RSA Conference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: HTA-F03

From Ukraine to Pacemakers! The Real-World Consequences of Logical Attacks

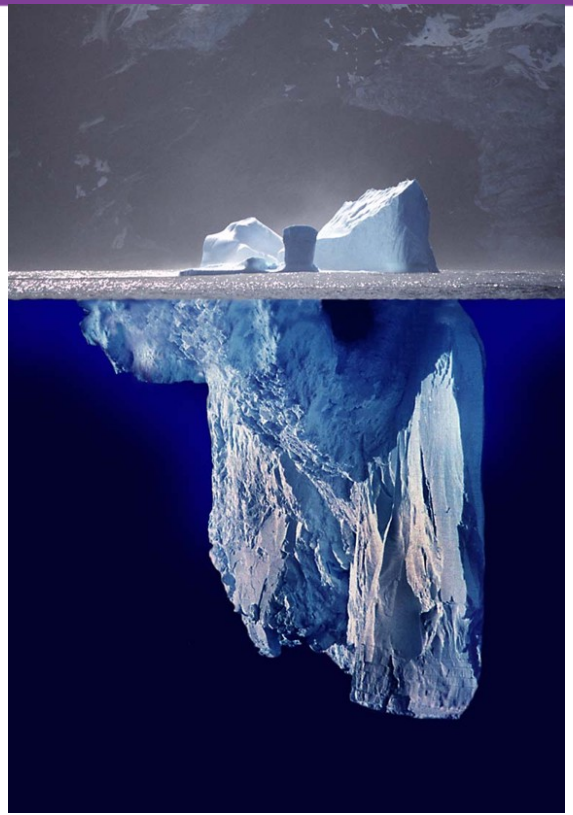
Éireann Leverett
Founder and CEO
Concinnity Risks
@concinnityrisks

Marie Moe
Research Scientist
SINTEF
@MarieGMoe

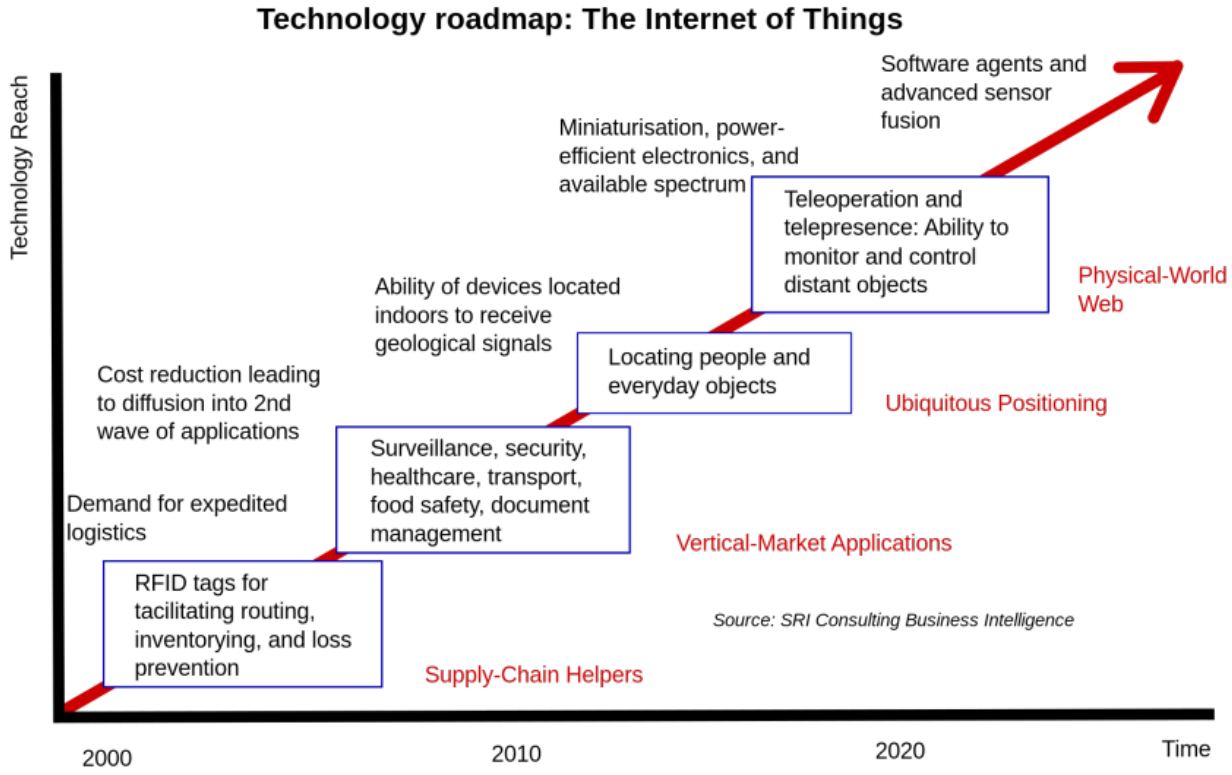
A tale of engineers and integrity…

The internet isn't virtual.

- In fact it never was.
- It just wasn't 'embodied' yet.
- What can we expect of cyber-physical security and failures?
- In other words, how deep is the iceberg?



