

European Organization for Particle Physics
Exploring the frontiers of knowledge



Finding the Balance between Academic Freedom, Operations & Security

Dr. Stefan Lüders
CERN Computer Security Officer

CERN/CNAF Seminar, 2020/5/27

“Security”: The state of being free from danger or threat.

Security is like contraception...

- Will never be 100% effective.
- Does not contribute to performance.
- Never sure you actually need it all the time.
- Don't know whether it has worked until after (even long after..) the event
- The measure of effectiveness is in terms of failures.
- A combination of methods gives the greatest reduction in risk.
- Should never rely on someone else's precautions - *take care yourself.*

<https://www.lexico.com/en/definition/security>



EUROPEAN COMMISSION
DIRECTORATE-GENERAL
INFORMATICS

FIRST Conference -Sevilla – June 2007

Slide: 65



Scope:

CERN – Know your (security) footprint

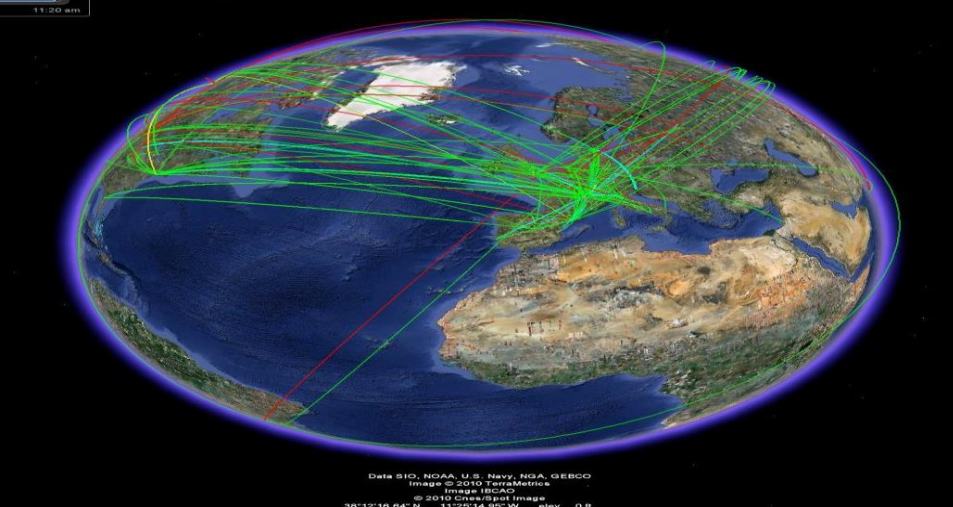
Risks:

Adversaries & Limitations

Controls:

Protection, Detection & Response





Date: 8/10, NOAA, U.S. Navy, NGA, GEBCO
Image © 2010 TerraMetrics
Image: Bing
© 2010 Chesapeake
38°12'16.64" N 112°25'14.95" W elev. 0 ft



Finding the Balance for Security
Dr. Stefan.Lueders@cern.ch
CNAF/CERN Seminar, May 27th 2020

Sectors of “Security” Operation



**One flat office, wireless & data centre network
plus an external visitor network**

**5 Class-B IPv4 & 4 IPv6 networks
(+many non-routable networks)**

**200Gb/s to Internet, >20 Gb/s flat throughput,
>5000 switches, 100s routers,
6k firewall openings**

**~40k heterogeneous devices:
any hardware, any operating system, any (legal) application**

~37k user account & mailboxes, 2M emails/d, 70% SPAM

**6 data centres serving
users, infrastructure, compute &
storage, accelerators & experiments**

**17k servers, 300k cores, 35k virtual machines,
625PB storage (133k hard disks + 30k tapes)**



**Provisioning of operating systems, anti-virus software,
printing, office/engineering/HR/finance apps,
databases, versioning/build systems,
virtualisation & container services,
collaboration tools, video/audio conferencing, ...**

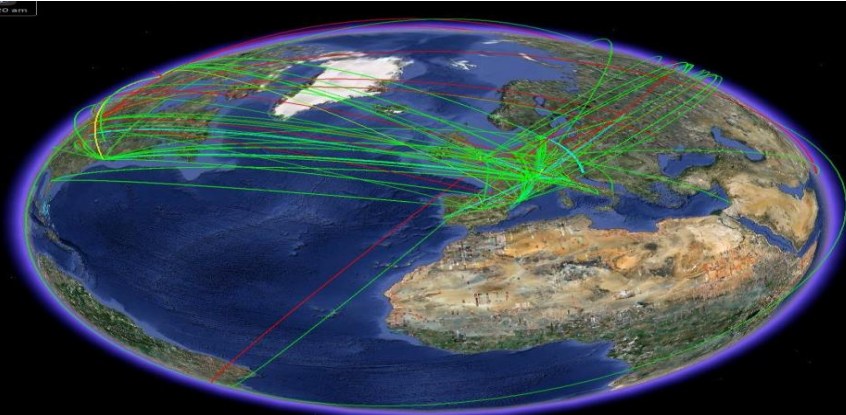
**50 central + 500 non-central web servers,
>10k websites, >1.5M webpages, webcast**



Worldwide LHC Computing Grid (WLCG):

- Tier-0 (CERN: ~7k nodes)
- 13 Tier-1s, >150 Tier-2s and 3s

Permanently running >300k analysis jobs
on >650k CPU cores
at >20Gb/s through-put



Data SIO, NOAA, U.S. Navy, NGA, GEBCO
Image © 2010 TerraMetrics
Image Source
© 2010 CNN/Sat Image
38°12'18.64"N 11°55'14.95"W Elev. 0 m

Adeli	Media-Lite SA
BIT (Swiss Confederation)	Opentransit (France Telecom Network Services Switzerland)
CERN	Orange Business Services - GIBN
COLT	RIPE-RIS
CTI	Sunrise (TDC Switzerland AG)
euNetworks (was Fibrelac)	Swisscom / IP-Plus
Init7	T-Systems Schweiz AG (Deutsche Telekom)
K-Net / K-Sys	UPC Cablecom
K-root (RIPE)	VTX Services SA
KPN Eurorings BV	

CERN Internet Exchange Point (CIXP):
Peering of 20 ISPs & TelCos



Experiments:

ALICE, ATLAS, CMS, LHCb, LHCf and TOTEM

AD, AMS, Cast, Cloud, Collaps, Compass, Dirac, Gamma Irradiation Facility, ISOLDE/ISOLTRAP, MICE R&D, Miniball, Mistral, NA48/3, NA49, NA60, NA62, nTOF, Witch, ...

