



SECURITY is not complete without **U**

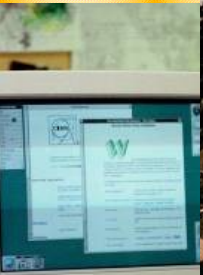
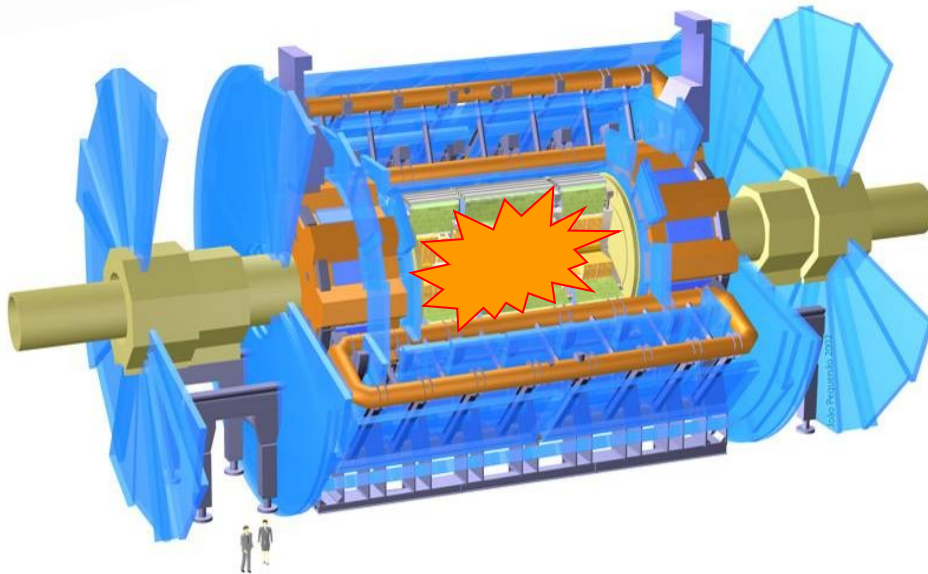
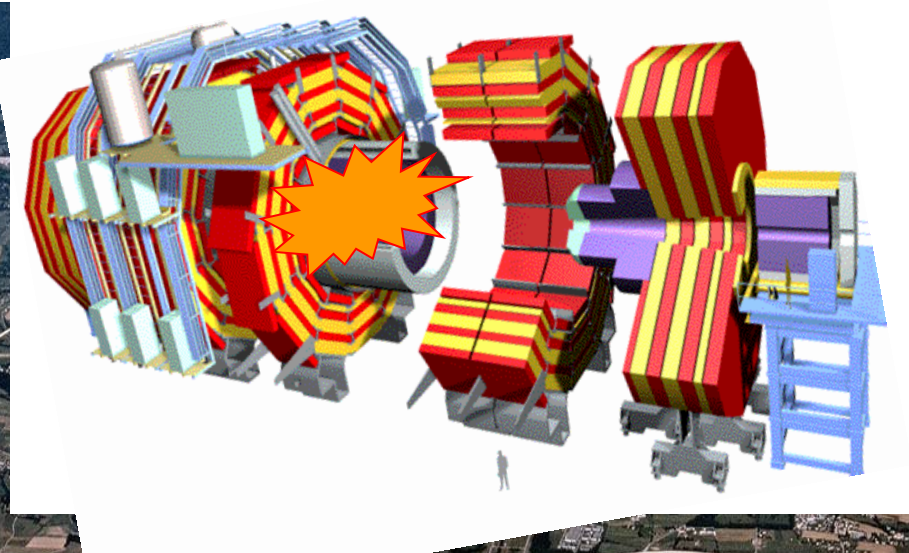
CERN
Computer & Grid Security

Dr. Stefan Lüders
(CERN Computer Security Officer)
ITU SG17 Tutorials, Geneva, September 5th 2012



CERN in a Nutshell

Stefan Lueker U SG17 Tutorials — September 5th 2012



Tim Berners-Lee



CERN's security footprint



Operational Noise



Securing the LHC Computing Grid



This is a “people” problem



CERN's security footprint

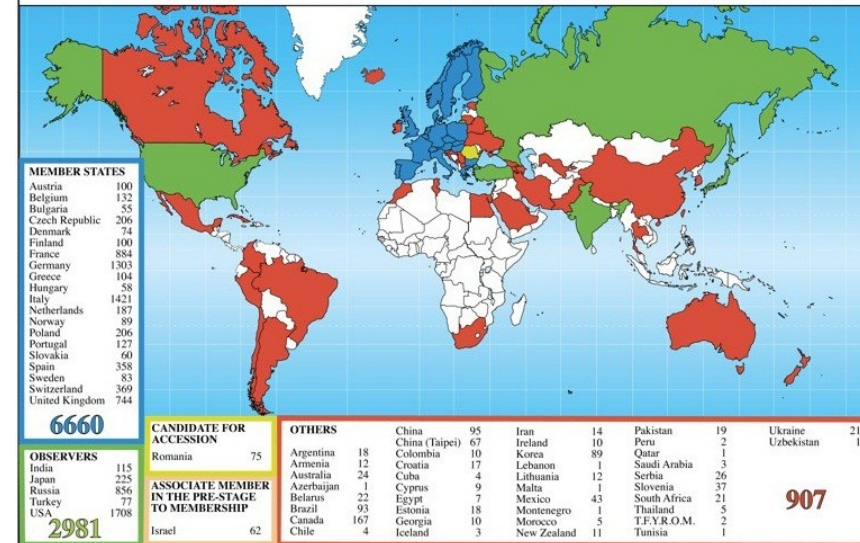
Academic Freedom at CERN

Stefan.Lueders@cern.ch — ITU SG17 Tutorials — September 5th 2012

CERN's Users:

- ▶ ...from 100s of universities worldwide
- ▶ Pupils, students, post-docs, professors, technicians, engineers, physicists, ...
- ▶ **High turn-over** (~10k per year)
- ▶ **Merge of professional and private life:** Social Networks, Dropbox, Gmail, LinkedIn, ...

Distribution of All CERN Users by Nation of Institute on 9 January 2012



Academic Freedom in Research:

- ▶ **No limitations** and boundaries if possible
- ▶ **Free** communication & **freedom** to publish
- ▶ Difficult to change people, impossible to force them
- ▶ Trial of the new, no/very fast life-cycles, all-time prototypes
- ▶ **Open campus attitude:** I consider CERN being an ISP!

Academic Freedom at CERN

CERN's Users:

- ▶ ...from 100s of universities worldwide
- ▶ Pupils, students, post-docs, professors, technicians, engineers, physicists, ...
- ▶ High turn-over (~10k per year)
- ▶ Merge of professional and personal: Social Networks, Dropbox, LinkedIn, ...



