3rd Control System Cyber-Security Workshop

Exchanging ideas on HEP security

Dr. Stefan Lüders (CERN Computer Security Officer)

3rd (CS)²/HEP Workshop, Grenoble (France)

October 9th, 2011



Year 1 after Stuxnet

3rd Control System Cyber-Security Workshop

Exchanging ideas on HEP security

Dr. Stefan Lüders (CERN Computer Security Officer)

3rd (CS)²/HEP Workshop, Grenoble (France)

October 9th, 2011


Security in a Nutshell

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)

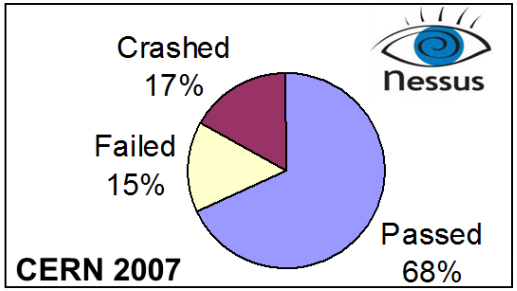
Security cannot be proven (phase-space-problem)

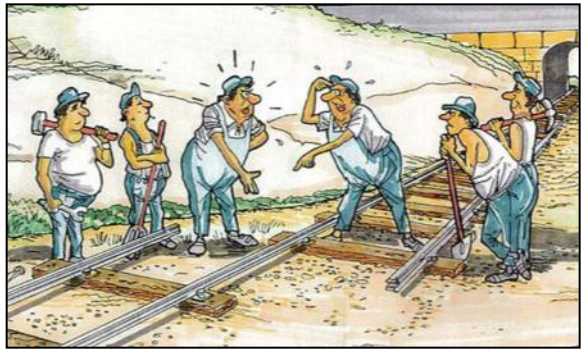
Security is difficult to achieve, and only to 100%-ε.

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

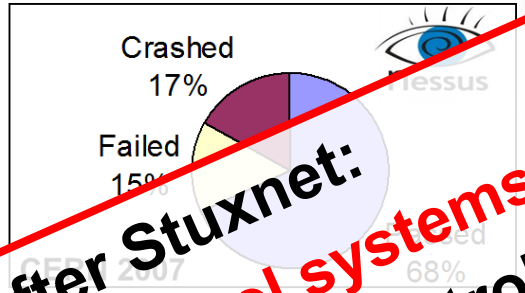
BTW:
Security is *not* a synonym for safety.


(R)Evolution, all over again!!!!



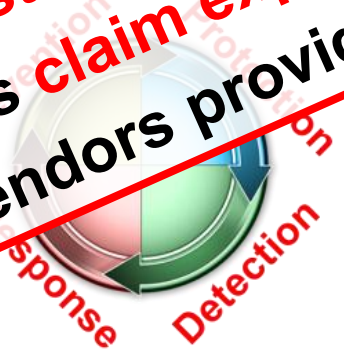


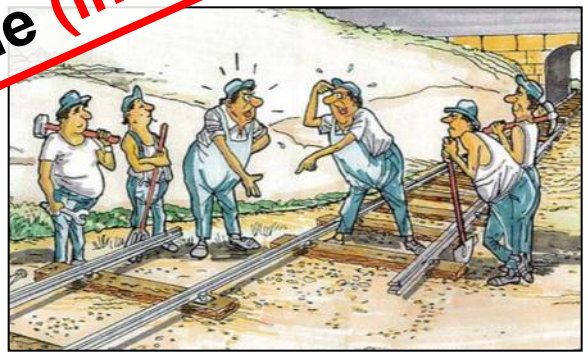

(R)Evolution, all over again!!!!



