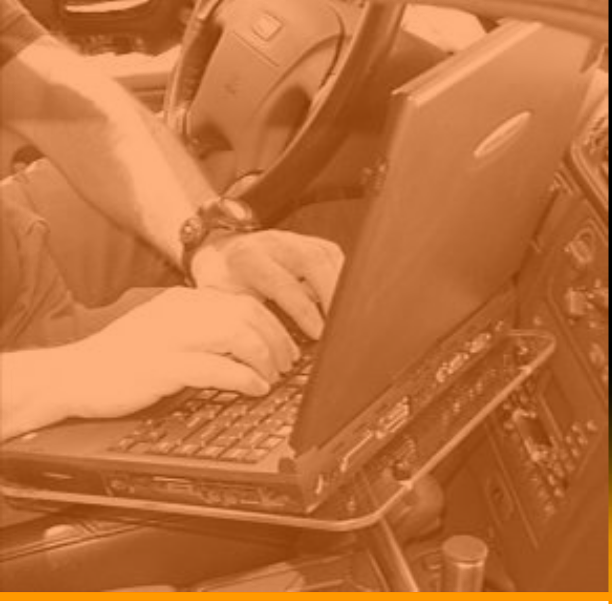


$(CS)^2$

HEP

Control System Cyber-Security Workshop

A Summary of Yesterday’s Meeting

Dr. Stefan Lüders (CERN Computer Security Officer)
with slides from B. Copy (CERN), T. McGuckin (JLab), R. Lee (BNL),
R. Petkus (BNL), T. Sugimoto (Spring8), P. Wang (FNAL)

ICALEPCS, Kobe (Japan), October 12th 2009

About Security…

Security is as good as the weakest link:

- ► Attacker chooses the time, place, method
- ► Defender needs to protect against all possible attacks (currently known, and those yet to be discovered)

Security is a system property (not a feature)

Security is a permanent process (not a product)

Security is difficult to achieve, and only to 100%-ε

- ► YOU define ε as user, developer, system expert, admin, project manager

BTW: Security is *not* a synonym for safety

(R)Evolution of Control Systems

standard desktop PCs
redhat LINUX
applicom
WinCC
TRANE
ORACLE
WAGO
SIEMENS
iseg high voltage
OPC FOUNDATION
WorldFIP
PcVue
HIRSCHMANN
WIENER
W3C
CVS
MySQL
Tektronix
LynxOS
Schneider Electric
BECKHOFF INDUSTRIE ELEKTRONIK
LeCroy
SONICMU
I²C BUS
PROFI BUS PROCESS FIELD BUS
AIR LIQUIDE
PVSS II
VMEbus Technology
NATIONAL INSTRUMENTS
Modbus-IDA
CAN
CORBA
Linde
Wizcon Systems
Microsoft
Sun microsystems

Ethernet & Wireless

Modbus/TCP, OPC & Telnet

Common of the shelf HW

Desktop PCs & Laptops

Windows & Linux

WWW & Emails

C++, Java, XML, Corba…

Oracle, Labview…

Shared Accounts & Passwords

Standard Vulnerabilities

Ethernet & Wireless
Modbus/TCP, OPC & Telnet

Common of the shelf HW
Desktop PCs & Laptops
Windows & Linux

WWW & Emails
C++, Java, XML, Corba…
Oracle, Labview…

Shared Accounts & Passwords

Vulnerabilities are Proven Fact !

Continuous load capability test

Achievements and findings

Force the Vendors on Boar

“Problems to Overcome” — Dr. Stefan Lüders — CS2/HEP Workshop — October 11th 2009

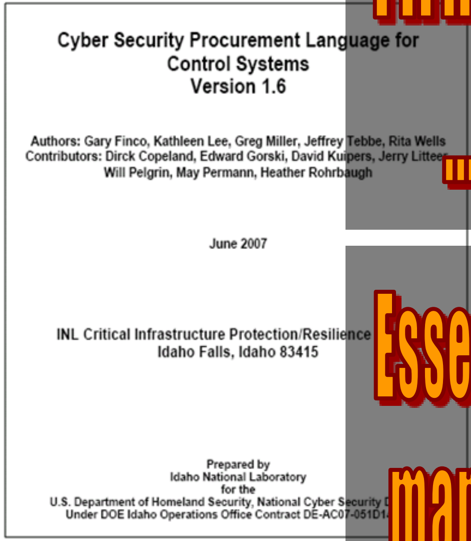
- **Manufacturers and vendors are part of the solution !**
  - Security demands must be included into orders and call for tenders