GCS, MCS, MSS, and Cryogenics System

Accelerators:

AB/OP, AD, CNGS, CCC, CLIC, ELENA, ISOLDE, ISOLDE offline, LEIR, LHC, Linac 2/3/4, PS, PS Booster, REX, SM18, and SPS

Accelerator

Infrastructure:

ADT, ACS, BQE, BPAWT, BDI, BIC, BLM, BOF, BPM, BOB, BSRT, BTU, BRA, CWAT, Cryo (Frigo, SM18 & Tunnel), BCTDC, BCTF, FGC, LEIR Low Level RF, LHC Beam Control System, LBDS, HC, LHC Logging Service, LTI, MKQA, APWL, BPL, OASIS, PIC, QDS/QPS, BQS, SPS BT, BQK, Vacuum System, WIC, and BWS

Safety:

ACIS, AC PS1, AC PS2, AC SPS1, AC SPS2, Alarm Repeater, ARCON, ADS, CCTV, CSA, SGGAZ, SFDIN, CSAM, CESAR, DSS, LACS, LASS, LASER, Radmon, RAMSES, MSAT, Radio Protection Service, Sniffer System, SUSI, TIM

Infrastructure:

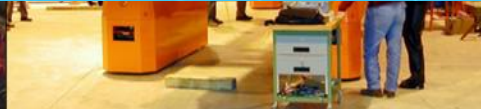
CV, ENS, FM, DBR, Gamma Spectroscopy, TS/CSE, and YAMS





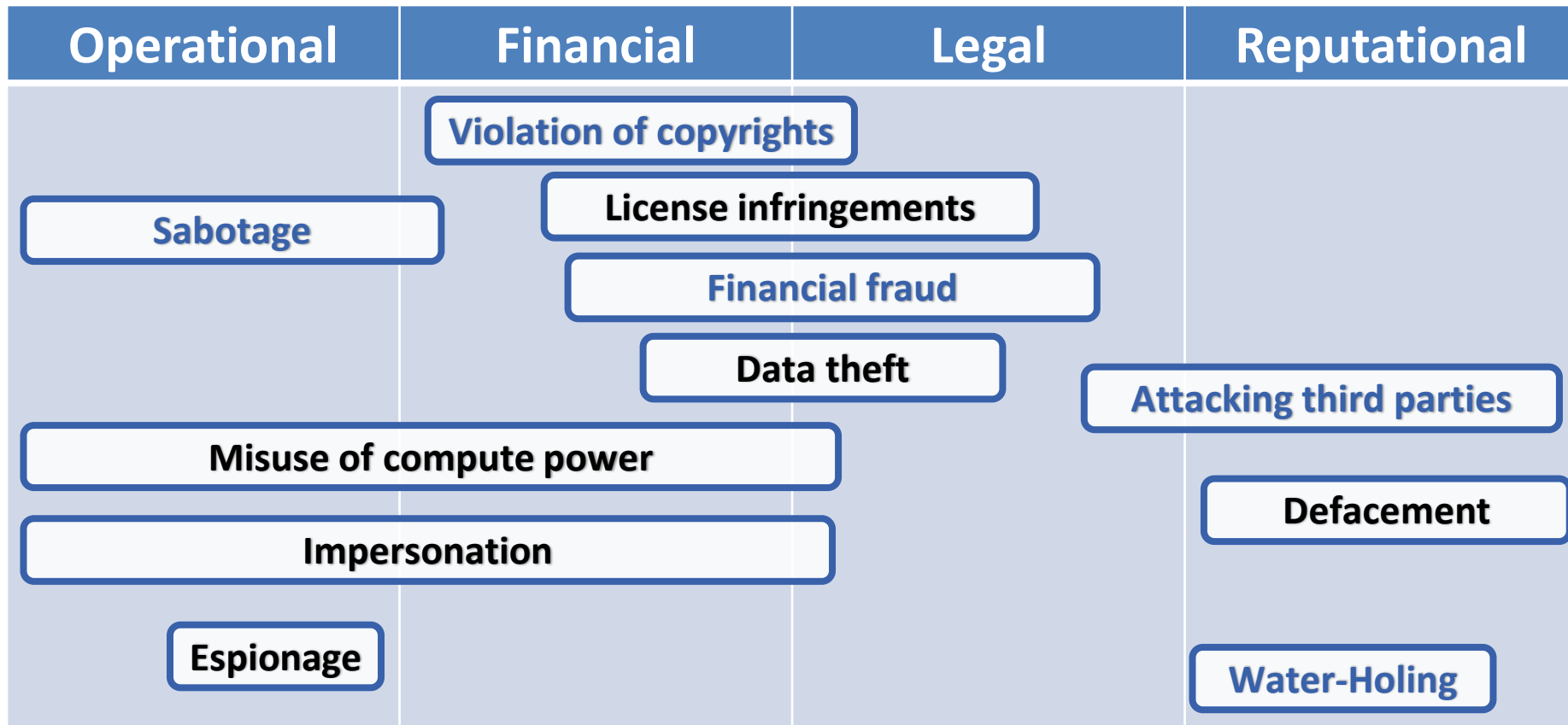
Finding the Balance for Security
Dr. Stefan.Lueders@cern.ch
CNAF/CERN Seminar, May 27th 2020

Examples of Control Systems / IoT



Finding the Balance for Security
 Dr. Stefan.Lueders@cern.ch
 CNAF/CERN Seminar, May 27th 2020

And the Human Factor...



Scope:

CERN – Know your (security) footprint

Risks:

Adversaries & Limitations



**Like any other company,
organization or university,
CERN is under permanent
attack.**



Search Twitter Have an account? Log in

C3 ~ RET @c3retc3 Follow

#CERN discloses passwords, source code and tickets to Web spiders

6:03 a.m. · 29 Sep 2015

C3 ~ RET @c3retc3 · 2h
@c3retc3 There are 150 Oracle DB hosts at least!

Kate Kahle @katekahle · 2h
@c3retc3 Thanks for the heads-up! What about sharing details with us via Computer.Security[at]cern.ch?

C3 ~ RET @c3retc3 · 51m
@katekahle Surely I will write you. You have really surprised me with the reaction - glad to see this approach to security of the org.

© 2015 Twitter About Help Terms Privacy Cookies Ads info



@reversemode

Rubén Santamarta

Writing a post involving CERN, LHC, SCADA, passwords... one of the most curious cases I've found.

9 Aug via [TweetDeck](#)



Dan Tentler

@Viss

Follow

someone asked earlier if I was gonna find CERN - here's one (I got their CERT guys email. I'll notify) pic.twitter.com/zu180KzyBo

Reply Retweet Favourite More

```
Welcome to CERN Virtual Machine, version 2.6.0
sun2209200-01 login: --- a new cntuser directory has been created in your HOME directory
--- LHCb Login 07r10p4 ---
Building with gcc46 on s1c5 x86_64 system (x86_64-s1c5-gcc46-opt)
--- User release_area is set to /opt/dirac/cntuser
--- LHCbPROJECTPATH is set to:
/cmfss/lhcb.cern.ch/11b/lhcb
/cmfss/lhcb.cern.ch/11b/lcg/releases
/cmfss/lhcb.cern.ch/11b/lcg/app/releases
/cmfss/lhcb.cern.ch/11b/lcg/external
```

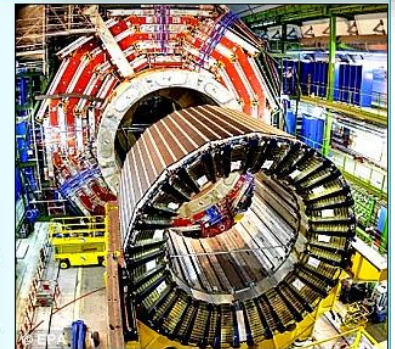


If you look after the Large Hadron Collider you should read this...

THREE CLICKS AND WE WERE IN CERN'S PRIVATE WEBSITE

The Shodan search engine is so powerful, it could even put the world's most expensive science experiment at risk.