IT / OT Big Picture

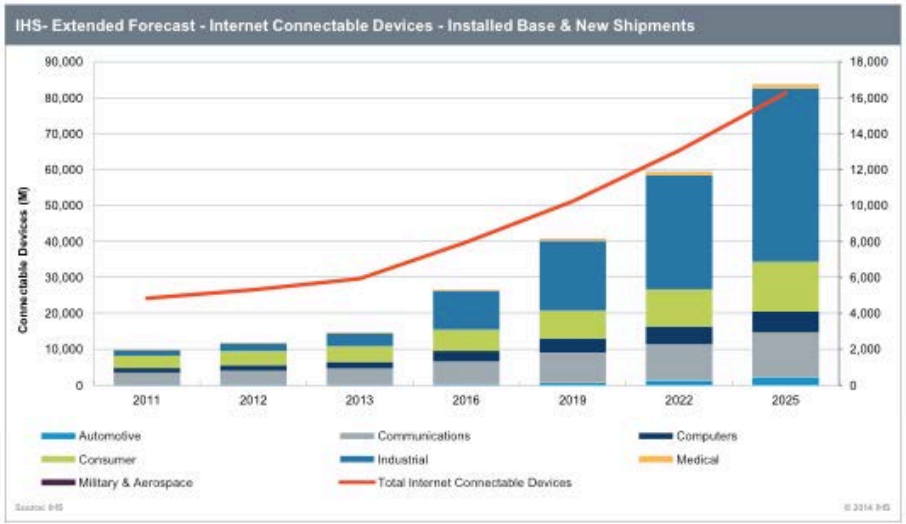


C02 Model (Let go of the CIA)

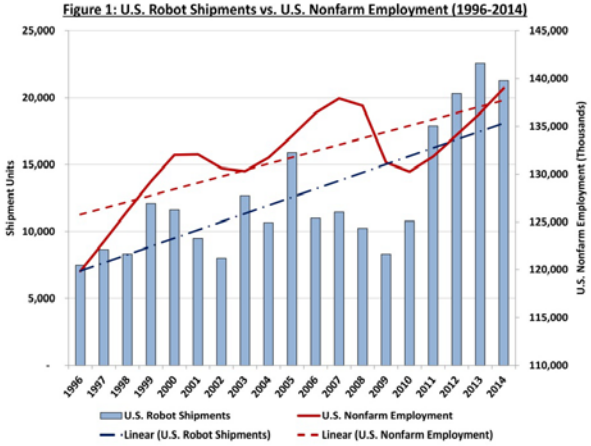
Controllability	Observability	Operability
Inability to bring the process or system into a desired state. Example failures include: • Control network not in a controllable state • There is no longer a control sequence which can bring the system into an intended state • The sequence of the control commands is unknown to the operator (because it has been altered or potentially altered) • Actuator has lost connectivity or power	Inability to measure state and maintain situational awareness. Example failures include: • Inability to monitor sensors (data integrity loss and/or loss of availability) • Untrustworthy measurement (data has lost veracity) • Measurement of all necessary quantities at the right locations is no longer possible • Inability to interpret the measurements e.g. changing the language of alerts	Inability of the device to achieve acceptable operations. Example failures include: • Inability to maintain optimal operations under attack • The physical device has been damaged e.g. motor burnt out, gear teeth ground down, pressure vessel burst • Inability to safely shut down • Multiple operators working against each other through same control channel

Let's simplify: How many actuators?

IoT Extended Forecast, 2011-2025



It is the growth of actuator sales that will define cyber-physical hacking, even more so than the hackers themselves.



Insecurity is a transitive property

Security isn't!

- If my computer is secure
- And my house is secure
- It doesn't imply my phone is secure

If my email is insecure:

- my passwords are known

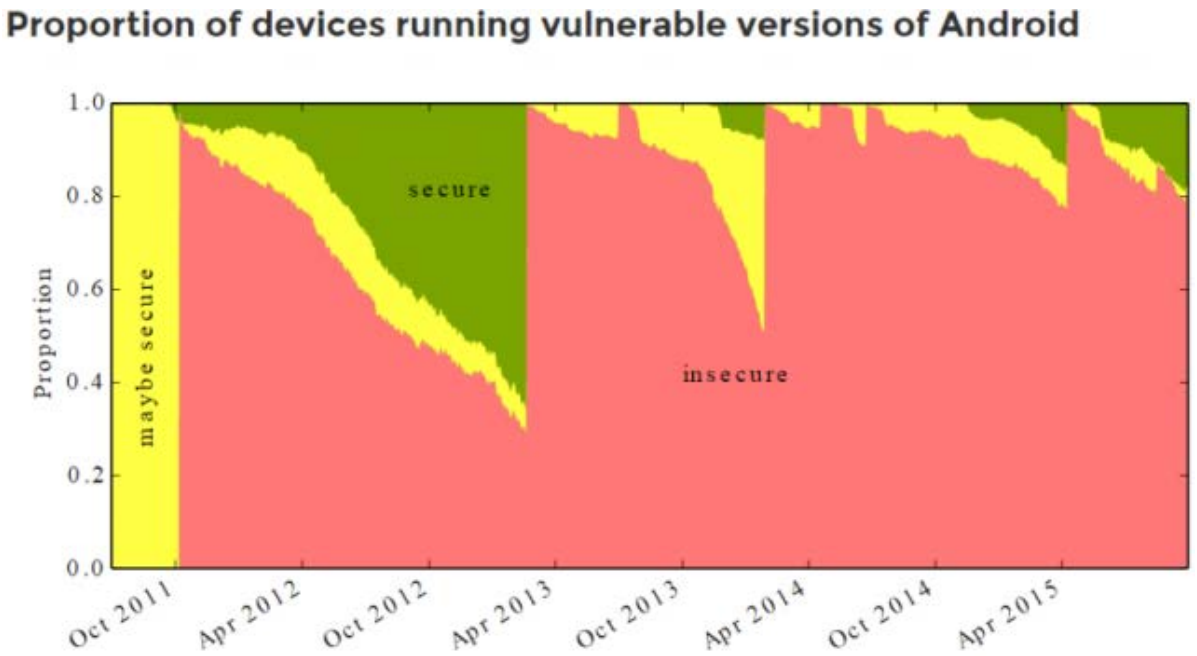
If my computer *was* insecure:

- my private keys are known
- it could ***still*** be spawning reverse shells

So insecurity is transitive in time also!

