

4th Control System Cyber-Security Workshop

Exchanging ideas on HEP security

Dr. Stefan Lüders (CERN Computer Security Officer)

4th (CS)2/HEP Workshop, San Francisco (California)

October 6th, 2013

Attackers vs. Defense

- There is no 100% security.
- Security is as good as weakest link:
  Attacker chooses time, place, method
  Defender needs to protect against all…

theguardian

PlayStation Network hack: why it took Sony seven days to tell the world

Sony's company blog says forensic analysis of the PlayStation Network hack took 'several days' to complete and extent of intrusion wasn't understood until Tuesday

THE DAILY BEAST
READ THIS SKIP THAT

HOME | POLITICS | BUSINESS | INNOVATION | ENTERTAINMENT | BEAST TV | BOOKS | ART | WOMEN IN T

Featured: ELECTION • FASHION • ANDREW SULLIVAN • HOWARD KURTZ • DAVID FRUM

CHEAT SHEET
MUST READS FROM ALL OVER

WE DID IT

Anonymous Hacked Justice Dept., FBI Sites

Frederic J. Brown / AFP-Getty Images

So much for staying Anonymous. The hacking group has admitted to crashing the Justice Department and FBI websites, after federal officials took down the popular file-sharing site Megaupload. Seven executives from Megaupload were indicted Thursday for disobeying copyright laws and protection, though the site's attorney denied the charges. Hours later, the websites of the Justice Department and Universal Music and the FBI's homepage all malfunctioned. Anonymous didn't steal any information from the sites—the attacks were meant to flood the pages with more traffic than they could handle and were targeted at the Stop Online Piracy Act. The founder of an online think tank


Attackers vs. Defense

- There is no 100% security.
- Security is as good as weakest link:
  Attacker chooses time, place, method
  Defender needs to protect against all…

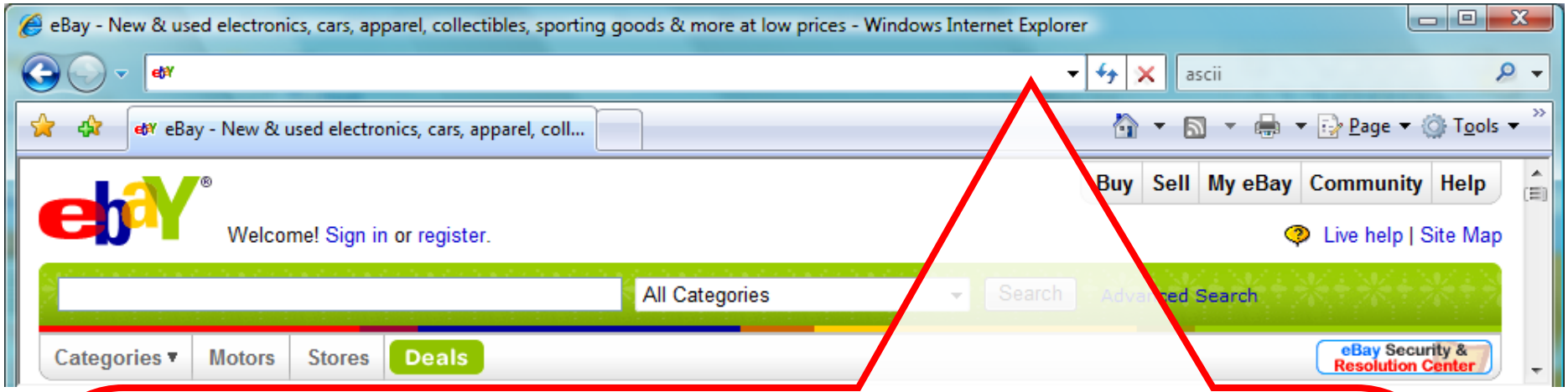
- Targeted attackers (➔APTs) are focused and keen, have better skills/networks, are better financed/resourced
- The untargeted/stupid attackers might be caught…
- Automatisms, at least, can be fought.

> "Anonymous is a handful of geniuses surrounded by a legion of idiots."
> Cole Stryker

- Defense usually lacks money/resources/networks.
- (International) Law is always a step behind.


