

Problems to Overcome

Implementation Issues at CERN

Dr. Stefan Lüders (CERN Computer Security Officer)

(CS)^2/HEP Workshop, Kobe (Japan)

October 11th 2009


Overview

The (r)evolution of control systems...

...omitted security aspects!

Why worry, HEP ?

Mitigation: Defense-in-Depth


Why worry ?




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

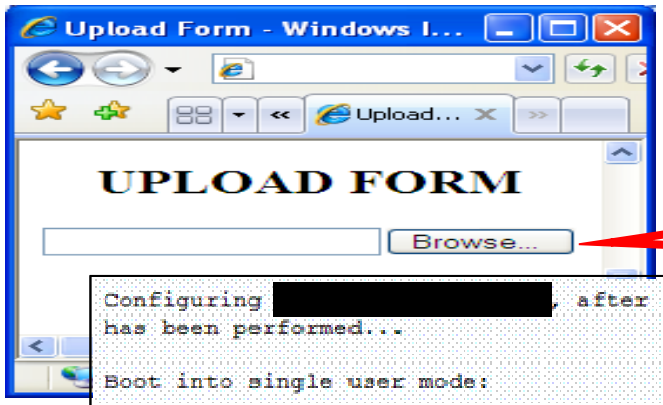
..etc...etc....

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

…on 10/09/2008:
Just coincidence ?

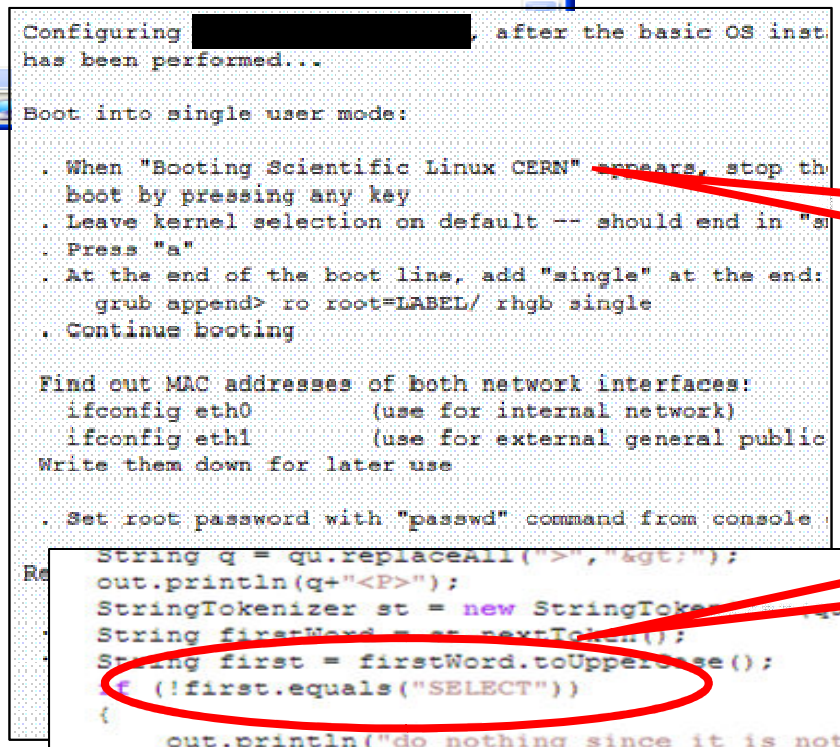
A "flame" message
to some Greek
"competitors"…


Violation of *Basic* Principles !