In the wake/hype/rush/panic… after Stuxnet:

- **Attackers and analysts turn to control systems**
- **Security companies claim expertise in control systems**
- **Control system vendors provide (immature) solutions**






The Bad Example: Smart Meters

Use case:

- Measuring your consumption at home
- Online with the grid: Optimizing the power usage
- Publicly accessible, off-the-shelf, open networks

Risks:

- Exploitation of meter vulnerabilities: registration process, firmware, data, …
- Loss of confidentiality: customer data available to others
- Loss of integrity: manipulation of reading data
- Loss of availability: data not available in a timely manner
- Misuse as attack platform


Power Grid Is Found Susceptible to Cyberattack

PCWorld

Robert McMillan, IDG News Service

Saturday, March 21, 2009 12:10 PM PDT

An emerging network of intelligent power switches, called the Smart Grid, could be taken down by a cyberattack, according to researchers with IOActive, a Seattle security consultancy.

IOActive researchers have spent the past year testing Smart Grid devices for security vulnerabilities and have discovered a number of flaws that could

PEOPLE WH
ALSO READ

courtesy of M. Tritschler (KEMA)

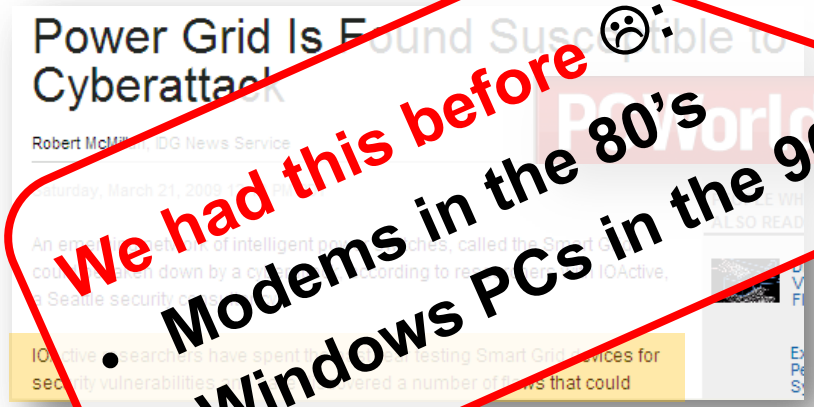

The Bad Example: Smart Meters

Use case:

- Measuring your consumption at h
- Online with the grid: Optimi
- Publicly accessible, off-th

Risks:

- Exploitation of meter
  (e.g. Windows XP < SP2)
- Loss of privacy:
  customer data available to others
- Loss of integrity:
  manipulation of reading data
- Loss of availability:
  data not available in a timely manner
- Misuse as attack platform


Power Grid Is Found Susceptible to Cyberattack

Robert McMillan, IDG News Service

PCWorld

...and can do better!!

We had this before ☹:

- Modems in the 80's
- Windows PCs in the 90's (b

courtesy of M. Tritschler (KEMA)


$(CS)^2$ in HEP — The Objectives

Scope:

- All security aspects related with HEP control systems
- Control PCs, control software, controls devices, accounts, …
- Planning aspects, implementation aspects, operational aspects, …

Objectives:

- Raise awareness
- Exchange of good practices, ideas, and implementations
- Discuss what works & what not, pros & cons
- Report on security events, lessons learned & successes
- Update on the progress made since the last workshop

If there are questions, feel free to ask at anytime!!!

The agenda is very flexible to accommodate any changes !