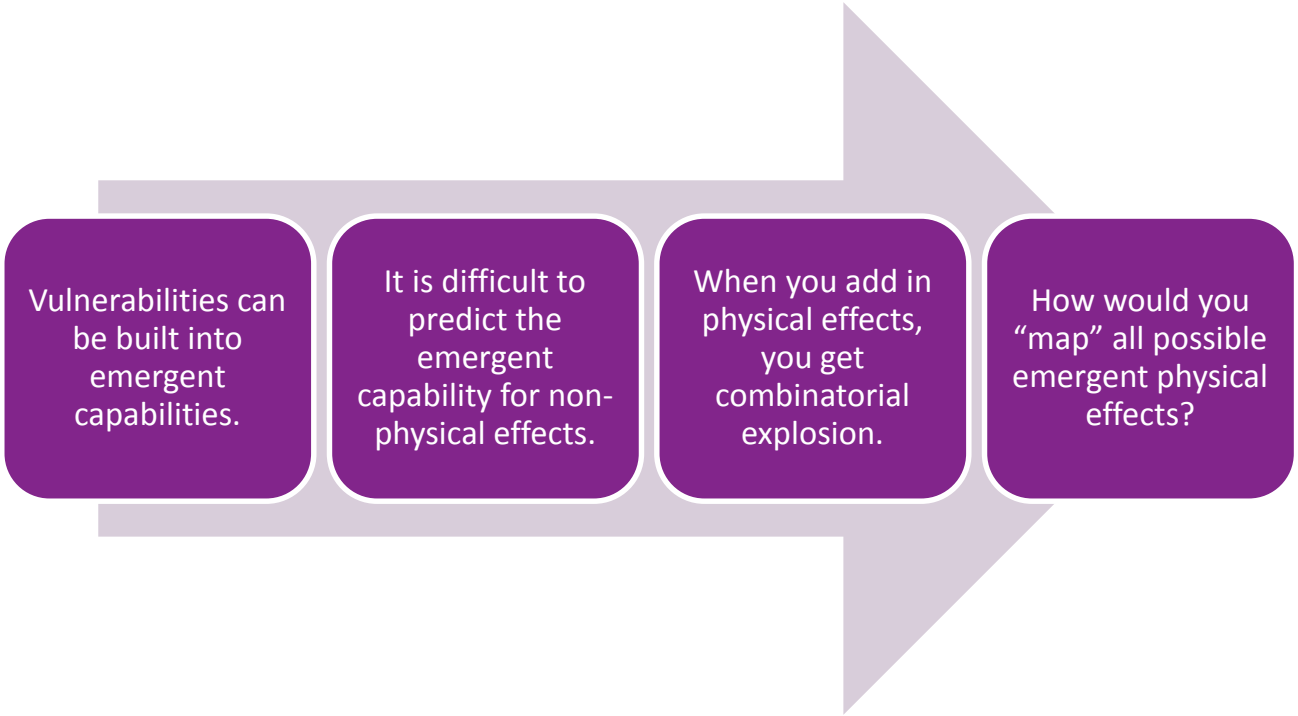
- What is the sum of vulnerabilities?
- Let's see how insecurity transitivity looks in time…

Vulnerable populations as a timeline.



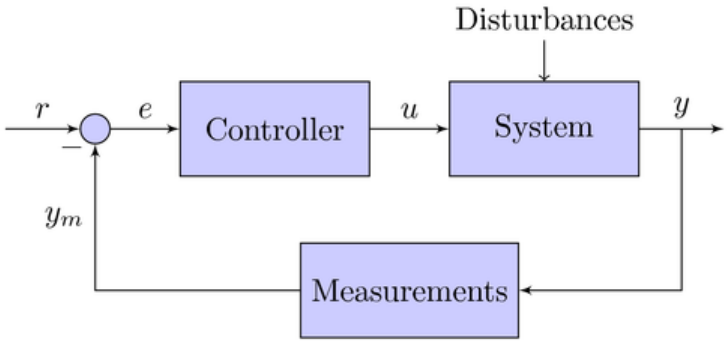
2015 Security Metrics for the Android Ecosystem (Thomas, Beresford, Rice)

Insecurity is compose-able

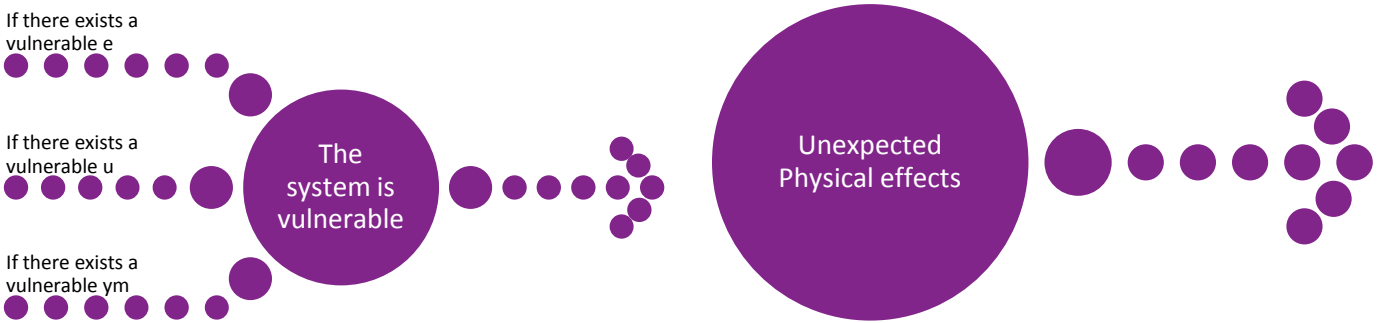


Now with added physical effects!

Remember the C02 Model?