“Procurement Language” document

- *“… collective buying power to help ensure that security is integrated into SCADA systems.”*

However:

- This will increase the *visible* costs
- Who takes the responsibility ?
- Manufacturers not always prepared to handle such demands
- What if no vendor will/can deliver ?



Cyber Security Procurement Language for
Control Systems
Version 1.6

Authors: Gary Finco, Kathleen Lee, Greg Miller, Jeffrey Tebbe, Rita Wells
Contributors: Dirck Copeland, Edward Gorski, David Kuipers, Jerry Litteer,
Will Pelgrin, May Permann, Heather Rohrbaugh

June 2007

INL Critical Infrastructure Protection/Resilience
Idaho Falls, Idaho 83415

Prepared by
Idaho National Laboratory
for the
U.S. Department of Homeland Security, National Cyber Security D
Under DOE Idaho Operations Office Contract DE-AC07-051D14

http://www.msisac.org/scada

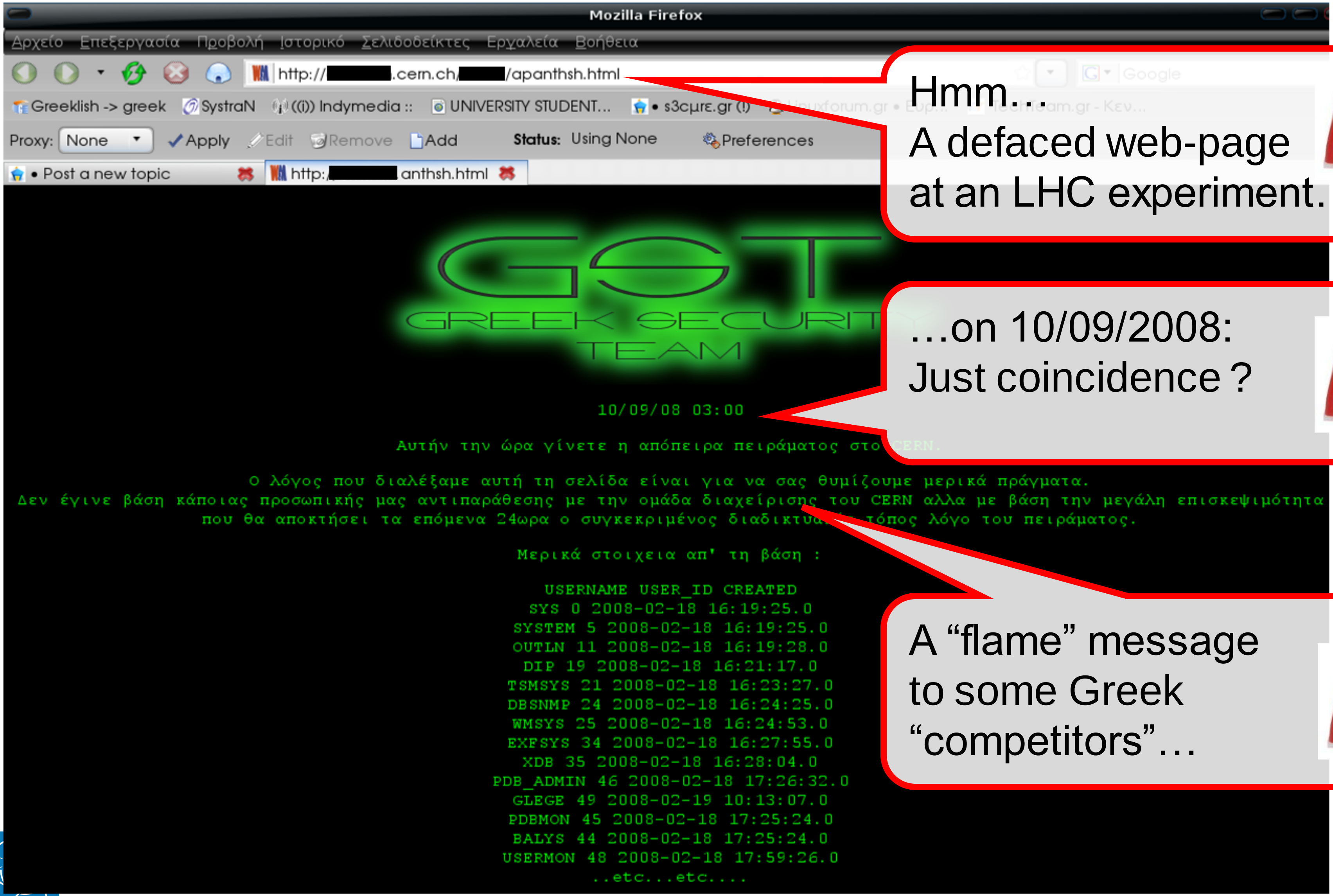
Eur

Multi-casts on Ethernet blocked controller

Firmware improves… … or does not?

Essential to convince the manufactures with $¥€

Attacks are Fact, too !!!



http://[redacted].cern.ch/[redacted]/apanthsh.html

Status: Using None

http:[redacted]anthsh.html

10/09/08 03:00

Αυτήν την ώρα γίνετε η απόπειρα πειράματος στο CERN.

Ο λόγος που διαλέξαμε αυτή τη σελίδα είναι για να σας θυμίζουμε μερικά πράγματα.
Δεν έγινε βάση κάποιας προσωπικής μας αντιπαράθεσης με την ομάδα διαχείρισης του CERN αλλα με βάση την μεγάλη επισκεψιμότητα
που θα αποκτήσει τα επόμενα 24ωρα ο συγκεκριμένος διαδικτυακός τόπος λόγο του πειράματος.

Μερικά στοιχεια απ' τη βάση :