Attackers vs. Defense

A small quiz.



Quiz: Which URL leads you 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

From the Newsroom

The Washington Post
NATIO

Posted at 09:26 AM ET, 09/20/2011
After Stuxnet, waiting on Pandora's box

Report: Stuxnet Virus May Have Improved Iran's Ability To Enrich Uranium

HUFFPOST TECH

Huffington Post UK | By Michael Rundle
Posted: 1

Iran hacks energy firms, U.S. says

FRIDAY, 24 MAY 2013

IRAN FOCUS
NEWS & ANALYSIS

ELECTRIC GRID VULNERABILITY

Industry Responses Reveal Security Gaps

May 21, 2013

The Washington Times

Cyber we
war

AP Associated Press

Email Rec

Obama hits pause on U.S. action in face of crippling cyber strikes from Syria, Iran

By Shaun Waterman - The Washington Times

Wednesday, August 28, 2013

RELATED CONTE

In this Feb. 19, 2010 photo, Richard A. Clarke, a former advisor to the president ...

so vulnerable to attack that it should deter U.S. leaders from going to war with other nations, a former top U.S. cybersecurity official

China, North Korea, Iran and Russ
could destroy power grids, bankin

The U.S. military, he said, is entire
conflict in which troops trot out onto a battlefield "and nothing works."

Clarke said a good national security adviser would tell the president that the U.S. might be able to blow up a nuclear plant somewhere, or a terrorist training center somewhere, but a number of countries could strike back with a cyberattack and "the entire us economic system could be crashed in retaliation ... because we can't defend it today."


$(CS)^2$ 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

	Introduction to the 4th Control System Cyber-Security Workshop Seacliff D, Bayview Level, The Hyatt Regency Embarcadero Center	Dr. Stefan LUEDERS 09:30 - 09:45
	Controls Cyber Security at PSI Seacliff D, Bayview Level, The Hyatt Regency Embarcadero Center	Renata KREMPASKA 09:45 - 10:10
10:00	IEC 61850 industrial communication standards under test Seacliff D, Bayview Level, The Hyatt Regency Embarcadero Center	Filippo Maria TILARO 10:10 - 10:35
	Coffee Break Seacliff D, Bayview Level, The Hyatt Regency Embarcadero Center	10:35 - 10:55
	Remote Access to Experiment Controls Seacliff D, Bayview Level, The Hyatt Regency Embarcadero Center	Peter CHOCHULA 10:55 - 11:20
11:00	Renewal of the remote maintenance system for the SPring-8 control system Seacliff D, Bayview Level, The Hyatt Regency Embarcadero Center	Dr. Takashi SUGIMOTO 11:20 - 11:45
	Authentication and Authorization for the ESS Control System Seacliff D, Bayview Level, The Hyatt Regency Embarcadero Center	Suzanne GYSIN 11:45 - 12:10
12:00	Benefits of Virtualisation for LHCb Controls Seacliff D, Bayview Level, The Hyatt Regency Embarcadero Center	Enrico BONACCORSI 12:10 - 12:35
	Lunch Break Seacliff D, Bayview Level, The Hyatt Regency Embarcadero Center	12:35 - 13:30
13:00	Disconnecting controls --- implications and findings Seacliff D, Bayview Level, The Hyatt Regency Embarcadero Center	Dr. Stefan LUEDERS 13:30 - 13:55
	Technical, Legal, and Social Issues in Control Systems: Past, Present, Future Seacliff D, Bayview Level, The Hyatt Regency Embarcadero Center	Stefani BANERIN 13:55 - 14:20
14:00	Integrating Controls Cyber Security with Corporate IT: a management perspective Seacliff D, Bayview Level, The Hyatt Regency Embarcadero Center	Mr. Enzo CARRONE 14:20 - 14:45
	Coffee Break Seacliff D, Bayview Level, The Hyatt Regency Embarcadero Center	14:45 - 15:05
15:00	Discussion	Dr. Stefan LUEDERS

ENJOY!

https://indico.cern.ch/conferenceDisplay.py?confId=217457