Neglected "Rule of Least Privileges":

Everyone could upload whatever he/she wants…



Configuration well documented in Google…

Lack of input validation & sanitization


Defense-in-Depth



Devices & Hardware

Firmware & Operating Systems
(Network-) Protocols

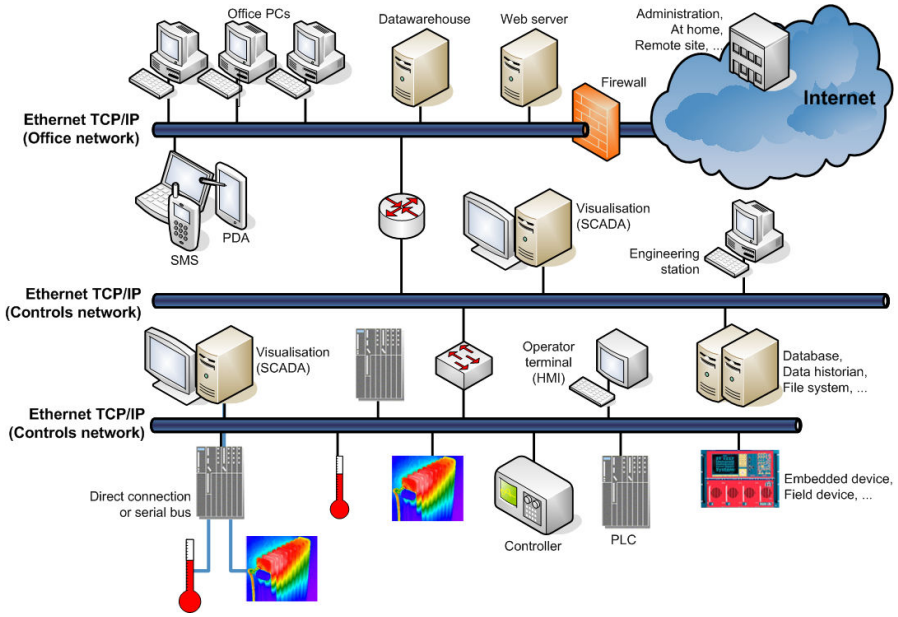
Software & Applications
Third party applications

Operators & User
Developers & System Experts

Separate Networks

Deploy different networks for different purposes:

- …for accelerator, experiments, offices
- …no Internet connectivity
- …controlled remote access
- …no wireless nor (GPRS) modems



However:

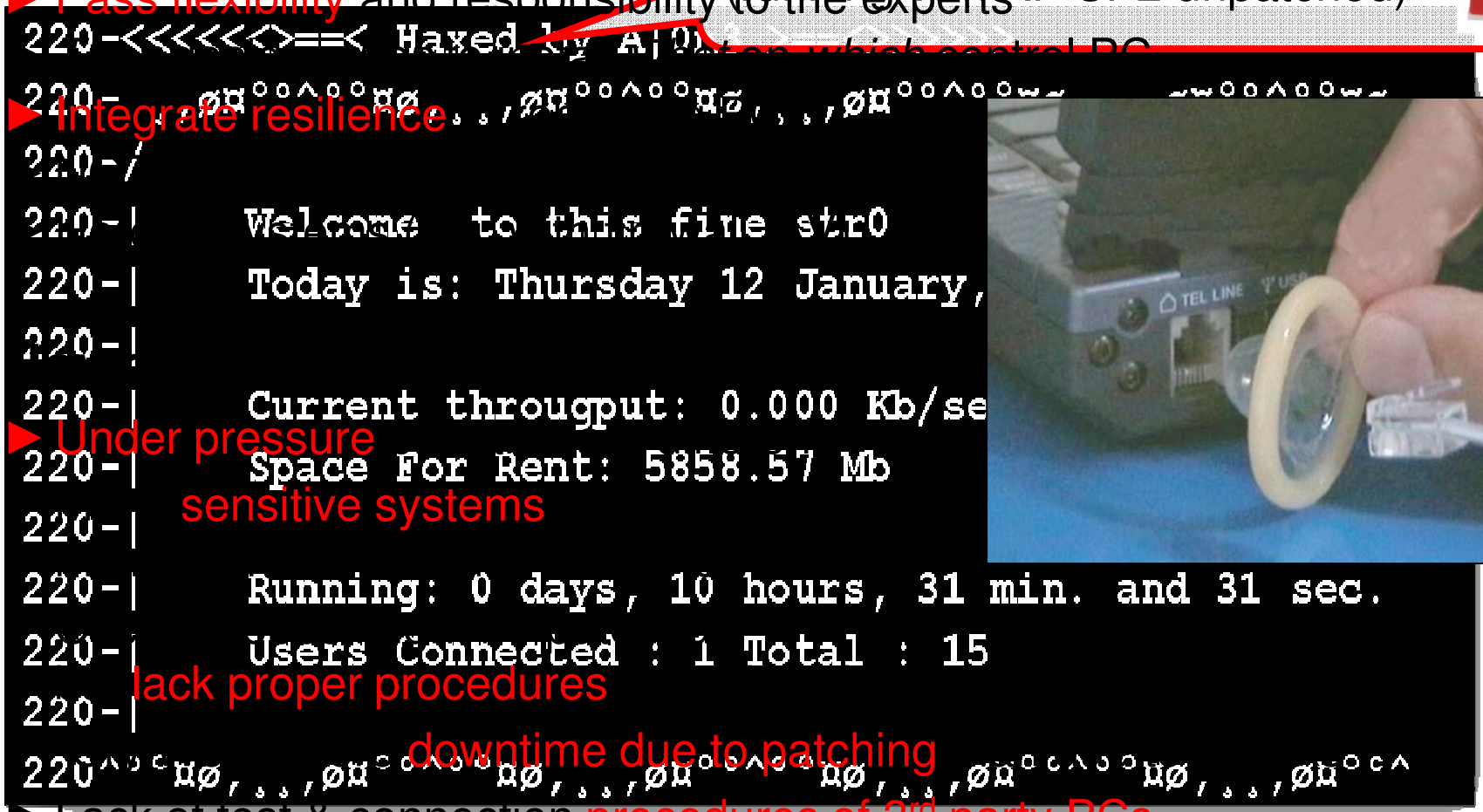
- LHC status data needs to be transmitted to experiments (e.g. run info)
- Informational web-sites need to be visible to the inside *and* outside (logbooks, status pages, expert instructions)
- Developers need sufficient access for further development & debugging ("This is an all-time, permanent prototype.")
- Laptops needed in vast underground areas for commissioning
- Some remote sites are not connected by the "right" network (or at all)


Patch, Patch, Patch !!!

Ensure prompt security updates!

- Pass flexibility and responsibility to the experts
- Integrate resilience
- Under pressure
  - sensitive systems
  - lack proper procedures
  - downtime due to patching
- Lack of test & connection procedures of 3rd party PCs

Hacked oscilloscope at CERN
(running Win XP SP2 unpatched)




Control (Remote) Access

Follow "Rule of Least Privilege":

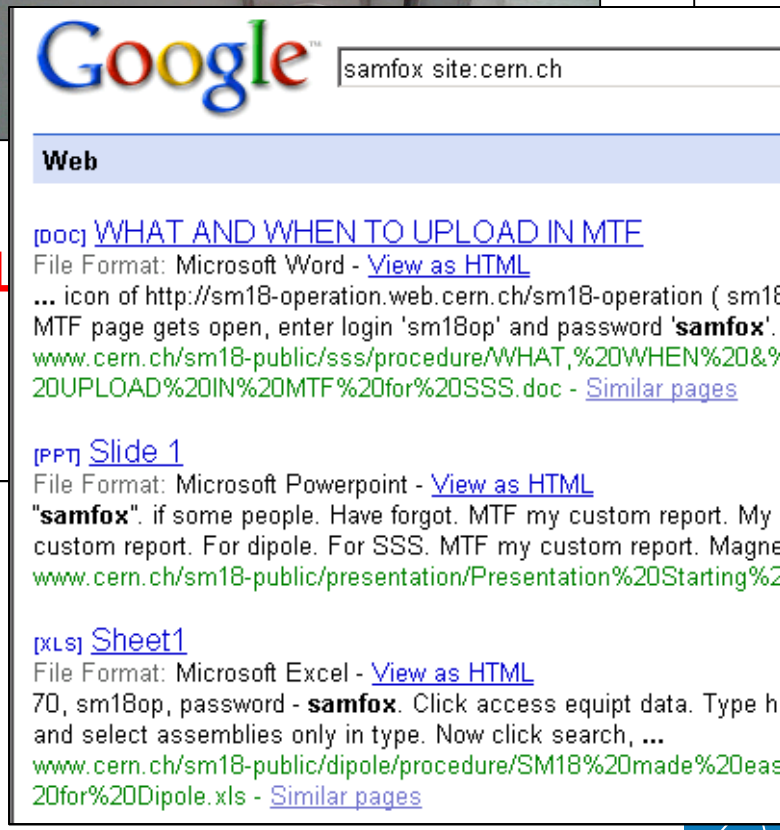
- Restrict all access to minimum
- Ensure traceability (who, when, and from where)
- Deploy role-based access system