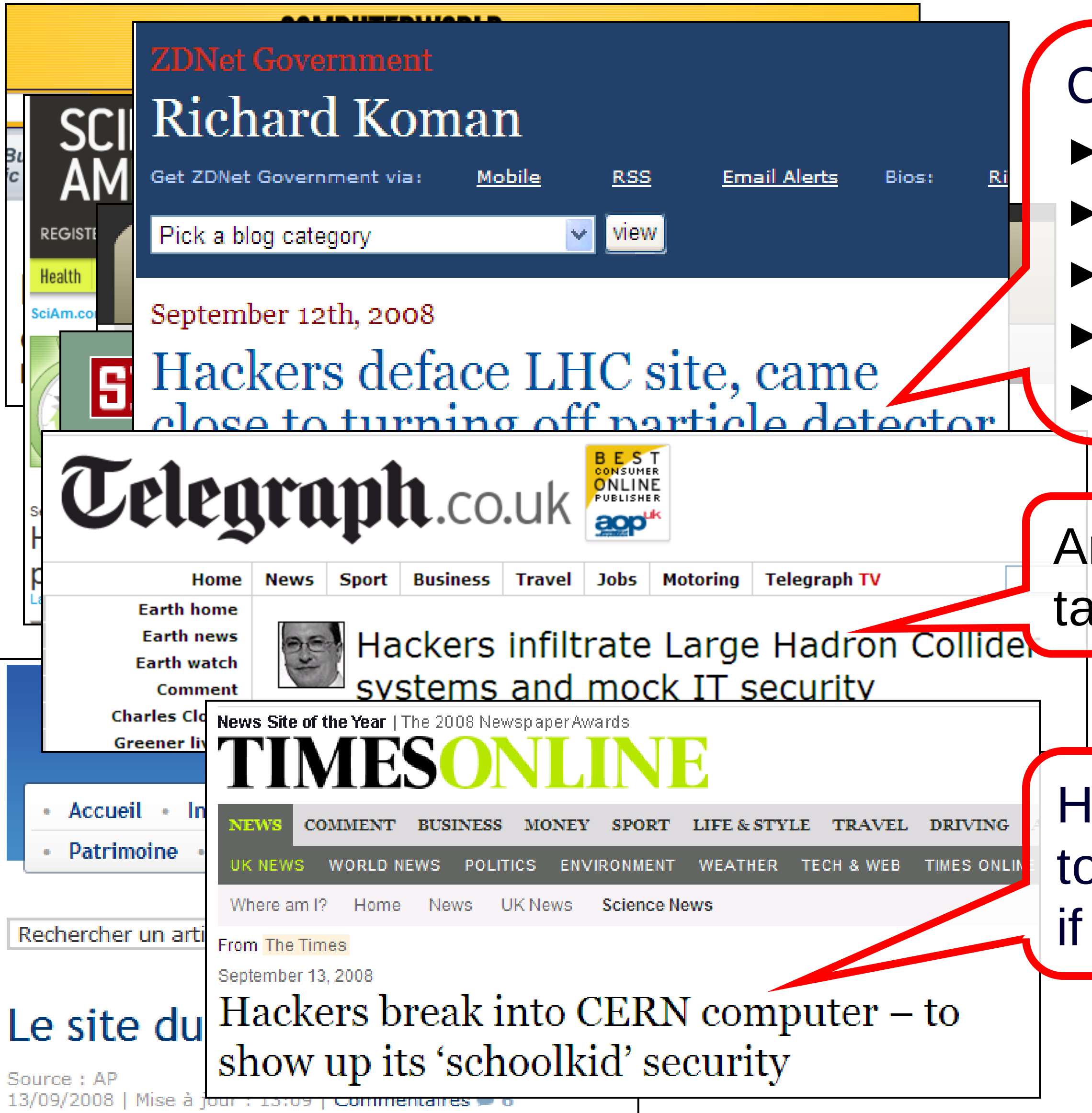
```
USERNAME USER_ID CREATED
SYS 0 2008-02-18 16:19:25.0
SYSTEM 5 2008-02-18 16:19:25.0
OUTLN 11 2008-02-18 16:19:28.0
DIP 19 2008-02-18 16:21:17.0
TSMSYS 21 2008-02-18 16:23:27.0
DBSNMP 24 2008-02-18 16:24:25.0
WMSYS 25 2008-02-18 16:24:53.0
EXFSYS 34 2008-02-18 16:27:55.0
XDB 35 2008-02-18 16:28:04.0
PDB_ADMIN 46 2008-02-18 17:26:32.0
GLEGE 49 2008-02-19 10:13:07.0
PDBMON 45 2008-02-18 17:25:24.0
BALYS 44 2008-02-18 17:25:24.0
USERMON 48 2008-02-18 17:59:26.0
..etc...etc....
```

Hmm…
A defaced web-page
at an LHC experiment…

…on 10/09/2008:
Just coincidence ?

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

Who owns the consequences ?



ZDNet Government

Richard Koman

Get ZDNet Government via: Mobile RSS Email Alerts Bios:

Pick a blog category view

September 12th, 2008

Hackers deface LHC site, came close to turning off particle detector

Telegraph.co.uk

Home News Sport Business Travel Jobs Motoring Telegraph TV

Earth home
Earth news
Earth watch
Comment

Hackers infiltrate Large Hadron Collider systems and mock IT security

News Site of the Year | The 2008 Newspaper Awards

TIMESONLINE

NEWS COMMENT BUSINESS MONEY SPORT LIFE & STYLE TRAVEL DRIVING

UK NEWS WORLD NEWS POLITICS ENVIRONMENT WEATHER TECH & WEB

Where am I? Home News UK News Science News

From The Times

September 13, 2008

Hackers break into CERN computer – to show up its ‘schoolkid’ security

Accueil
Patrimoine

Rechercher un arti

Le site du

Source : AP
13/09/2008 | Mise à jour : 13:09 | Commentaires 8

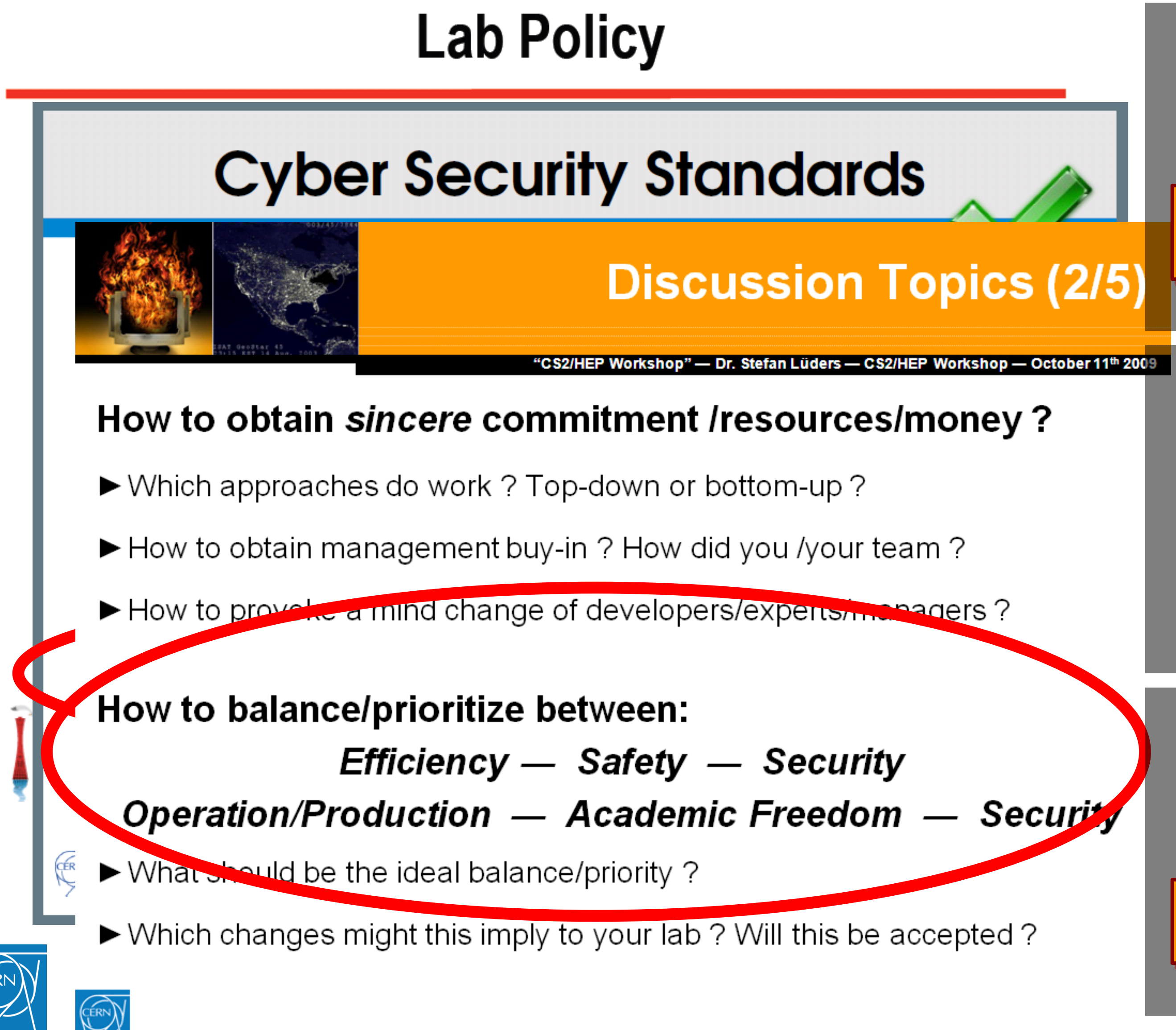
Can you allow for loss of

- functionality
- control or safety
- efficiency & beam time
- hardware or data
- reputation…?

Are you prepared to take *full* responsibility?

