposed without you knowing it.
- Protect your data. Restrict access to your documents and folders, and follow the principle of least privilege: ensure that only people who need to access your files and data can do so.

Finally, make “computer security” a small part of your daily life - here at CERN as well as at home! Try to subconsciously think of doing IT the secure way whenever you touch a keyboard, mouse or touchscreen. Remember that in the open academic environment of CERN, “computer security” has been delegated to you. You are, in the first instance, responsible for the security of the laptops, smartphones and PCs that you use, your accounts and passwords, your files and documents, the programs and applications you have installed or, particularly, those you have written, and the computer services and systems you manage. The Computer Security team is ready to help you assume this responsibility. Alternatively, you can turn to the IT department, which provides a multitude of secured computing services.

Geneva, Suisse Romande and beyond (2014)

To ensure good computer security, it is essential for us to keep in close contact and collaboration with a multitude of official and unofficial, national and international bodies, agencies, associations and organisations in order to discuss best practices, to learn about the most recent (and, at times, still unpublished) vulnerabilities, and to handle jointly any security incident. A network of peers - in particular a network of trusted peers - can provide important intelligence about new vulnerabilities or ongoing attacks much
earlier than information published in the media. In this article, we would like to introduce a few of the official peers we usually deal with.\(^1\)

Directly relevant for CERN are SWITCH, our partner for networking in Switzerland, and our contacts within the WLCG, i.e. the European Grid Infrastructure (EGI), and the U.S. Open Science Grid (OSG). All three are essential partners when discussing security implementations and resolving security incidents. SWITCH, in particular, runs twice yearly a dedicated security workshop for Swiss universities and labs discussing a multitude of aspects surrounding “security”. SWITCH also provides monthly reports, which are available via our public website.

Outside this academic circle is the “Geneva Information Security Special Interest Group” ("GISSIG") which is attended by chief information security officers, computer security officers and IT security experts from different international organisations based in Geneva. Generally, the GISSIG coordinates security implementations across UN organisations, but also discusses different security solutions and threat scenarios relevant to all members. The current members are (in alphabetical order): CERN, the Global Fund, the ILO, the International Committee and the International Federation of the Red Cross and Red Crescent, the Office of the UN High Commissioner for Human Rights, the IOM, the ITU, the UN Offices at Geneva, the UNHCR, the UN International Computing Centre, WIPO, the WHO and the WTO.

In addition to these dedicated, closed forums, three distinct associations provide more open, public forums for organisations, companies, enterprises and individuals interested in computer security, privacy and data protection. All three schedule regular evening sessions where different security aspects are presented and discussed. The GRIFES sessions happen 2-3 times a year and are usually open to the general public once you’ve registered with them. The CLUSIS sessions are open to all its members and the CERN Computer Security Team holds an enterprise membership (for CLUSIS) so that all CERN people can freely attend. It provides a wide programme, with many presentations scheduled almost every other month. The annual membership fee for the Swiss Romande chapter of the International Information Systems Security Certification Consortium (\((ISC)2\)) is around 20 CHF and enables you to attend their meetings. All of these meetings are open to any interested parties and usually take place in the evenings - so feel free to attend! Please refer to their websites for their upcoming programmes. You might also find a few \textit{presentations and training sessions} given by the CERN Computer Security Team to these forums.

Finally, there is a rather loose collaboration between organisations, labs and institutes concerned about the cyber-security of control systems deployed for their experiments

\(^1\) Of course, in parallel to these “official” partners, every security expert has built up during his/her career a network of unofficial peers whom he/she trusts and by whom he/she is trusted. However, those peers usually prefer to remain unnamed…
and accelerators (“CS2HEP”). This community meets every other year just prior to the ICALEPCS conference.

The end of encryption (2014)

Sigh! Pandora’s box has been opened (once again). Recent documents leaked by whistle-blower Edward Snowden have revealed that the NSA project “Bullrun” is intruding deeply into the confidentiality of our documents and the privacy of our lives.