"At CERN, several Windows ... compromised ..." — re

However:

- Typing passwords vs. convenience
- Is "I know" an authentication factor?
- Developers need elevated privileges
- "Rule of Least Privilege" not always known/followed, e.g. when publishing data
- Difficult to integrate commercial hardware
- Remote access for too many developers and experts is a nightmare

It is indicated that [CONTROLS_SOFTWARE] install MS-SQL database account Password empty by default ...

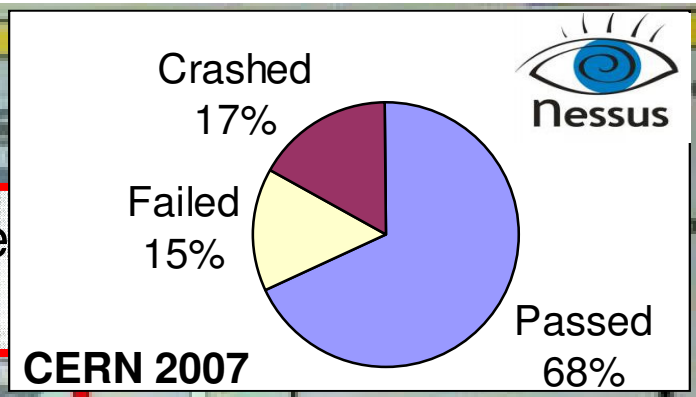


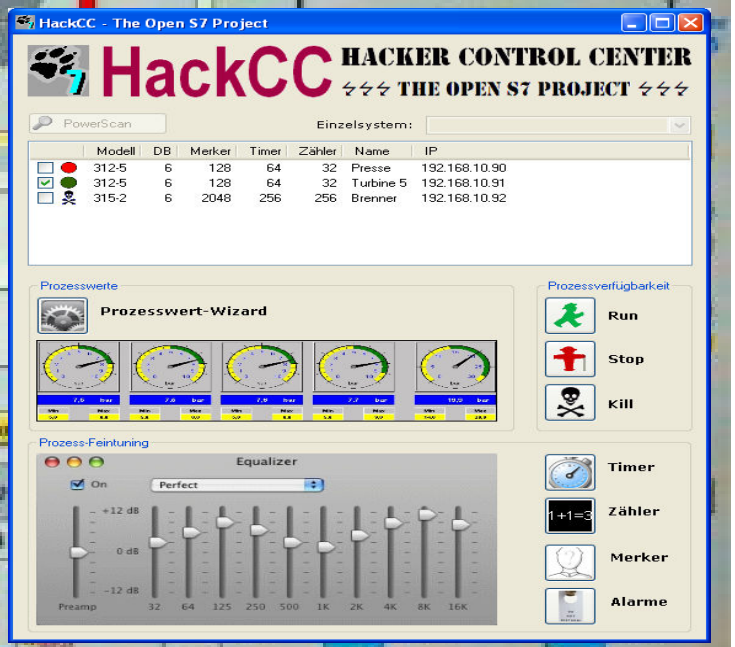

Increase Robustness

Protecting PLCs and other controls devices:

- Run vulnerability tools on everything
- Harden configuration settings
- Deploy additional protective measures if needed (VPN, ACL, …)

"Your software lice
(Not at CERN ☺)





However:

- Protection difficult in "mesh-type" inter-communications…
- …and under complex dependencies
- Vulnerability scans can do harm !
- Hardening not always supported by system
- Lack of integrated access control inside the device is challenging !


