POLITECNICO DI MILANO





Security of Cyber-Physical Systems

Stefano Zanero, PhD

Assistant Professor, Politecnico di Milano

Buongiorno!

- I'm an assistant professor at Politecnico di Milano, Italy's largest engineering school, with ~38.000 students
- My laboratory deals with Novel, Emerging Computing System Technologies, and encompasses the system security research efforts
- Black Hat review board member

NECST laboratory

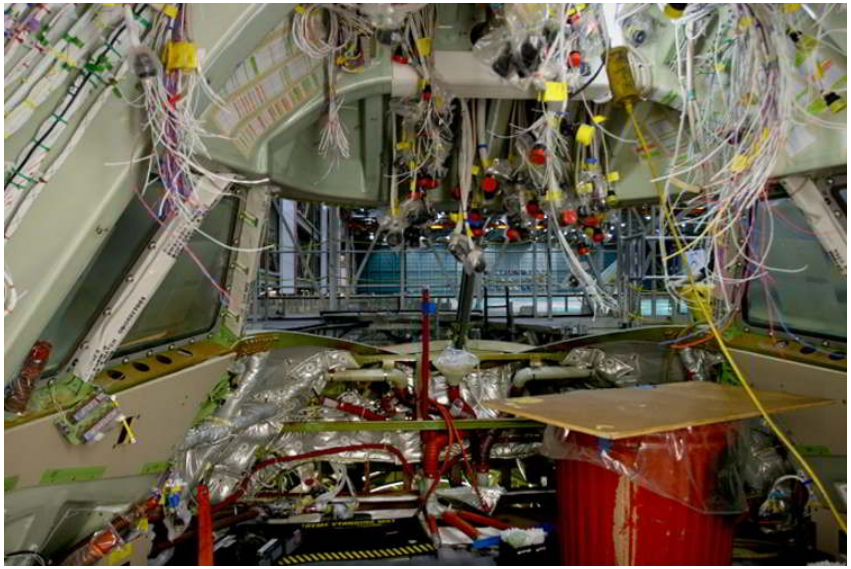
POLITECNICO DI MILANO

Scope of this talk

- This talk deals with *security* of *cyber-physical* systems
- In particular, with the *vulnerabilities* at the separation layer of such systems

Cyber-physical systems

- Evolution of the traditional embedded systems for control
- E.g. SCADA systems, avionics, vehicular control and infotainment, “smart grid”
- Do you know what's the “naked” CPS on the left?



Vulnerabilities

- In information security, a vulnerability is a weakness which allows to reduce a system's *information assurance*
- More generally, a vulnerability is a *weakness* in a system that makes it susceptible to being dama*ged, or* more generally makes it unfit to withstand some external condition
- We should not confuse the existence of a *vulnerability* with the existence of a *threat* (e.g. an attacker), or with the existence of one or more specific *exploits* for that vulnerability

Security as managing risks

- All (information) systems are vulnerable
- This is not a self-justifying mantra, it's a basic fact of life: invulnerability, just like perfection, is but an illusion
- *Vulnerabilities*, their *exploitability* and the existence and prevalence of *threats* combine with the potential of *damage* to create *risks*
- Security is the discipline of managing *risk* reducing it to a tolerable level, balancing the costs
- The issue of securing *critical systems* is that it is very difficult to gauge the product of very low probabilities times very high potential damage

Fact check

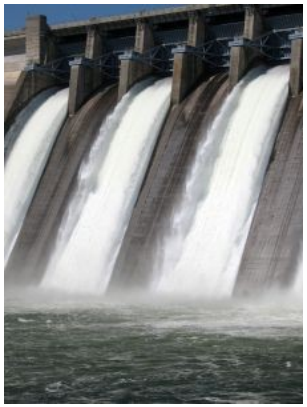
- Want to check with you some facts
- Fact 1: CPS are increasingly involved in *critical infrastructures* and *safety-critical* systems
- Fact 2: CPS are increasingly becoming control loops closed *without humans in the middle*
- Fact 3: CPS are evolving towards *complex networks of complex systems*, rather than single, embedded, simple systems
- Fact 4: threat level by actors likely to act against these systems is constantly on the rise