In their continuous effort to kill privacy on the Internet, the US National Security Agency (NSA) and the British Government Communications Headquarters (GCHQ) have made significant progress in breaking almost every basic encryption protocol or have developed the means to bypass them. “US and British intelligence agencies have successfully cracked much of the online encryption relied upon by hundreds of millions of people to protect the privacy of their personal data, online transactions and e-mails.” - The Guardian

So what’s left? With “Prism” and “Tempora”, our public communication on the Internet was already filtered and analysed (see our Bulletin article “Prison or “Prism”? Your data in custody”). “Bullrun” takes this to the next level and is said to be capable of analysing our private, encrypted communications. According to the New York Times, “the [NSA] has circumvented or cracked much of the encryption, or digital scrambling, that guards global commerce and banking systems, protects sensitive data like trade secrets and medical records, and automatically secures the e-mails, Web searches, Internet chats and phone calls of Americans and others around the world, the documents show”.

The details of “Bullrun” programme are nicely summarised in a blog post by Prof. Matthew Green, a cryptographer and research professor at Johns Hopkins University:

- Tampering with national standards (NIST is specifically mentioned) to promote weak or otherwise vulnerable cryptography.
- Influencing standards committees to weaken protocols.
- Working with hardware and software vendors to weaken encryption and random number generators.
- Attacking the encryption used by 'the next generation of 4G phones'.
- Obtaining clear text access to 'a major internet peer-to-peer voice and text communications system' (Skype?).
- Identifying and cracking vulnerable encryption keys.
- Establishing a Human Intelligence division to infiltrate the global telecommunications industry.
- And worst of all: somehow decrypting SSL connections.

And there is nothing we can do but watch how a new reality unfolds. Cryptography forms the basis for trust online. With these leaks, online trust has been destroyed.
Perhaps if only nations do it, it might be OK, as this is intended for our own protection (isn’t it?). However, although the details of “Bullrun” are still sparse, when the technology is leaked (and classified information always has a tendency to go “public” at some point) and attackers learn how the NSA broke or by-passed encryption, then the doors will be wide open for criminals. Online banking, online shopping and passwords would no longer be secure. Identity theft will become much easier. All our good advice about how to protect your data (“Jekyll or Hyde? Better browse securely”) will become obsolete.

Like everyone else, CERN is also affected. As we usually run standard IT technologies, there is little we can do… but a good start would be to phase out weak encryption protocols like DES, begin using 3072-bit (4096-bit!) RSA keys for public key encryption and eventually kill SSH version 1. Also, we should refrain from SSL and move our web pages, web sites and web services to TLS1.2 as there are already known weaknesses in them (see BEAST attack; or CRIME).

In addition, we can finally deploy multi-factor authentication to better protect sensitive computer services like accelerator controls, finance applications or important signature rights on EDH. Technology is ready to be used that requires you to log-in with not only your standard NICE password but also a second “one-time-password”. This could be sent via SMS to your mobile phone – created on a USB-dongle (“Yubikey”) or by the “GoogleAuthenticator” app – or just using a certificate installed on your CERN Access Card.

Of course, you can do more: if you want to take action, check out the Guardian’s 5 tips to stay secure. Meanwhile, we should consider what data is really worth protecting and what can be made public. If less is marked “confidential”, then we have less to worry about. Is “raw” data really worth protecting? Are meeting minutes really confidential? Can’t your photo on your CERN access card just be published online? The new CERN Data Protection Policy (OC11) should be able to give guidelines on that.

A short tale of the black sheep of –ITY (2013)

Once upon a time, computer engineers of the ancient world used the abbreviation of “-ITY” ([eye-tee]) as a shorthand for “Information TechnologY”. It was an appropriate abbreviation as it reminded everyone of the core purposes and aspects of information technology, which made not only the computer engineers, but also their clients, happy.

Whenever the engineers were programming a software application or setting up a computing service to cover the needs of their clients, they stuck to the four paradigms of -ITY:

- “Functional-ITY”, i.e. ensuring that a service or application has a purpose and a justification of being;
- “Avalabil-ITY”, i.e. ensuring that this service or application is functional whenever a client wants to use it;
- “Usabil-ITY”, i.e. ensuring that this client does not get fed up by a badly designed user interface or disappointed by the service’s or application’s workings, and, thus, avoiding that either is abandoned;
- “Maintainabil-ITY”, i.e. ensuring that the developers do not get fed up by the application’s architecture or service configuration and, thus, avoiding that either is orphaned.