Review Development Life Cycle

Review procedures for

A Boeing 777 u
to Process Cor

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

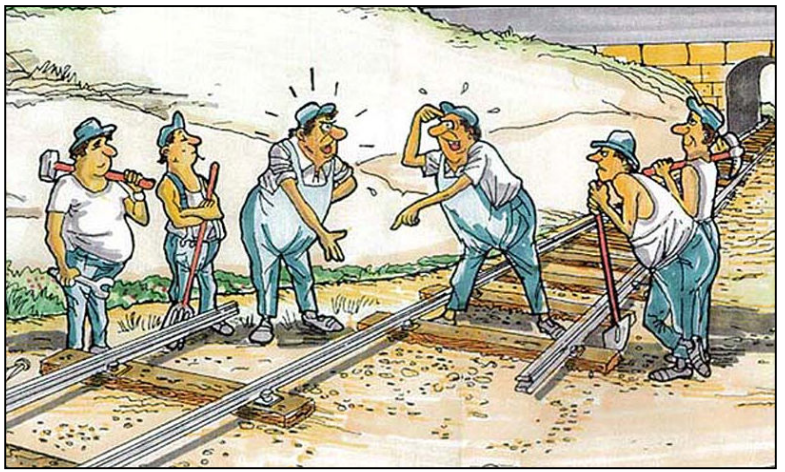
However,

- Lack of proper test-benches, which are 100% realistic & cover all aspects ("This is an all-time, permanent prototype")
- (Secure) Software Development Life-Cycles require a change-of-culture
- Static source code analysers & code reviews necessary...
  ...but either for low-hanging-fruits or expensive


Foster Collaboration & Policies

Make security an objective

- Get management buy-in (security has a cost – successful attacks, too)



Bring together control & IT experts:

- Win mutual trust
- Gain synergy effects

Train users and raise awareness

Secure coding for Java	24-Nov-09 to 24-Nov-09	1 day
Secure coding for PHP	25-Nov-09 to 25-Nov-09	1 day
Secure coding for Perl	26-Nov-09 to 26-Nov-09	4 hours
Secure coding for Python	26-Nov-09 to 26-Nov-09	4 hours
Secure coding for Web Applications and Web Services	23-Nov-09 to 23-Nov-09	1 day
Secure coding in C/C++	to be scheduled	1 day

However:

- Difficult to get buy-in when developers & management are under pressure
- Old (negative) feelings and perceptions difficult to eradicate
- Duplication of services part of the "academic freedom"


Force the Vendors on Board

Manufacturers and vendors are part of the solution !

