RiskBased
SECURITY

Internet of Things Gone Wild

Carsten Eiram
Chief Research Officer
che@riskbasedsecurity.com / @CarstenEiram

Risk Based Security – Who Are We?

Community offerings:

OSVDB

MY PRIVACY AUDIT

DATALOSS db open security foundation

SECore .info beta

Commercial offerings:

VulnDB Risk Based Security

Cyber Risk Analytics

YOUR CISO

Important Words From the Previous Talk

CISOs must understand the effects of successful attacks

What damage will it do?

- Hanns Proenen

Internet of Things – Definition?

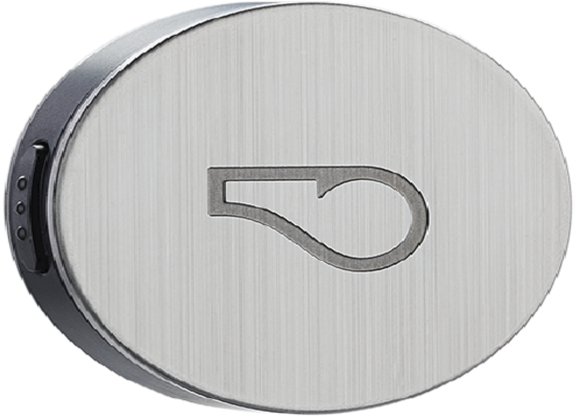
Internet of Things – Our Definition For This Talk

1. Needs to be networked / connected

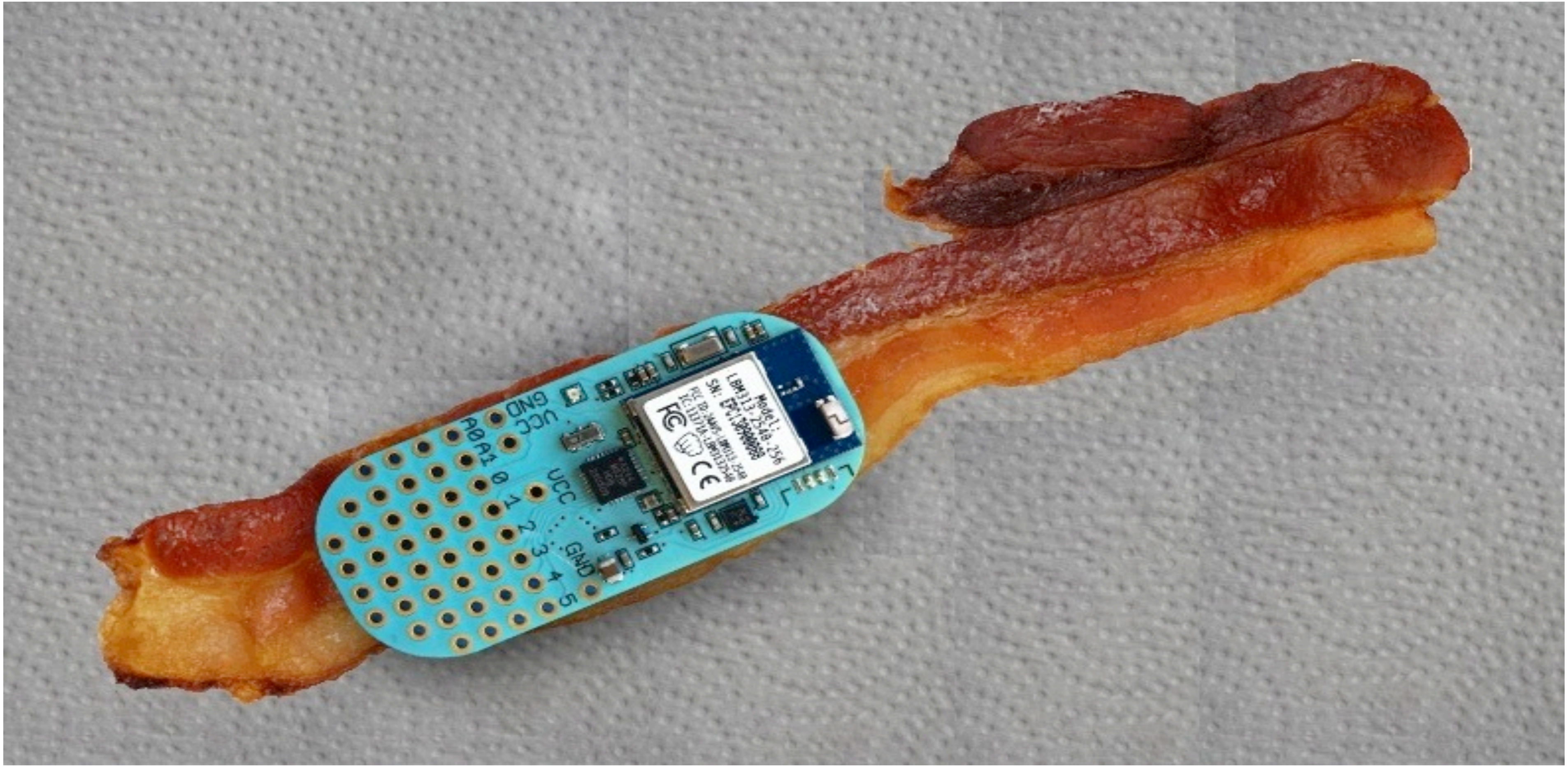
2. Some capability of sensing and decision making without human interaction/control

IoT Products Gone Wild!

Internet of Things – Examples (Everyday Life)



Internet of Things – It’s Everywhere



Internet of Things – Examples (Just because we can...)

Internet of Things - Definition

Looking past all the hype, IoT does not just pertain to consumers.

From a business perspective, it can:

- help to cut costs
- save time
- improve productivity and efficiency.