Fact 1: critical systems

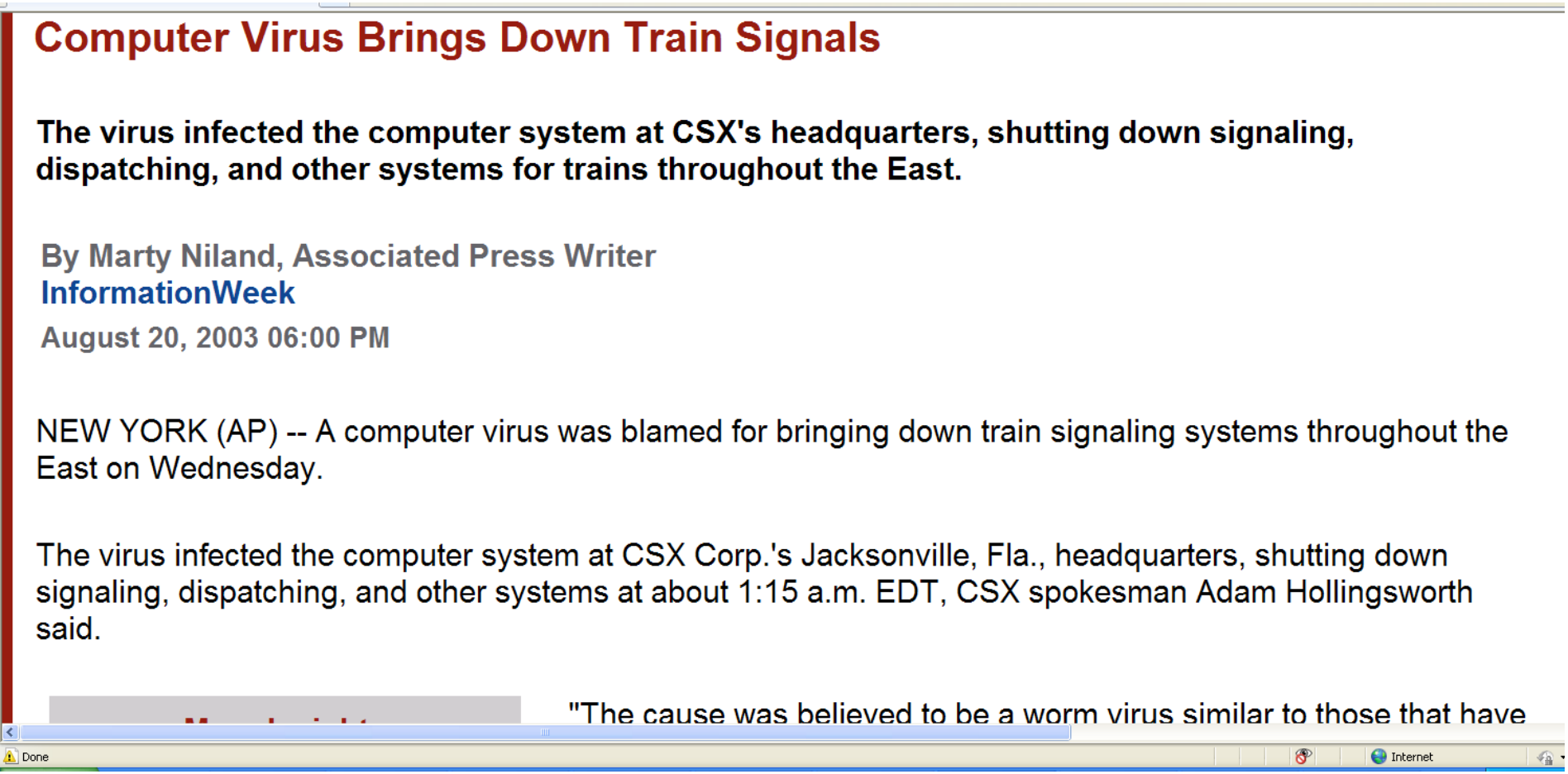
"… potential (cyber)attacks against network infrastructures may have widespread and devastating consequences on our daily life: *no more electricity or water* at home, *rail and plane accidents, hospitals out of service*"

Viviane Reding

VP of European Commission



Train signals...



Computer Virus Brings Down Train Signals

The virus infected the computer system at CSX's headquarters, shutting down signaling, dispatching, and other systems for trains throughout the East.

By Marty Niland, Associated Press Writer
InformationWeek
August 20, 2003 06:00 PM

NEW YORK (AP) -- A computer virus was blamed for bringing down train signaling systems throughout the East on Wednesday.

The virus infected the computer system at CSX Corp.'s Jacksonville, Fla., headquarters, shutting down signaling, dispatching, and other systems at about 1:15 a.m. EDT, CSX spokesman Adam Hollingsworth said.

"The cause was believed to be a worm virus similar to those that have

Done Internet

Connected cars...

WIRED SUBSCRIBE » SECTIONS » BLOGS » REVIEWS » VIDEO » HOW-TOS »

Sign In | RSS Feeds

THREAT LEVEL

PRIVACY, CRIME AND SECURITY ONLINE

Hacker Disables More Than 100 Cars Remotely

By Kevin Poulsen March 17, 2010 | 1:52 pm | Categories: Breaches, Crime, Cybersecurity, Hacks and Cracks

More than 100 drivers in Austin, Texas found their cars disabled or the horns honking out of control, after an intruder ran amok in a web-based vehicle-immobilization system normally used to get the attention of consumers delinquent in their auto payments.

Police with Austin's High Tech Crime Unit on Wednesday arrested 20-year-old Omar Ramos-Lopez, a former Texas Auto Center employee who was laid off last month, and allegedly sought revenge by bricking the cars sold from the dealership's four Austin area lots

Done

The power grid...

Fighter planes...

Telegraph.co.uk

Home | News | Election 2010 | Sport | Finance | Lifestyle | Comment | Travel | Culture

UK | World | Celebrities | Obituaries | Weird | Earth | Science | Health News | Education | Topics

USA | Barack Obama | Europe | Asia | China | Middle East | Africa and Indian Ocean | Austra

HOME > NEWS > WORLD NEWS > EUROPE > FRANCE

French fighter planes grounded by computer virus

French fighter planes were unable to take off after military computers were infected by a computer virus, an intelligence magazine claims.

by Kim Willsher in Paris
Published: 11:43AM GMT 07 Feb 2009

Share | 663 diggs digg it | 0 tweet | Email | Print | Text Size

Done

Fact 2: no human in the middle

In the real world...

DealB%k
ANDREW ROSS SORKIN
EDITOR-AT-LARGE

The New York Times

SEARCH DEALBOOK Go

MERGERS & ACQUISITIONS | INVESTMENT BANKING | PRIVATE EQUITY | HEDGE FUNDS | I.P.O./OFFERINGS | VENTURE CAPITAL | LEGAL/REGULATORY

LEGAL/REGULATORY | AUGUST 2, 2012, 9:07 AM | 357 Comments

Knight Capital Says Trading Glitch Cost It $440 Million

BY NATHANIEL POPPER

Brendan McDermid/Reuters

1 2 3 4 ➤

Errant trades from the Knight Capital Group began hitting the New York Stock Exchange almost as soon as the opening bell rang on Wednesday.

4:01 p.m. | Updated

$10 million a minute.