By searching the site's 'most popular' searches, reporters at The Mail on Sunday were able to find out the internet location of the home of the Large Hadron Collider, the world's largest particle accelerator.



Hacking risk: CERN's Large Hadron Collider in Switzerland

Anonymous Coward

User ID: 69274093

United States

05/25/2015 11:18 PM

[Report Abusive Post](#)

[Report Copyright Violation](#)

Re: Do you think it's possible for the CERN LHC to be hacked?

Scary thought. Hollywood hit..

Really cern has been hacked, it is ran by mad scientists, hell bent on crazy.

These are the type of people that jump from rocks with wing suits with life mentality.

They want crazy. Cern is a weapon, the biggest and most psychotic ever created.



By the
the log

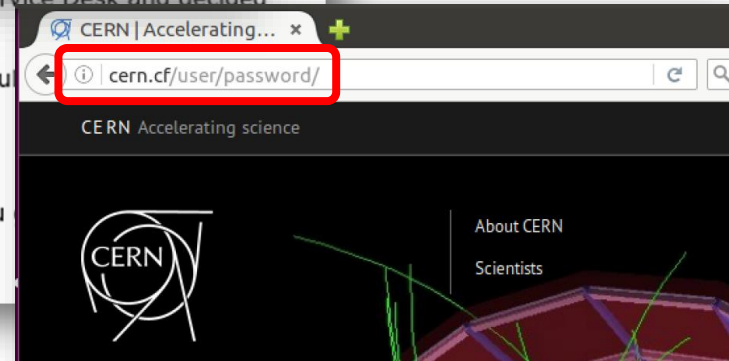
three passwords. So I thought it was a joke from someone that noticed I am not really CERN Service Desk and decided to troll me a little. I totally forgot about other login methods.

So I made NICE login of my own with Windows/Kerberos authentication included. This is the result

<http://its.cern.cf/jira/browse/FWINS-1224>

Thanks for giving me this chance without legal trouble. I had fun and learned a lot thanks to you

Looking forward to hearing from you. It would be really a privilege for me to work at CERN.



```
<sc0rp> nice
<MLT> using the exploit on CERN would be win, ha
```



Lab Mouse Security @InfoSecMouse · Jul 7

Hacking CERN - Exploiting python Particles and Profit

From: [REDACTED]
To: Press Office
Cc:
Subject: URGENT

Sent: Fri 2012/03/23 15:02

Hello,
I'm contacting you because I've an important thing to let you know.
I've found some vulnerabilities on cern.ch system and I've hacked it.

I didn't get access of databases but hacked the website with a XSS attack. Would like know if you're the right person to talk about this and try make a deal to give you all details, all strings I used, the links and all stuff that I did.

If you aren't the right person to talk just give me a email to contact to let him know the details please.

I'm waiting your reply ASAP,

black01white Greek Hacking Documentary trailer ripped

5,788 likes

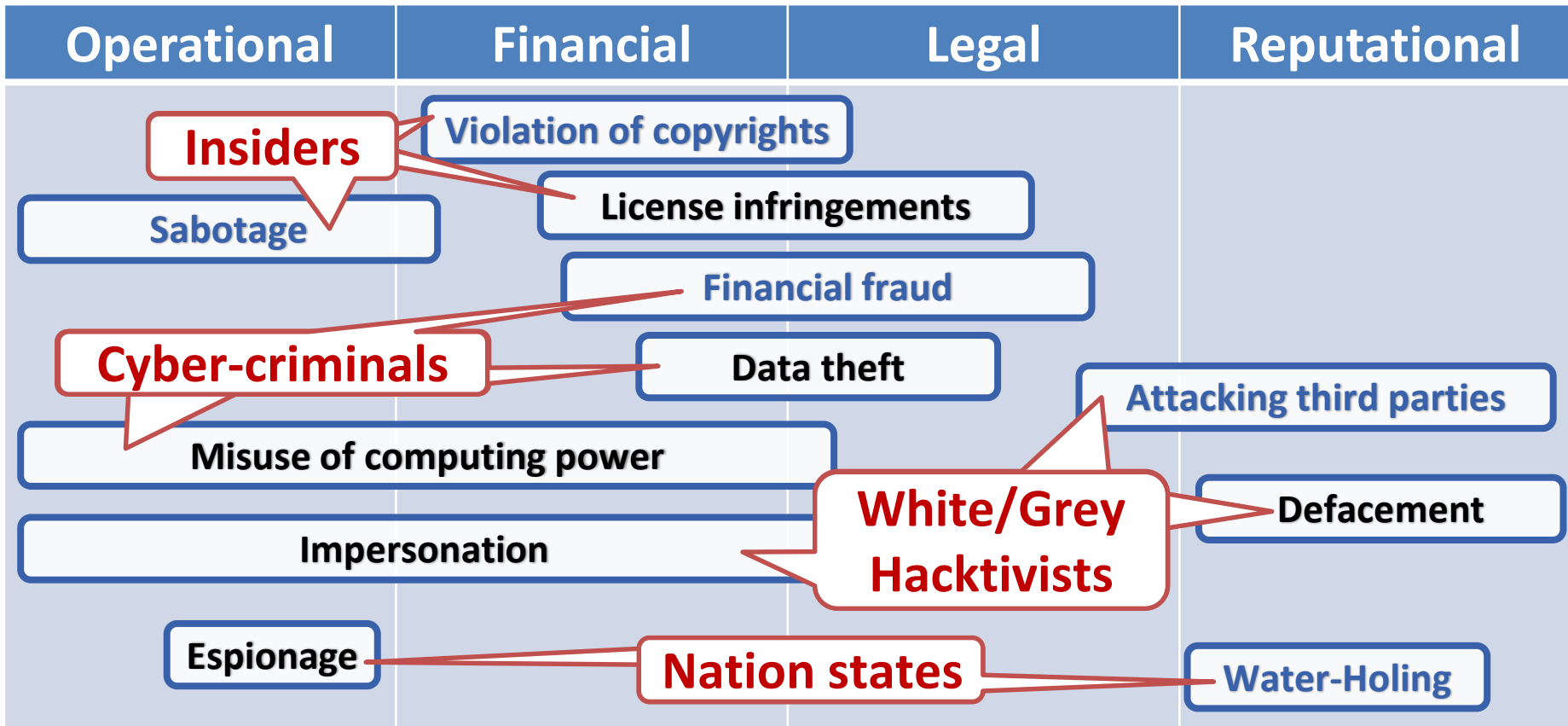
PART 1: HACKING THE LARGE HADRON COLLIDER (XSS VULNERABILITY)

Published by camilla c. | Filed under [General](#), [News](#), [Spreadin'](#)

PART 2: HACKING THE LARGE HADRON COLLIDER (AUTHORIZATION BYPASS)

Published by camilla c. | Filed under [General](#), [News](#)





Scope:

CERN – Know your (security) footprint

Risks:

Adversaries & Limitations

Controls:

Protection, Detection & Response



Mandate:

**Protect the operations and reputation
of CERN against cyber-threats**



Find an appropriate balance between academic freedom, operations & security.

“Academic Freedom” implies “Responsibility”!

CERN Cyber-Security is everyone’s responsibility and not that of the Computer Security Officer alone!

Responsibility can be (partially) delegated to CERN’s IT department.

The Computer Security Team acts as facilitator & enabler.