Internet of Things – Process

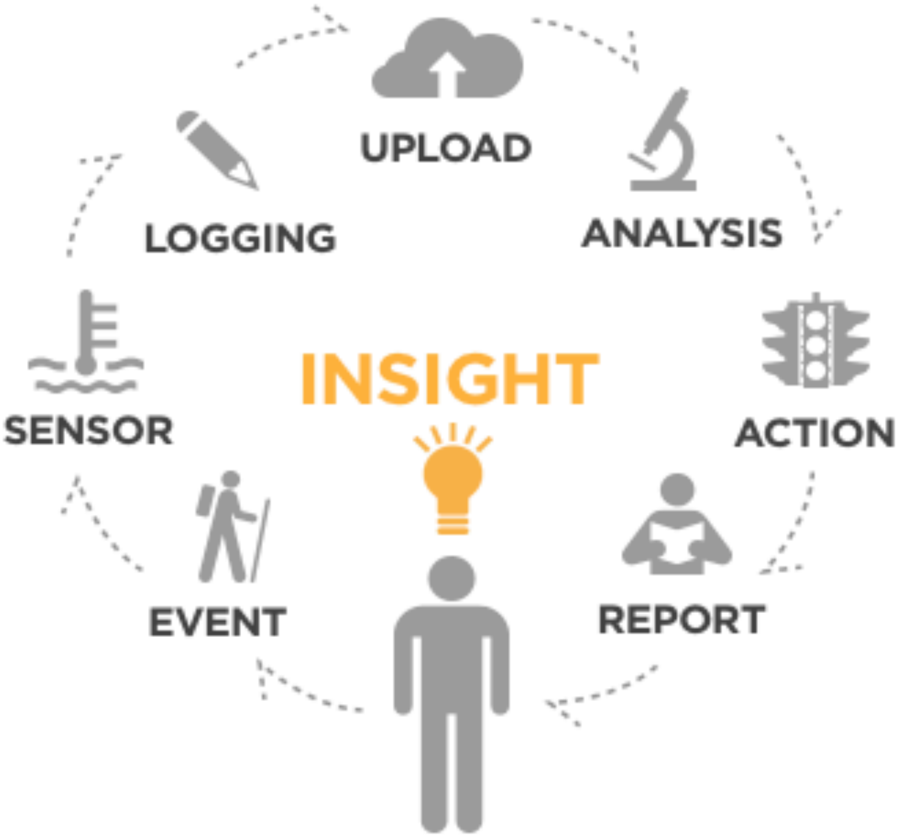
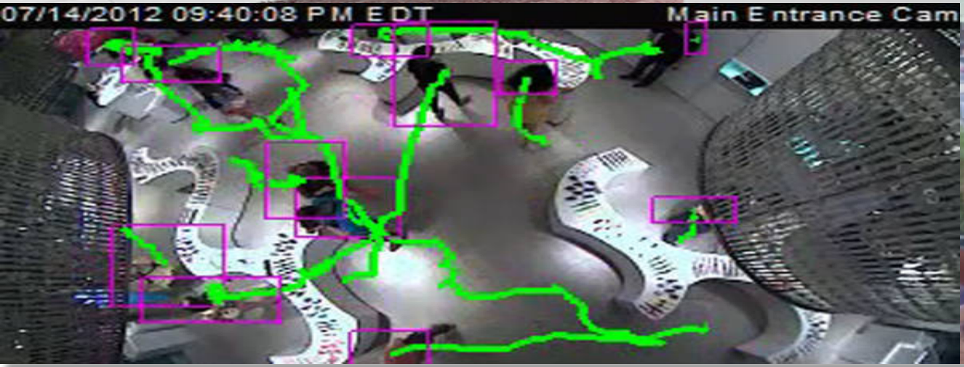
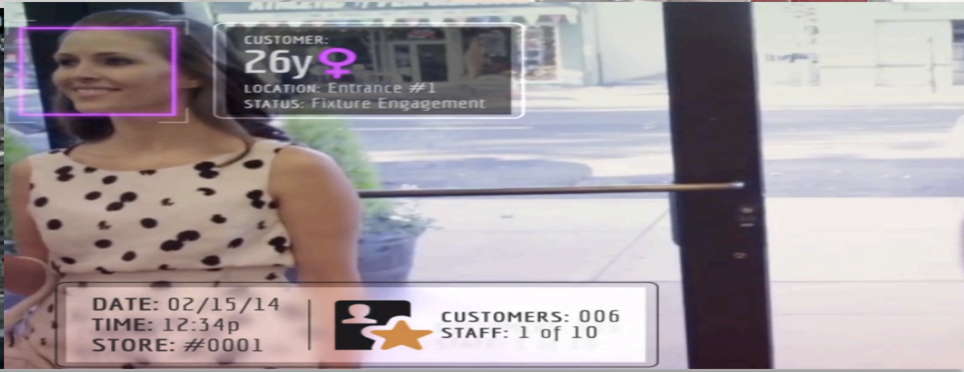


Image source: http://www.business2community.com/tech-gadgets/four-internet-of-things-trends-0273289

Internet of Things – Examples (Retail)



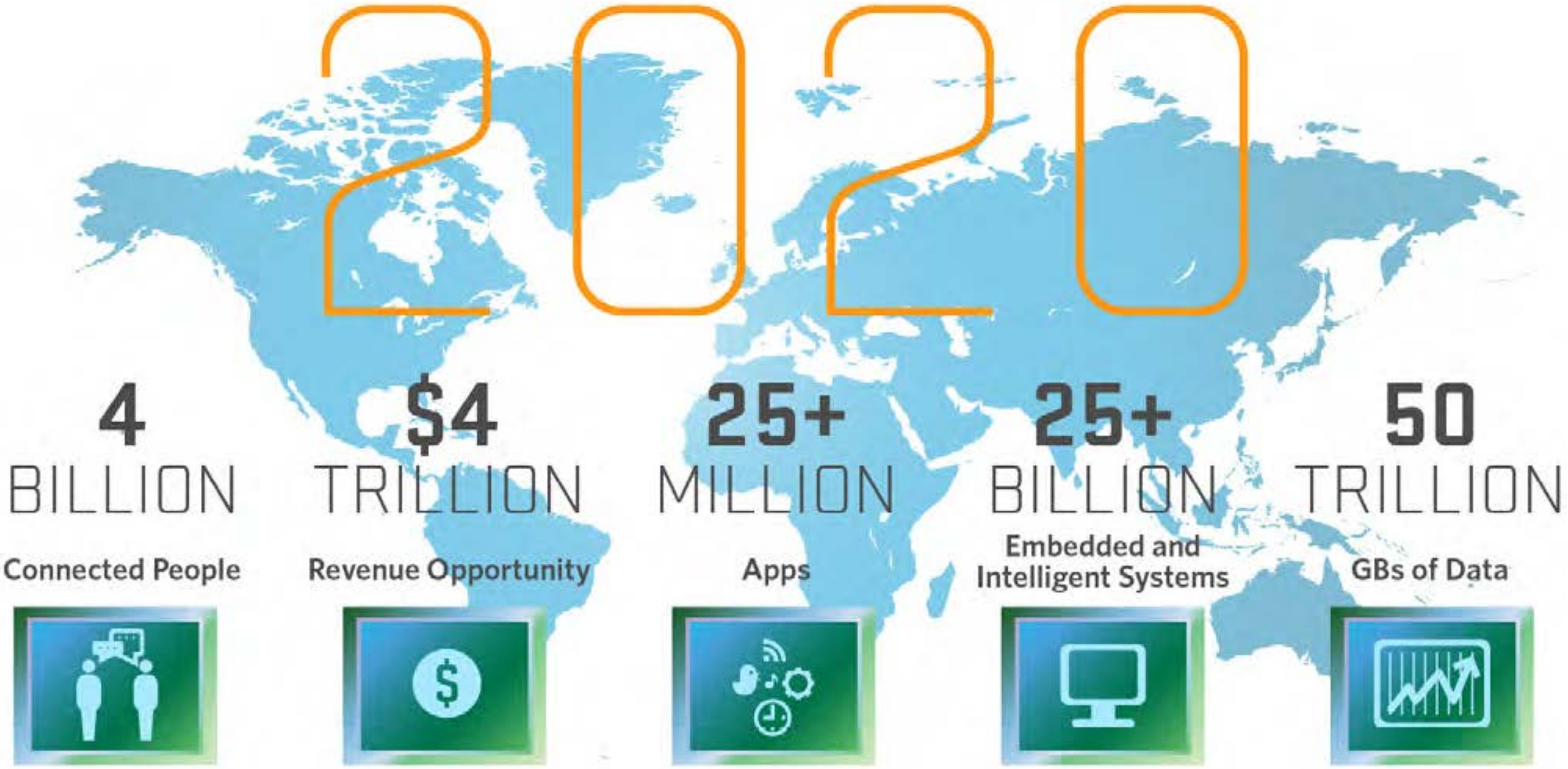


Internet of Things – Examples (Environmental)

Internet of Things – Examples (Your Network?)

Internet of Things – Examples (Your Network?)

Internet of Things – Why Should You Care?



2020

4 BILLION
Connected People

$4 TRILLION
Revenue Opportunity

25+ MILLION
Apps

25+ BILLION
Embedded and Intelligent Systems

50 TRILLION
GBs of Data

Source: Mario Morales, IDC

Internet of Things – What About YOUR Network?