Let's deep dive into that…



Sensors are vulnerable

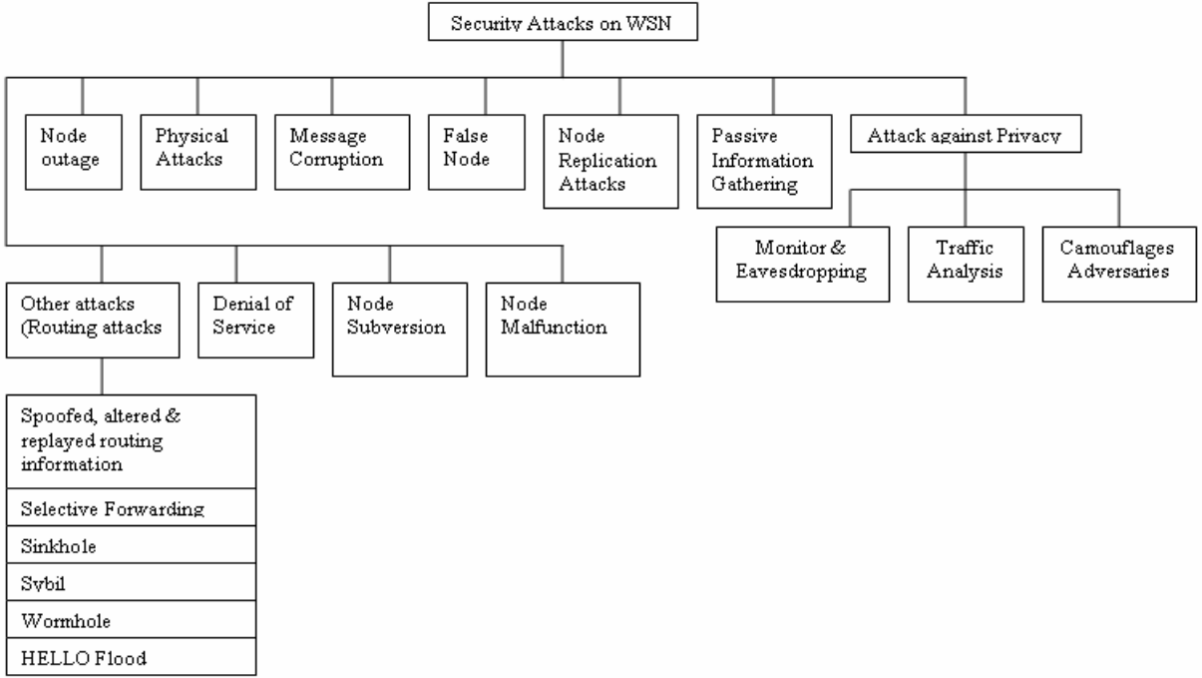


Figure 2. Classification of Security Attacks on WSN

Padmavathi, Dr G., and Mrs Shanmugapriya. "A survey of attacks, security mechanisms and challenges in wireless sensor networks."

Actuators are vulnerable

- “I Cannot Be Played on Record Player X”
- Has been true since (at least):
  - von Neumann’s Self-replicating kinematics
- A simple example is cars driving themselves off the road
- A complex example would be a robotic arm unplugging its’ network or power cable.
- We haven’t even discussed how they’re ‘digitally’ vulnerable yet, but that is true too.

Network devices are vulnerable

Switches Get Stitches

If connectivity is required by your business model, then every networking device is my point of subversion against your business.

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

HOME | ABOUT | ICSJWG | INFORMATION PRODUCTS | TRAINING | FAQ

Control Systems
- Home
- Calendar
- ICSJWG
- Information Products
- Training
- Recommended Practices
- Assessments
- Standards & References
- Related Sites
- FAQ

Advisory (ICSA-15-013-04A)
GE Multilink Switch Vulnerabilities (Update A)
More Advisories
Original release date: January 13, 2015 | Last revised: August 04, 2015
Print | Tweet | Send | Share

Legal Notice

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.

OVERVIEW

This updated advisory is a follow-up to the original advisory titled ICSA-15-013-04 GE MultiLink Switch Vulnerabilities that was published January 13, 2015, on the NCCIC/ICS-CERT web site.

--------- Begin Update A Part 1 of 3 ---------

Eireann Leverett of IOActive has identified three vulnerabilities in the General Electric (GE) Multilink ML800 series managed switches. GE Digital Energy has validated these vulnerabilities through testing and confirms that the issues affecting the ML800 will also affect the MultiLink series of managed Ethernet switches including the ML1200, ML1600, ML2400, ML810, ML3000, and ML3100. GE recommends that its customers upgrade switch firmware and disable the configuration web server to mitigate these vulnerabilities. These vulnerabilities have been publicly disclosed.

These vulnerabilities could be exploited remotely.

AFFECTED PRODUCTS

The following GE Multilink Ethernet switch is affected:

- GE Multilink ML800/1200/1600/2400 Version 4.2.1and prior, and
- GE Multilink ML810/3000/3100 series switch Version 5.2.0 and prior.

Protocols are Vulnerable

4.1.4 Redesign Network Protocols for Security

ICS network protocols and the service applications that implement them need to be redesigned for security. Most ICS network protocols were designed with the original ICS code base to be fast and only avoid failure issues and are not designed to provide robust authentication and integrity checks. Many protocol designs contain common security pitfalls. A number of characteristics of a secure protocol are relevant to this discussion.

1. Secure protocols should be simple. The more complex a protocol is, the higher the likelihood of bugs and vulnerabilities within the implementation.

developed, and one should expect to see more given the increasing interest in ICS security.

5. When possible, network protocols should be redesigned to improve security by avoiding common security pitfalls, avoiding designs that lead to implementation issues, and by including secure authentication and encryption methods.

