

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


Preamble

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%-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 ?

Mitigation: Defense-in-Depth

(R)Evolution of Control Systems

Ethernet & Wireless
Modbus/TCP, OPC & Telnet

(R)Evolution of Control Systems

Ethernet & Wireless
Modbus/TCP, OPC & Telnet

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

(R)Evolution of Control Systems

standard desktop PCs

applicom, WinCC, ORACLE, TRANE, WAGO, redhat, SIEMENS, iseg, OPC FOUNDATION, WorldFIP, PcVue, HIRSCHMANN, WIENER, W3C, CVS, MySQL, Tektronix, LynxOS, SUNICMU, Schneider Electric, BECKHOFF, INDUSTRIE ELEKTRONIK, LeCroy, PROFI BUS, AIR LIQUIDE, PVSS II, Modbus-IDA, VMEbus, NATIONAL INSTRUMENTS, 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...

(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




Standard Vulnerabilities

Ethernet & Wireless
Modbus/TCP, OPC & Telnet




Standard Vulnerabilities

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


Why worry ?




Risk =

Threat

× Vulnerability

× Consequence

Threat or No Threat ?!

W32.Blaster.Worm
out three days earlier

Cracked road-sign

Threat or No Threat ?!

W32.Blaster.Worm
out three days earlier

Cracked road-sign

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

Threat or No Threat ?!

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 !

THE WALL STREET JOURNAL. | TECH

Europe Edition | Today's Paper · Video · Columns · Blogs · Graphics · Journal Community

Home | World | Business | Markets | Market Data | Tech | Life & Style | Opinion

Congress > Legislation > 2009-2010 (111th Congress) > S. 773

ShareThis

Text of S. 773: Cybersecurity Act of 2009

Show this version:
Introduced in Senate
Download PDF
Full Text on THOMAS
Go to Bill Status

Compare to this version:

GovTrack's bill text viewer has been recently updated. While we work out the kinks in the new viewer, archival legislative text may not be available. Your comments and suggestions for the new viewer are welcome.

This version: Introduced in Senate. This is the original text of the bill as it was written by its sponsor and submitted to the Senate for consideration. This is the latest version of the bill available on this website.

S 773 IS

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.

IN THE SENATE OF THE UNITED STATES

Threat or No Threat ?!

W32.Blaster.Worm
out three days earlie

Cracked

al grid in
dy (April 2009)

U.S. congress faces
this Wind of Change !

THE WALL STREET JOURNAL. | TECH

Europe Edition | Today's Paper · Video · Columns · Blogs

Home World Business Markets

Congress > Legislation > 2009-2010 (111th Congress) > S. 773

Text of S. 773: Cybersecurity Act of 20

Show this version:
Introduced in Senate
Download PDF
Full Text on THOMAS
Go to Bill Status

GovTracker's bill viewer, architecture are

This was written by its sponsor and the bill available on this website.

ailure to protect cyberspace is one of the most urgent national security
ems facing the country.

IN THE SENATE OF THE UNITED STATES

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 [redacted]

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 διαδικτυα[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

Posted by Richard Koman @ September 12, 2008 @ 8:35 AM

heise online

LE FIGARO·fr

Accueil · International · Politique · Economie · Patrimoine · Emploi · Sciences · Culture · Impô

Rechercher un article

Le site du Cern piraté

Source : AP

13/09/2008 | Mise à jour : 13:09 | Commentaires 6

Leserforum

des neuen Teilchenbeschleuniger

TELEPOLIS « Vorige | Nä

chleunigers gehackt

Can you allow for loss of

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

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

Posted by Richard Koman @ September 12, 2008 @ 8:35 AM

heise online

LE FIGARO·fr

Accueil · International · Politique · Economie · Patrimoine · Emploi · Sciences · Culture · Impô

Rechercher un article

Le site du Cern piraté

Source : AP

13/09/2008 | Mise à jour : 13:09 | Commentaires 6

Leserforum

des neuen Teilchenbeschleuniger

TELEPOLIS « Vorige | Nä

chleunigers gehackt

Can you allow for loss of

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

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

Can you allow for loss of

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

Telegraph.co.uk

BEST CONSUMER ONLINE PUBLISHER aop

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

Are you prepared to take *full* responsibility?