The threat is already inside.
A good security paradigm must balance this "Academic Freedom"

Acad

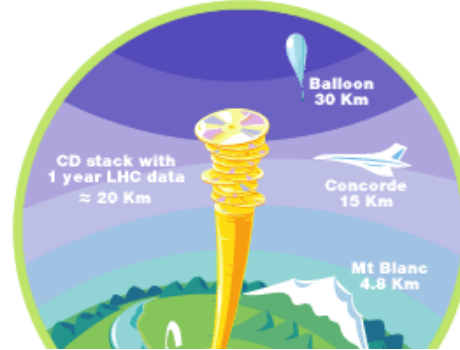


- ▶ ...possible
- ▶ ...om to publish
- ▶ ...people, impossible to force them
- ▶ ...w, no/very fast life-cycles, all-time prototypes
- ▶ Campus attitude: I consider CERN being an ISP!



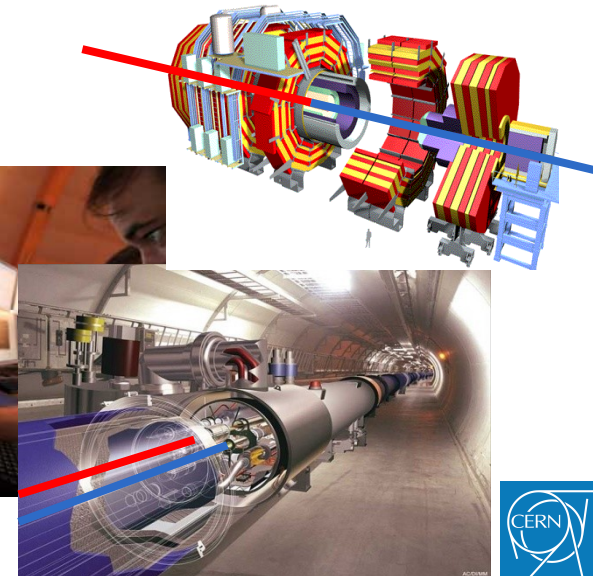
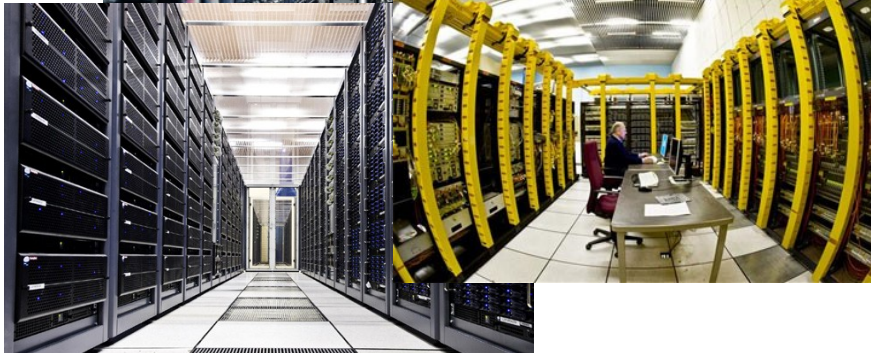
CERN Sectors of Operations

Stefan.Lueders@cern.ch — ITU SG17 Tutorials — September 5th 2012



Office Computing Security
Computing Services Security

Grid Computing Security
Control Systems Security





CERN's security footprint



Operational Noise

Under Permanent Attack

Stefan.Lueders@cern.ch — ITU SG17 Tutorials — September 5th 2012

CERN is under permanent attack... even now.

Servers accessible from Internet are permanently probed:

- ▶ ...attackers trying to brute-force passwords;
- ▶ ...attackers trying to break Web applications;
- ▶ ...attackers trying to break-in servers and obtain administrator rights.

Users are not always aware/cautious/proactive enough:

- ▶ ...attackers trying to harvest credentials outside CERN;
- ▶ ...attackers trying to “phish” user passwords.

Security events happen:

- ▶ Web sites & web servers, data-base interfaces, computing nodes, mail accounts, ...
- ▶ The office network is very liberal: free connection policy and lots of visitors. Thus, there are always devices being infected/compromised.



Under Permanent Attack

Stefan.Lueders@cern.ch — ITU SG17 Tutorials — September 5th 2012

CERN is under permanent attack... even now.

Servers accessible from Internet are permanent

- ▶ ...attackers trying to brute-force passwords;
- ▶ ...attackers trying to break Web applications;
- ▶ ...attackers trying to break-in servers.

Users are not always

- ▶ ...attackers trying to
- ▶ ...attack

enough:

Coming up:

- ▶ **My top-10 security events of the last 5yrs**
(There weren't much more)
- ▶ ...data-base interfaces, ...
- ▶ ...mail accounts, ...
- ▶ ...network is very liberal: free connection policy and lots of visitors.
- ▶ ...there are always devices being infected/compromised.



Phishing

Stefan.Lueders@cern.ch — ITU SG17 Tutorials — September 5th 2012

Date: Fri, 5 Sep 2008 15:53:42 -0700
From: Webmail IT Service <sandraward@charterint.com>
Reply-To: webITService@live.com

Targeted and untargeted
“Phishing” attacks in
English & French...



To: [redacted]
Subject: [redacted]

Dear [redacted]

Spoofed login pages...



Sign in with your CERN account

>>>Help Desk Error>>> Respond - ma

File Message

Delete Reply Reply All Forward Service Accounts To Manager Team E-mail Mark Un

From: Kim Thomas <kthomas@bbisd.org>
To: it@helpdesk.org
Cc:
Subject: >>>Help Desk Error>>> Respond

Dear User,

You have exceeded the service provider, you will be unable to receive
new emails and sent s as sent, you are Currently running on 91624
KB, You have has exce To prevent this, please click to reset your
account. [CLICK HERE](https://docs.google.com/spreadsheet/viewform?formkey=dfphslvithy5dmuws3zmotdxqvjrv66ma)

Thanks
Administrator.

...on “trusted” hoster!



Data Leakage (1)

Stefan.Lueders@cern.ch — ITU SG17 Tutorials — September 5th 2012

CERN LHC portal • View topic - What is where in LHC sectors? - Windows Internet Explorer

http://www.lhcportal.com/Forum/viewtopic.php?f=4&t=384

Google

CERN LHC portal • View topic - What is where in LHC s...

Page Safety Tools

Harbles **Post subject:** Re: What is where in LHC sectors? **Posted:** Sun Mar 07, 2010 5:03 pm

OFFLINE
LHCPortal Guru
Joined: Sat Nov 28, 2009 10:22 pm
Posts: 110

Hi Serych,

Perhaps this document will usefull <http://cdsweb.cern.ch/record/1129806/record/1129806/file/s08001.pdf> It's a 7.5 MB .pdf overview of the LHC machine.