It was to the benefit of everyone. Following those four paradigms guaranteed properly designed applications and services. A win-win situation and a paradise for clients.

But with the dawn of the Internet, the nice-and-cosy world of -ITY was threatened. Evil coders and attackers entered the scene and started to harass and violate the four paradigms. With evil coders introducing vulnerabilities and bugs in applications, suboptimal “Functional-ITY” was exploited by attackers. Denial-of-service attacks diminished the “Avalabil-ITY” of services. “Usabil-ITY” became a double-edged sword of friendly use-cases as well as misguided abuse-cases. And “Maintainabil-ITY” was under pressure as more and more services and applications went out of operation in order to recover from successful attacks.

It did not take long for computer engineers to establish a fifth paradigm meant to protect the other from the wrong-doers of the Internet: “Secur-ITY”. But “Secur-ITY” was clumsy and has never been able to fit in with its brothers. When “Functional-ITY” was key, “Secur-ITY” made it complicated. When “Avalabil-ITY” was asked for, “Secur-ITY” shouted “reboot!”. And when “Usabil-ITY” “had the priority, “Secur-ITY” put up hurdles and barriers. Only “Maintainabil-ITY” was happy, as it would benefit whenever “Secur-ITY” introduced a break. “Secur-ITY” tried hard to overcome its weaknesses and disadvantages, but to no avail... Instead it was perceived as the one “-ITY” to rule them all... and in the darkness bind them.

“Secur-ITY” became the Black Sheep of the family. Computer engineers despised it and ignored it, as “Secur-ITY” introduced more problems than it did good. It was of no help. Years passed by in darkness with all the paradigms struggling for survival. Today, the question is: can applications and services be sustained without protection and defence? Or will evil prevail in the end and kill the paradigms one after the other? Shouldn’t computer engineers stop and reflect on how “Secur-ITY” can become inherent partner of the other paradigms?

Will there be a happy ending? Will evil will seal the doom of “-ITY”? Will “Secur-ITY” ever be welcomed back into the flock? Will “Functional-ITY”, “Avalabil-ITY”, “Usabil-ITY”, “Maintainabil-ITY” and “Secur-ITY” live happily ever after? It is up to you.

Recall from last year’s articles (“Security” is YOU! and Why “Security” is not ME...), that “Secur-ITY” needs your help. At CERN or at home, “Computer Security” is not complete without YOU!
The Open Days are here!! From tomorrow onwards, we will be welcoming thousands of people to CERN. No barriers, no boundaries!

For decades, we have welcomed researchers and visitors from around the world to work at CERN, discuss physics research and attend our training sessions, lectures and conferences. This is how fundamental research should be conducted!!! But have you ever noticed how you are welcome at CERN in the digital world, too? Once you are affiliated and are registered with CERN, you receive a CERN computing account and e-mail address. You can register your laptops, PCs and smartphones to use our (wireless) network, you can easily create your personal webpage, and profit from a vast disk space for file storage (AFS and DFS). CERN is indeed an Open Campus and not only during the Open Days. CERN is an Open Campus in the digital world.

This digital Open Campus culture is exactly the reason why “computer security” has been delegated to you. With academic freedom comes responsibility for everything you do: you are responsible for the computer security of the laptops, smart phones and PCs you use, the accounts and passwords you own, the files and documents you store, the programmes and applications you have installed or written, and the computer services and systems you manage. Because we do not control the operating systems you run, we are not responsible for the programmes and applications you install and the webpages you browse (“Why “Security” is not ME…”).

Alternatively, we could change that: we could block network access for every incompliant PC and laptop; we could close the CERN outer perimeter firewall completely and deny access to news pages, Facebook, YouTube and others; we could impose on you the Windows 7 and SLC6 operating systems; and we could allow only certain programming languages to be used. But dictating and restricting you would contradict the freedom and liberty of CERN’s academic work. In fact, it would interfere with CERN’s academic freedom, and we would rather get the balance right!

