Securing Control Systems against Cyber-Attacks

About becoming aware, not ignorant nor paranoid

Dr. Stefan Lüders (CERN Computer Security Team)
PAC 2009, Vancouver, Canada
May 6th 2009
Security is as high 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%-\(\varepsilon\)
- YOU define \(\varepsilon\) as user, developer, system expert, admin, project manager

BTW: Security is not a synonym for safety
The (r)evolution of control systems...

...omitted security aspects!

Why worry, HEP?

Mitigation: Defense-in-Depth
(R)Evolution of Control Systems

Ethernet & Wireless
Modbus/TCP, OPC & Telnet

“Securing Control Systems against Cyber-Attacks” — Dr. Stefan Lüders — PAC2009 — May 6th 2009
(R)Evolution of Control Systems

“Securing Control Systems against Cyber-Attacks” — Dr. Stefan Lüders — PAC2009 — May 6th 2009

Ethernet & Wireless
Modbus/TCP, OPC & Telnet
Common of the shelf HW
Desktop PCs & Laptops
Windows & Linux
(R)Evolution of Control Systems

Ethernet & Wireless
Modbus/TCP, OPC & Telnet
Common of the shelf HW
Desktop PCs & Laptops
Windows & Linux
WWW & Emails
C++, Java, XML, Corba...
Oracle, Labview...
(R)Evolution of Control Systems

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

“Securing Control Systems against Cyber-Attacks” — Dr. Stefan Lüders — PAC2009 — May 6th 2009
Standard Vulnerabilities

"Securing Control Systems against Cyber-Attacks" — Dr. Stefan Lüders — PAC2009 — May 6th 2009

Ethernet & Wireless
Modbus/TCP, OPC & Telnet
Ethernet & Wireless
Modbus/TCP, OPC & Telnet
Common of the shelf HW
Desktop PCs & Laptops
Windows & Linux
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...
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
Risk = Threat × Vulnerability × Consequence
W32.Blaster.Worm out three days earlier

Cracked road-sign
Threat or No Threat?!

“Securing Control Systems against Cyber-Attacks” — Dr. Stefan Lüders — PAC2009 — May 6th 2009

*W32.Blaster.Worm out three days earlier*

*Cracked road-sign*

*U.S. electrical grid in jeopardy (April 2009)*

*The Wall Street Journal* | TECH

*Top Stories in Technology*

*Best Buy Expands Private-Label Brands*

*Taking Helm MySpace*

*Electricity Grid in U.S. Penetrated By Spies*
W32.Blaster.Worm out three days earlier

Cracked road-sign

U.S. electrical grid in jeopardy (April 2009)

U.S. congress faces this Wind of Change!

SEC. 2. FINDINGS.
The Congress finds the following:

(1) America’s failure to protect cyberspace is one of the most urgent national security problems facing the country.
Securing Control Systems against Cyber-Attacks — Dr. Stefan Lüders — PAC2009 — May 6th 2009

Threat or No Threat?!

W32.Blaster.Worm out three days earlier

Cracked: A US critical grid in jeopardy (April 2009)

THE WALL STREET JOURNAL | TECH

U.S. congress faces this Wind of Change!

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

Can you allow for loss of:
- functionality
- control or safety
- efficiency & beam time
- hardware or data
- reputation...?
Who owns the consequences?

Can you allow for loss of:
- functionality
- control or safety
- efficiency & beam time
- hardware or data
- reputation...?
Who owns the consequences?

Can you allow for loss of:
- functionality
- control or safety
- efficiency & beam time
- hardware or data
- reputation...?

Are you prepared to take full responsibility?
Defense-in-Depth

“Securing Control Systems against Cyber-Attacks” — Dr. Stefan Lüders — PAC2009 — May 6th 2009

Devices & Hardware

Firmware & Operating Systems
(Network-) Protocols

Software & Applications
Third party applications

Operators & User Developers & System Experts
Deploy **different networks** for different purposes:

- for operations with sub-nets for different functions
- for development and basic testing
- for beam-lines & experiments
- Campus network for office computing

Restrict their usage:

- Assign responsibilities and deploy authorization procedures
- Drop Internet connectivity, (GPRS) modems, wireless access points
- Control inter-communication between networks
- Block laptops, email & control web pages
- Control remote access
- Deploy traffic monitoring & Intrusion Detection Systems
220-<><><><>==< Haxed by A|0n3 >=<><><><>
220-  ,ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°
220- /
220- Welcome to this fine str0
220- Today is: Thursday 12 January, 2006
220- Current throughput: 0.000 Kb/sec
220- Space For Rent: 5858.57 Mb
220- Running: 0 days, 10 hours, 31 min. and 31 sec.
220- Users Connected : 1 Total : 15
220- ^ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°ο°
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

Deploy protective measures:
- Local firewalls
- Anti-virus software & updated signature files
- Control remotely accessible folders

Linux or Macs are not more secure:
- Trend towards application-based attacks (e.g. Adobe Reader, Firefox)
- Trend towards web-based attacks (e.g. web browser plug-ins)
Follow “Rule of Least Privilege”:

- Restrict all access to minimum
- Ensure traceability (who, when, and from where)
- Keep passwords secret

...for all assets:

- Control PCs & operating systems
- SCADA applications & user interfaces
- Procedures, documentation, etc.

“Role Based Access Control” for op’s:

- Avoid “shared” accounts
- Multi-factor authentication for critical assets
- Full control for the shift leader of operations
PLCs and other controls devices are completely unprotected:
► No firewall, no anti-virus, nothing
Review procedures for

- development of hardware & applications
- system testing
- deployment
- operations
- maintenance & bug fixing
- Use software versioning systems, configuration management, and integration frameworks (CVS, SVN, Git)

Protect operations

- Keep development separated from operations (eventually debugging might need access to full accelerator hardware)
Make security an objective
▶ Get management buy-in (security has a cost – successful attacks, too)
▶ Produce “Security Policy for Controls”
▶ Follow the basic standards of Industry

Bring together control & IT experts:
▶ Control system experts know their systems by heart – but IT concepts?
▶ IT people often don’t know controls – but IT security they do
▶ Win mutual trust
▶ Gain synergy effects

Train users and raise awareness
The (r)evolution of control systems...
...omitted security aspects!
Do you want to act **BEFORE** or **AFTER** the incident?