

Control System Cyber-Security Workshop

Exchanging ideas on HEP security

Dr. Stefan Lüders (CERN Computer Security Officer)

(CS)²/HEP Workshop, Kobe (Japan)

October 11th 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

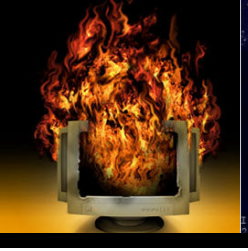
BTW: Security is *not* a synonym for safety


Overview

The (r)evolution of control systems...

...omitted security aspects!

Why worry, HEP ?




(R)Evolution of Control Systems

standard desktop PCs

applicom, WinCC, ORACLE, TRANE, WAGO, SIEMENS, iseg, WorldFIP, PcVue, HIRSCHMANN, WIENER, W3C, CVS, MySQL, Tektronix, LynxOS, SUNICMU, Schneider Electric, BECKHOFF, LeCroy, PROFI BUS, AIR LIQUIDE, PVSS II, VMEbus, NATIONAL INSTRUMENTS, Modbus-IDA, CAN, CORBA, Linde, Wizcon, 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


Why worry ?

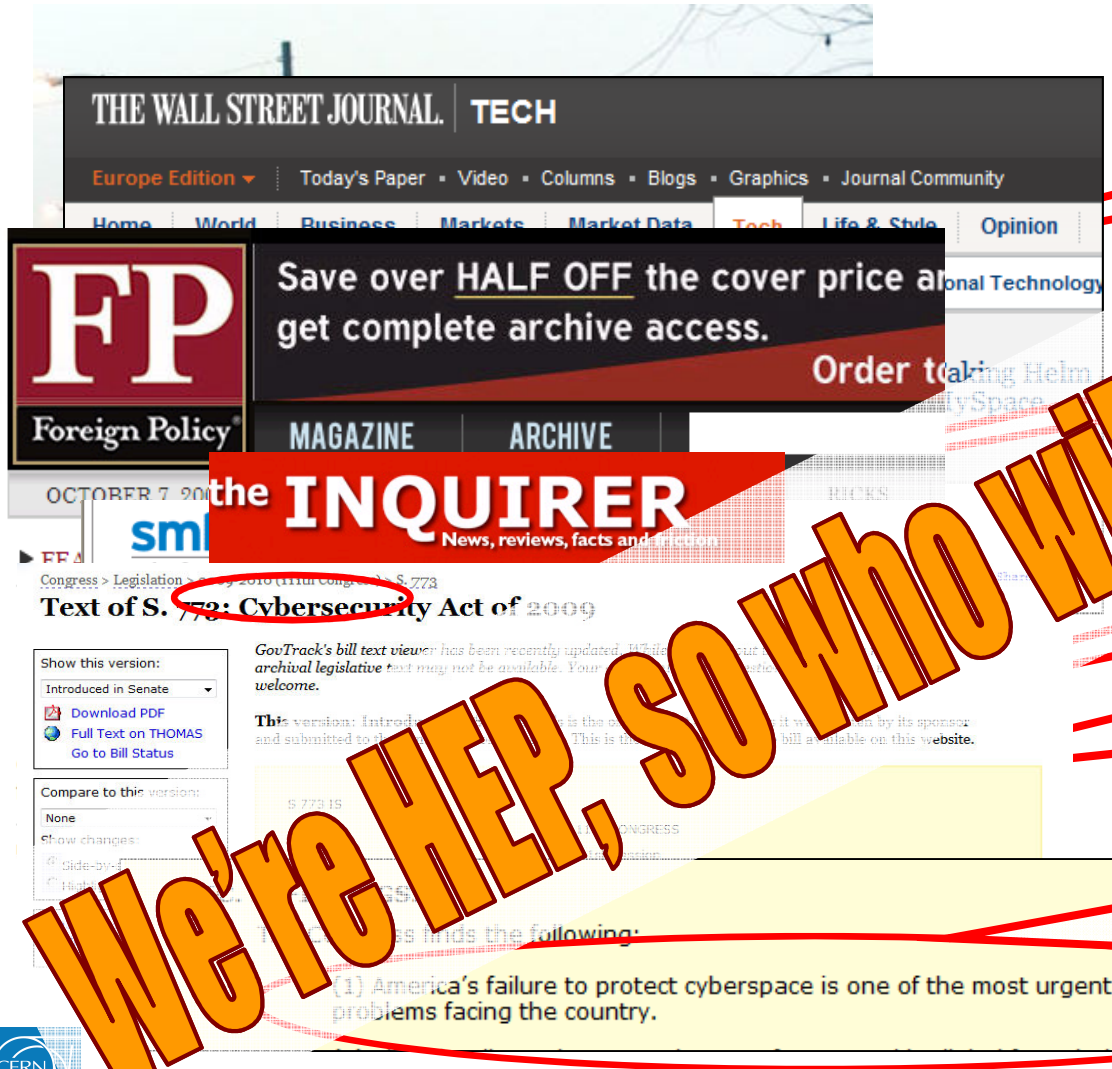

Risk =

Threat

× Vulnerability

× Consequence


Threat or *No* Threat ??