How long does it take you to reinstall your system, if requested *right now* ?

Bottom-up vs. Top-down



Lab Policy

Cyber Security Standards

Discussion Topics (2/5)

“CS2/HEP Workshop” — Dr. Stefan Lüders — CS2/HEP Workshop — October 11th 2009

How to obtain *sincere* commitment /resources/money ?

- ► Which approaches do work ? Top-down or bottom-up ?
- ► How to obtain management buy-in ? How did you /your team ?
- ► How to provoke a mind change of developers/experts/managers ?

How to balance/prioritize between:

Efficiency — Safety — Security

Operation/Production — Academic Freedom — Security

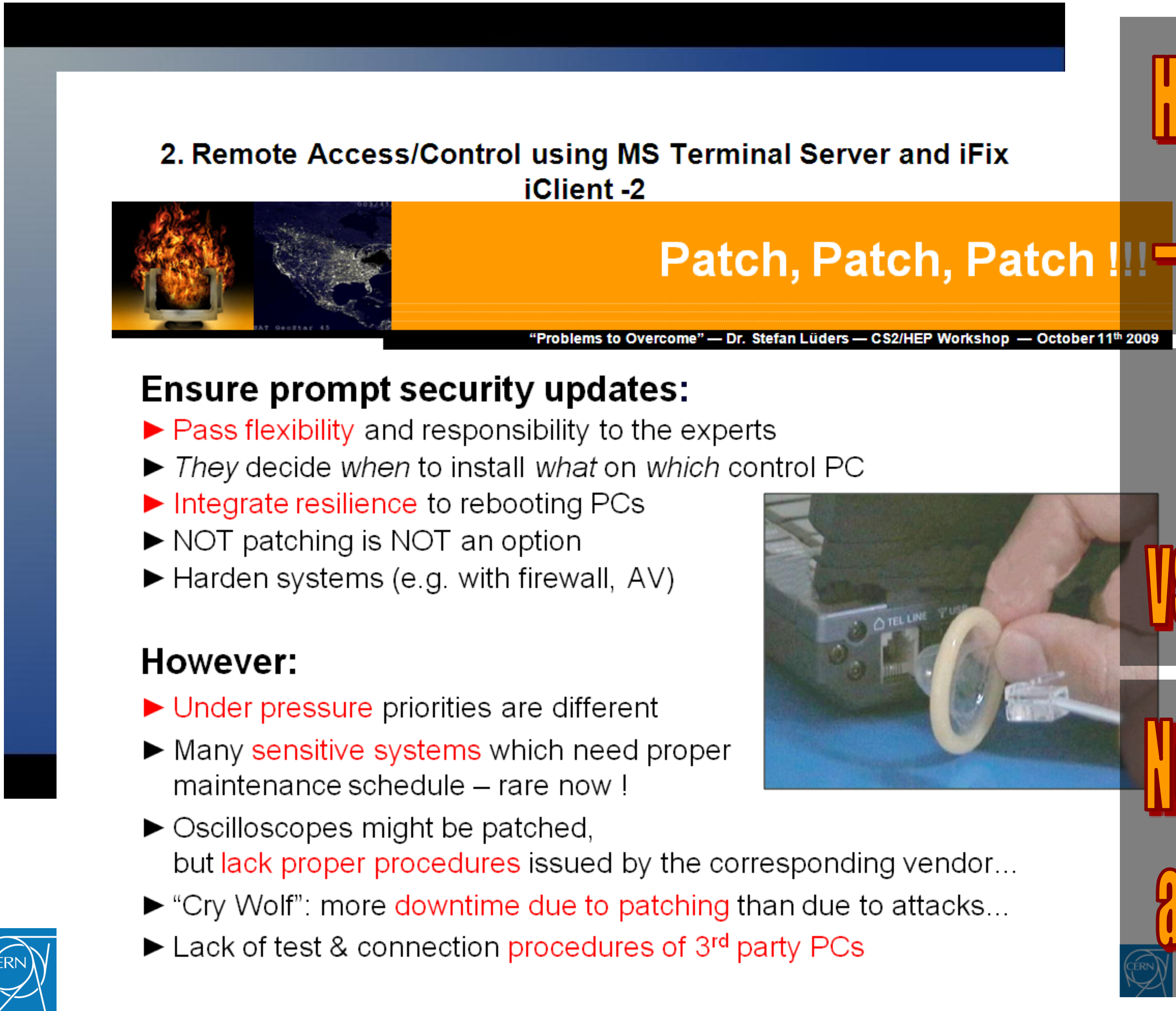
- ► What should be the ideal balance/priority ?
- ► Which changes might this imply to your lab ? Will this be accepted ?