**We help people to do their job securely. We secure CERN.
We take over responsibility when handling security incidents.**



“Security” is the responsibility of every individual at CERN

Everyone is bound to CERN’s Staff Rules & Regulations (SRR), CERN’s Code of Conduct (CoC) and administrative & operational circulars (e.g. “OC5”)

In particular, ideally, CERN IT experts directly manage the security of their services (e.g. email, DBs, O/S, storage, web)

"These functions, allowing access to personal data or other confidential and/or sensitive information, imply strict conformance to the rules laid down in OC11 and OC5, in particular those governing confidentiality.."

IT professionals at CERN usually also come with some “security” expertise. Depending on the department/group this is tested during their job interview.

11. Which of the following values/fields coming from HTTP client can be easily forged by malicious attacker on the client side, and set to any arbitrary value:
- GET arguments
 - GET and POST arguments, cookies, hidden form fields
 - GET and POST arguments, cookies, hidden form fields, user-agent, referer**
 - GET and POST arguments, cookies, hidden form fields, user-agent, referer, remote (client) IP address
12. Which of the following HTTPS protocol does *not* offer:
- Client authentication
 - Protection against eavesdropping
 - Prevention against man in the middle attack
 - Prevention against cross site request forgery attack**
13. Security-wise, which of the following PHP settings would you consider the best:
- register globals" disabled, "display errors" disabled**
 - "register globals" disabled, "display errors" enabled
 - "register globals" enabled, "display errors" disabled
 - "register globals" enabled, "display errors" enabled
14. Which of the following file permissions can be represented as 0536?
- r-x-wxrw-**
 - rw-r-xr--
 - wxr--rw-
 - r-xrw--wx



HEP community, in particular with the WLCG/EGI, and multiple ties with academia in general (e.g. REN-ISAC, SWITCH WG, IHEP/CAS)

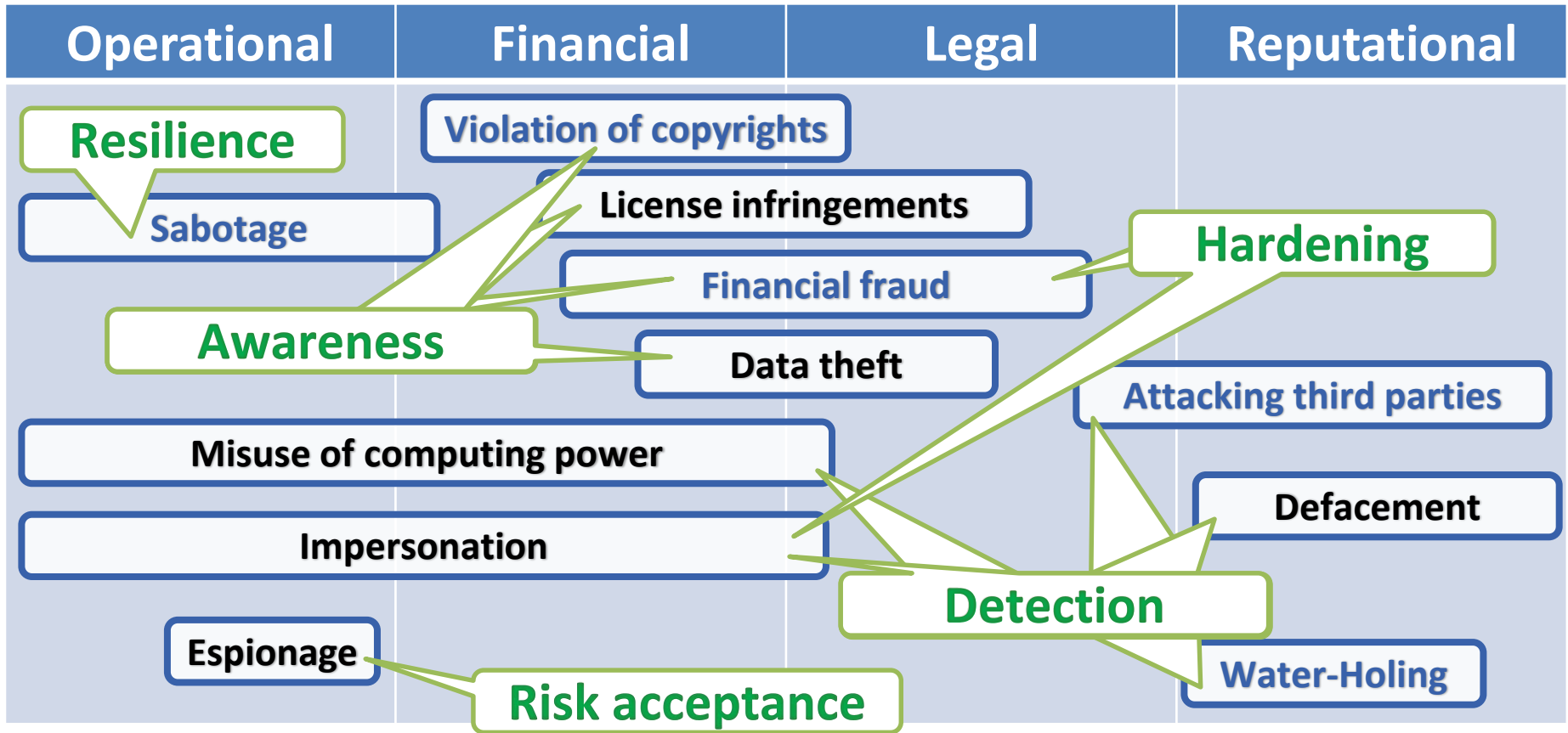
Geneva-based int'l organizations (The Global Fund, ICRC, IFRC, ILO, ITU, OHCHR, UN, UNHCR, WHO, WIPO, WTO)

Governments (e.g. CH, D, EU, F, N, NL, S, UK) and int'l & local law enforcement (e.g. Europol, FBI, Geneva police, Interpol)

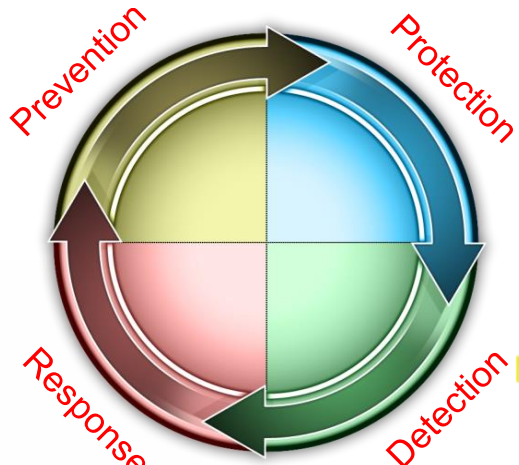
Security & software companies, and industry in general (e.g. CERT-CH forum, ENISA ICS-SG)

Member of vetted closed security forums





resource inventories Defense-in-Depth training
 pen testing change of culture
 central/agile patching network segregation
 security intelligence awareness networking
 keeping informed audits firewalling static code analyzers
 SSO/2FA baselining reviews
 central anti-virus resource life-cycles
 ID federations consulting security policies



WhiteHat Challenges
 vulnerability scanning
 statistical traffic analysis
 netflow
 integrity checkers
 DNS verification
 credential hunts SSHgrep
 URLgrep IDS
 monitor-the-monitoring
 remote login receipts
 syslog/netlog analysis/Snoopy
 web application checking

triage
 CSIRT/CERT
 costing
 forensics

WLCG Grid Security Officer

Security Event Self-Mitigation Portal



Accounts

Name, mail, login or ID

Search login only

Stefan Lueders (slue)

Website review

Please review the sta

Commitment

LUI

Website

Show

Website

apeg

aprilfo

New Firewall Opening Request

You are requesting an opening in the main CERN Firewall to allow Internet access to your machine. Please be aware that machines directly exposed to the Internet will be continually attacked and create a risk for the rest of the site. To avoid this you should access your machine from off-site using an intermediate gateway system, as described here. In general, you should reach your system via LXPLUS which has additional intrusion checks.