There are others for each experiment;

Atlas <http://cdsweb.cern.ch/record/1129811/record/1129811/file/s08003.pdf> 36MB
Alice <http://cdsweb.cern.ch/record/1129812/record/1129812/file/s08002.pdf> 23MB
CMS <http://cdsweb.cern.ch/record/1129810/record/1129810/file/s08004.pdf> 18MB
LHCb <http://cdsweb.cern.ch/record/1129809/record/1129809/file/s08005.pdf> 22MB

PROFILE

serych **Post subject:** Re: What is where in LHC sectors? **Posted:** Sun Mar 07, 2010 5:03 pm

OFFLINE



Thanks Harbles

[Redacted]

Thanks once again!

Let the protons colide!

Jakub

PROFILE

Harbles **Post subject:** Re: What is where in LHC sectors? **Posted:** Mon Mar 08, 2010 1:33 am

OFFLINE
LHCPortal Guru
Joined: Sat Nov 28, 2009 10:22 pm
Posts: 110

Serych,

[Redacted]

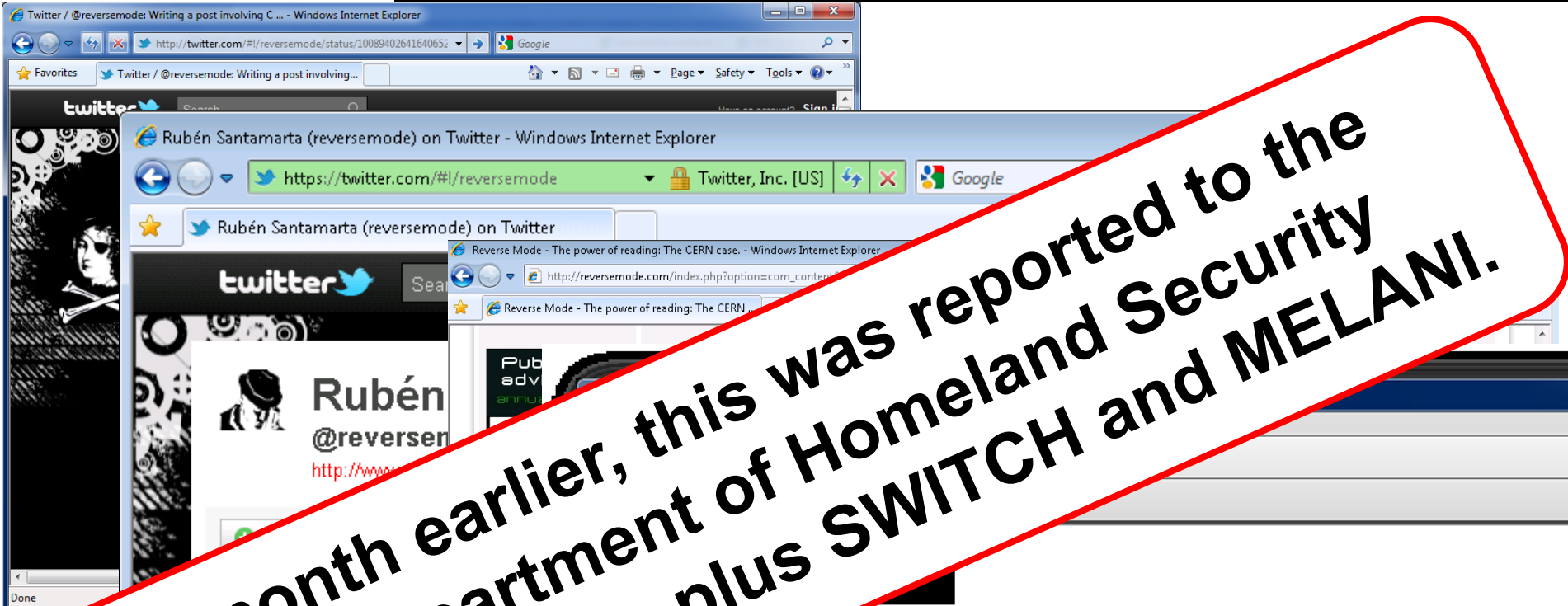
Enjoy!

Sensitivity levels are user dependent!



Data Leakage (2)

Stefan.Lueders@cern.ch — ITU SG17 Tutorials — September 5th 2012



A month earlier, this was reported to the U.S. Department of Homeland Security who informed us plus SWITCH and MELANI.

PVSS
Graphical Editor

- Exécuter « Remote Desktop Connection »
 - Se connecter sur [REDACTED]
 - User name : [REDACTED]
 - Password : [REDACTED]
- Ouvrir C:\Dev_Disk\PVSS_Projects\unicos_pvss_OWS
 - Exemple : BTPCS
 - Exécuter « Atlas_Cryo_Unity.Editeur.bat »
- Ouvrir Panel Editor

Break-Ins

th 2012

```
220-<<<<<<=>=< Haxed by A!0n3 >=>=>>>>
220- ,,øæ°°^°°æø, ,,øæ°°^°°æø, ,,øæ°°^°°æø, ,,øæ°°^°°æø
220-/
```

Unpatched oscilloscope
(running Win XP SP2)



Lack of input
validation & sanitization



Unpatched web server
(running Linux)