PREVIOUS ARTICLE
Former Treasury Official to Join Romney Campaign

NEXT ARTICLE
Apollo's 2nd-Quarter Profit Falls 84%

The Wire

AUG 15, 12:53 PM .... WSJ.COM — **Punk Band Crashes Russia's Investment Case**

AUG 15, 12:50 PM .... AP — **Deere and Drought: An Outlook for Crop Demand**

AUG 15, 12:50 PM .... NYTIMES — **AIG Not on the Hook for Policyholders' Madoff Claims: U.S. Court**

AUG 15, 12:40 PM .... WSJ.COM — **Tencent Profit Rises Despite Headwinds**

AUG 15, 12:14 PM .... WSJ.COM — **That Ten Commandments Statue Isn't Going Anywhere Fast**

News by Sector

Energy
Industrials
Cyclical Goods & Services
Autos
Media
Non-Cycl. Goods & Services
Food & Beverage
Technology
Financials
Real Estate
Basic Materials
Health Care
Telecom
Utilities

More New York Times News by Sector

GLOBAL | ENERGY | MEDIA | TECH | HEALTH CARE

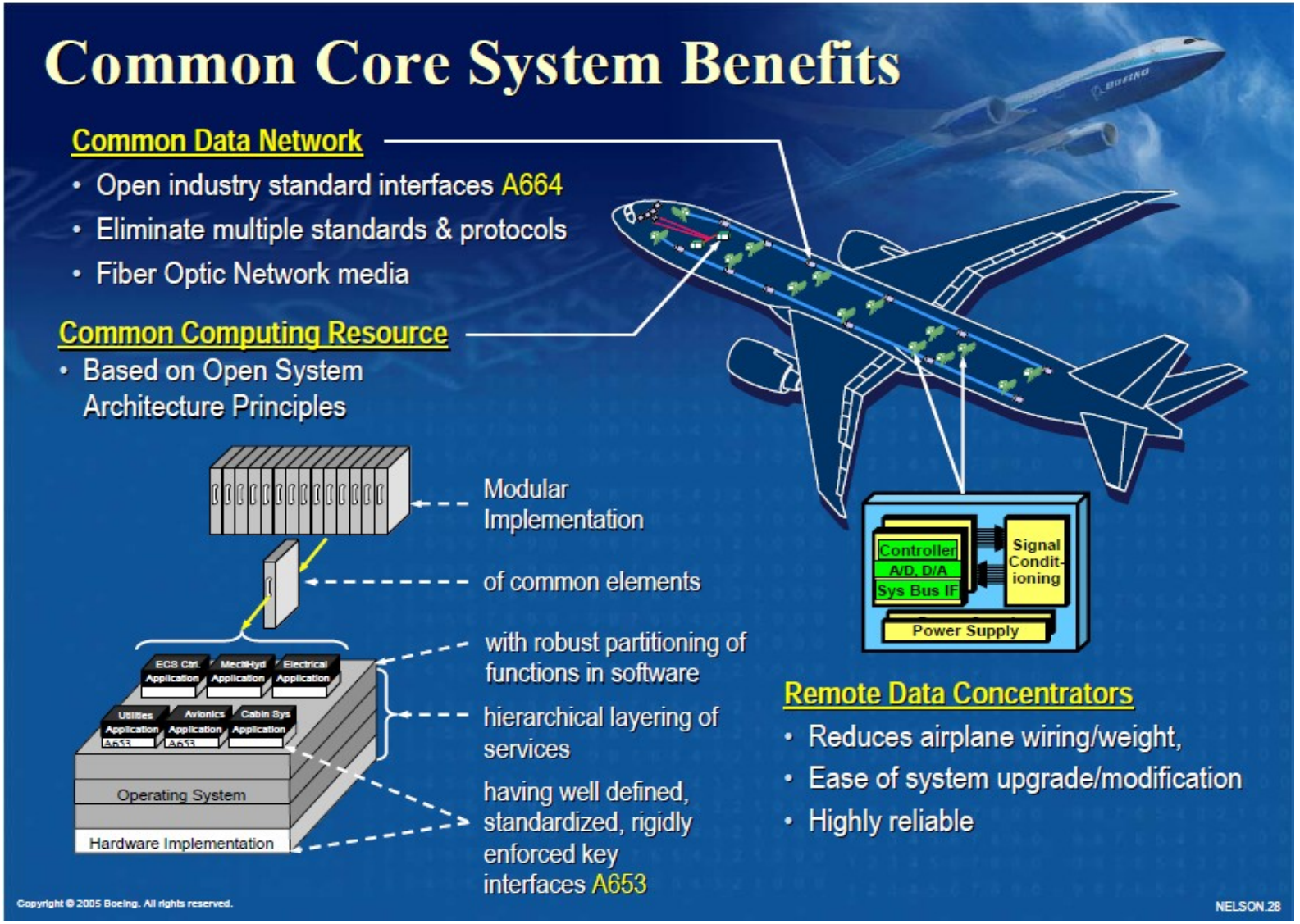
State of the Art: Samsung's Rival for the iPad Loads on the Features
Samsung's new iPad rival, the Galaxy Note 10.1, is loaded