Device

- Devi
- Loca
- Mani
- Mod
- Gen
- Desc
- Tag:
- Serie
- Oper
- CER
- Netw
- Resp

- Main
- HCP
- IPv6
- Last changed:

1. Request Information

Interface Name

Interface Name

Service

Dual Web server (HTTP and HTTPS) on ports 80/tcp and 443/tcp

Port number

80, 443

Protocol

TCP

Application

Give the name of the application listening on this port.

HTTP/HTTPS

Expiration Date

This firewall opening, if authorised, will be automatically deleted on this date. The maximum time span at any given time is two years. You will be notified before expiration in order to reconfirm and prolong this firewall opening.

25-05-2021

14-07-2016 (10:32)

Firewall: Approval process with pentest & assessment



skipfish
web application security scanner

**Regular verification:
Opened service still listening?
Network traffic to that opening?**



Log in with your CERN account

Username

Password

I have read and agreed to the [CERN Computing Rules](#) and taken into account the [website lifecycle policy](#).

3

Confirmation

DO NOT submit this request if the contact person does not know you or is not aware of your request!

An email will be sent to the contact person for your approval.

After the operation is completed, a confirmation message will be sent to your email address.

By submitting this form, you agree to comply with the [CERN computing rules](#).

I confirm that I have read and understood the [Computing Rules](#).

[Change password](#)

OC5

Please be aware that repeated, or a single sufficiently grave, infringement of CERN's Computing Rules (OC5) can result in the consequences defined in Section V 21, including the withdrawal of access to CERN computing facilities.

I confirm that I have read, understood and will abide by the [CERN Computing Rules \(OC5\)](#).

[Submit](#)

```
* *****  
* Welcome to lxplus722.cern.ch, CentOS, 7.8.2003  
* Archive of news is available in /etc/motd-archi  
* Reminder: you have agreed to the CERN  
* computing rules, in particular OC5. CERN impl  
* the measures necessary to ensure compliance.  
* https://cern.ch/ComputingRules
```





SECURITY is not complete without U

SECURITY is not complete without U

Protect your computers

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 when you are online.
- Use anti-virus software.**
Use the CERN anti-virus solution as a main line for your home and private usage.
- Do not install untrusted software.**
Untrusted software from untrusted sources may infect or compromise your computer... or violate copyrights.
- Lock your screen with a password.**
When you leave your office.

Let us help you:
<http://cern.ch/Computer.Security> or contact Computer.Security@cern.ch

SECURITY is not complete without U

Be careful with e-mail & Web

Cybercriminals are trying to trick you!

- Do not open unexpected or suspicious e-mails or attachments.**
Click on them if they do not concern you or if they appear valid. 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.
- Protect your passwords.**
Do not reuse them on untrusted computers or Web sites.
- Do not install untrusted software or plug-ins.**
Indeed, software from untrusted sources may infect or compromise your computer... or violate copyrights.

Let us help you:
<http://cern.ch/Computer.Security> or contact Computer.Security@cern.ch

SECURITY is not complete without U

Protect your passwords

A cybercriminal, who knows your password, will abuse your computing account.

- Never share your passwords with anybody.**
Do not make them public, and beware of attempts to trick you into revealing them (so-called "phishing" attempts).
- Choose good passwords.**
Passwords should be hard to guess and cannot be found in any dictionary.
- Do not reuse old passwords.**
Do not use the same password for different purposes or on different sites.
- Change your passwords regularly.**

Let us help you:
<http://cern.ch/Computer.Security> or contact Computer.Security@cern.ch

“Home” Awareness

Utilisez les systèmes d'exploitation fournis par le département IT du CERN. Protégez votre ordinateur privé : utilisez l'antivirus du CERN, appliquez les mises à jour logicielles et installez les logiciels uniquement pour vos besoins personnels.

Soyez prudent lorsque vous naviguez sur le Web : ne cliquez pas sur des liens suspects et n'ouvrez pas les fichiers joints de personnes que vous ne connaissez pas. Utilisez un navigateur sécurisé et évitez les téléchargements de fichiers de sources non officielles. Suivez les règles formatiques de sécurité informatique et évitez d'autoriser des personnes non autorisées à accéder à vos données. Limitez l'accès à vos documents et répertoires, appliquez les principes de sécurité minimale.

Induction & On-Boarding
Mandatory online courses
Technical trainings

Consulting & audits

SECURITY is not complete without U

Protect your files & data

Cybercriminals are trying to find confidential or sensitive information, also here at CERN.

- Restrict access to your documents and folders.**
This includes access to help files and free applications, shared folders, contacts, shared files, software repositories, public or private folders.
- Follow the principle of least privilege.**
Ensure that only people who need to access your files and data can do so.
- Do not run file sharing applications.**
Use alternative storage, enable backup to software support centers.

Let us help you:
<http://cern.ch/Computer.Security> or contact Computer.Security@cern.ch

SECURITY is not complete without U

Follow the computing rules

Help us to protect CERN's mission and reputation.

- Follow the CERN Computing Rules.**
These are part of the "Top and Order" Operational Circularity.
- Take responsibility.**
Everyone is responsible for securing their PCs, data, systems & services.
- Do not run restricted applications.**
e.g. software which has negative impact on CERN's network or computer security.
- Respect confidentiality and copyrights.**
... of music, videos and software applications.

Let us help you:
<http://cern.ch/Computer.Security> or contact Computer.Security@cern.ch

SECURITY is not complete without U

Respect copyright

Don't break the law!

- Do not distribute copyrighted material.**
... without explicit consent from the copyright owners.
This includes music, films, videos or software.
- Refrain from file sharing applications or file hosting services.**
Like BitTorrent, eMule, RapidShare.com, MegaUpload.com.
- Violating copyright is not a trivial offense.**
Unauthorized distribution of copyrighted material is against the law in many countries, including France and Switzerland.
- Protect the Organization.**
Unauthorized distribution of copyrighted material on the CERN network or from CERN computers will affect negatively on the Organization and could harm its reputation.