4.1.5 Increase Robustness of Network Parsing Code

The robustness of network parsing code should be dramatically improved. Part of every network protocol is an associated program to build packets or process the traffic off the network. These applications are written by the ICS vendor for their propriety protocols as well as for common

Common Cybersecurity Vulnerabilities in Industrial Control Systems DHS 2011

Alarms are vulnerable

Vulnerability Note VU#662676

Digital Alert Systems DASDEC and Monroe Electronics R189 One-Net firmware exposes private root SSH key

Original Release date: 26 Jun 2013 | Last revised: 07 May 2014

Print Tweet Send Share

Overview

Digital Alert Systems DASDEC and Monroe Electronics One-Net E189 Emergency Alert System (EAS) devices exposed a shared private root SSH key in publicly available firmware images. An attacker with SSH access to a device could use the key to log in with root privileges.

Description

The Digital Alert Systems DASDEC-I and DASDEC-II and Monroe Electronics R189 One-Net/R189SE One-NetSE are Linux-based EAS encoder/decoder (ENDEC) devices that are used to broadcast EAS messages over digital and analog channels. IOActive has reported several security issues affecting these devices. The most severe of these issues is the public disclosure of the default private root SSH key. The less severe issues could also contribute to an attacker's ability to compromise a vulnerable device.

Compromised root SSH key (CVE-2013-0137)
Publicly available firmware images for these devices included a private root SSH key that was authorized to log in to the devices (CWE-798, CWE-321). The fingerprint for the compromised SSH key is 0c:89:49:f7:62:d2:98:f0:27:75:ad:e9:72:2c:68:c3. Although this key is not hard-coded, it may be impractical for less technical users to manually disable or change they key prior to firmware version 2.0-2.

Predictable session ID
IOActive reports that the administrative web server uses a predictable, monotonically increasing session ID. This finding is based on running the web server in a test environment. Testing on a variety of firmware versions on devices both at the factory and in the field, Monroe Electronics could not reproduce this finding.

Log information disclosure
Logs available via the web server provide a variety of information about the configuration, operation, and status of the device (CWE-532). Some of the log information is public and may be required by regulation.

Predictable password generation

Background

Siemens SIMATIC HMI is a software package used as an interface between the operator and the programmable logic controllers (PLCs) controlling the process. SIMATIC HMI performs the following tasks: process visualization, operator control of the process, alarm display, process value and alarm archiving, and machine parameter management. This software is used in many industries, including food and beverage, water and wastewater, oil and gas, and chemical.

Cross-Site Scripting[1]

WinCC web applications are susceptible to reflected cross-site scripting because they do not filter out characters when parsing URL parameters. Exploitation of this vulnerability may give an attacker authenticated access to WinCC web applications.

CVE-2012-2595 has been assigned to this vulnerability. A CVSS v2 base score of 4.3 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:N/I:P/A:N).

XML (XPATH Injection)[2]

Web applications do not filter out special characters when parsing URL parameters. An attacker may exploit this vulnerability to read or write settings on the system.

CVE-2012-2596 has been assigned to this vulnerability. A CVSS v2 base score of 5.5 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:S/C:P/I:P/A:N).

Directory Traversal[3]

Web applications do not sanitize URL parameters. An authenticated attacker can read arbitrary files on the system.

CVE-2012-2597 has been assigned to this vulnerability. A CVSS V2 base score of 6.8 has also been assigned; the CVSS vector string is (AV:N/AC:L/Au:S/C:C/I:N/A:N).

Buffer Overflow

The DiagAgent Web server is used for remote diagnostic purposes and is disabled by default. If the service is enabled, it does not sanitize user input correctly. Specially crafted input can crash the DiagAgent, disabling the remote diagnostic service.

CVE-2012-2598 has been assigned to this vulnerability. A CVSS V2 base score of 4.3 has also been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:N/I:N).

Cross-Site Scripting[4]

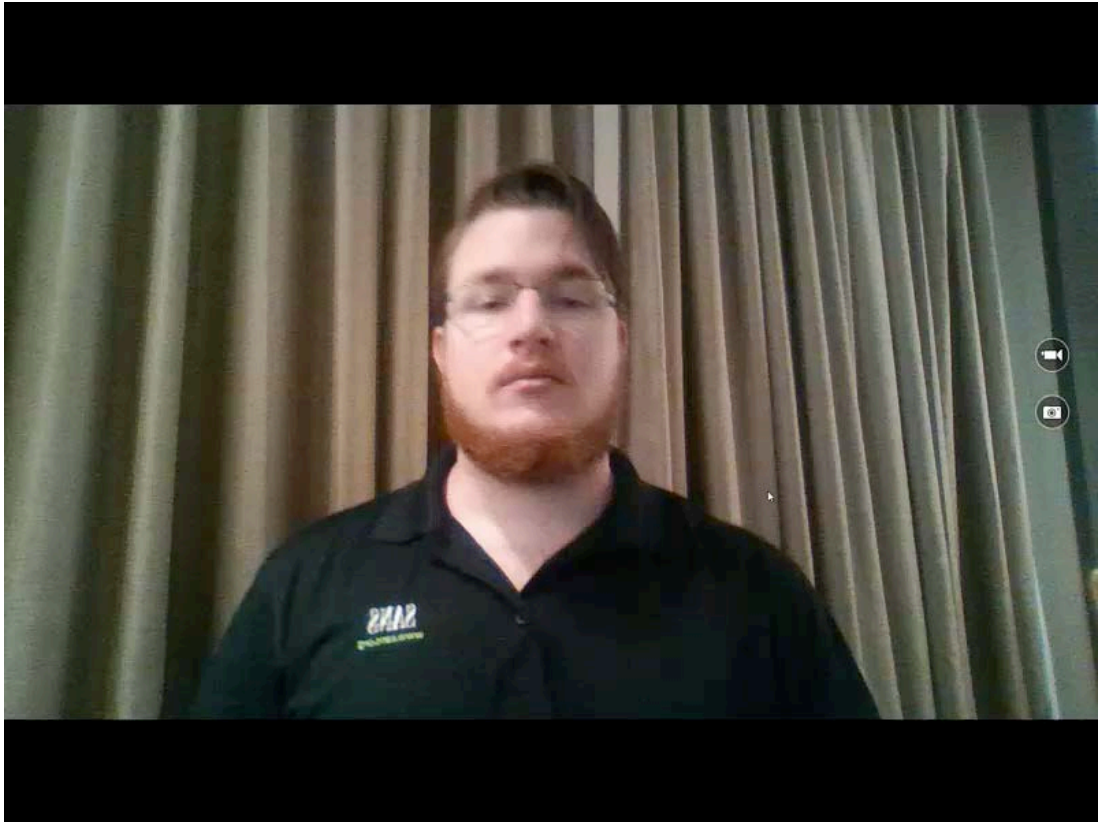
A Web application accepts a parameter in a HTTP GET request and interprets it as a URL. The victim's browser is then redirected to that URL.