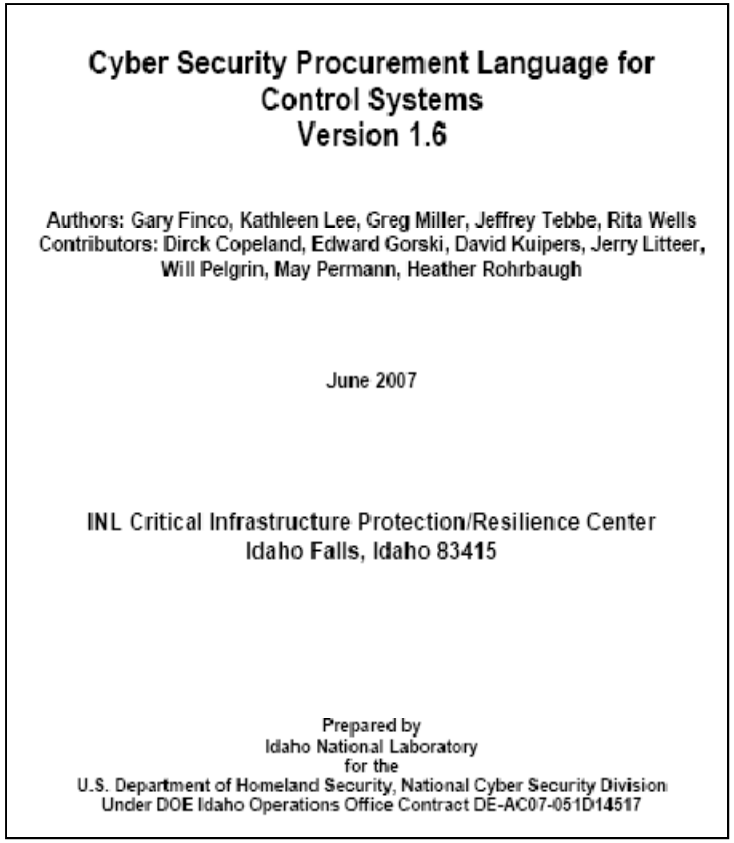
- Security demands must be included into orders and call for tenders

"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 Center
Idaho Falls, Idaho 83415

Prepared by
Idaho National Laboratory
for the
U.S. Department of Homeland Security, National Cyber Security Division
Under DOE Idaho Operations Office Contract DE-AC07-051D14517

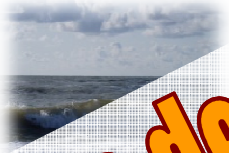
http://www.msisac.org/scada


Summary

The (r)evolution of control systems...

...omitted security aspects!!!

The devil is in the details!!!

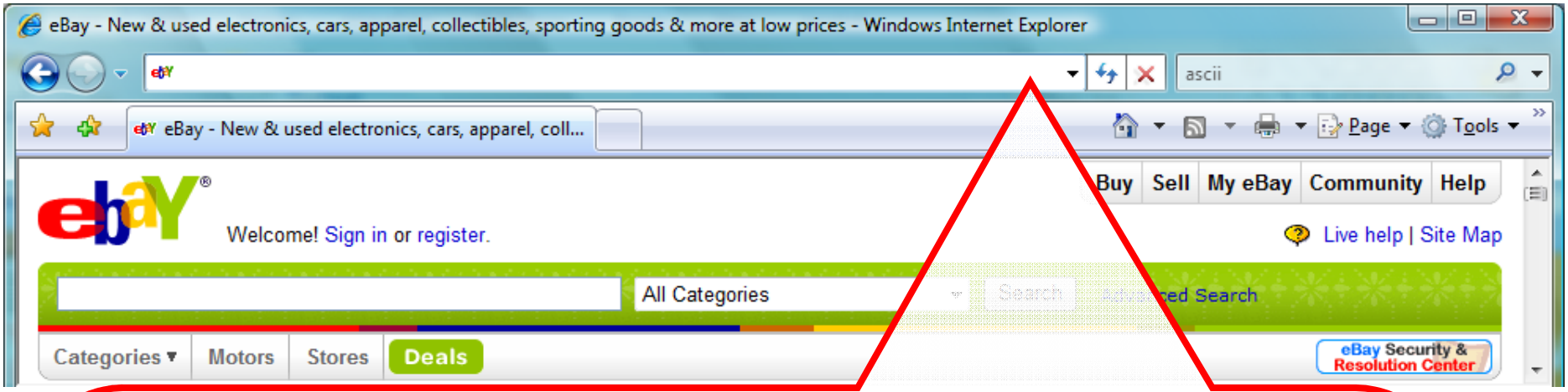


Security is not considered to be important!!!

Risk equation

Mitigation: Defense-in-Depth

Thank you very much !!!



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