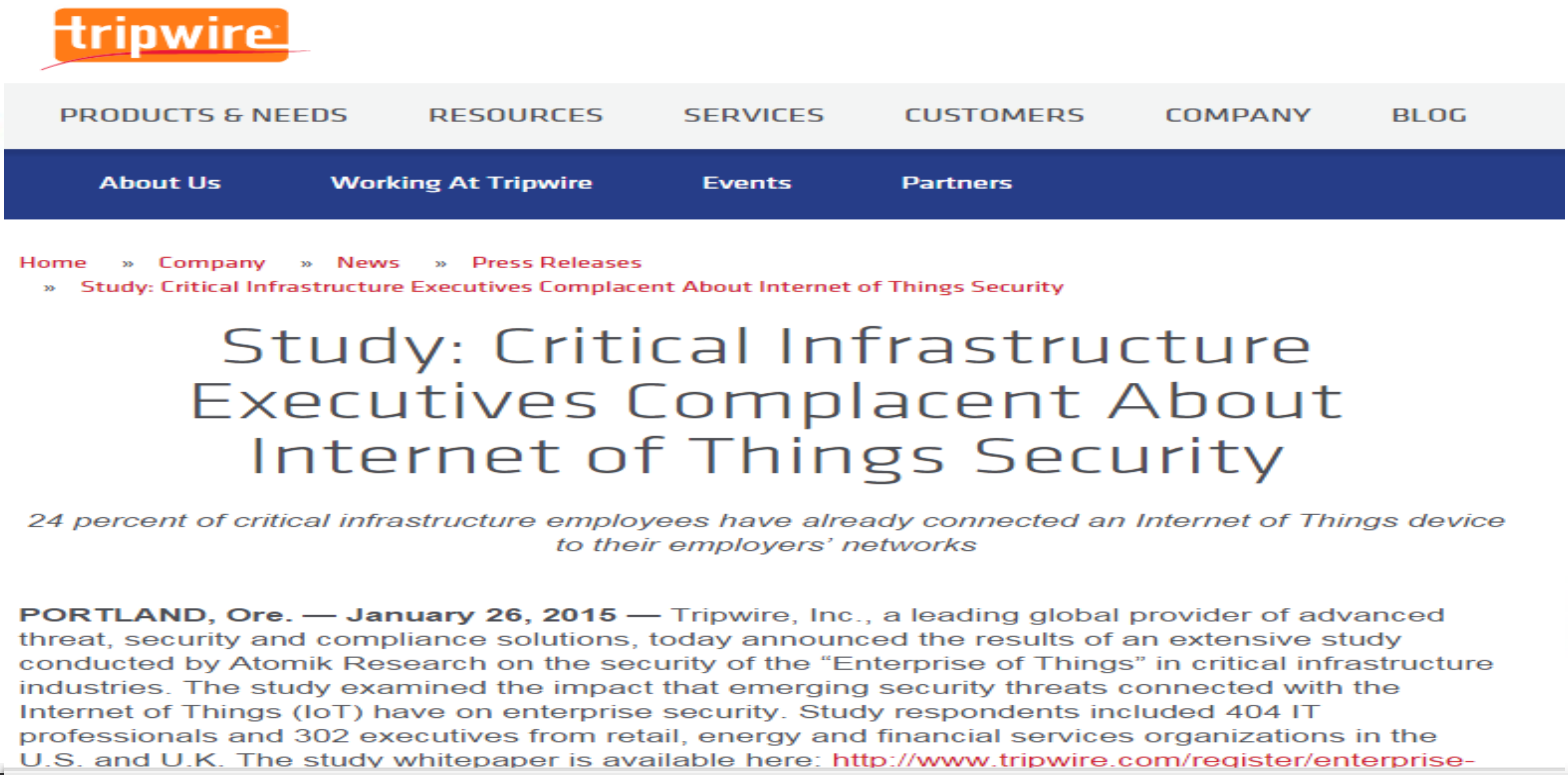
How many IoT devices are on your network today?

How many of them do you know about?

If they are not already on your company network,
they will be soon!

IoT Concern Gone Wild!

Internet of Things – Tripwire Study


PRODUCTS & NEEDS
RESOURCES
SERVICES
CUSTOMERS
COMPANY
BLOG
About Us
Working At Tripwire
Events
Partners
Home » Company » News » Press Releases » Study: Critical Infrastructure Executives Complacent About Internet of Things Security

Study: Critical Infrastructure Executives Complacent About Internet of Things Security

24 percent of critical infrastructure employees have already connected an Internet of Things device to their employers' networks

PORTLAND, Ore. — January 26, 2015 — Tripwire, Inc., a leading global provider of advanced threat, security and compliance solutions, today announced the results of an extensive study conducted by Atomik Research on the security of the "Enterprise of Things" in critical infrastructure industries. The study examined the impact that emerging security threats connected with the Internet of Things (IoT) have on enterprise security. Study respondents included 404 IT professionals and 302 executives from retail, energy and financial services organizations in the U.S. and U.K. The study whitepaper is available here: http://www.tripwire.com/register/enterprise-

Internet of Things – Tripwire Key Findings

63% of executives expect business efficiencies and productivity to force adoption of IoT devices despite security risks

46% say that IoT has the potential to become "the most significant risk" on their networks

http://www.tripwire.com/company/news/press-release/study-critical-infrastructure-executives-complacent-about-internet-of-things-security/

Internet of Things – Tripwire Key Findings

59% of IT personnel working in medium- and large-sized businesses are concerned that IoT could become "the most significant security risk" on their networks

http://www.tripwire.com/company/news/press-release/study-critical-infrastructure-executives-complacent-about-internet-of-things-security/

Internet of Things – Tripwire Key Findings

Only 30% of IT professionals believe their company has the technology necessary to adequately evaluate the security of IoT devices

1/5 of the respondents stated that they have ***"no visibility"*** into current protection levels

http://www.tripwire.com/company/news/press-release/study-critical-infrastructure-executives-complacent-about-internet-of-things-security/

Internet of Things – It's Hard!

Internet of Things – Tripwire Key Findings

24% of employees have connected at least one IoT device to their enterprise networks

http://www.tripwire.com/company/news/press-release/study-critical-infrastructure-executives-complacent-about-internet-of-things-security/

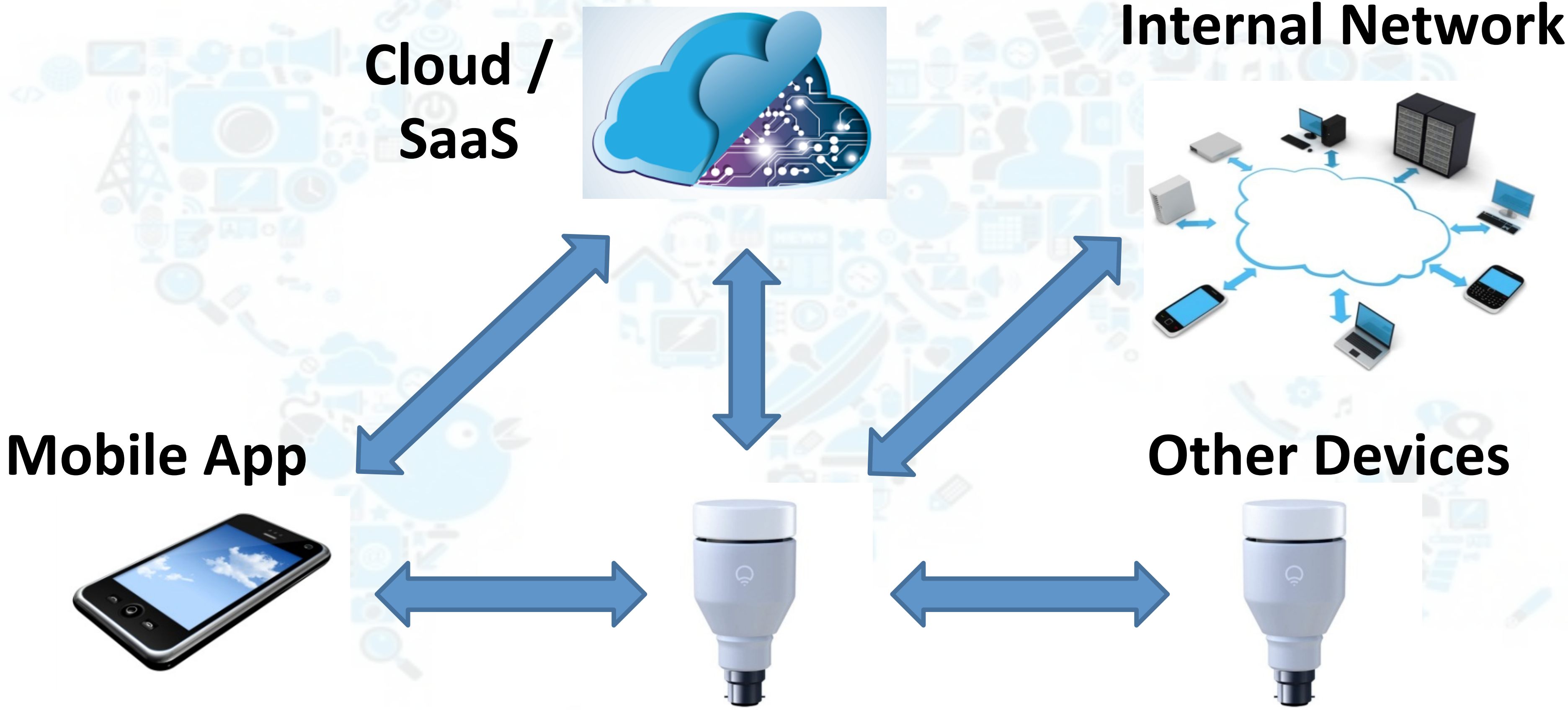
Internet of Things – More Shadow IT With IoT!