Algorithmic trading fails

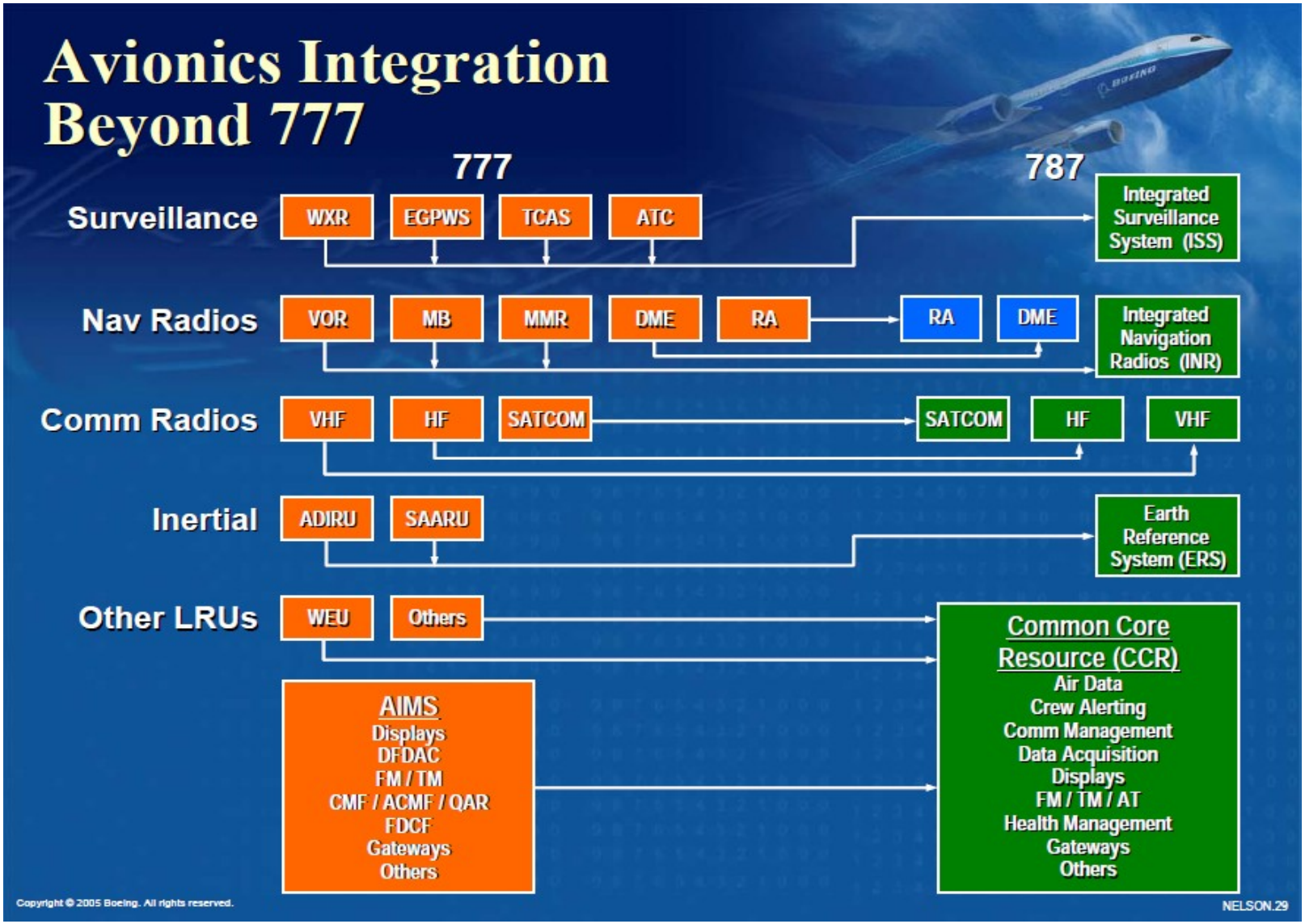
- ~40% of share orders in Europe by algorithmic trading; 5 yrs ago, 20%. In the U.S. 37%. (src: Tabb Group)
- Knight trading is just the latest failure
- Svend Egil Larsen (Norwegian trader) in 2007 reversed the trading algorithm of Timber Hill, a unit of US-based Interactive Brokers, found a flaw and exploited it for $50,000 (U.S.) in a few months. Not guilty, btw.
- Deutsche Bank's trading algorithms in Japan took out a $182-billion stock position by mistake in 2010
- "Flash crash" in 2010, Dow Jones Industrial Average swung hundreds of points in 20 minutes – exacerbated by trading algorithms kicking in

Fact 3: complexity of networks

Interconnection...



… and convergence

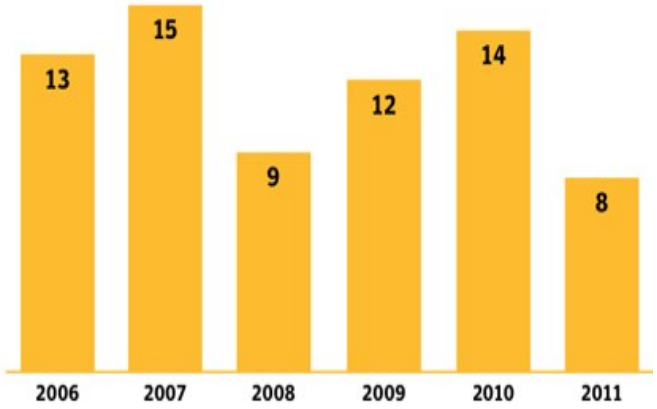


Interconnection (too much of it)

Fact 4: rising threats

Figure D.4

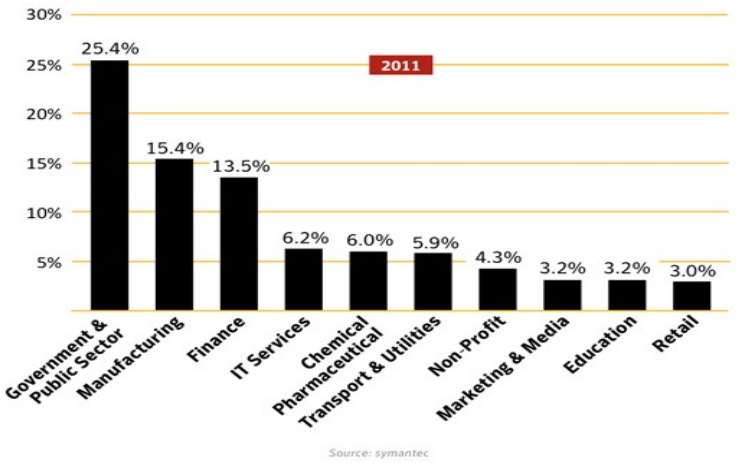
Volume Of Zero-Day Vulnerabilities 2006 – 2011