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 ONLINE

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 • In
• Patrimoine

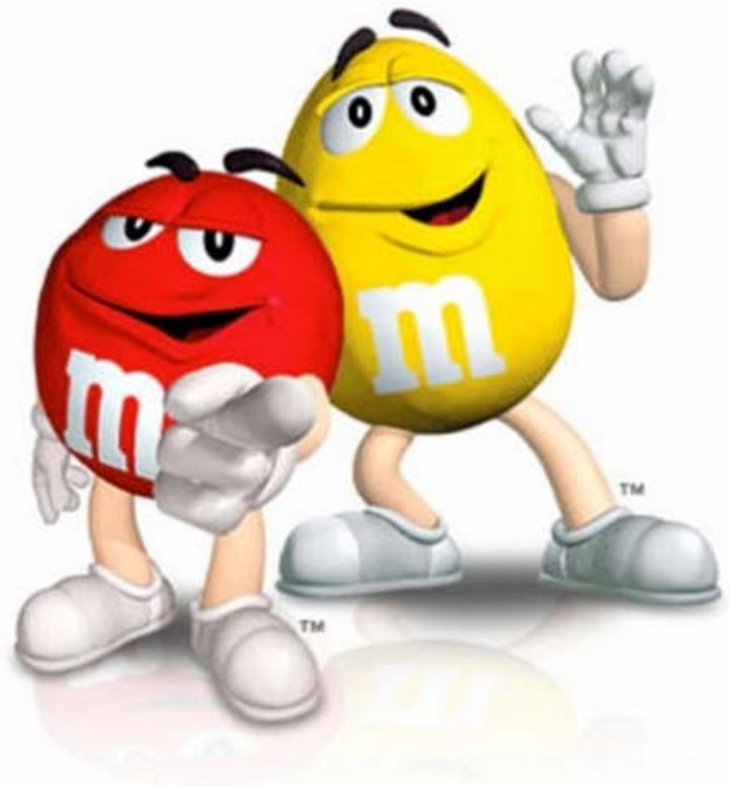
Rechercher un arti

Le site du

Source : AP
13/09/2008 | Mise à jour : 15:09 | Commentaires 6


Defense-in-Depth






Defense-in-Depth



Devices & Hardware

Firmware & Operating Systems
(Network-) Protocols

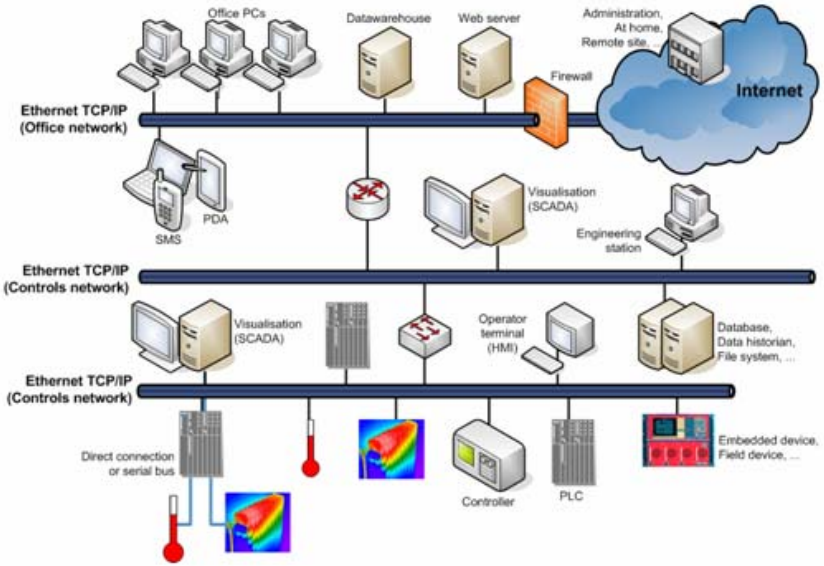
Software & Applications
Third party applications

Operators & User
Developers & System Experts


Separate Networks

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

Patch, Patch, Patch !!!

Hacked oscilloscope at CERN
(running Win XP SP2 unpatched)

```
220-<<<<<<>==< Haxed by A|0n3 >==<>>>>>>
220-  ,,øø°°^°°øø,,,,øø°°^°°øø,,,,øø°°^°°øø,,,,øø°°^°°øø,,
220-/
220-|     Welcome  to this fine str0
220-|     Today is: Thursday 12 January, 2006
220-|
220-|     Current througput: 0.000 Kb/sec
220-|     Space For Rent: 5858.57 Mb
220-|
220-|     Running: 0 days, 10 hours, 31 min. and 31 sec.
220-|     Users Connected : 1 Total : 15
220-|
220^°°øø,,,,øø°°^°°øø,,,,øø°°^°°øø,,,,øø°°^°°øø,,,,øø°°^
```


Patch, Patch, Patch !!!