SHADOW IT

COMING TO A DEPARTMENT NEAR YOU.

IoT Attack Surface
Gone Wild!

Internet of Things - Communication



Cloud / SaaS

Internal Network

Mobile App

Other Devices

Internet of Things – Devices (ASA)

- Remotely accessible services with proper authentication / authorization?
- Secured communication with other devices, clients, cloud?
- Secure firmware updating?

Internet of Things – It's Not Just WiFi

During a wireless assessment of a client's WiFi network, InGuardians sniffed for ZigBee, Z-wave, and other 900 MHz traffic common for IoT devices

It was found that the building contained a ZigBee network that the client was not aware of

This network supported devices controlling the building's HVAC system, which put the company's manufacturing process at risk

http://www.forbes.com/sites/sungardas/2015/01/29/the-internet-of-things-has-a-growing-number-of-cyber-security-problems/

Internet of Things – Mobile App (ASA)

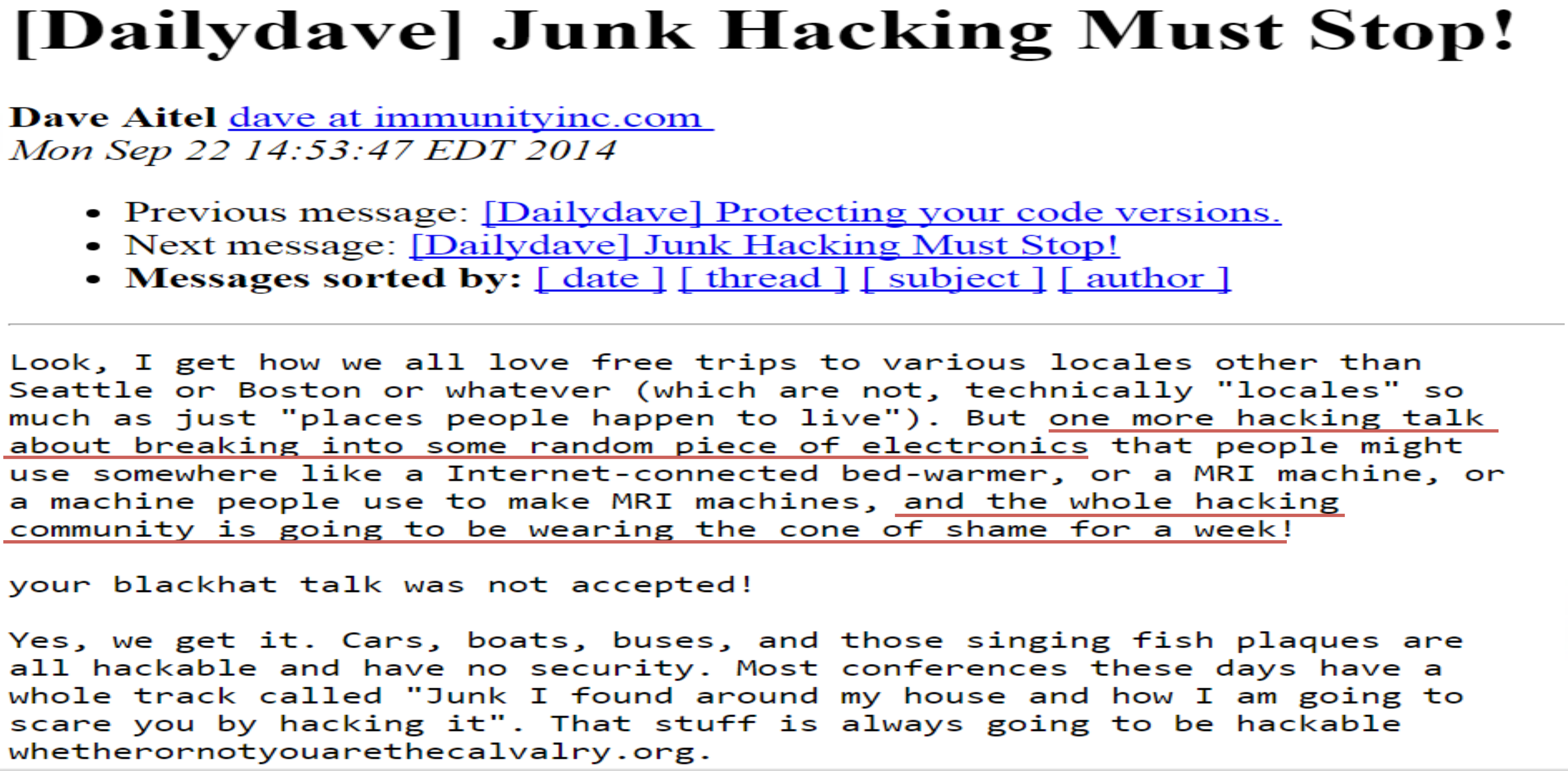
- Remotely accessible services with proper authentication / authorization?
- Secure storage of data? Loss of device may be similar to losing keys to the kingdom.
- Secure communication to cloud and devices?

Internet of Things – Cloud (ASA)

- Servers securely configured?
- Mature patch strategy e.g. using VI solution?
- Secure storage of data?
- Redundancy and do devices work if no connectivity to cloud?

IoT Research Gone Wild!

Internet of Things – Junk Hacking



[Dailydave] Junk Hacking Must Stop!

Dave Aitel dave at immunityinc.com
Mon Sep 22 14:53:47 EDT 2014

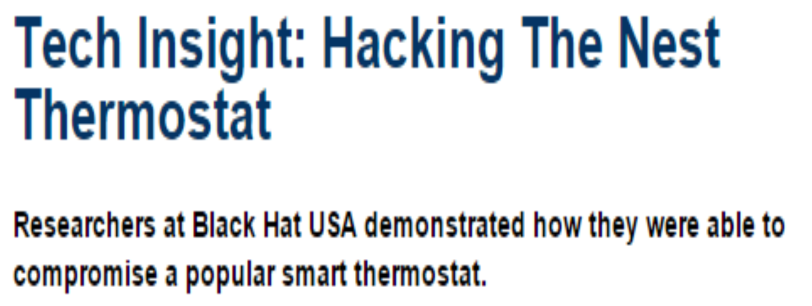
- Previous message: [Dailydave] Protecting your code versions.
- Next message: [Dailydave] Junk Hacking Must Stop!
- **Messages sorted by:** [date] [thread] [subject] [author]

Look, I get how we all love free trips to various locales other than Seattle or Boston or whatever (which are not, technically "locales" so much as just "places people happen to live"). But one more hacking talk about breaking into some random piece of electronics that people might use somewhere like a Internet-connected bed-warmer, or a MRI machine, or a machine people use to make MRI machines, and the whole hacking community is going to be wearing the cone of shame for a week!

your blackhat talk was not accepted!

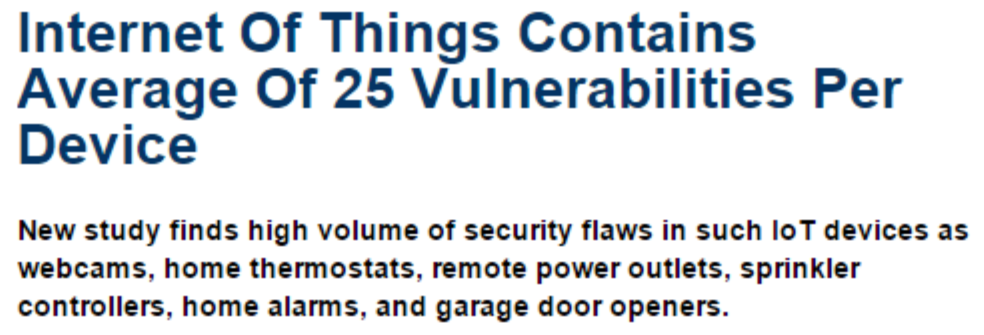
Yes, we get it. Cars, boats, buses, and those singing fish plaques are all hackable and have no security. Most conferences these days have a whole track called "Junk I found around my house and how I am going to scare you by hacking it". That stuff is always going to be hackable whetherornotyouarethecalvalry.org.