The screenshot shows a web browser window with a terminal window open. The terminal window displays the following output:

```
Detectors: LAr
https://
Terminal — ssh — ttys000 — 80x24
ssh
3200K ..... 95% 10.85 MB/s
3250K ..... 96% 11.49 MB/s
3300K ..... 98% 10.99 MB/s
3350K ..... 99% 11.24 MB/s
3400K ..... 100% 10.83 MB/s

15:03:29 (11.18 MB/s) - `exploit2.tgz' saved [3492005/3492005]

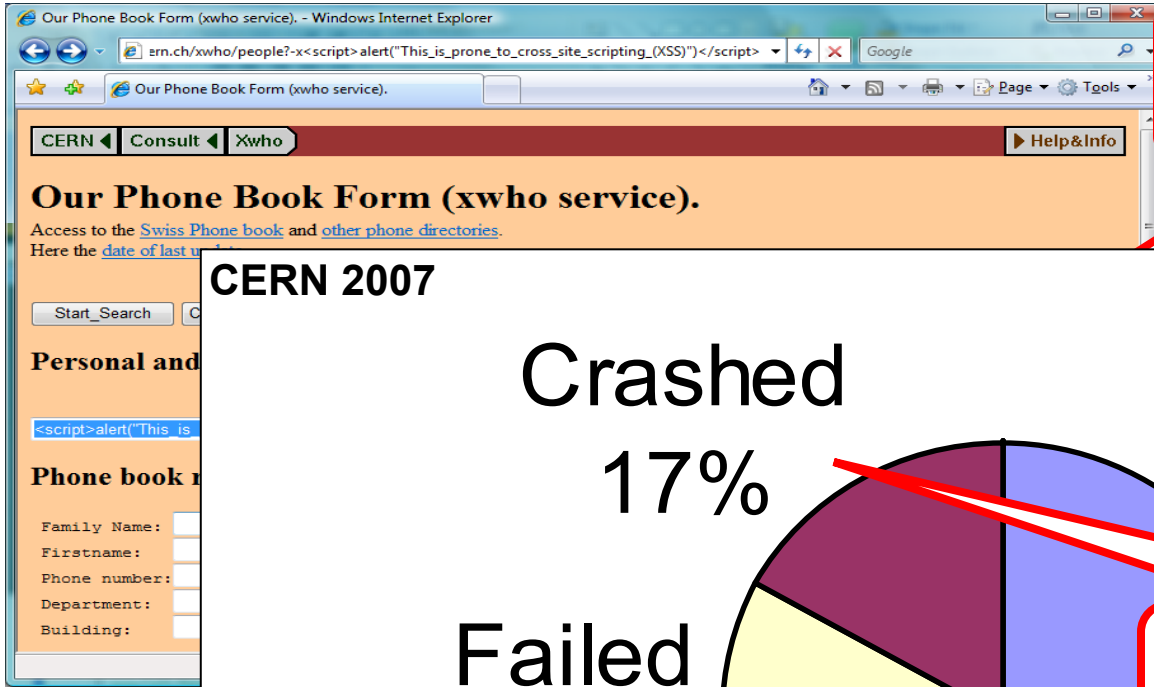
tar -zxvf exploit2.tgz && cd wunderbar_emporium
wunderbar_emporium/
wunderbar_emporium/pwnkernel.c
wunderbar_emporium/tzameti.avi
wunderbar_emporium/wunderbar_emporium.sh
wunderbar_emporium/exploit.c
id
uid=48(apache) gid=48(apache) groups=48(apache),50004(ticketgroup),1100241092 context=root:system_r:system_mail_t
./wunderbar_emporium.sh
sh: mplayer: command not found
sh: no job control in this shell
sh-3.00# id
uid=0(root) gid=0(root) groups=48(apache),50004(ticketgroup),1100241092 context=root:system_r:system_mail_t
sh-3.00#
```


One error in opening the page. For more information, choose Window > Activity.



Suboptimal configuration (1)

Stefan.Lueders@cern.ch — ITU SG17 Tutorials — September 5th 2012

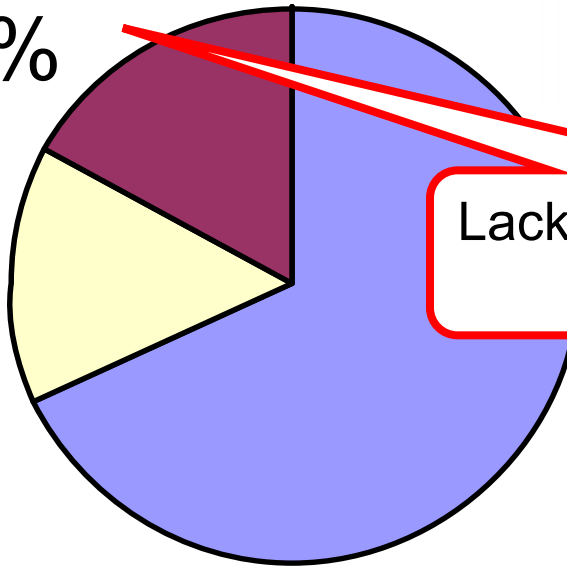



Lack of input validation/sanitization 

CERN 2007

Crashed
17%

Failed
15%



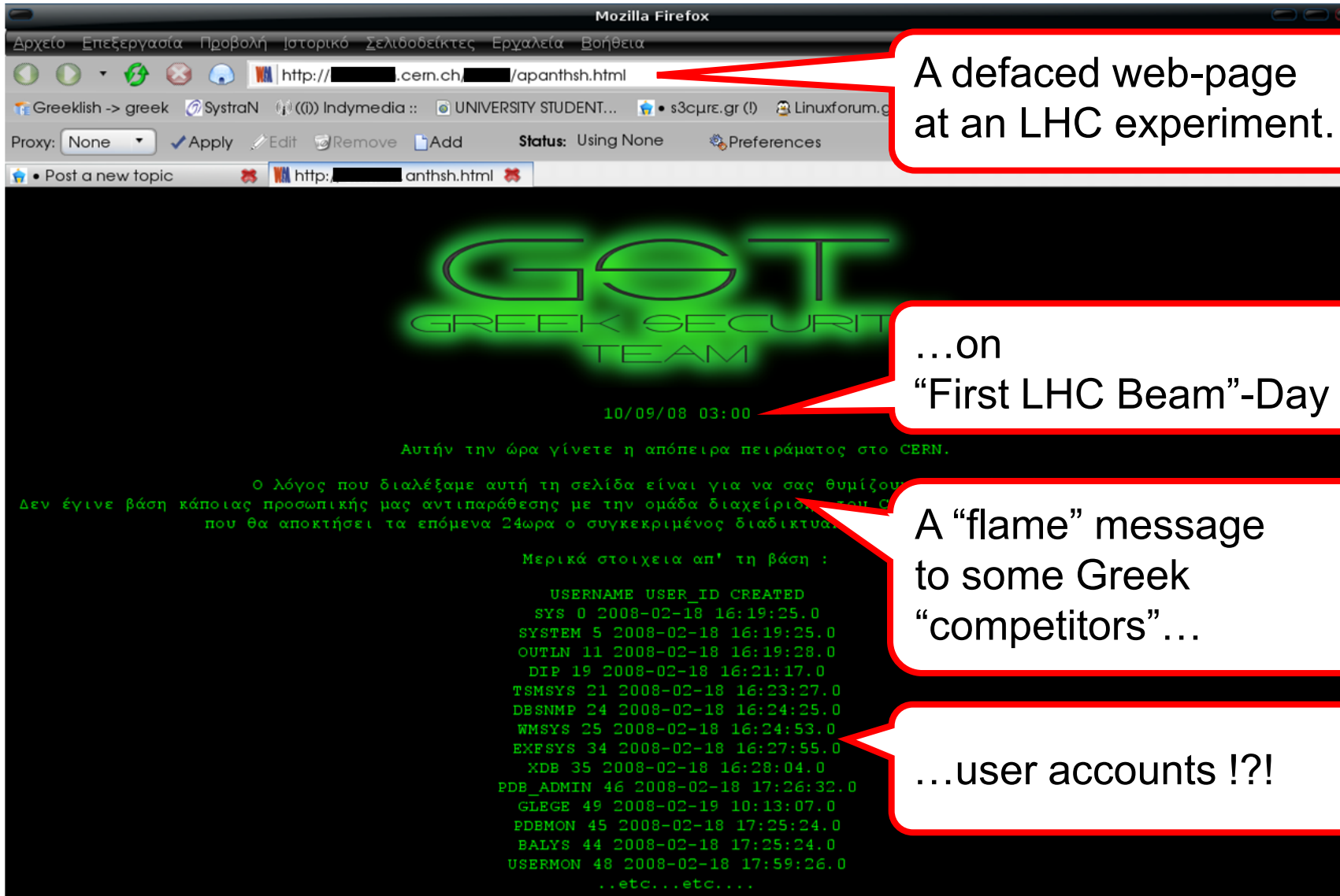
Lack of robustness ☹️ 

Passed
68%



Suboptimal configuration (2)

Stefan.Lueders@cern.ch — ITU SG17 Tutorials — September 5th 2012



A defaced web-page at an LHC experiment..