Therefore, while breathing the Open Campus air at CERN, that balance requires you to take your share: ““Security” is YOU!” We are, of course, ready to help you take on this responsibility. If you feel uncomfortable with it, you can delegate that responsibility to the IT Department which provides a multitude of secured computing services such as up-to-date operating systems, anti-virus software, protected file storage space, secured web servers and databases. Contact them and avoid reinventing the wheel (see our Bulletin article on “Stop fighting alone, let synergy rule!”). Rather, focus on your core work and don’t fiddle with issues where you might not be an expert ☺. Avoid the blunder of others who presented us with awesome web applications, fully functional with lots of bells and whistles, but which, after scrutiny, turned out to be flawed and posed a security risk to the Organization, and was eventually scrapped by a dismayed developer…
Security vs. nations: A lost battle? (2013)


“Know the enemy” is one of the basic recommendations of the ancient Chinese military strategist Sun Tzu (544–496 BC). In the cyber-world, the usual suspects are not only script kiddies, criminals and hacktivists, but also nation states.

Companies worldwide have prepared their defences to fight off the first three. Likewise, CERN, despite its wish for academic freedom, is constantly considering how best to prevent successful attacks. But when nation states are the antagonists, defence is impossible (unless you have plenty of money).

Today, the most popular computing services in the western hemisphere are run from the US. We already know that the US and the UK are tapping into Facebook, Google, Yahoo and others (see our Bulletin article on “Prison or “Prism”? Your data in custody”). But what about one level down?

Nowadays, IT hardware (routers, laptops, smartphones, etc.) is built in China. How can we be sure that these hardware devices do not contain chips manipulating the device (spying on activities, stopping functions, destroying data) using an external trigger? Meanwhile, a lot of software is written in India. How can we be sure that this software does not contain bugs inserted during the implementation phase, allowing adversaries to (you guessed it) spy on activities, stop functions and destroy data?

Modern hardware and software are now so complex that uncovering malicious functions is difficult (impossible!) for most organisations. Chips are usually sealed to protect intellectual property (according to chip manufacturers). Software contains millions of lines of code. Even if this code is “open source” it can be cumbersome to sift through. And can you be sure that your compiler doesn’t add functionality? Finally, understanding the resulting “assembly” code is difficult in itself. And even if you discover a vulnerability, it will be labelled a bug - accidentally introduced by careless or untrained computer programmers, and not deliberately inserted by a nation. It is not without reason that many nations have their own “bounty” programmes, paying for newly discovered software bugs and vulnerabilities, and trying (and succeeding!) to break common encryption protocols. Russia is running one of the largest dark markets for vulnerabilities and stolen credentials.

Of course, there are many other nations preparing for our cyber-future. Still, the world is at a new watershed. With the “Internet-of-Things”, a term coined in 1999 by visionist Kevin Ashton, all our devices will be interconnected in the near future. In fact, we already live in symbiosis with the Internet-of-Things. We are sitting like the proverbial frogs in the slowly boiling water, while nations prepare the Internet-of-Things as a new battlefield to be infiltrated, undercut and controlled. The “Great Firewall of China” as well as the US’s “Prism” and the UK’s “Tempora” programmes that spy on innocent citizens are the first cuts to the free Internet. The “Stuxnet” cyber-attack against Iran,
generally deemed to be one of the first ever conducted, exploited four unknown (until then) vulnerabilities (“zero-day exploits”) of the Windows XP operating system, presumably as part of the US and Israeli bounty programmes. In the civil war in Syria, the “Syrian Electronic Army” brought down the New York Times homepage and that of “Marines.com” to show off its power. They also threatened to strike back more severely once the US drops bombs on Syria.

Without being paranoid, is the battle already lost? Has the age of the free Internet already passed? Is our privacy gone? How much security are we willing to accept before our world turns into George Orwell’s 1984 or Aldous Huxley’s Brave New World? In the warmth of the upcoming holiday season, maybe this is the right time to reflect and discuss what we can all do to keep the Internet a free and public place, and not a battlefield for paranoid nations.

Security Bingo (2011)

Want to check your security awareness and win one of three marvellous books on computer security? Just print out this page, mark which of the 25 good practices below you already follow, and send the sheet back to us by 31 October 2011 at either Computer.Security@cern.ch or P.O. Box G19710.

Winners must show that they fulfil at least five good practices in a continuous vertical, horizontal or diagonal row. For details on CERN Computer Security, please consult http://cern.ch/security.