Internet of Things – IoT Vulns So Far?



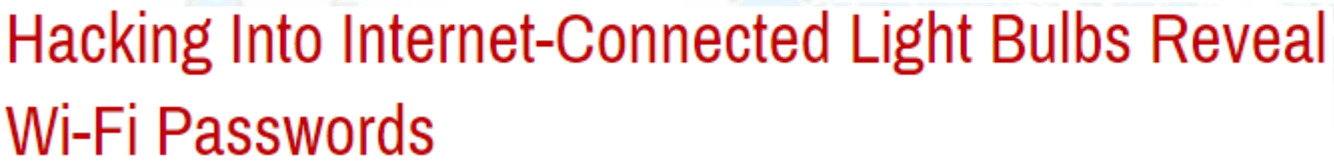
Tech Insight: Hacking The Nest Thermostat

Researchers at Black Hat USA demonstrated how they were able to compromise a popular smart thermostat.

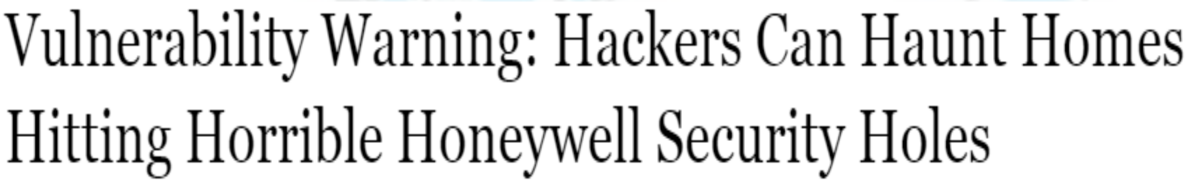


Internet Of Things Contains Average Of 25 Vulnerabilities Per Device

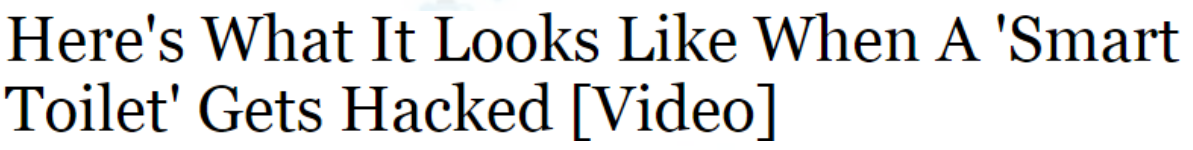
New study finds high volume of security flaws in such IoT devices as webcams, home thermostats, remote power outlets, sprinkler controllers, home alarms, and garage door openers.



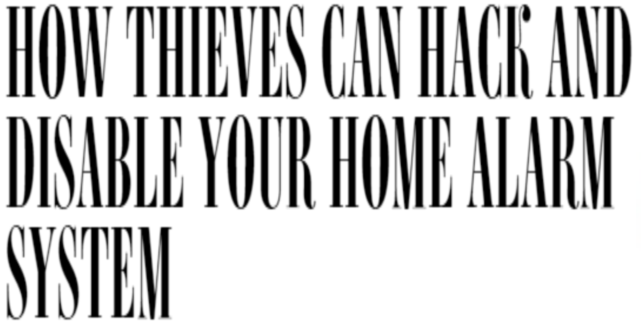
Hacking Into Internet-Connected Light Bulbs Reveal Wi-Fi Passwords



Vulnerability Warning: Hackers Can Haunt Homes Hitting Horrible Honeywell Security Holes



Here's What It Looks Like When A 'Smart Toilet' Gets Hacked [Video]



HOW THIEVES CAN HACK AND DISABLE YOUR HOME ALARM SYSTEM

Why so relatively few critical vulnerabilies?

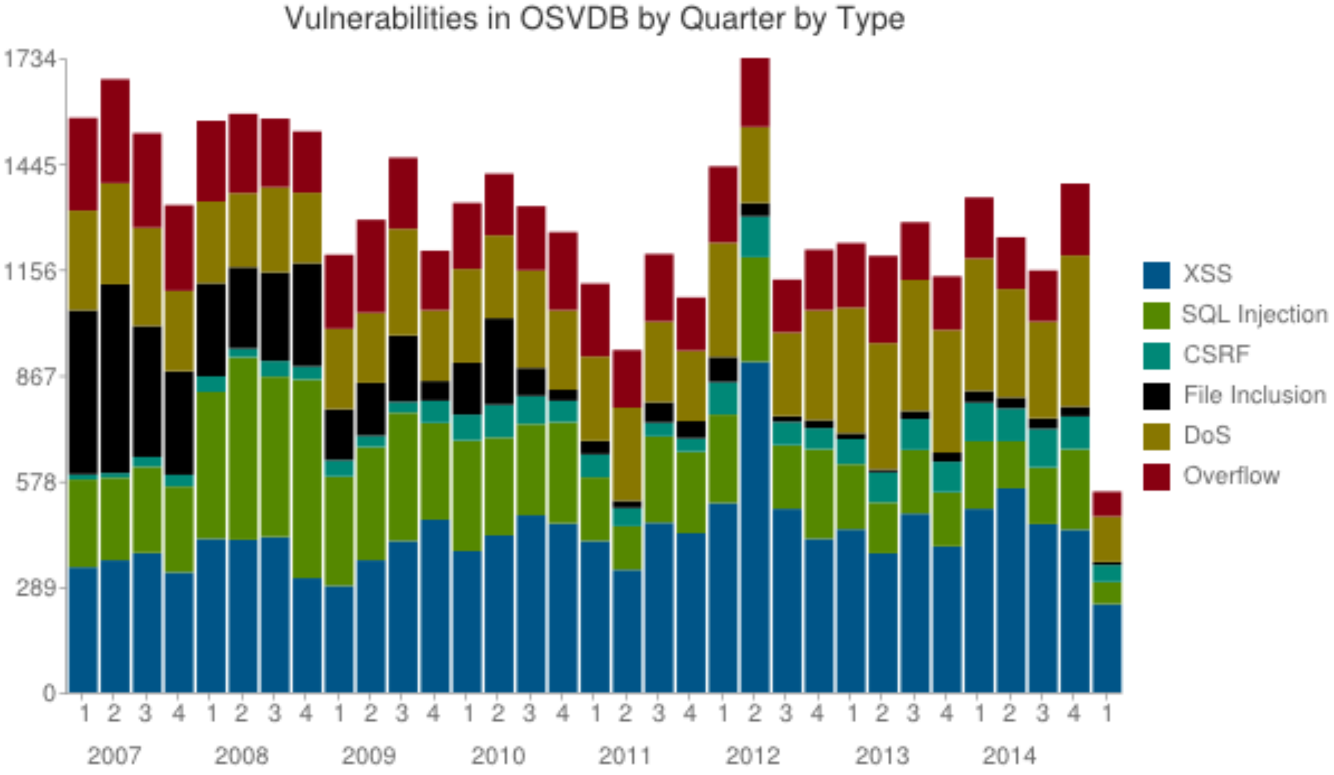
Requires access to devices and often extracting firmware from them, as it's not otherwise readily available

Internet of Things – State of Security

RiskBased SECURITY

Since there still isn't much IoT vulnerability information (yet!) are there lessons learned from regular embedded devices?