Source: Symantec

Figure B.17

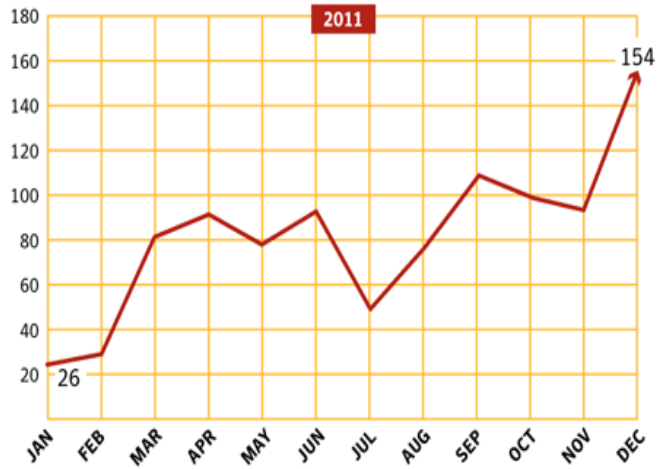
Analysis Of Targeted Attacks By Top-10 Industry Sectors, 2011



Source: symantec

Figure B.12

Average Number Of Targeted Email Attacks Per Day, 2011



Source: symantec.cloud

All the data comes from the Internet Security Threat Report 2011

Find the differences...

- China's Chengdu J-20 fighter (circa oct. 2010) vs. Northrop YF-23 (1994)
- Remember that Northrop was one of the first targets of the APT (Advanced Persistent Threat) campaign in 2009
- Suggestive, isn't it?

It's not just about the business

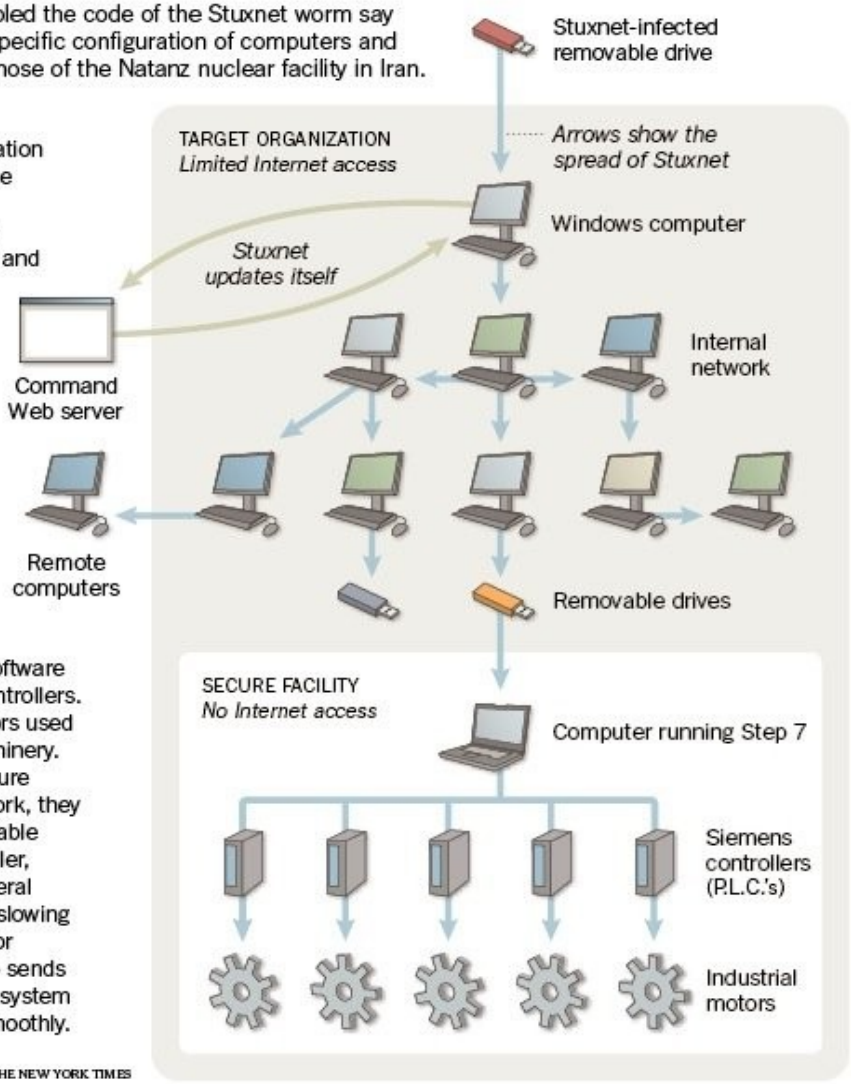
How Stuxnet Spreads

Experts who have disassembled the code of the Stuxnet worm say it was designed to target a specific configuration of computers and industrial controllers, likely those of the Natanz nuclear facility in Iran.

INITIAL INFECTION
Stuxnet can enter an organization through an infected removable drive. When plugged into a computer that runs Windows, Stuxnet infects the computer and hides itself.

UPDATE AND SPREAD
If the computer is on the Internet, Stuxnet may try to download a new version of itself. Stuxnet then spreads by infecting other computers, as well as any removable drives plugged into them.

FINAL TARGET
Stuxnet seeks out computers running Step 7, software used to program Siemens controllers. The controllers regulate motors used in centrifuges and other machinery. While the computers in a secure facility may not be on a network, they can be infected with a removable drive. After infecting a controller, Stuxnet hides itself. After several days, it begins speeding and slowing the motors to try to damage or destroy the machinery. It also sends out false signals to make the system think everything is running smoothly.