If a victim clicks on a link that was prepared by an attacker, the victim's browser could be redirected to a malicious Web site instead of the WinCC system.

CVE-2012-3003 has been assigned to this vulnerability. A CVSS V2 base score of 3.4 has also been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:N/I:P).


LITTLE BOBBY
by Robert M. Lee and Jeff Haas
I HEARD THERE WAS AN ATTACK IN UKRAINE ON THE POWER GRID!
YES-- A CYBER ATTACK THAT ACTUALLY CAUSED A POWER OUTAGE.
GOOD THING THAT CAN'T HAPPEN HERE!
THE IMPACT WOULD BE DIFFERENT-- BUT IT CAN DEFINITELY HAPPEN HERE.
NOT IF I CHOOSE TO BELIEVE IT CAN'T!
THAT'S NOT HOW REALITY WORKS.
HAAS

Guest: Robert M Lee



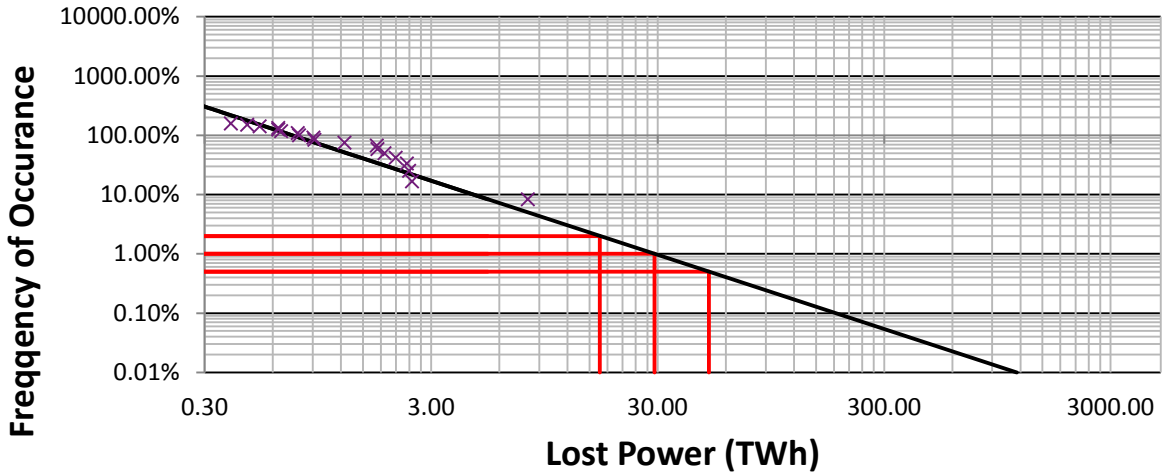
@RobertMLee

For deeper analysis:

ics.sans.org/duc5

Please tweet widely ☺

Ukranian Outage Return Period



- 0.8 Twh lost maps to roughly a 1 in 2 year event by US standards
- So while this is significant from a hacking perspective, it is not very significant from a power engineering perspective.

The cost of US power outages

Table 7 lists the predictors of outage cost (also known as "parameters") by customer class in the Tobit regression equations. The intercept represents the point at which the plotted line crosses the y axis (the y-axis-intercept point, βo) from the following standard statistical Tobit multiple regression expression which is not linear due to the logarithmic nature of outage costs:

$$Y = Exp[\beta_o + \beta_1 X_1 + \beta_2 X_2 + ... + \beta_n X_n + \varepsilon] + e$$

where X_n is the independent variable, β_n is the regression coefficient for each predictor, and ε and e represent error terms. This intercept point where the trend line for the points in the plot of outage costs crosses the y-axis is a starting point for the outage cost estimate, which is then refined and adjusted according to the other parameters listed in Table 7.

Table 10. Tobit Regression Estimated Cost-per-Outage-per-Customer for the U.S.[1]

Duration	Residential	Commercial	Industrial
0 sec	$2.18	$605	$1,893
1 hour	$2.70	$886	$3,253
Sustained Interruption	$2.99	$1,067	$4,227

[1]Costs shown in U.S. 2002 CPI-weighted dollars

LaCommare, Kristina Hamachi, and Joseph H. Eto. "Understanding the cost of power interruptions to US electricity consumers." Lawrence Berkeley National Laboratory (2004)

"IoT cannot be immortal and unfixable."
-Dan Geer
BlackHat 2014

- Who will be responsible for IR costs for IoT?
  - Are we privatising sales and socialising IR?
  - Is insurance starting to make sense yet?
  - If not for critical infrastructure, then are you ready to talk about medical device cyber insurance?