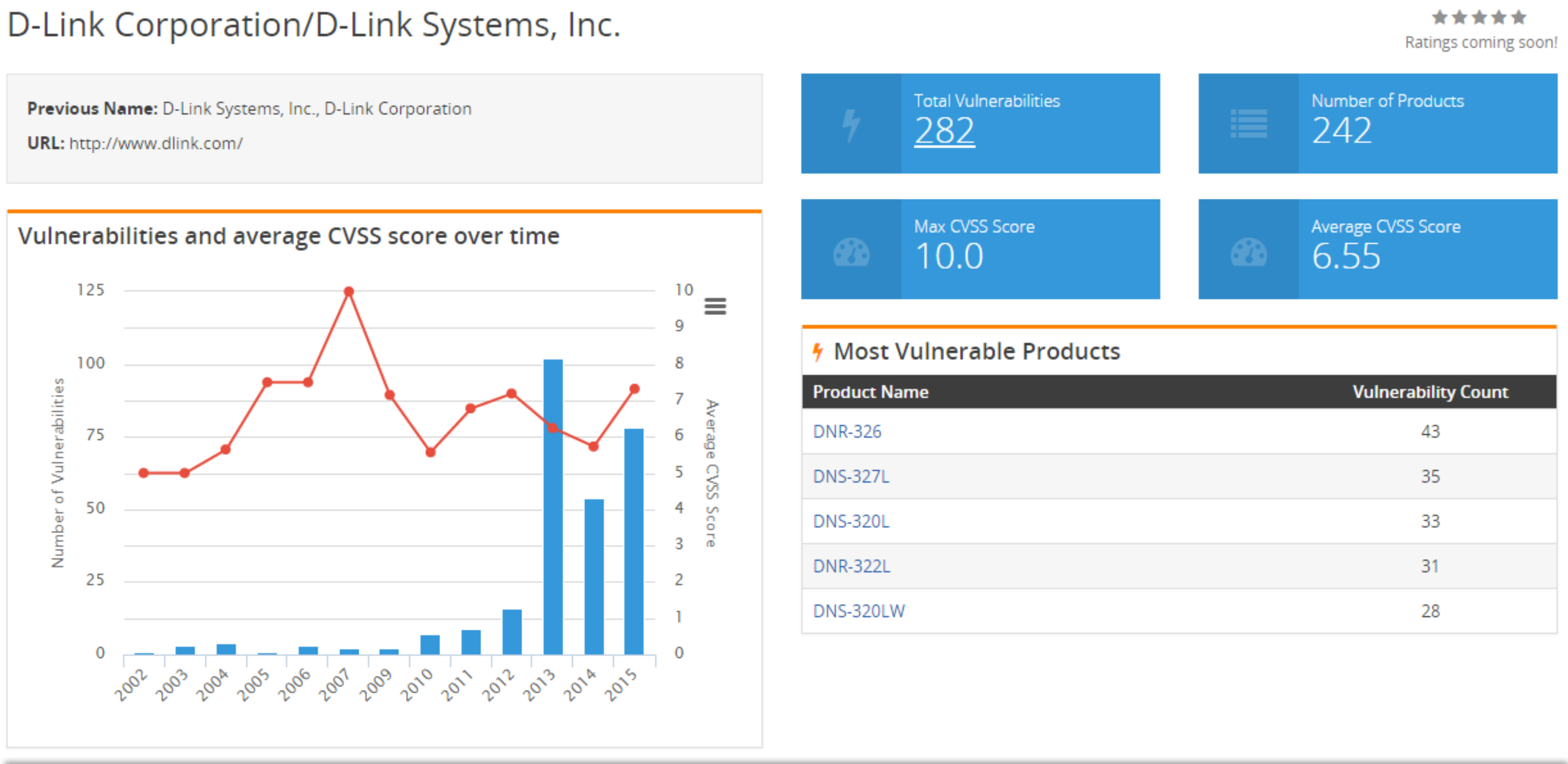
Internet of Things – State of Security



2015*:	8,482
2014:	13,527
2013:	11,178
2012:	10,372
2011:	7,921
2010:	9,165
2009:	8,183
2008:	9,806
2007:	9,587
2006:	11,049

Source: RBS VulnDB
*YTD Aug 23rd, 2015

Internet of Things – D-Link



D-Link Corporation/D-Link Systems, Inc.

★★★★★
Ratings coming soon!

Previous Name: D-Link Systems, Inc., D-Link Corporation

URL: http://www.dlink.com/

Total Vulnerabilities
282

Number of Products
242

Max CVSS Score
10.0

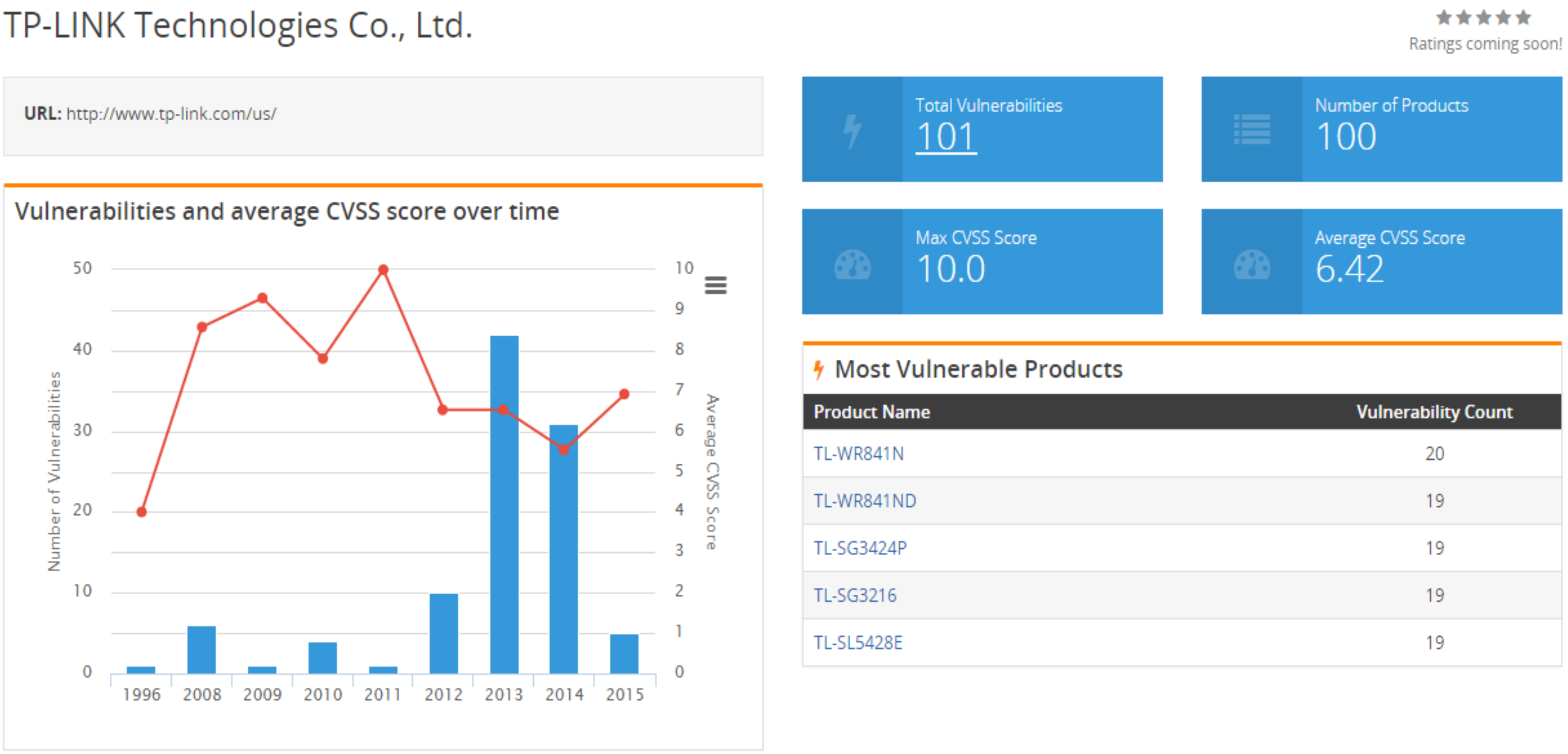
Average CVSS Score
6.55

Vulnerabilities and average CVSS score over time

Most Vulnerable Products

Product Name	Vulnerability Count
DNR-326	43
DNS-327L	35
DNS-320L	33
DNR-322L	31
DNS-320LW	28

Internet of Things – TP-LINK



TP-LINK Technologies Co., Ltd.