Let us help you:
<http://cern.ch/Computer.Security> or contact Computer.Security@cern.ch

https://cern.ch/security/training/en/posters.shtml



Finding the Balance for Security
Dr. Stefan.Lueders@cern.ch
CNAF/CERN Seminar, May 27th 2020

Prevention: Six Recurrent Themes

Static Code Analysis Tools

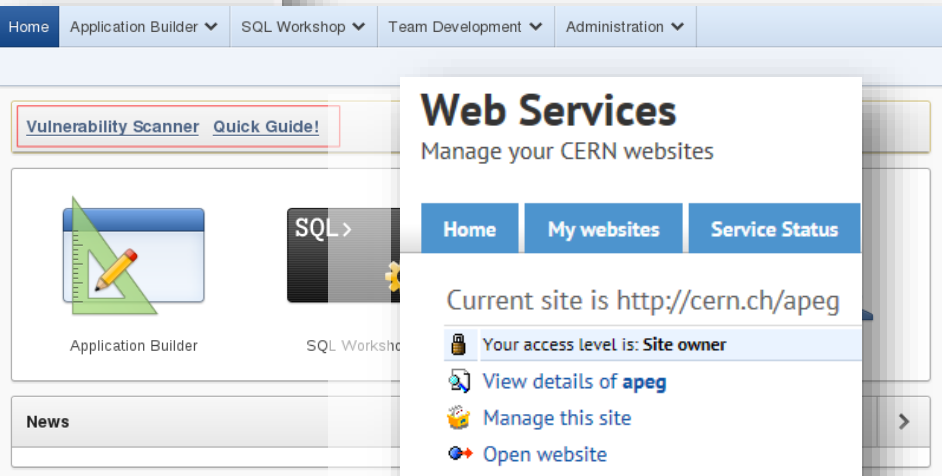
Below you find a list of **static source code analysis tools** recommended for **developers**. These tools are supposed to allow developers quickly, looking for some common potential bugs and vulnerabilities (not only security-related), thus increasing reliability and security.

This is a summary of an evaluation of code analysis tools by the Computer Security Team. It is by no means a comprehensive list, nor is it a list of the most complete tools. The tools presented are selected for their ease of use, simplicity and by their efficiency. Another list can be found [here](#).

The tools and the documentation provided are for Linux, but many are also available on Windows as well (links are provided). If you have a [Gitlab-CI \(Continuous Integration\) service](#), note that all tools are provided through a dedicated Docker image. See [these examples](#) for details.

C / C++

CppLint	Free	stand-alone script	CppLint is a script that checks for compatibility of code with Google's style guide for the C++ language. It can find some dangerous constructions and report general bad practices, syntax errors and style inconsistencies.
Flawfinder	Free	stand-alone script	Flawfinder checks for calls to known potentially vulnerable library function calls.





University of Applied Sciences and Arts Northwestern
School of Engineering



Web security & pentesting



**EXERCISE
ONLY**



BREAKING NEWS

CERN - EUROPEAN ORGANIZATION FOR NUCLEAR RESEARCH 'VICTIM OF CYBER ATTACK'
Personal details of around 1,000 CERN employees for sale on the dark web

SVN24

FOR EXERCISE PURPOSES ONLY – THIS CLIP CONTAINS FICTITIOUS INFORMATION – FOR E





Oops... The link you've just clicked is evil!

(Version française ici/en-dessous)

You just fell for a scam. The e-mail whose link you just have clicked is fake. Your "click" could have had severe operational and financial consequences for CERN... Let us explain to you how you can better identify such emails and which consequences clicking on such a malicious link might have for you and your digital assets...

How to identify malicious e-mails

Is the sender familiar to you?

Does the sender's name correspond with the shown e-mail-address?

Is the message addressed to you?

Hover your mouse pointer on top. Does the text correspond with the link?

Does the link look reasonable, is not too complex or unreadable?

Does the message concern you? Is it one of your businesses?

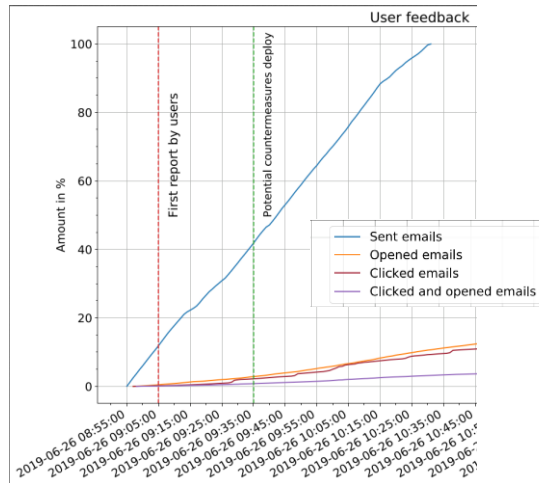
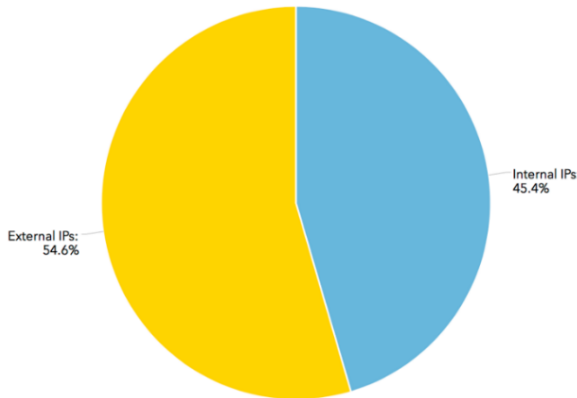
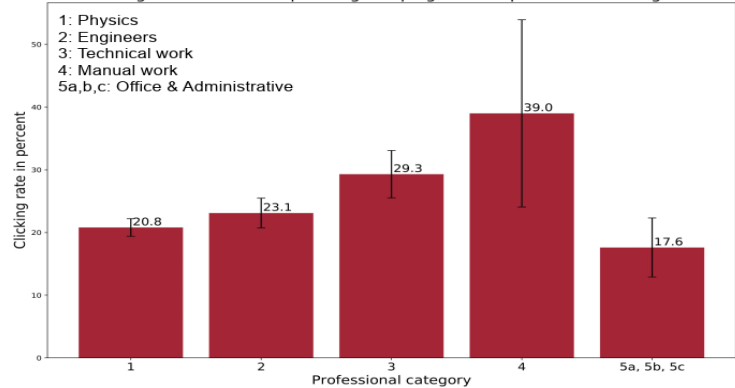
Is the message signed (with a signature icon)?

Is the message correctly phrased, without blunt typos, in a language you are able to comprehend?

If you have answered any one of those questions with "NO" be vigilant and careful! Delete that message or check with us at Computer.Security@cern.ch when in doubt.



Clicking rate of the 2019 phishing campaign across professional categories



Click rate: ~20.0%
 (2018: 15.3%; 2017: 18.7%; 2016: 19.8%; HEPix BNL 2015: 29%)

DNS blocking catches only 50%...

...and you have to be Sick!

Human aspects of email security

Subject: FW: Testing of new booking system

Hello,

I received the email below from the mail address @cern.COM and unfortunately I clicked on the link. What should I do? To: cert-snow@cern.ch

Best R I didn't click, but I forwarded it to

Regards,

To: cert-snow@cern.ch, sen...
 ...[security concern]...

...ned that this might compromise CERN's security.

...ething to worry...