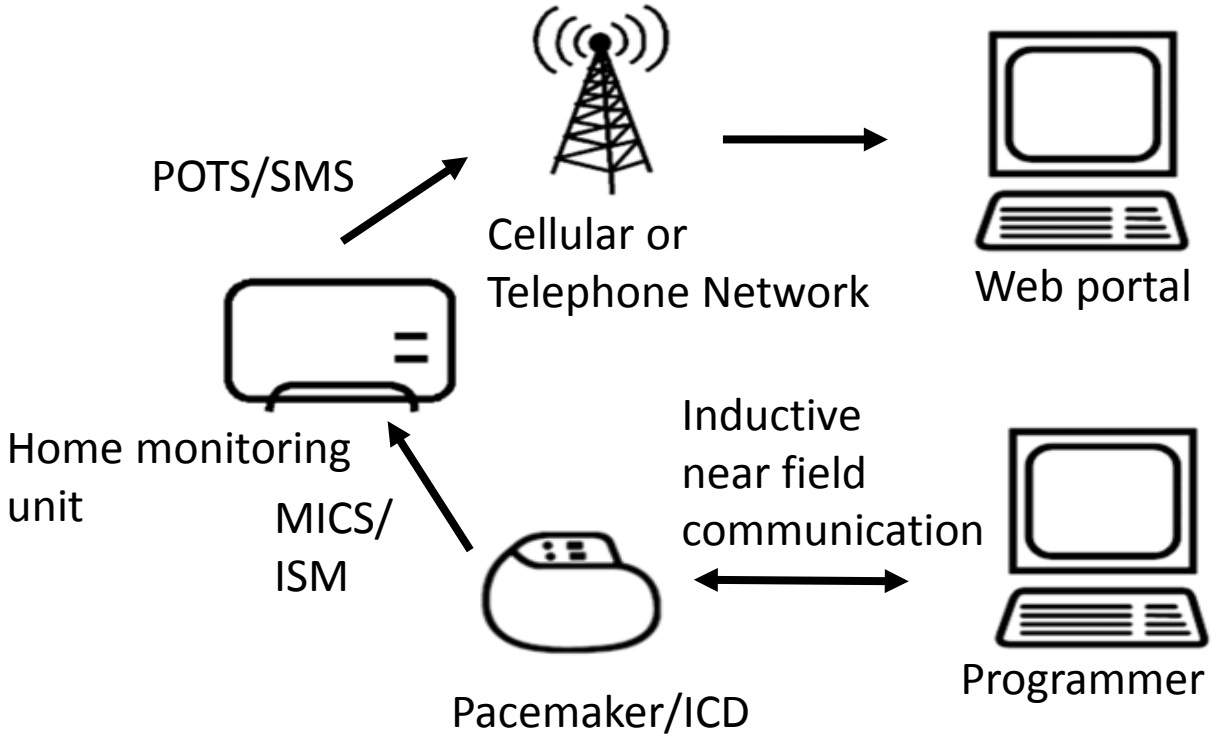
Personal Infrastructure

Your reliance on an infrastructure is inversely proportional to how invisible it is to you.

We all rely on oxygen, our lungs, and our hearts, but how often to we think about them?

How often do we do maintenance or debug them?

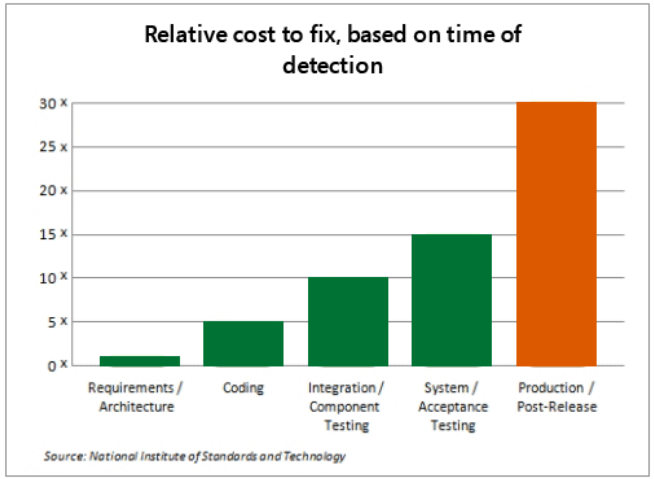
My Personal Critical Infrastructure



Debugging me

What is the same between big and little infrastructure?

- The cost of failure is “embedded” (damage)
- The Economic Impacts of Inadequate Infrastructure for Software Testing (2002)



This table should be extended table to include:

Vulnerability exploited in the wild

And

Vulnerability exploited in an infrastructure

Now our vulnerability is “embodied”

Vehicle to Vehicle	Smart Grid	Robotics
Traffic Control	Maritime	Industrial manufacturing
Autonomous Vehicles	Logistics Systems	Aircraft

So is the cost of failure!

Asymmetric adversarial economics.