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)


Control (Remote) Access

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.

```
// If same day then simple querie

if ((StartDay == $EndDay)&& ($StartMonth == $EndMonth
$DateClause = " WHERE PROCESSINGDAY = TO_DATE('$Start
}
else {
$DateClause = " WHERE PROCESSINGDAY BETWEEN TO_DATE('
$DateClause .=" AND TO_DATE('$EndDay-$EndMonth-$EndYe
}


// do the query and show tables
$user = [redacted]
$pass =
#$db =
$db = "

$db_conn = ocilogon($user,$pass,$db);

$qstring = "Select sum(NROFRECORDS),execluster,jobsta
$qstring .=  $DateClause;
```

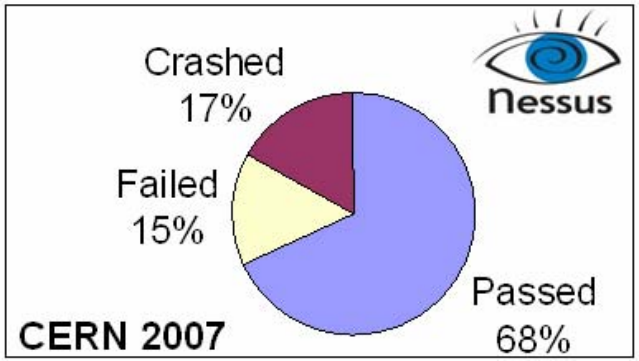
"Role Based Access Control" for op's:

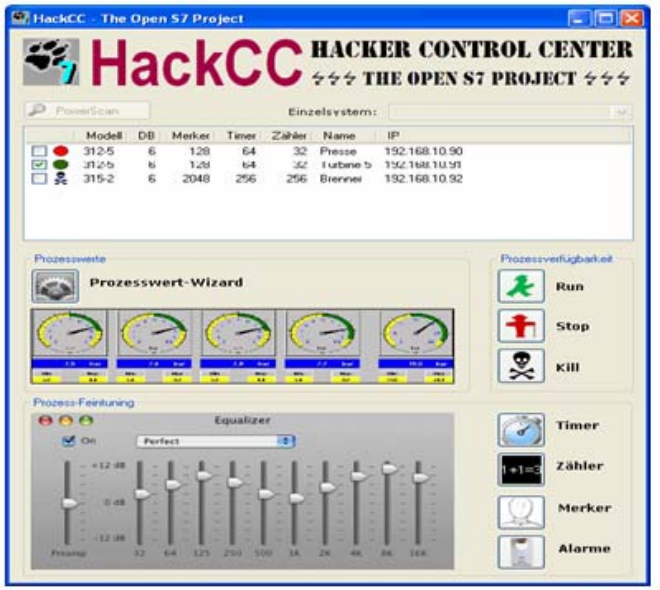
- Avoid "shared" accounts
- Multi-factor authentication for critical assets
- Full control for the shift leader of operations


Increase Robustness

PLCs and other controls devices are completely unprotected:

- No firewall, no anti-virus, nothing






Review Development Life Cycle

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)

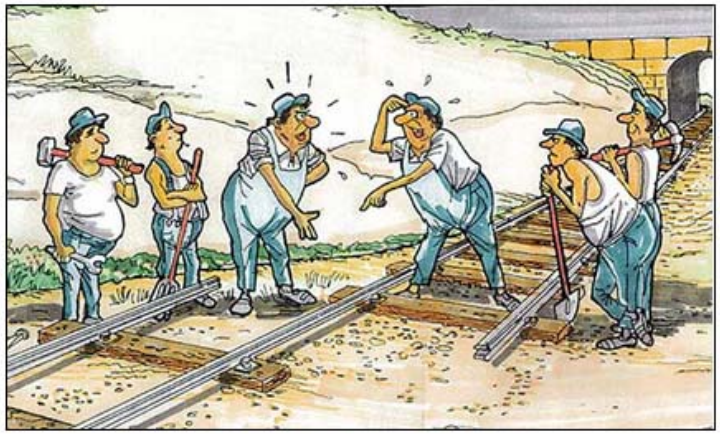

Foster Collaboration & Policies

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


Summary

The (r)evolution of control systems...

...omitted security aspects!


Summary

Do you want to act BEFORE or AFTER the incident ?