...on "First LHC Beam"-Day



A "flame" message to some Greek "competitors" ...



...user accounts !?!





CERN's security footprint



Operational Noise



Securing the LHC Computing Grid

The Worldwide LHC Computing Grid

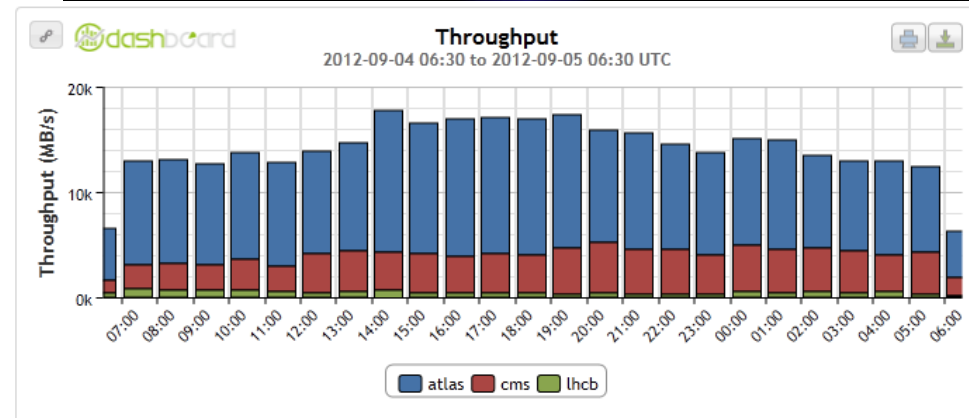
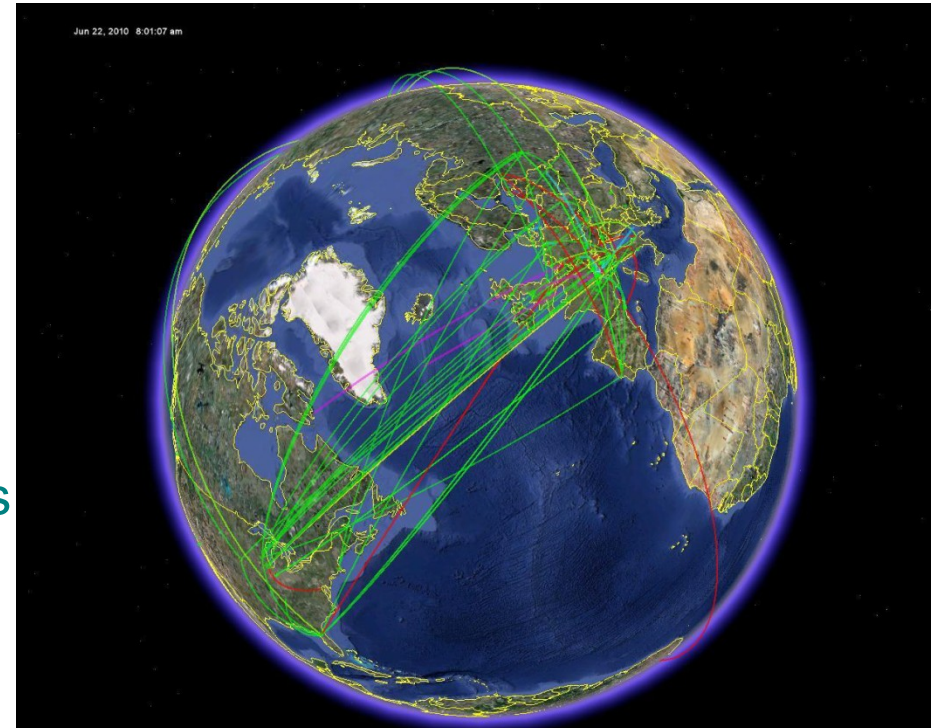
Stefan.Lueders@cern.ch — ITU SG17 Tutorials — September 5th 2012

LHC Data Challenge:

- ▶ LHC produces 25PB data per year
- ▶ Permanent growth of demands

Worldwide LHC Computing Grid (WLCG):

- ▶ Tier-ed network of computer centres
- ▶ CERN is Tier-0; 11 Tier-1s
- ▶ Re-processing of all LHC data
Production of “Monte Carlos”
- ▶ Back up of data
- ▶ Provisioning of computing power for data analysis to O(10 000) physicists worldwide



The GRID: A network of trust

Stefan.Lueders@cern.ch — ITU SG17 Tutorials — September 5th 2012

WLCG/European Grid Initiative (EGI) security governed through policies:

- ▶ High-level “Grid Security Policy”
- ▶ For users: “Grid Acceptable Use Policy” (AUP)
- ▶ For sites: “Grid Site Operations Policy”
- ▶ ...plus many more

Foster collaboration:

- ▶ ...between users and security people
- ▶ ...between all Grid sites:
EGI/NGIs, WLCG, TeraGrid, OSG,...
- ▶ Information sharing essential!
(incident forensics, vulnerabilities,
good practises, policies)



e-infrastruc

Documents

The policy documents produced by the former JSPG are valid since 1st May 2010 for the EGI partners. They are in the process of being imported into new documents template. You can reference the security policy documents by using the new permanent links:

Top-level Grid Security Policy:

- [Grid Security Policy](#)

For all Users:

- [Grid Acceptable Use Policy](#)

For all Sites:

- [Grid Site Operations Policy](#)

	Affects EGI	Affects OSG	Affects NDGF	Affects academic community
Incident 1		X		
Incident 2	X			
Incident 3	X	X	X	X
Incident 4	X	X		X