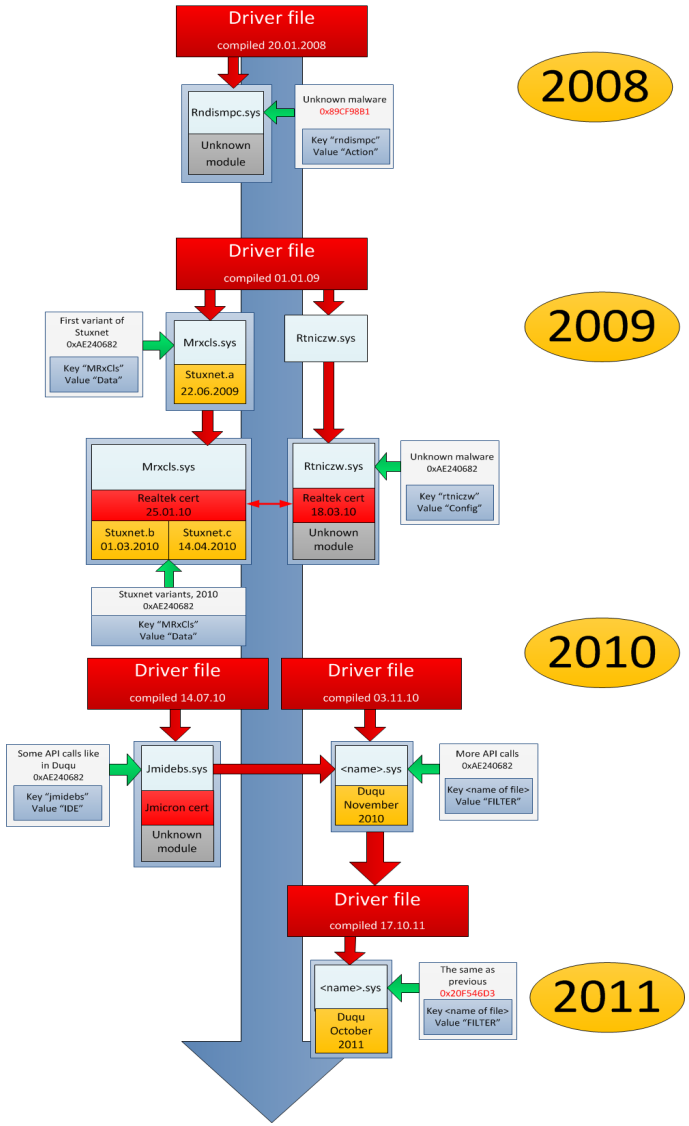


Source: Symantec

THE NEW YORK TIMES

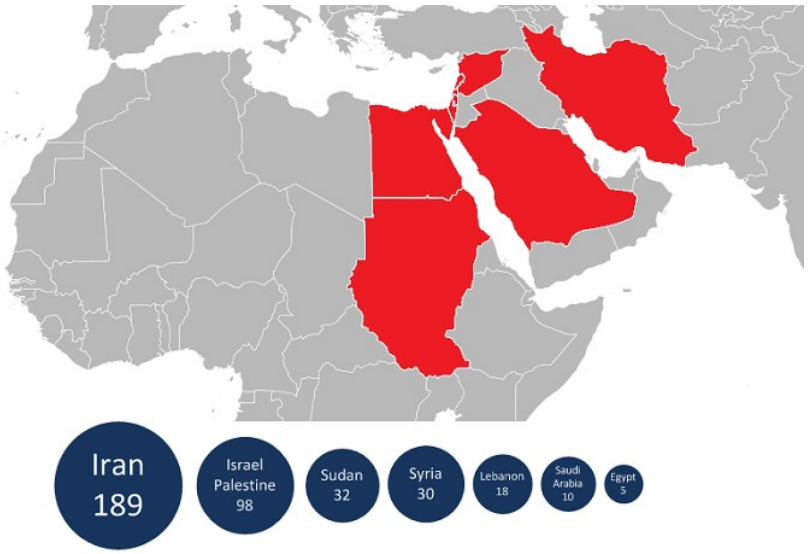
The slippery slope of cyberwar

- Stuxnet: designed to sabotage Iran's nuclear facilities
- Duqu: discovered a few months later, possibly created earlier, same platform as Stuxnet; uses zero-day; designed to collect data on the Iranian nuclear program (which ended up in the ends of UN)