Dedicated appliance to block sophisticated malicious emails & attachments



CERN
CH-1211 Geneva 23
Switzerland

Document
Security Baseline for Hardened PC

CERN Div./Group or Supplier/Contractor Document No.
Computer Security Officer

EDMS Document No.
1593100

JUNE 20th, 2016

**SECURITY BASELINE FOR
HARDENED PCS AND LAPTOPS**



PC Hardening & Alternative PDF Reader



Finding the Balance for Security
Dr. Stefan.Lueders@cern.ch
CNAF/CERN Seminar, May 27th 2020

Protection: Mail & MS Windows

slide #35

Blocking certain malicious & typo-squatting domains in the Domain Name Servers (DNS)



CERN Computer Security

Computer security emergency contact
✉ Computer.Security@cern.ch ☎ 70500
Contact en cas d'incident de sécurité informatique



Home Computing Rules Recommendations Training Services Reports & Presentations



Oops... We prefer you not going there...

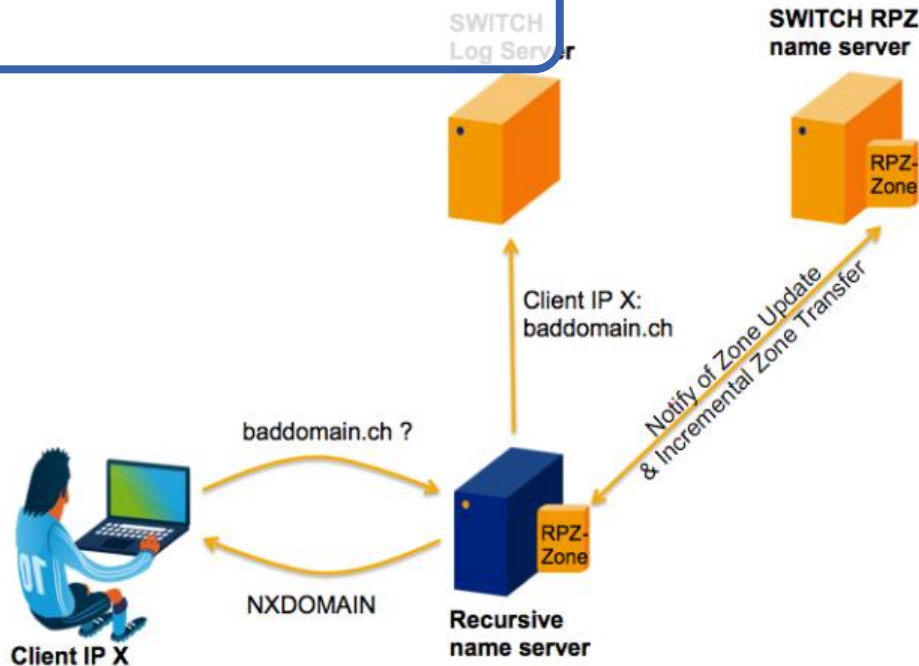
The page you were looking for has been blocked as it is likely hosting malicious contents.

"Malicious contents" is either malware, i.e. software aiming at infecting your PC, or a "Phishing" portal, where "Phishing" is a technique to trick you in disclosing your password. In the latter case, probably you just clicked on a link in a corresponding "Phishing" email sent to your CERN mail address? If so, just delete this email and ignore the web-site!

If you think that this web-site should be accessible from CERN, please contact us at Computer.Security@cern.ch.

Oops... C'est mieux si vous n'y allez pas...

<https://cern.ch/security/blocked.shtml>



Synchronizing with SWITCH's list of bad domains

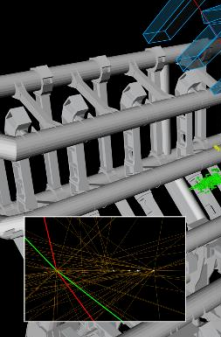
Protection: DNS Filtering



**Safety first
Availability next
Security third**

Impact & criticality analyses

**Rigorous safety systems
prevent (malicious) damage,
but reduce availabilities**



6 Challenges to Secure the LHC
Dr. Stefan.Lueders@cern.ch
CCCC 2016, June 9th 2016, Copenhagen (DK)

#1: Controlling Impact & Consequences

Run: 18270
Event: 7050664
2011-05-30 07:54:29 CEST



Finding the Balance for Security
Dr. Stefan.Lueders@cern.ch
CNAF/CERN Seminar, May 27th 2020

Protection: Rigorous Safety Systems



Insecure embedded devices

Wireless to the plant floor

(No) Network segregation

One Data Center to serve them all

Remote development and testing

Why (Control System) Cyber-Security sucks...

**Control System
Cyber-Security**

Headache #1 still to be Overcome



Transparency is paramount for successfully running an ethical and trustworthy Computer Security Team.

https://cern.ch/security/home/en/privacy_statement.shtml

Digital Privacy Statement of CERN's Computer Security Team

2016/11/15 by CSO

Introduction

The CERN Computer Security Team ("the Team") takes great care to protect the personal data collected or accessed by us. This Privacy Statement describes how and when the Team gathers, accesses, uses and shares information about you or your usage of CERN's computing facilities and how the Team protects this information.

Scope

This Privacy Statement applies to all persons accessing or using CERN computing facilities, including websites hosted at CERN. It complements the CERN's Computing Rules, i.e. the Operational Circular No. 5 on the [Use of CERN Computing Facilities](#), in particular its subsidiary rules, and [Administrative Circular No. 10](#) on Personal Data Protection.

Information Collection and Use

The CERN Computer Security Team automatically records information ("Log Data") created by your use of CERN's computing facilities in order to detect and understand any abuse of CERN's computing facilities as well as any other violation of the [CERN Computing Rules](#) in real time and/or in retrospect.

Log Data contains information on your digital access to CERN's computing facilities including access to the wired and wireless networks, unencrypted network traffic of your device(s) with external services on the Internet, as well as all your activities linked to CERN's interactive computing clusters and its web services. Log Data is always registered with an accurate time stamp. In detail, Log Data includes:

- Usage information when connecting your device(s) to CERN's wired or wireless networks (i.e. [ARP](#) and [DHCP](#) meta data)

Information Security and Retention

Log Data is stored using the computing facilities provided by CERN's IT department. CERN makes best efforts to protect this Log Data from unauthorized access, or alteration, disclosure or destruction (also see [CERN's Digital Privacy Statement](#)). Past experience has shown that a retention period of one year is sufficient to perform the analysis of security related events in retrospect, but this is subject to periodical reviews. Log Data linked with any abuse of CERN's computing facilities as well as any other violation of the [CERN Computing Rules](#) is kept indefinitely.

Information Access, Sharing and Disclosure

As stipulated in the [CERN Computing Rules](#), access to Log Data is limited to members of the CERN Computer Security Team, i.e. a limited number of individuals appointed ad-personam by CERN's Computer Security Officer, and only authorized when suspicious activity or activity potentially violating CERN's Computing Rules related with your activity, account(s) or device(s) has been detected by or reported to the Team. In those cases, the Team may preserve or disclose your information only if deemed by CERN to be necessary for legal purposes; to protect the safety of any person; to address fraud, security or technical issues; or to protect CERN's rights or property. In particular, the Team reserves the right to disclose (parts of) your data promptly to third parties in order to avert any further harm to you, your account(s), your device(s) or your data.

Revisions

This Privacy Statement may be periodically revised. Prior versions of the Privacy Statement will be archived and kept available.