EGI Policy Group: <https://wiki.egi.eu/wiki/SPG>

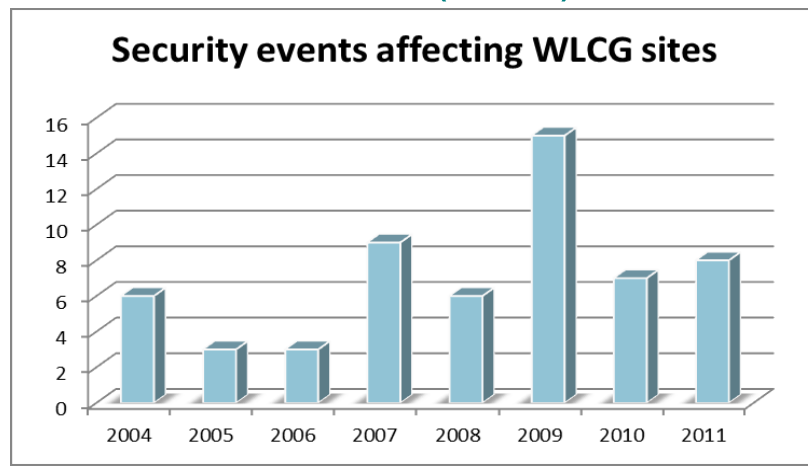


A vast attack surface

Stefan.Lueders@cern.ch — ITU SG17 Tutorials — September 5th 2012

A typical attack against the community since 2008:

- ▶ **Exploitation of vulnerable (unpatched) hosts** somewhere in the community
 - Installation of a rootkit (hidden code)
 - **Compromised account(s)**, i.e. stolen passwords, keys, certificates
- ▶ **Attack against other hosts**, also at other sites
 - SSH into other sites e.g. listed in `known_hosts` file
 - Trying for **root privilege escalation** via known vulnerabilities
 - Also checking for traditional injection techniques e.g. through `/dev/mem` or via loadable kernel modules (LKM)
 - **More compromised hosts & accounts**
- ▶ Periodic rootkit updates and new versions
- ▶ **Difficult to contain** since this requires *all* sites to be clean & patched ☹
- ▶ **Difficult to detect** (running annual Security Challenges to improve)



“Thou shall patch!”

Stefan.Lueders@cern.ch — ITU SG17 Tutorials — September 5th 2012

Critical vulnerabilities published regularly:

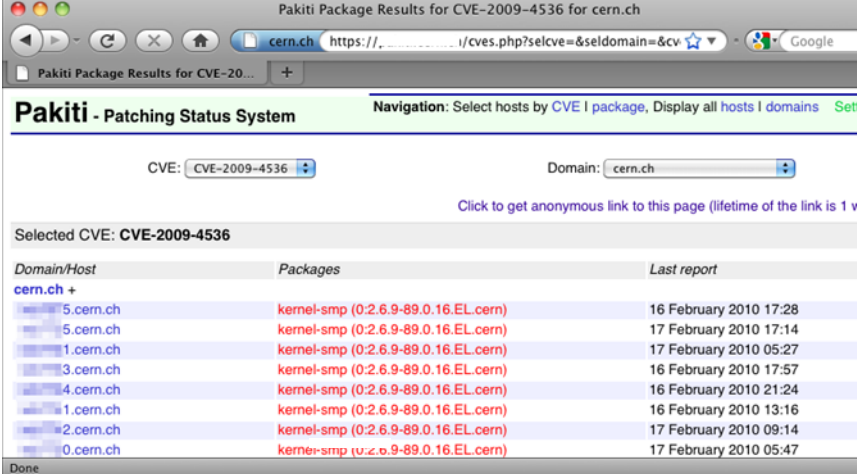
► Exploits out in the wild quickly after CVE announcement

→ Need to patch immediately

► Permanent monitoring of patching statuses

► Coordinated effort to many national CERTS and WLCG security officer to get patches applied

► Sometimes, sites have to be banned ☹️



The screenshot shows the Pakiti Patching Status System interface. It displays the CVE ID 'CVE-2009-4536' and the domain 'cern.ch'. Below this, a table lists the patching status for various hosts. The table has three columns: 'Domain/Host', 'Packages', and 'Last report'. The 'Domain/Host' column shows 'cern.ch' with a plus sign. The 'Packages' column lists 'kernel-smp (0:2.6.9-89.0.16.EL.cern)'. The 'Last report' column shows various dates and times in February 2010.

Domain/Host	Packages	Last report
cern.ch +		
5.cern.ch	kernel-smp (0:2.6.9-89.0.16.EL.cern)	16 February 2010 17:28
5.cern.ch	kernel-smp (0:2.6.9-89.0.16.EL.cern)	17 February 2010 17:14
1.cern.ch	kernel-smp (0:2.6.9-89.0.16.EL.cern)	17 February 2010 05:27
3.cern.ch	kernel-smp (0:2.6.9-89.0.16.EL.cern)	16 February 2010 17:57
4.cern.ch	kernel-smp (0:2.6.9-89.0.16.EL.cern)	16 February 2010 21:24
1.cern.ch	kernel-smp (0:2.6.9-89.0.16.EL.cern)	16 February 2010 13:16
2.cern.ch	kernel-smp (0:2.6.9-89.0.16.EL.cern)	17 February 2010 09:14
0.cern.ch	kernel-smp (0:2.6.9-89.0.16.EL.cern)	17 February 2010 05:47

<http://pakiti.sourceforge.net>

Example: CVE-2010-3081 took CERN two days to patch.

► ~60 LXPLUS nodes: kick-off & patch

► ~2800 LXBATCH nodes: drain/kill & patch

► ...and much longer for all the Linux-based control systems for the LHC

From Tier to P2P to Cloud (1)

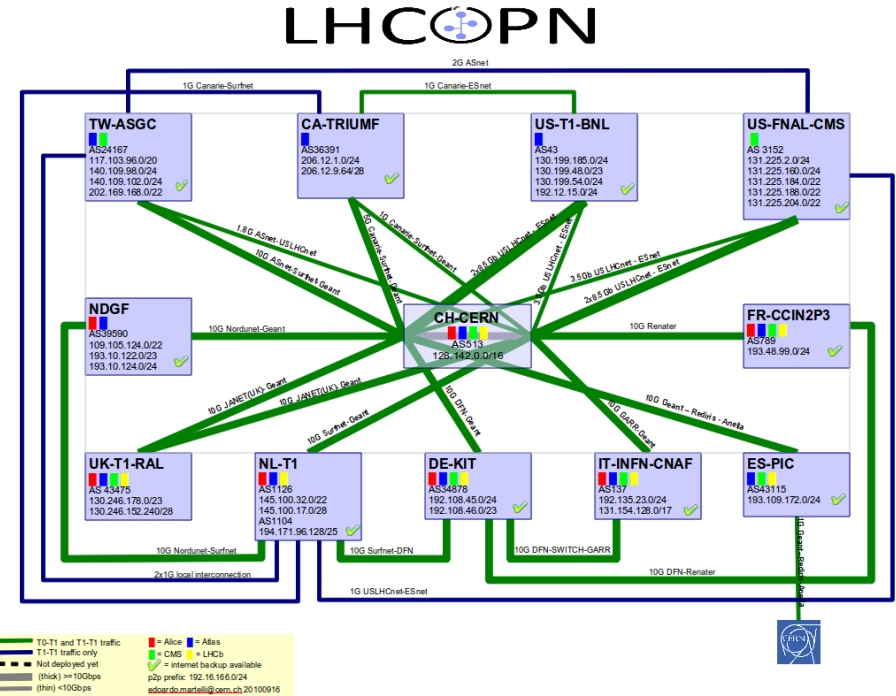
Stefan.Lueders@cern.ch — ITU SG17 Tutorials — September 5th 2012