And then came the flame

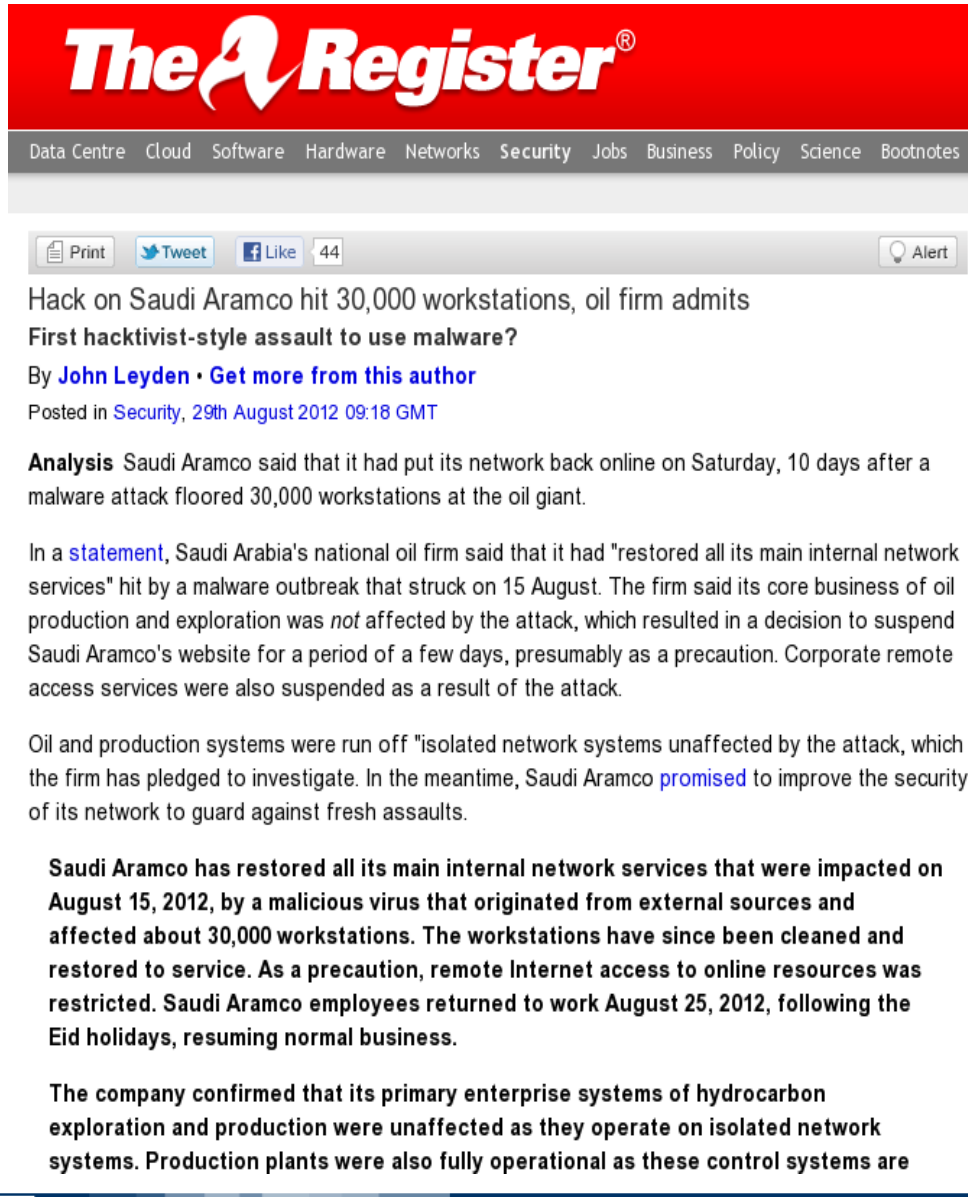
- Flamer: enormous malware specimen discovered in 2012 by ITU; intelligence gathering; encryption zero day (!); component link to Stuxnet (!!)
- Gauss: similar to the others in many way, includes banking trojan and an encrypted payload which wasn't cracked yet



No comment to the above image (detailing diffusion of Flame) is probably needed.

What next?

- Shamoon: a very different beast, targeting critical files from a specific company (Saudi Aramco)
- Still, a targeted attack with usage of signed driver component like Flamer
- Overwrote critical files on 30.000 machines (¾) on the corporate network with a burning American flag
- Claimed by unknown “Cutting Sword of Justice” group on Pastebin
- What's next?



The Register®

Data Centre Cloud Software Hardware Networks **Security** Jobs Business Policy Science Bootnotes

Print Tweet Like 44 Alert

Hack on Saudi Aramco hit 30,000 workstations, oil firm admits

First hacktivist-style assault to use malware?

By John Leyden • Get more from this author

Posted in Security, 29th August 2012 09:18 GMT

Analysis Saudi Aramco said that it had put its network back online on Saturday, 10 days after a malware attack floored 30,000 workstations at the oil giant.

In a statement, Saudi Arabia's national oil firm said that it had "restored all its main internal network services" hit by a malware outbreak that struck on 15 August. The firm said its core business of oil production and exploration was *not* affected by the attack, which resulted in a decision to suspend Saudi Aramco's website for a period of a few days, presumably as a precaution. Corporate remote access services were also suspended as a result of the attack.

Oil and production systems were run off "isolated network systems unaffected by the attack, which the firm has pledged to investigate. In the meantime, Saudi Aramco promised to improve the security of its network to guard against fresh assaults.

Saudi Aramco has restored all its main internal network services that were impacted on August 15, 2012, by a malicious virus that originated from external sources and affected about 30,000 workstations. The workstations have since been cleaned and restored to service. As a precaution, remote Internet access to online resources was restricted. Saudi Aramco employees returned to work August 25, 2012, following the Eid holidays, resuming normal business.

The company confirmed that its primary enterprise systems of hydrocarbon exploration and production were unaffected as they operate on isolated network systems. Production plants were also fully operational as these control systems are

Facts checked!

- Fact 1: CPS are increasingly involved in *critical infrastructures* and *safety-critical* systems
- Fact 2: CPS are increasingly becoming control loops closed *without humans in the middle*
- Fact 3: CPS are evolving towards *complex networks of complex systems*
- Fact 4: threat level by (state/nonstate)-actors likely to act against these systems is constantly on the rise
- All of this leads, at the same time, to increasing *attack surfaces*, *vulnerability exposure*, *threat prevalence*, *potential damage*
- ***What about defense then?***