★★★★★ Ratings coming soon!

URL: http://www.tp-link.com/us/

Total Vulnerabilities 101

Number of Products 100

Max CVSS Score 10.0

Average CVSS Score 6.42

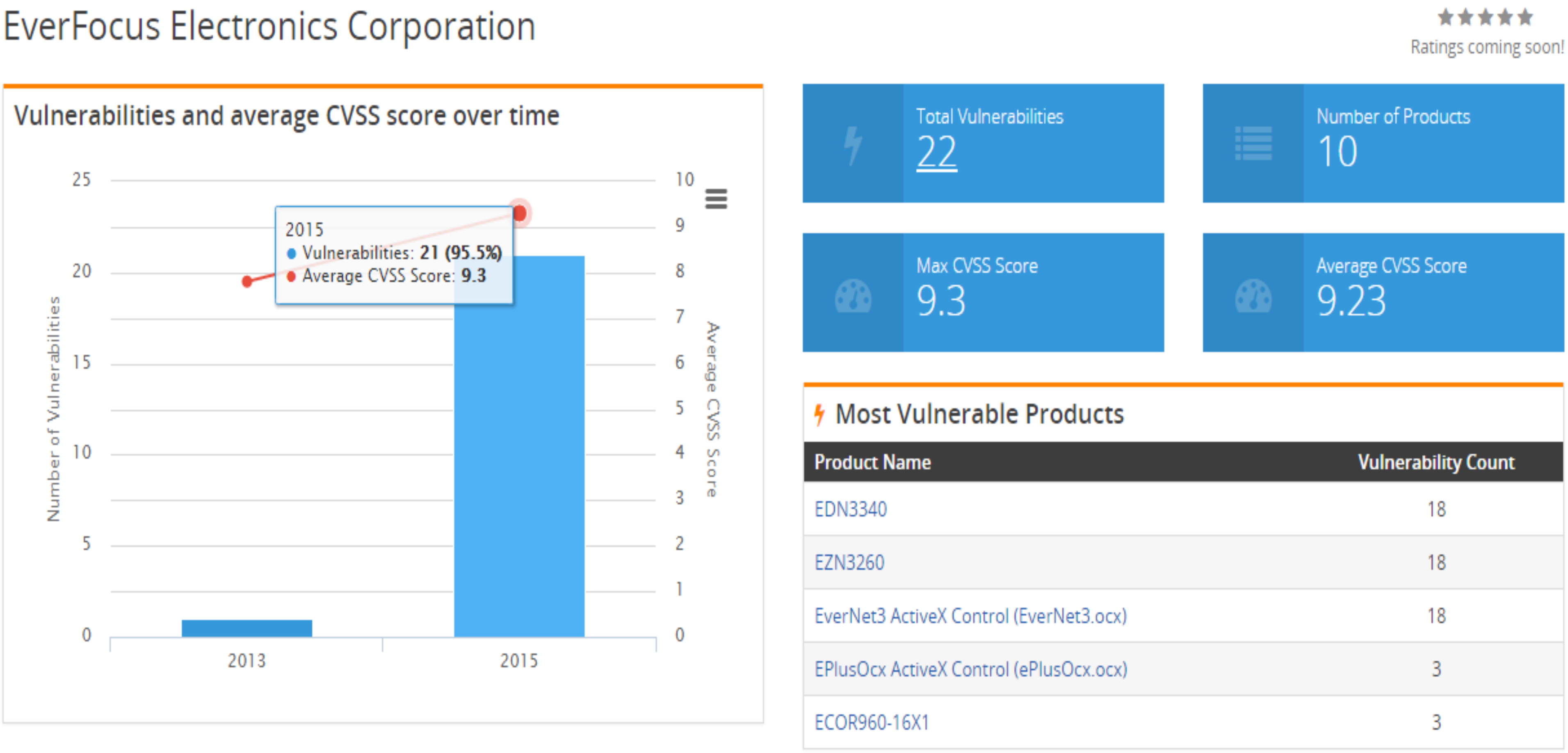
Vulnerabilities and average CVSS score over time

Most Vulnerable Products

Product Name	Vulnerability Count
TL-WR841N	20
TL-WR841ND	19
TL-SG3424P	19
TL-SG3216	19
TL-SL5428E	19

NOT JUST SECURITY, THE RIGHT SECURITY

Internet of Things – Everfocus



EverFocus Electronics Corporation

★★★★★
Ratings coming soon!

Vulnerabilities and average CVSS score over time

25
20
15
10
5
0
Number of Vulnerabilities
10
9
8
7
6
5
4
3
2
1
0
Average CVSS Score
2013
2015
2015
● Vulnerabilities: 21 (95.5%)
● Average CVSS Score: 9.3

Total Vulnerabilities
22

Number of Products
10

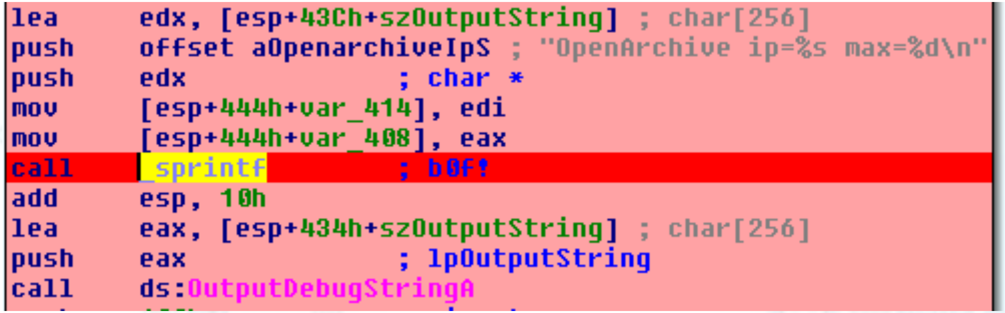
Max CVSS Score
9.3

Average CVSS Score
9.23

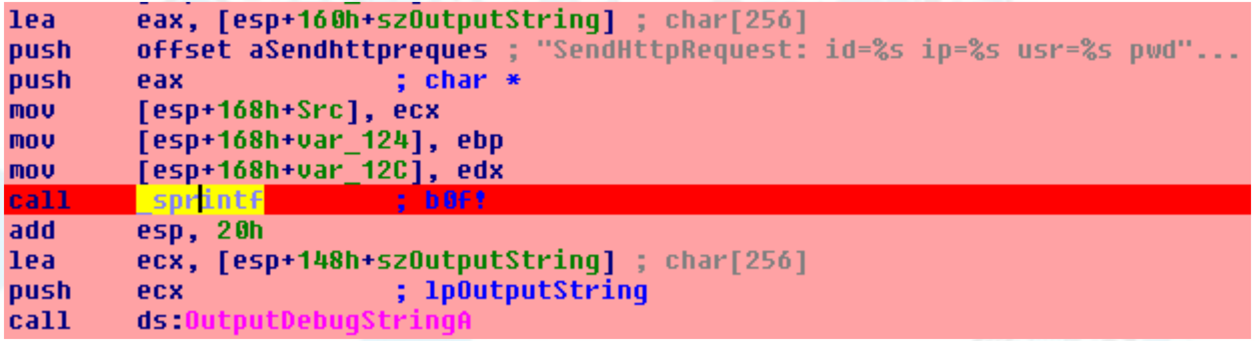
Most Vulnerable Products

Product Name	Vulnerability Count
EDN3340	18
EZN3260	18
EverNet3 ActiveX Control (EverNet3.ocx)	18
EPlusOcx ActiveX Control (ePlusOcx.ocx)	3
ECOR960-16X1	3