(CS)² in HEP — The Agenda

	How things go wrong.	*LUEDERS, Stefan*
	Kilimandjaro Nord, WTC Convention Center, Grenoble (France)	09:45 - 10:00
10:00	**Review of a cyber-security event at Jefferson Lab accelerator network**	*MCGUCKIN, Theo*
	Kilimandjaro Nord, WTC Convention Center, Grenoble (France)	10:00 - 10:30
	Coffee Break	
	Kilimandjaro Nord, WTC Convention Center, Grenoble (France)	10:30 - 10:45
	Cybersecurity for the Control System Engineer	*HARTMAN, Steven*
11:00	*Kilimandjaro Nord, WTC Convention Center, Grenoble (France)*	10:45 - 11:15
	Experiences with ISO/IEC 27001 Implementation at NSCL	*VUPPALA, Vasu*
	Kilimandjaro Nord, WTC Convention Center, Grenoble (France)	11:15 - 11:45
	Inventory and Risk assessment of the CERN Technical Network	*CHARRUE, Pierre*
12:00	*Kilimandjaro Nord, WTC Convention Center, Grenoble (France)*	11:45 - 12:15
	Can off-the-shelf control systems be compliant with CERN computer security policy?	*HAKULINEN, Timo*
	Lunch Break	
13:00	*Kilimandjaro Nord, WTC Convention Center, Grenoble (France)*	12:45 - 13:30
	Cyber security from the ALICE user's perspective	*CHOCHULA, Peter*
	Kilimandjaro Nord, WTC Convention Center, Grenoble (France)	13:30 - 14:00
14:00	**IT security for the LHCb Experiment**	*BONACCORSI, Enrico*
	Kilimandjaro Nord, WTC Convention Center, Grenoble (France)	14:00 - 14:30
	Application and Virus Detecting Firewall on the SPring-8 Experimental User Network	*SUGIMOTO, Takashi*
15:00	**Industrial Devices Robustness Assessment and Testing against Cyber Security Attacks**	*TILARO, Filippo*
	Coffee Break	
	Kilimandjaro Nord, WTC Convention Center, Grenoble (France)	15:30 - 15:45
	Discussion	*LUEDERS, Stefan*
16:00	*Kilimandjaro Nord, WTC Convention Center, Grenoble (France)*	15:45 - 16:30

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


(CS)² in HEP — The Agenda

	How things go wrong.	*LUEDERS, Stefan*	
	Kilimandjaro Nord, WTC Convention Center, Grenoble (France)		09:45 - 10:00
10:00	**Review of a cyber-security event at Jefferson Lab accelerator network**	*MCGUCKIN, Theo*	
	Kilimandjaro Nord, WTC Convention Center, Grenoble (France)		10:00 - 10:30
	Coffee Break		
	Kilimandjaro Nord, WTC Convention Center, Grenoble (France)		10:30 - 10:45
	Cybersecurity for the Control System Engineer	*HARTMAN, Steven*	
11:00	*Kilimandjaro Nord, WTC Convention Center, Grenoble (France)*		10:45 - 11:15
	Experiences with ISO/IEC 27001 Implementation at NSCL	*VUPPALA, Vasu*	
	Kilimandjaro Nord, WTC Convention Center, Grenoble (France)		11:15 - 11:45
	Inventory and Risk assessment of the CERN Technical Network	*CHARRUE, Pie*	
12:00	*Kilimandjaro Nord, WTC Convention Center, Grenoble (France)*		11:45 - 12:15
	Can off-the-shelf control systems be compliant with CERN computer security policy?	*HAVIND, Jo*	
	Lunch Break		
13:00	*Kilimandjaro Nord, WTC Convention Center, Grenoble (France)*		12:45 - 13:30
	Cyber security from the ALICE user's perspective	*CHOCHULA, Peter*	
	Kilimandjaro Nord, WTC Convention Center, Grenoble (France)		13:30 - 14:00
14:00	**IT security for the LHCb Experiment**	*BONACCORSI, Enrico*	
	Kilimandjaro Nord, WTC Convention Center, Grenoble (France)		14:00 - 14:30
	Application and Virus Detecting Firewall on the SPring-8 Experimental User Network	*SUGIMOTO, Takashi*	
15:00	**Industrial Devices Robustness Assessment and Testing against Cyber Security Attacks**	*TILARO, Filippo*	
	Coffee Break		
	Kilimandjaro Nord, WTC Convention Center, Grenoble (France)		15:30 - 15:45
	Discussion	*LUEDERS, Stefan*	
16:00	*Kilimandjaro Nord, WTC Convention Center, Grenoble (France)*		15:45 - 16:30

Enjoy!

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