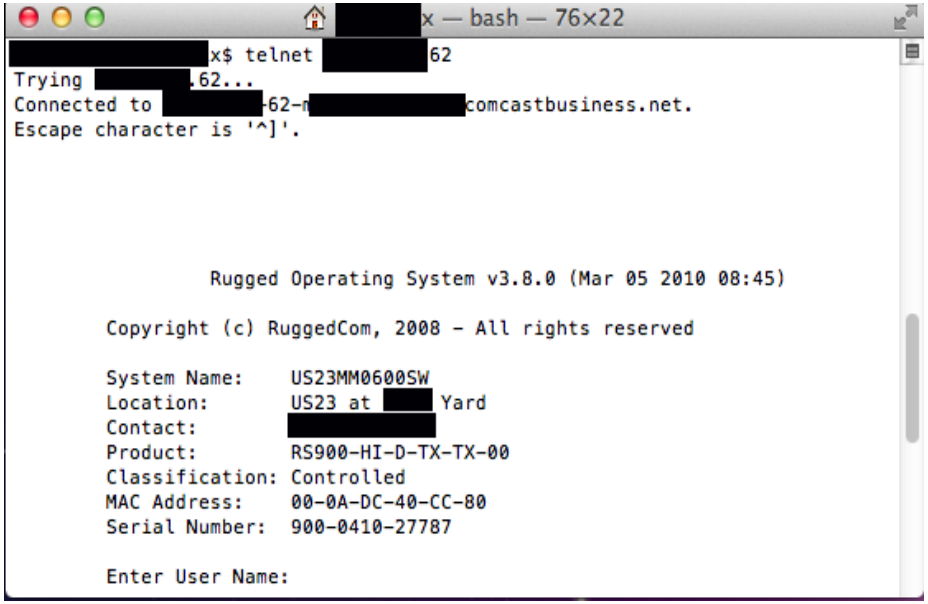
Where we are: legacy woes

© Scott Adams, Inc./Dist. by UFS, Inc.

© Scott Adams, Inc./Dist. by UFS, Inc.

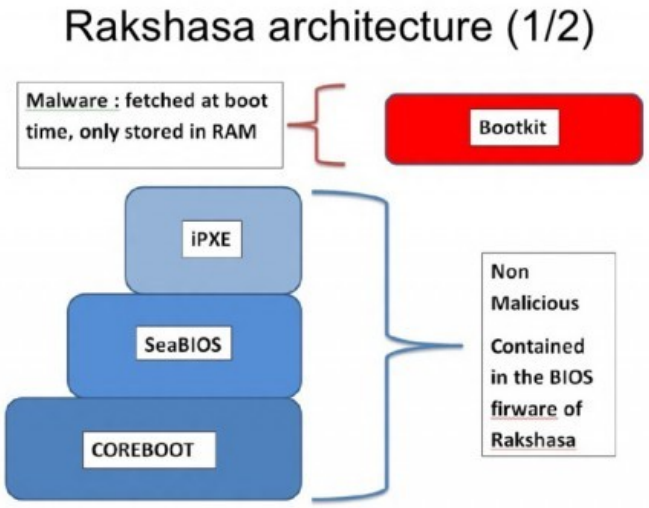
Forever day bugs

- Zero-day: an unknown vulnerability exploited by an attacker
- Forever day: an old, beaten-to-death vulnerability still around
- Most CPS are change averse, and thus prone to forever day bugs
- RuggedCom is in good company with ABB, Schneider Electric, and Siemens



RuggedCom forever day:
Known username,
fixed password easy to crack,
impossible to disable

Where we are going: hardware attacks



Rakshasa is a fully functional bootkit resident in RAM and invoked by a seemingly sane BIOS/firmware

Cambridge Scientist Defends Claim That US Military Chips Made In China Have 'Backdoors'

Eloise Lee and Robert Johnson | May 29, 2012, 1:39 PM | 8,499 | 32

Recommend 75 Share 35 Tweet 107 +1 13 Email More

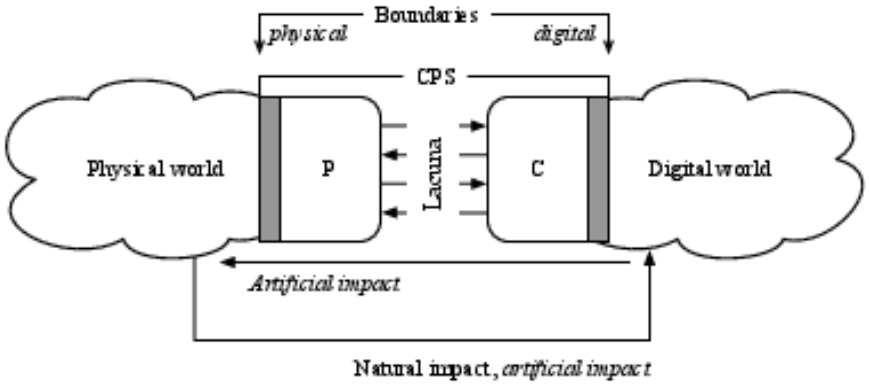
Cambridge

A powerful new report by Cambridge scientist Sergei Skorobogatov hit the Internet over the weekend confirming Chinese computer chips used in U.S. military systems have hidden "back doors" that can disable everything from American fighter jets to nuclear power plants.

It's a bold claim that until now has been impossible to prove, but Skorobogatov says he has developed a new ultra-sensitive technology that's able to detect "malicious insertions" into chips. "The scale and range of possible attacks," he says, "has huge implications for National Security and public infrastructure."

After the initial flurry of excitement, a response cropped up on the security blog Errata saying Skorobogatov's claim was bogus and there is actually no back door at all. We asked the scientist to respond to that post specifically in our list of questions and answers below.

The perfect storm



- Vulnerabilities arising at the boundary where digital and physical connect
- The trading algorithms are a first example
- Smart grid vulnerabilities are another excellent example of possible positive feedback loops between the two realms

Conclusions

- We are brewing a perfect digital storm with unfathomable consequences
- We are using complex networks of digital systems to control *critical infrastructures* and *safety-critical* systems, without humans in the loop
- Threat level by (state/nonstate)-actors likely to act against these systems is constantly on the rise, and we are actively contributing to legitimize this
- We have issues with zero-days as well as forever-days, and we have significant upcoming threats (malicious hardware and interstitial layer threats)
- **We need significant engineering and research efforts** to get this done and avert the storm

Questions?

- Thank you for your attention!
- You can reach me at stefano.zanero@polimi.it
- Or just tweet @raistolo

Our research on these topics has been partially funded by the European Commission under FP7 project SysSec, and by NATO under SfP grant 983805