Cracked road-sign in Texas (2009)

U.S. electri… jeop…

… for real money …ugust 2009)

Malware infected PCs (October 2009)

U.S. congress faces this Wind of Change !

We're HEP, so who will attack us ?!


LHC First Beam Day

Mozilla Firefox

Αρχείο Επεξεργασία Προβολή Ιστορικό Σελιδοδείκτες Εργαλεία Βοήθεια

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

Greeklish -> greek SystraN ((i)) Indymedia :: UNIVERSITY STUDENT... • s3cure.gr (!)

Proxy: None Apply Edit Remove Add Status: Using None Preferences

• Post a new topic http:/[redacted]anthsh.html

GREEK SECURITY TEAM

10/09/08 03:00

Αυτήν την ώρα γίνετε η απόπειρα πειράματος στο

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 διαδικτυ[redacted] τόπος λόγο του πειράματος.

Μερικά στοιχεια απ' τη βάση :

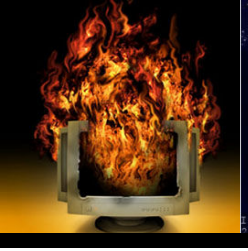
USERNAME	USER_ID	CREATED
SYS	0	2008-02-18 16:19:25.0
SYSTEM	5	2008-02-18 16:19:25.0
OUTLN	11	2008-02-18 16:19:28.0
DIP	19	2008-02-18 16:21:17.0
TSMSYS	21	2008-02-18 16:23:27.0
DBSNMP	24	2008-02-18 16:24:25.0
WMSYS	25	2008-02-18 16:24:53.0
EXFSYS	34	2008-02-18 16:27:55.0
XDB	35	2008-02-18 16:28:04.0
PDB_ADMIN	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

BEST CONSUMER ONLINE PUBLISHER aop 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 TIMES ONLIN

Where am I? Home News UK News Science News

From The Times

September 13, 2008

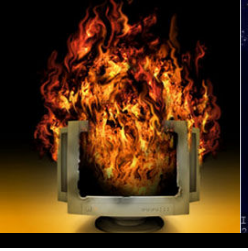
Hackers break into CERN computer – to show up its 'schoolkid' security

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* ?




$(CS)^2$ in HEP — The Agenda

Scope:

- ▶ All security aspects
- ▶ Control PCs, contr
- ▶ Planning aspects, i

Objectives:

- ▶ Raise awareness
- ▶ Exchange of good
- ▶ Discuss what work

If there arequesti

The agenda is ve

09:00	[9] **Introduction to the 2nd Control System Cyber-Security Workshop** (09:00 - 09:15)
	[5] **Standards Based Measurable Security for Embedded Devices** by Mr. Brice COPY (CERN) (09:15 - 09:45)
	Coffee Break (09:45 - 10:00)
10:00	[8] **A study of network vulnerability in embedded devices** by Takashi SUGIMOTO (Japan Synchrotron Radiation Research Institute) (10:00 - 10:30)
	[3] **Managing Proficy iFix SCADA Nodes and Client in Technical Division at Fermilab** by Mrs. Ping WANG (Fermilab/Technical Division) (10:30 - 11:00)
11:00	[11] **NSLS-II Control System Cybersecurity** by Robert PETKUS (BNL) (11:00 - 11:30)
	Lunch Break (11:30 - 12:30)
12:00	[7] **Kiosk Mode For Instruments Using Windows Platform** slides by Roger LEE (Brookhaven National Lab.) (12:30 - 13:00)
13:00	[2] **Integrated Access Control for PVSS-based SCADA Systems at CERN** by Piotr GOLONKA (CERN EN/ICE-SCD) (13:00 - 13:30)
	Coffee Break (13:30 - 13:45)
14:00	[6] **Security Design of a Computer-Based Personnel Safety System Logbook** by Theo MCGUCKIN (Jefferson Lab) (13:45 - 14:15)
	[0] **Problems to Overcome: Implementation Experience at CERN** by Dr. Stefan LUEDERS (CERN) (14:15 - 14:45)
	Coffee Break (14:45 - 15:00)
15:00	[10] **Discussion** (15:00 - 16:00)

http://indico.cern.ch/conferenceDisplay.py?confId=57050