Data ingestion



Data processing

Storage and visualisation

Incident response

- Sources of data
- IDS systems: Zeek, Snort / Suricata
 - System logs
 - Netlog
 - Execlog
 - Active Directory / Krb
 - Single Sign On logs
 - Web logs
 - DNS logs
 - Automatic scan results
 - Webhole logs



~3TB/d

Flume parse & normalize

Malware Information Sharing Platform

Intelligence framework

Data enrichment Aggregation Correlation Stream processing

Go

Kafka

Central data backbone

Network database Active Directory

DNS / DHCP Geo IP

Sources of information

Flume

Spark

Batch & custom jobs

HDFS

Long term storage

Custom CLI

Elasticsearch

Real time indexing

Dashboards / visualisation

Kibana

FIR

SIEM

The Hive

Incident Response

Cortex

Observable enrichment

Enrichment correlation and aggregation

Remote forensics

GRR





Serving CERN, the WLCG and the HEP and academic community

Synchronized with CH law enforcement & CH CERTs

Also from external feeds:

**SOC/MISPI
Bro/Zeek**

Detection: Intelligence

Events	
<input type="checkbox"/>	2020-05-22 Network activity domain branter.tk
<input type="checkbox"/>	2020-05-22 Artifacts dropped regkey {59031A47-3F72-44A7-80C5-5595FE6B30...}
<input type="checkbox"/>	2020-05-27 5/27/2020, 12:26:31 AM ?_Cern.ch Caller.html
<input type="checkbox"/>	2020-05-26 5/26/2020, 4:35:45 PM Lars.80451447MCI0U2J947MCI0U2J947MCI0U2J94->7MCI0U2J94.html
<input type="checkbox"/>	2020-05-26 5/26/2020, 10:41:51 AM Purchase-Order.html





Suspicious activity detected on device

Europe/

[Redacted]

https://cern.ch/security/services/en/sms.shtml

List all your

What has been detected?

Date	Category	Subject	Business Lines	Severity	Status
2020-05-25	Devices/SuspiciousActivity	Suspicious activity detected on device [Redacted]	[Redacted]	2	Open
2020-05-22	Devices/SuspiciousActivity	Suspicious activity detected on device [Redacted]	[Redacted]	2	Open
2020-05-22	Devices/SuspiciousActivity	Suspicious activity detected on device [Redacted]	[Redacted]	2	Open
2020-05-18	Devices/VulnerableWebserver	Your device [Redacted] has not had a Puppet-run in 2020	[Redacted]	2	Open
2020-05-18	Devices/VulnerableWebserver	Your device [Redacted] has not had a Puppet-run in 2020	[Redacted]	2	Open
2020-05-14	Webservices/VulnerableWebsite	Directory traversal vulnerability on the CERN [Redacted] website	[Redacted]	3	Open

CERN Computer Security
Computer security emergency contact
✉ Computer.Security@cern.ch ☎ 70500
Contact en cas d'incident de sécurité informatique

Home | Computing Rules | Recommendations | Training | Services | Reports & Presentations

Privacy Statement
Computer Security Incident Response
Emergencies
Self-mitigation portal
Audits & Reviews
...on request
CERN WhiteHat Challenge
Host-Based Intrusion Detection
Central security logging
"SSH receipts"
Traffic Control & Monitoring
DNS analysis
Network-based intrusion detection
The CERN outer perimeter

What to do in an Emergency

If you have detected or encountered a security event, there are four basic steps to take:

- **Don't panic:** Security events develop and spread quickly. Panicking now and taking hectic actions is usually worsening the situation. If any damage has been done, it has been done already by now;
- If this concerns a device, **keep it connected and leave it "on"**: Do *not* disconnect the system/service/device from the CERN network by pulling out its Ethernet cable or by disabling the wireless adapter. Do *not* switch the power off !!!
- If this concerns an account, **Reset your password**: Do so via the [CERN account portal](#). You might be asked to reset it again once that event has been understood;
- **Contact the Security Team**: Computer.Security@cern.ch or call 70500 (+41 22 767 0500) from inside (outside) CERN. Details as well as our PGP key can be found [here](#);
- **Don't touch anymore**: Wait for instructions before taking any further actions. Depending on the impact, we might have to understand the event in detail. Unnecessary actions might destroy evidence.

- Triage
- Taking over service
- Coordinating comm's
- "Avalanching"
- Forensics

- Close out

CERN also provides incident response & forensics services



Current system status and maintenance notific

Home / Security Advisory: BusyWinman Linux Intrusion – July 21, 2017 15:40 PT

Security Advisory: BusyWinman Linux Intrusion – July 21, 2017 15:40 PT

Operation Windigo – the vivisection of a large Linux server-side credential-stealing malware campaign



BY PIERRE-MARC BUREAU POSTED 18 MAR 2014 - 01:3

Security news, views and insight from the ESET experts

During the course of our analysis, we have had the opportunity to collaborate with various international organizations, including [CERT -Bund](#), the [Swedish National Infrastructure for Computing](#), the [European Organization for Nuclear Research \(CERN\)](#) and others forming an international Working Group. With the help of the working group, thousands of victims have been notified that their servers were infected, in an effort to clean as many systems as possible. We are now releasing a complete





CERN Computer Security

Computer security emergency contact
Computer.Security@cern.ch @70500



Home Computing Rules Recommendations Tra

Security Reports

Monthly reports on CERN security

Monthly security reports from SWITCH CERT

Articles & Announcements

Articles in the CERN Bulletin, Computing Newsletter & others

Announcement archive

SWITCH Security Blog

Monthly reports on CERN security

If you are interested to receive reports on CERN security, please contact us to the "cert-security-info@cern.ch"

2020

January - February - March

2019

January - February - March - November - December

Computer Security Report for April 2020

Corona Warning Please be extremely skeptical when receiving emails around the subject "Corona"/"COVID-19", in particular if those emails containing links or attachments. STOP --- THINK --- DON'T CLICK! ...and don't open any attachment. If you are in doubt, cross-check with us at Computer.Security@cern.ch.

Blackmailed with your password? If you received recently an email with a password similar to one of yours, claiming that they "know every think about you", and asking you to transfer Bitcoins to them, don't worry and don't answer. This is a scam. The password, eventually a real one, has been exposed in a data breach, likely already a while ago, and was made public in so-called "password dumps" containing of millions of other passwords. The scammers here just took advantage of those dumps to blackmail you. If you recall that password and still use it somewhere, time to change it now. In parallel, we continue to inform owners of exposed passwords if we get hold of similar password dumps... More details can be found in those two [Bulletin articles](#).

iOS/iPhone/iPad Exploit A zero-day vulnerability, i.e. a vulnerability which has not patches ready yet, of the native mail client in the iOS operating system [has been reported](#) being actively exploited. Unfortunately, there is no fix out yet. Only option for the moment is avoiding having your emails pushed to your iPhone/iPad ("Settings" -> "Passwords & Accounts" -> have "Fetch New Data: Off" by disabling "Push" and



CERN values its open environment
⇒ **“Security” delegated to everyone**

Like others, permanently under attack

- **Training the minds of people**
- **Keeping inventories & life-cycles**
- **Being prepared + trying to detect early**



More “security” seminars coming every other week from now on: &

Hacking

Human aspects of email security

Web security & pentesting

Forensics

OpenBSD security

The Deep & Dark Web

Control system cyber-security

SOC/MISP/ Bro/Zeek

Shameless Advertisement

<https://indico.cern.ch/category/82/>





www.cern.ch

Thank you for listening!

Questions?