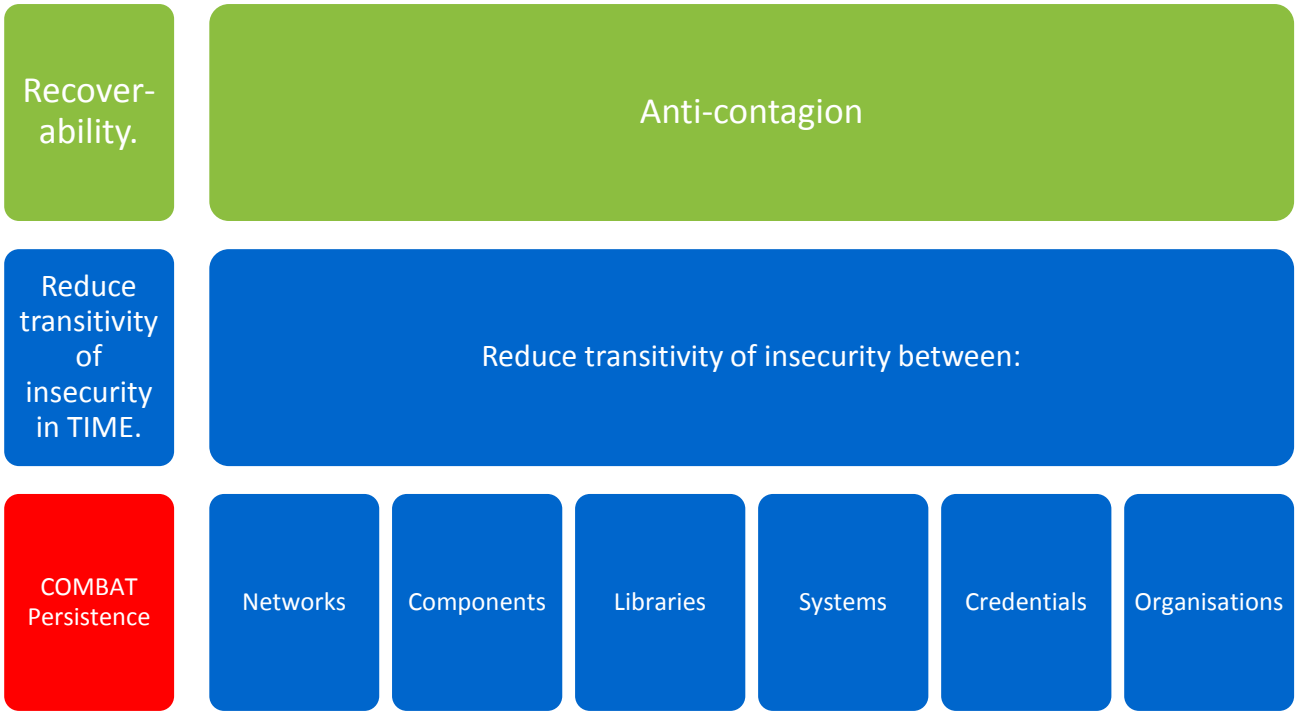
Harm Type	Impact	Payload reuse	Cost of remedy	Social cost
Data	Non-Zero Sum	High	Low	Individual
Physical	Zero Sum	Low	High	Collective

again highlights the asymmetrical economic nature of cyber escalation and disruption.

The cost of finding and exploiting critical infrastructure will continue to fall. The marginal cost of copying vulnerable infrastructure lists or exploits will tend towards zero. The cost of producing a disruption for attackers will continue to reduce, while the cost of disruption remediation will remain relatively constant. Therefore our best hope is if the cost of defending and technical security innovation is as low as the cost of discovering or disrupting vulnerable infrastructure.

Asymmetric digital warfare is an asymmetric economy, with falling costs for those bent on disruption and fixed costs for the society disrupted.

So what should our design goals be?



The hidden cost of the Solow residual?

1. Quantify the cost to society for a 10 hour outage to each critical infrastructure in the largest region covered by one company.
2. Quantify the cost of 70%/50%/30%/1% vulnerable IoT deployments.
3. Quantify the cost of medical device physical impacts on 1%/5%/20% of the population.

I think this is where we went wrong.
We focused on ”how does/can it fail;
... not how much will it cost us?”

I Am The Cavalry

The Cavalry isn't coming... It falls to us

Problem Statement

Our society is adopting connected technology *faster than we are able to secure it*.

Mission Statement

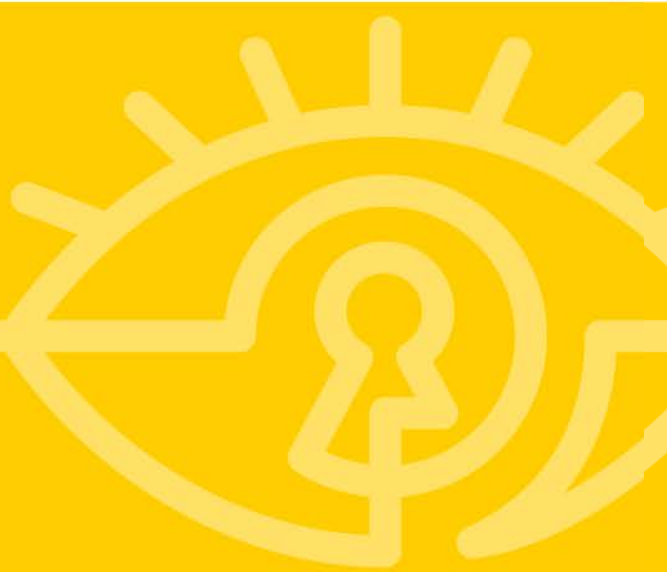
To ensure connected technologies with the potential to impact public safety and human life are *worthy of our trust*.

Why Trust, public safety, human life
How Education, outreach, research
Who Infosec research community
Who Passionate volunteers
What Long-term vision for cyber safety

Collecting existing research, researchers, and resources
Connecting researchers with each other, industry, media, policy, and legal
Collaborating across a broad range of backgrounds, interests, and skillsets
Catalyzing positive action sooner than it would have happened on its own

Apply what you have learned today

- Rename the IoT
  - Start writing use-cases!
- The failure of your code can ruin our future
  - Go home and quantify the cost of failure!
- The Siren song of impact assessment ranking
  - The payload is not the exploit
- Quantify the cost of a failure in your system.
- Are you resilient?



Questions & Thank you!

Éireann Leverett
www.concinnityrisks.com
@concinnityrisks
@blackswanburst

Robert M Lee
www.dragossecurity.com
@RobertMLee

Marie Moe
www.sintef.no/en
@MarieGMoe