Multi-Tier architecture today:

- ▶ 11 Tier-1s, >100 Tier-2s, ...
- ▶ ...store (some) LHC data each
- ▶ ...provide local computing services to allow physicist running their data analysis jobs
- ▶ Traffic & firewalls easy to control; #connected sites known & constant

Move to P2P:

- ▶ More centralized data storage (e.g. at CERN)
- ▶ More direct access between Tier's and to Tier-0 from Tier-2s/Tier-3s
- ▶ Increasing firewall complexity
- ▶ Frequent changes (“dynamic firewall punching”)

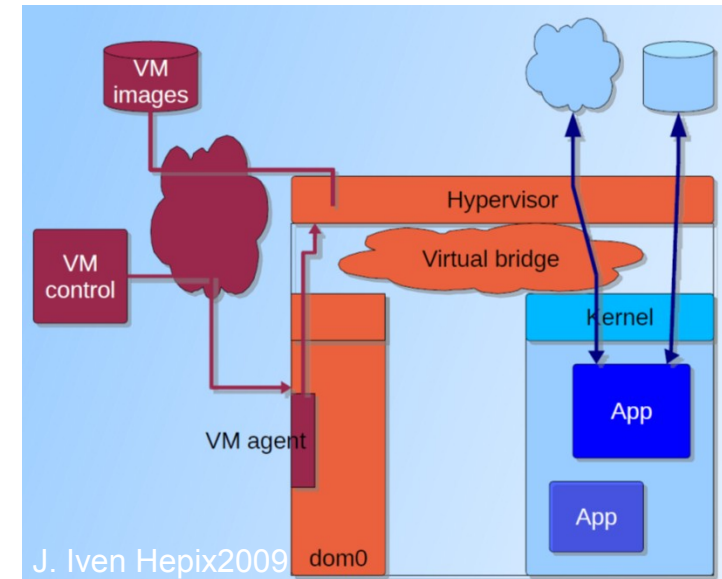


From Tier to P2P to Cloud (2)

Stefan.Lueders@cern.ch — ITU SG17 Tutorials — September 5th 2012

Move to a cloud model:

- ▶ Instead of running physics analysis jobs, submit fill-blown virtual images
- ▶ Additional abstraction layer: new code, new interfaces, new challenges
- ▶ Increasing the attack surface & enabling new attack vectors: (break out of VM, ...into hypervisor, ...into host OS, ...into other VMs)



New challenges:

- ▶ How to promptly patch / enforce patching?
- ▶ How to monitor, e.g. using a central syslog facility?
- ▶ Need for image certification, tracking, revoking & inventory
→ More stakeholders involved, more trust necessary...

From Tier to P2P to Cloud (2)

Stefan.Lueders@cern.ch — ITU SG17 Tutorials — September 5th 2012

Move to a cloud model:

- ▶ Instead of running physics analysis jobs, submit fill-blown virtual images
- ▶ Additional abstraction layer: new code, new interfaces, new challenges
- ▶ Increasing the attack surface & enabling new attack vectors (break out of VM ...into host)



Trust + collaboration are essential. Still, securing the Grid is a challenge in itself.

No



- ▶ ...patching?
- ▶ ...a central syslog facility?
- ▶ ...certification, tracking, revoking & inventory
- ▶ ...stakeholders involved, more trust necessary...



CERN's security footprint



Operational Noise



Securing the LHC Computing Grid



This is a “people” problem

CERN Security Paradigm

Stefan.Lueders@cern.ch — ITU SG17 Tutorials — September 5th 2012

Find balance between “Academic Freedom”, “Operations” and “Computer Security”

“Academic Freedom” means “Responsibility”

- ▶ (I, as Security Officer, decline to accept that responsibility)
- ▶ Instead, computer security at CERN is delegated to all users of computing resources.
- ▶ If they don't feel ready, they can pass that responsibility to the IT department using central services.

Change of culture & a new mind set:

- ▶ Enable users to fully assume this responsibility.
- ▶ Make security integral part of the overall.



Change of Culture

Stefan.Lueders@cern.ch — ITU SG17 Tutorials — September 5th 2012

Get the mind-set right:

- ▶ **Awareness raising:**
Dedicated awareness sessions,
Introduction sessions for newcomers,
Leaf sheets & posters
- ▶ Every owner of a computer account must follow an online security course every 3 yrs
- ▶ **Provisioning of static code analyzers:**
Make them hunt for the low-hanging fruits...
...and take compiler warnings seriously.
- ▶ **Dedicated training on secure development**
(Java, C/C++, Perl, Python, PHP, web, ...)
- ▶ **Baselining & consulting**

(Plus a Defense-In-Depth approach, still.)

SECURITY is not complete without U

SECURITY is not complete without U

SECURITY is not complete without U

Quelques astuces pour protéger votre ordinateur et vos données

- Utilisez les systèmes d'exploitation fournis par le département IT du CERN : ils sont configurés de manière sûre et mis à jour automatiquement pour vous.
- Protégez votre ordinateur privé : utilisez l'antivirus du CERN; appliquez les mises à jour logicielles; n'installez pas de logiciels douteux.
- Soyez prudent lorsque vous naviguez sur le Web : ne cliquez pas sur des liens suspects et n'installez pas de plug-in douteux.
- Protégez vos fichiers et données : limitez l'accès à vos documents et répertoires; appliquez le principe du droit d'accès minimal.
- Protégez vos mots de passe : ne les partagez jamais; prenez garde au phishing (technique qu'utilisent les escrocs en ligne pour voler votre mot de passe); ne les réutilisez pas (utilisez des mots de passe différents pour des applications différentes); ne les tapez pas sur des ordinateurs ou des sites Web suspects.
- Suivez les règles informatiques du CERN : respectez le droit d'auteur; n'utilisez pas de logiciels non-autorisés; consultez <http://cern.ch/ComputingRules>.
- Demandez conseil : l'équipe de sécurité informatique vous propose des cours de formation, des analyses de codes logiciels, des balayages Web ou serveur etc., et est là pour vous aider : contactez Computer.Security@cern.ch ou consultez <http://cern.ch/Computer.Security>.

Be careful with e-mail & Web

Cybercriminals are trying to trick you!

Change of Culture

Stefan.Lueders@cern.ch — ITU SG17 Tutorials — September 5th 2012

Get the mind-set right:

- ▶ **Awareness raising:**
Dedicated awareness sessions,
Introduction sessions for newcomers,
Leaf sheets & posters
- ▶ Every owner of a computer account should
follow an online security course
- ▶ **Provisioning of statistics**
Make them better
...and then



(Please use an In-Depth approach, still.)