I personally…

<table>
<thead>
<tr>
<th>…am concerned about computer security.</th>
<th>…run my computer with an anti-virus software and up-to-date signature files.</th>
<th>…lock my computer screen whenever I leave my office.</th>
<th>…have chosen a reasonably complex password.</th>
<th>…have restricted access to all my files and data.</th>
</tr>
</thead>
<tbody>
<tr>
<td>…am aware of the security risks and threats to CERN’s</td>
<td>…protect confidential documents and do not make them public.</td>
<td>…am vigilant before opening mail attachments.</td>
<td>…understand the risks of clicking on strange links.</td>
<td>…regularly patch my computer.</td>
</tr>
</tbody>
</table>

---

1 In the event of more than three credibly correct replies, we will draw from the pool of replies.
<table>
<thead>
<tr>
<th>computing facilities.</th>
<th>...will never disclose my password to someone else.</th>
<th>...do not run prohibited applications.</th>
<th>...have brought my mouse to the <a href="http://cdsweb.cern.ch/journal/CERNBulletin/2011/43/News%20Articles/1391753?ln=en">CERN Computer Animal Shelter</a>.</th>
<th>...respect copyrights and do not share music or films.</th>
<th>...immediately delete “Phishing” emails.</th>
</tr>
</thead>
<tbody>
<tr>
<td>...do not run file sharing applications.</td>
<td>...never install plug-ins.</td>
<td>...never type my CERN password at Internet cafés.</td>
<td>...know how to contact <a href="mailto:Computer.Security@cern.ch">Computer.Security@cern.ch</a>.</td>
<td>...have never installed rogue wireless access points.</td>
<td></td>
</tr>
<tr>
<td>...have followed one or more security training sessions.</td>
<td>...do not store my music or films in a public place.</td>
<td>...have read, understood, and agree to the CERN Computing Rules.</td>
<td>...have distinct passwords for CERN, Facebook, Amazon, and others.</td>
<td>...protect my laptop against theft.</td>
<td></td>
</tr>
</tbody>
</table>

### Security Bingo for the paranoid (2011)


We have received complaints that the previous SECURITY BINGO was too easy… So, are you extremely cautious of computer security? Show us and win one of three marvellous books on computer security! Just print out this page, mark which of the 25 good practices below you already follow, and send the sheet back to us at [Computer.Security@cern.ch](mailto:Computer.Security@cern.ch) or P.O. Box G19710, by October 31st 2011.

Winners¹ must show us that they follow at least five good practices in continuous horizontal row, vertical column or diagonal. For details on CERN Computer Security, please consult [http://cern.ch/security](http://cern.ch/security).

---

¹ In the event of more than three credibly correct replies, we will draw from the pool of replies.
I personally...

<table>
<thead>
<tr>
<th>...encrypt all files on my computer.</th>
<th>...have enabled Firefox’ NoScript plug-in.</th>
<th>...will always call you back to verify your identity.</th>
<th>...still employ a mobile phone without mail and Internet capabilities.</th>
<th>...use multifactor authentication for logging into CERN.</th>
</tr>
</thead>
<tbody>
<tr>
<td>...have a polarisation filter attached to my laptop screen.</td>
<td>...never use any wireless connections (Wifi or GSM).</td>
<td>...check all activity on my computer once a day.</td>
<td>...have deleted my Facebook and Twitter profiles long ago.</td>
<td>...never access my bank through their web-site.</td>
</tr>
<tr>
<td>...shred all unused CDs/DVDs/USB sticks with my data on.</td>
<td>...run static code analysers and check compiler outputs.</td>
<td>...have put Epoxy glue in the USB ports of my computer.</td>
<td>...only communicate through secure protocols (SSH, HTTPS,).</td>
<td>...only surf with the “Lynx” web browser.</td>
</tr>
<tr>
<td>...do not own a Visa/Mastercard.</td>
<td>...watch my back when using my computer in a public place.</td>
<td>...reinstall my computer every 6 months.</td>
<td>...keep a 16+ character-long passphrase as my CERN password.</td>
<td>...reset my password every month.</td>
</tr>
<tr>
<td>...accept only encrypted and signed mails.</td>
<td>...never print via the network.</td>
<td>...never need administrator or root privileges for normal activity on my computer.</td>
<td>...get all software written by me reviewed by colleagues.</td>
<td>...have given up on computers long time ago.</td>
</tr>
</tbody>
</table>
Security Bingo for administrators (2011)


Have you ever thought about the security of your service(s) or system(s)? Show us and win one of three marvellous books on computer security! Just print out this page, mark which of the 25 good practices below you already follow, and send the sheet back to us at Computer.Security@cern.ch or P.O. Box G19710, by November 14th 2011.