Standards available, but who applies them ?

External orders/laws: Friend or Foe ?

How to get the balance right ?

Defense-in-Depth



2. Remote Access/Control using MS Terminal Server and iFix iClient -2

Patch, Patch, Patch !!!

“Problems to Overcome” — Dr. Stefan Lüders — CS2/HEP Workshop — October 11th 2009

Ensure prompt security updates:

- Pass flexibility and responsibility to the experts
- *They* decide *when* to install *what* on *which* control PC
- Integrate resilience to rebooting PCs
- NOT patching is NOT an option
- Harden systems (e.g. with firewall, AV)

However:

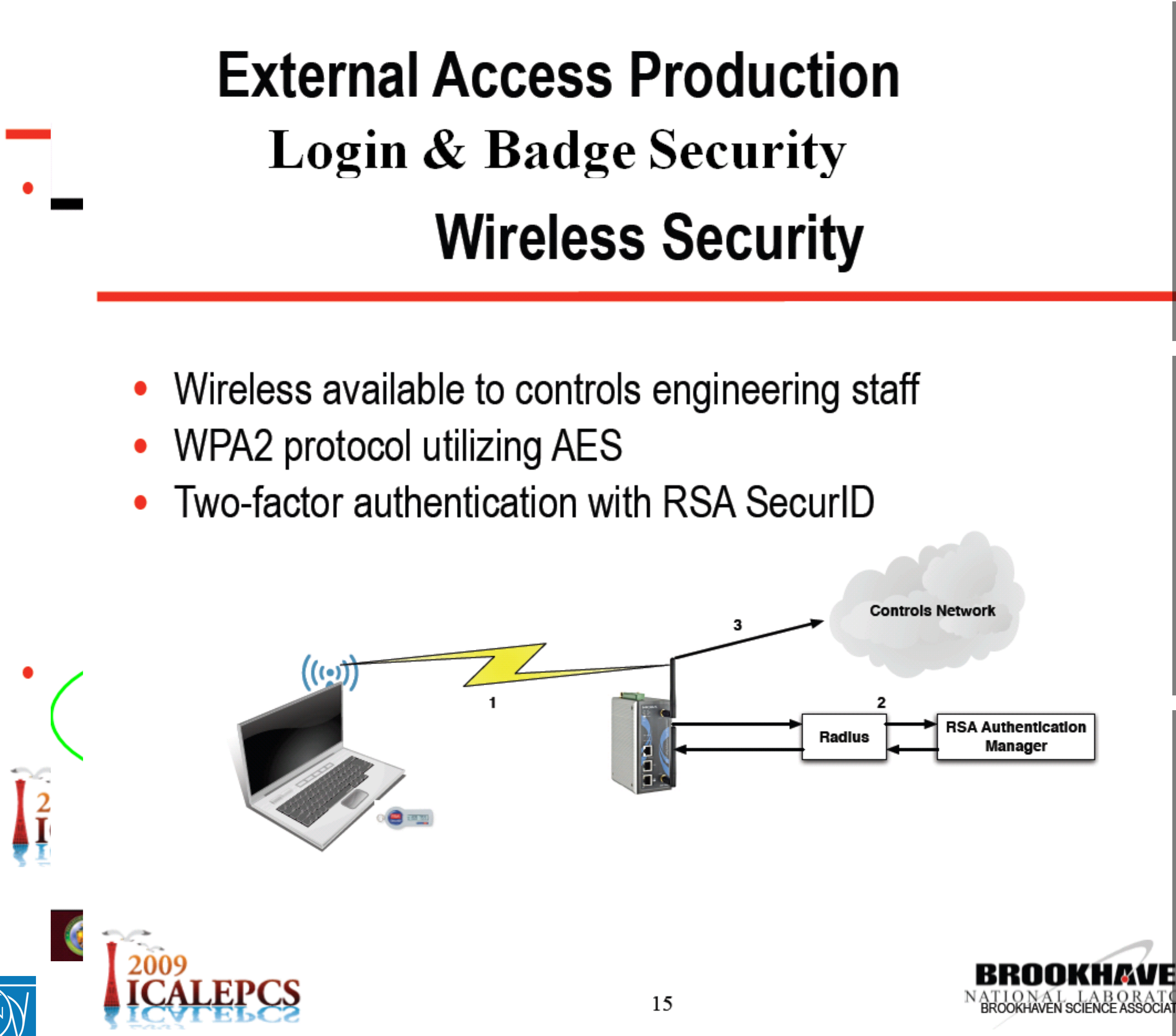
- Under pressure priorities are different
- Many sensitive systems which need proper maintenance schedule – rare now !
- Oscilloscopes might be patched, but lack proper procedures issued by the corresponding vendor…
- “Cry Wolf”: more downtime due to patching than due to attacks…
- Lack of test & connection procedures of 3rd party PCs