This is a “people” problem!
A good Computer Security Team is
facilitator and enabler, less “police”!

SECURITY is not complete without U

SECURITY is not

Protégez votre ordinateur privé : utilisez l'antivirus du CERN; appliquez les mises à jour logicielles; n'installez pas de logiciels douteux.

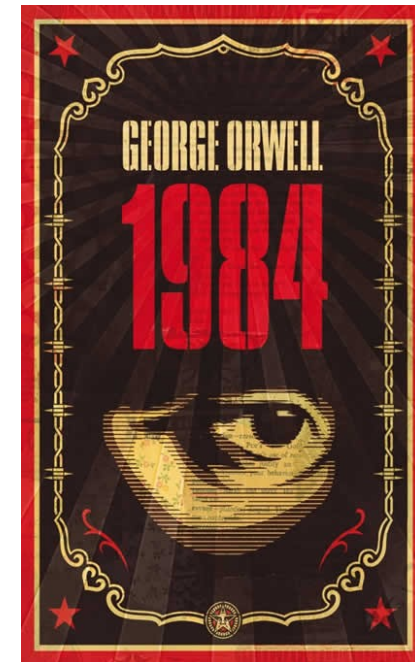
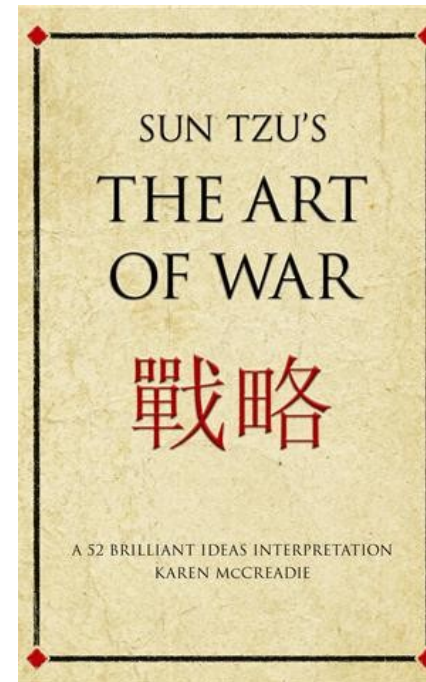
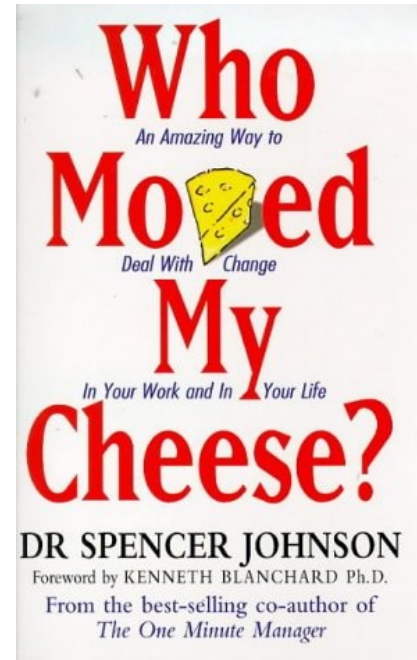
Protégez vos fichiers et données : limitez l'accès à vos documents et répertoires; appliquez le principe du droit d'accès minimal.

Suivez les règles informatiques du CERN : respectez le droit d'auteur; n'utilisez pas de logiciels non-autorisés; consultez <http://cern.ch/ComputingRules>.

Demandez conseil : l'équipe de sécurité informatique vous propose des cours de formation, des analyses de codes logiciels, des balayages Web ou serveur etc., et est là pour vous aider : contactez Computer.Security@cern.ch ou consultez <http://cern.ch/Computer.Security>.

Be careful with e-mail & Web

Cybercriminals are trying to trick you!





**CERN's Security Footprint
is heterogeneous and vast**



However, **security events** happen
and **will continue** to happen



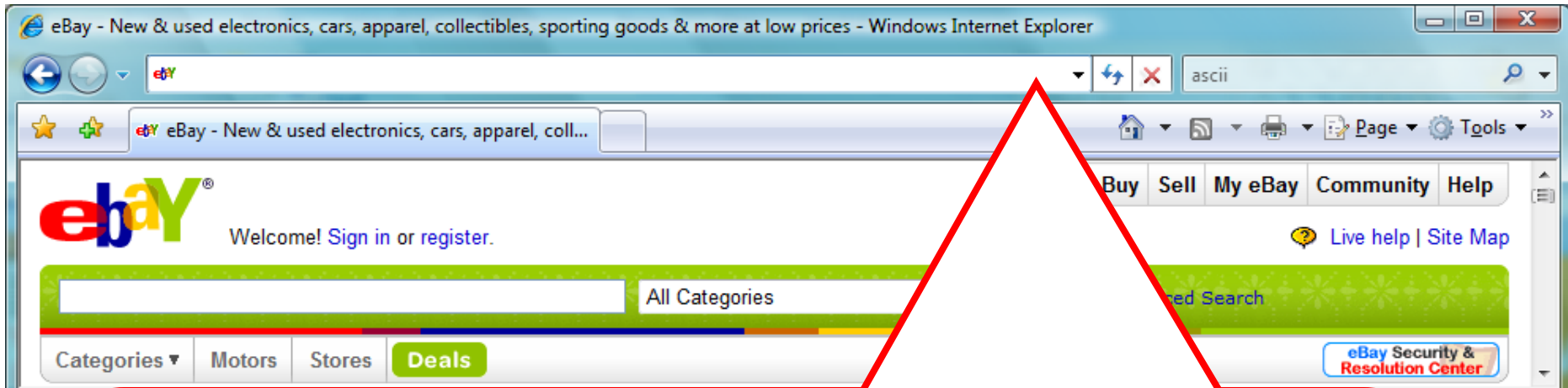
**WLCG Security:
Trust & collaboration are essential!**



**Enable users assuming responsibility.
Provoke a Change-of-Mind!!!**

A small quiz.

Stefan.Lueders@cern.ch — ITU SG17 Tutorials — September 5th 2012



Quiz: Which URL leads you to www.ebay.com ?

- ✘ <http://www.ebay.com/cgi-bin/login?ds=1%204324@%31%33%37%2e%31%33%38%2e%31%33%37%2e%31%37%37/p?uh3f223d>
- ✘ <http://www.ebay.com/ws/eBayISAPI.dll?SignIn>
- ✔ http://scgi.ebay.com/ws/eBayISAPI.dll?RegisterEnterInfo&siteid=0&co_partnerid=2&usage=0&ru=http%3A%2F%2Fwww.ebay.com&raflid=0&encRaflid=default
- ✘ <http://secure-ebay.com>