Winners must show us that they follow at least five good practices in a continuous horizontal row, vertical column or diagonal. For details on CERN Computer Security, please consult http://cern.ch/security.

My service or system…

<table>
<thead>
<tr>
<th>…is following a software development life-cycle.</th>
<th>…is patched in an automatic and timely fashion.</th>
<th>…runs a tightened local ingress/egress firewall.</th>
<th>…uses CERN Single-Sign-On (SSO).</th>
<th>…has physical access protections in place.</th>
</tr>
</thead>
<tbody>
<tr>
<td>…runs all processes / services / applications with least privileges.</td>
<td>…has a defined and documented disaster recovery plan.</td>
<td>…is logging remotely all accesses and critical actions.</td>
<td>…is maintained by administrators who followed dedicated security training sessions.</td>
<td>…has no openings in CERN’s outer perimeter firewall.</td>
</tr>
<tr>
<td>…restricts access to all privileged accounts to a very few people.</td>
<td>…does not use shared folders.</td>
<td>…adheres to the CERN “Security Baselines for Servers”.</td>
<td>…has all USB ports disabled.</td>
<td>…has a password protected BIOS, IPMI interface and boot loader.</td>
</tr>
<tr>
<td>…is managed by a configuration management system.</td>
<td>…has had all its code &amp; configuration reviewed.</td>
<td>…restricts user access.</td>
<td>…uses very few local accounts.</td>
<td>…has all unnecessary processes and services disabled.</td>
</tr>
</tbody>
</table>
The start-up of LHC is foreseen to take place in the autumn and we will be in the public spotlight again. This increases the necessity to be vigilant with respect to computer security and the defacement of an experiment’s Web page in September last year shows that we should be particularly attentive. Attackers are permanently probing CERN and so we must all do the maximum to reduce future risks. The start-up of LHC is foreseen to take place in the autumn and we will be in the public spotlight again. This increases the necessity to be vigilant with respect to computer security and the defacement of an experiment’s Web page in September last year shows that we should be particularly attentive. Attackers are permanently probing CERN and so we must all do the maximum to reduce future risks.

Security is a hierarchical responsibility and requires to balance the allocation of resources between making systems work and making them secure. Thus all of us, whether users, developers, system experts, administrators, or managers are responsible for securing our computing assets. These include computers, software applications, documents, accounts and passwords. There is no "silver bullet" for securing systems, which can only be achieved by a painstaking search for all possible vulnerabilities followed by their mitigation. Additional advice on particular topics can be obtained from the relevant IT groups or members of the security team, but we include here a basic list of items to be considered by all CERN computer users:

- Review access rights to your computers, documents (InDiCo, EDMS, TWiki, etc.), as well as files and directories on AFS, DFS and local disks. Don’t give write access if read access is sufficient and limit access only to those who need it.
- Protect web sites. Very few should be publicly accessible and those which are should not reveal details of system architecture and design, computer configurations or source code.
- Ensure that accounts have been closed for individuals who have left.
- Reduce the number of service accounts where possible.
- Harden computers by removing unnecessary applications, disable unneeded services such as for Web, FTP, etc., use automated update and patching.
services as well as up-to-date antivirus-software for PCs (but also for embedded devices like oscilloscopes), upgrade SLC3 to SLC5, use local firewalls to block both incoming and outgoing traffic which is not expected.

- Protect private SSH keys.
- For experiment networks, review central firewall openings and review whether devices need to be trusted or exposed.

Further information about how to improve computer security may be found on the Web sites [http://cern.ch/security/](http://cern.ch/security/) as well as [www.ISSEG.eu](http://www.ISSEG.eu) which include material on risk analysis, training and recommendations for general users, developers and system administrators. As well as the many security awareness presentations which are given, training courses are also available on writing secure code and secure Web applications (see [http://cern.ch/security/training](http://cern.ch/security/training)).