Harden every device – even oscilloscopes

Patch downtime vs. attack downtime

Network segregation allows buying time !

Strengthen (Remote) Access !



External Access Production

Login & Badge Security

Wireless Security

- Wireless available to controls engineering staff
- WPA2 protocol utilizing AES
- Two-factor authentication with RSA SecurID

Controls Network
3
1
2
Radius
RSA Authentication Manager

Control the gateways…

…use multi-factor authentication

Bypassed by laptops on controls network ?

Summary

The (r)evolution of control systems...

Safety – Efficiency – Security

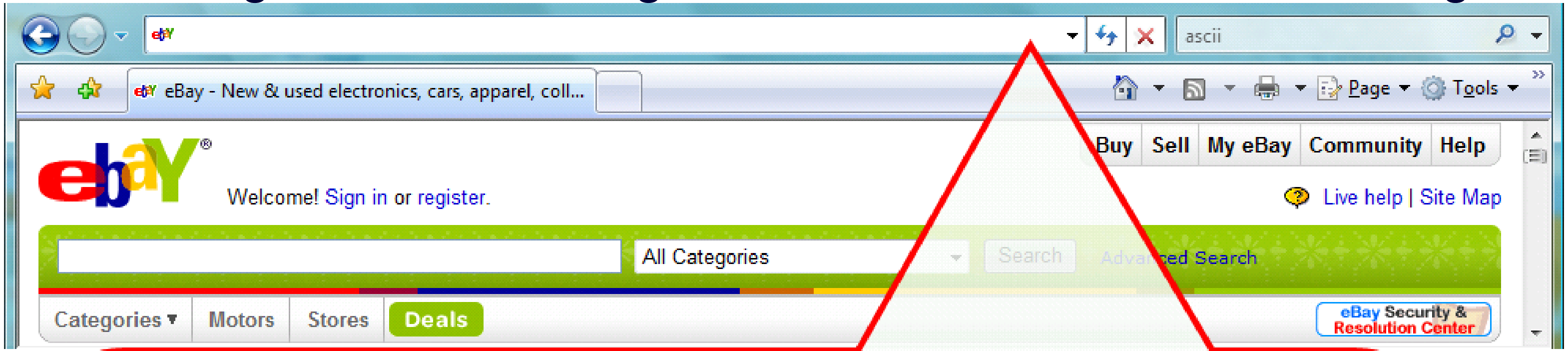
Make security priority #3 !!!

Mitigation: Defense-in-Depth

Thank You Very Much !

I would like to thank all presenters and participants, making this workshop such a success.

► Special thanks go to the local organization committee for the arrangements !!



Quiz: Which link leads 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&rafId=0&encRafId=default
- ► http://secure-ebay.com