Internet of Things – Everfocus (Code Maturity)



```
lea     edx, [esp+43Ch+szOutputString] ; char[256]
push    offset aOpenarchiveIpS ; "OpenArchive ip=%s max=%d\n"
push    edx             ; char *
mov     [esp+444h+var_414], edi
mov     [esp+444h+var_408], eax
call    _sprintf        ; b0f!
add     esp, 10h
lea     eax, [esp+434h+szOutputString] ; char[256]
push    eax             ; lpOutputString
call    ds:OutputDebugStringA
```



```
lea     eax, [esp+160h+szOutputString] ; char[256]
push    offset aSendhttpreques ; "SendHttpRequest: id=%s ip=%s usr=%s pwd"...
push    eax             ; char *
mov     [esp+168h+Src], ecx
mov     [esp+168h+var_124], ebp
mov     [esp+168h+var_12C], edx
call    _sprintf        ; b0f!
add     esp, 20h
lea     ecx, [esp+148h+szOutputString] ; char[256]
push    ecx             ; lpOutputString
call    ds:OutputDebugStringA
```

Full reports available at:

https://www.riskbasedsecurity.com/research/RBS-2015-001.pdf
https://www.riskbasedsecurity.com/research/RBS-2015-002.pdf

Internet of Things – Topica IP Cameras (TOP--788XMP)

No CSRF protection whatsoever

Allows e.g. rebooting device or creating user accounts

http://[IP]/cgi-bin/reboot.cgi?action=reboot

Internet of Things – Topica IP Cameras (TOP--788XMP)

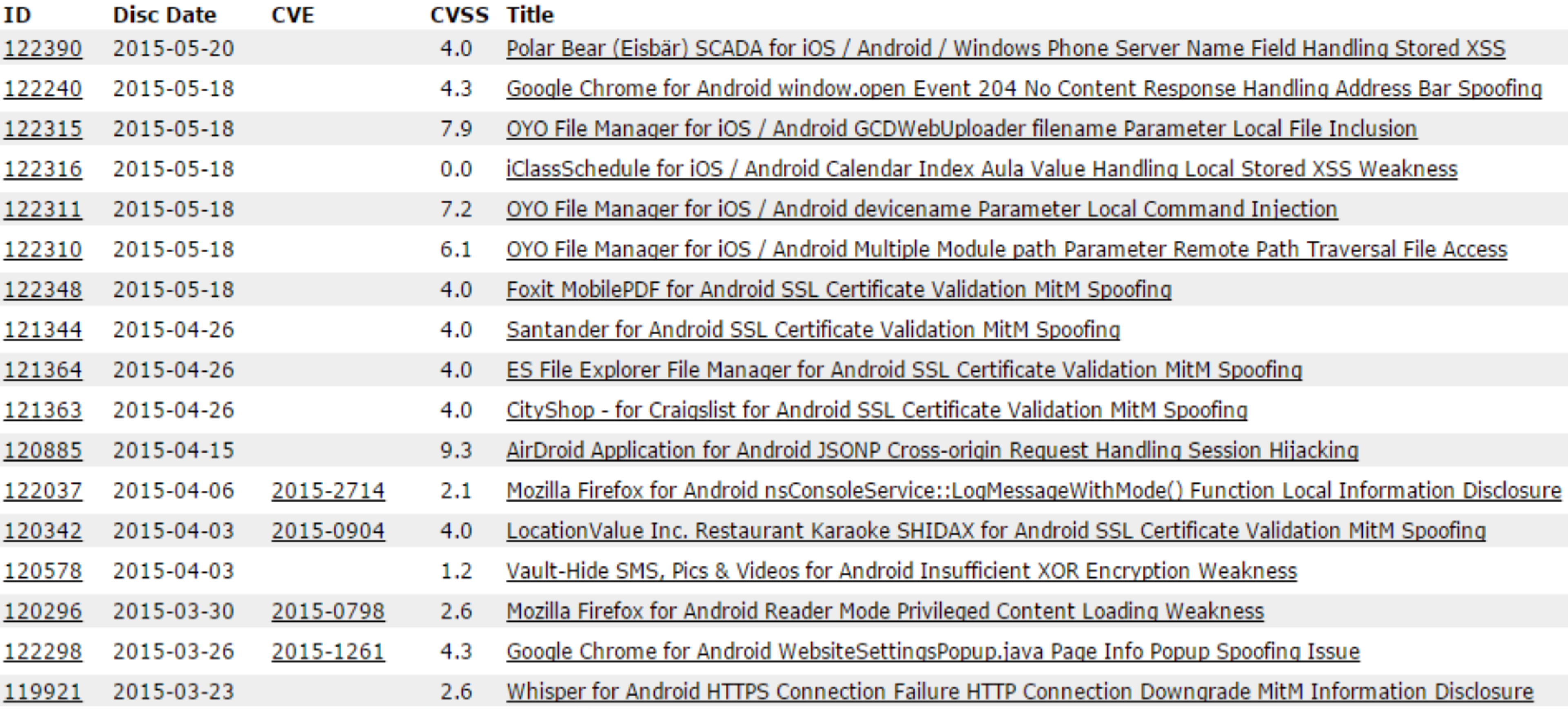
Supports 3 user types:

“Viewer”, “Remote Viewer”, and “Administrator”

Restricts access to *user_management_config.html* but not */cgi-bin/users.cgi*

action=add&index=5&username=test&password=test123&privilege=1

Internet of Things – Mobile Apps



ID	Disc Date	CVE	CVSS	Title
122390	2015-05-20		4.0	Polar Bear (Eisbär) SCADA for iOS / Android / Windows Phone Server Name Field Handling Stored XSS
122240	2015-05-18		4.3	Google Chrome for Android window.open Event 204 No Content Response Handling Address Bar Spoofing
122315	2015-05-18		7.9	OYO File Manager for iOS / Android GCDWebUploader filename Parameter Local File Inclusion
122316	2015-05-18		0.0	iClassSchedule for iOS / Android Calendar Index Aula Value Handling Local Stored XSS Weakness
122311	2015-05-18		7.2	OYO File Manager for iOS / Android devicename Parameter Local Command Injection
122310	2015-05-18		6.1	OYO File Manager for iOS / Android Multiple Module path Parameter Remote Path Traversal File Access
122348	2015-05-18		4.0	Foxit MobilePDF for Android SSL Certificate Validation MitM Spoofing
121344	2015-04-26		4.0	Santander for Android SSL Certificate Validation MitM Spoofing
121364	2015-04-26		4.0	ES File Explorer File Manager for Android SSL Certificate Validation MitM Spoofing
121363	2015-04-26		4.0	CityShop - for Craigslist for Android SSL Certificate Validation MitM Spoofing
120885	2015-04-15		9.3	AirDroid Application for Android JSONP Cross-origin Request Handling Session Hijacking
122037	2015-04-06	2015-2714	2.1	Mozilla Firefox for Android nsConsoleService::LogMessageWithMode() Function Local Information Disclosure
120342	2015-04-03	2015-0904	4.0	LocationValue Inc. Restaurant Karaoke SHIDAX for Android SSL Certificate Validation MitM Spoofing
120578	2015-04-03		1.2	Vault-Hide SMS, Pics & Videos for Android Insufficient XOR Encryption Weakness
120296	2015-03-30	2015-0798	2.6	Mozilla Firefox for Android Reader Mode Privileged Content Loading Weakness
122298	2015-03-26	2015-1261	4.3	Google Chrome for Android WebsiteSettingsPopup.java Page Info Popup Spoofing Issue
119921	2015-03-23		2.6	Whisper for Android HTTPS Connection Failure HTTP Connection Downgrade MitM Information Disclosure

Internet of Things – State of Security

Devices are likely affected by many basic vulnerabilities (low code maturity)

Mobile apps may not perform proper SSL/TLS certificate validation or store data securely

If this is the state of their devices and apps, how much do you trust their cloud with your data?

Actions and Response Gone Wild?

Internet of Things – Where To Start At Your Org?

Internet of Things – Security Needs A Seat!

Internet of Things – Find Your IoT!

- Get an inventory of your current IoT devices
  - Network scanning / mapping - know what is in use and where including IoT devices
  - Look at outgoing web traffic / logs to see what IoT devices are communicating outbound
- Know where risk is in your environment
  - Map and track in existing asset management data / CMDBs
  - Ensure you have proper vulnerability intelligence

Internet of Things – Basic Security Foundation!

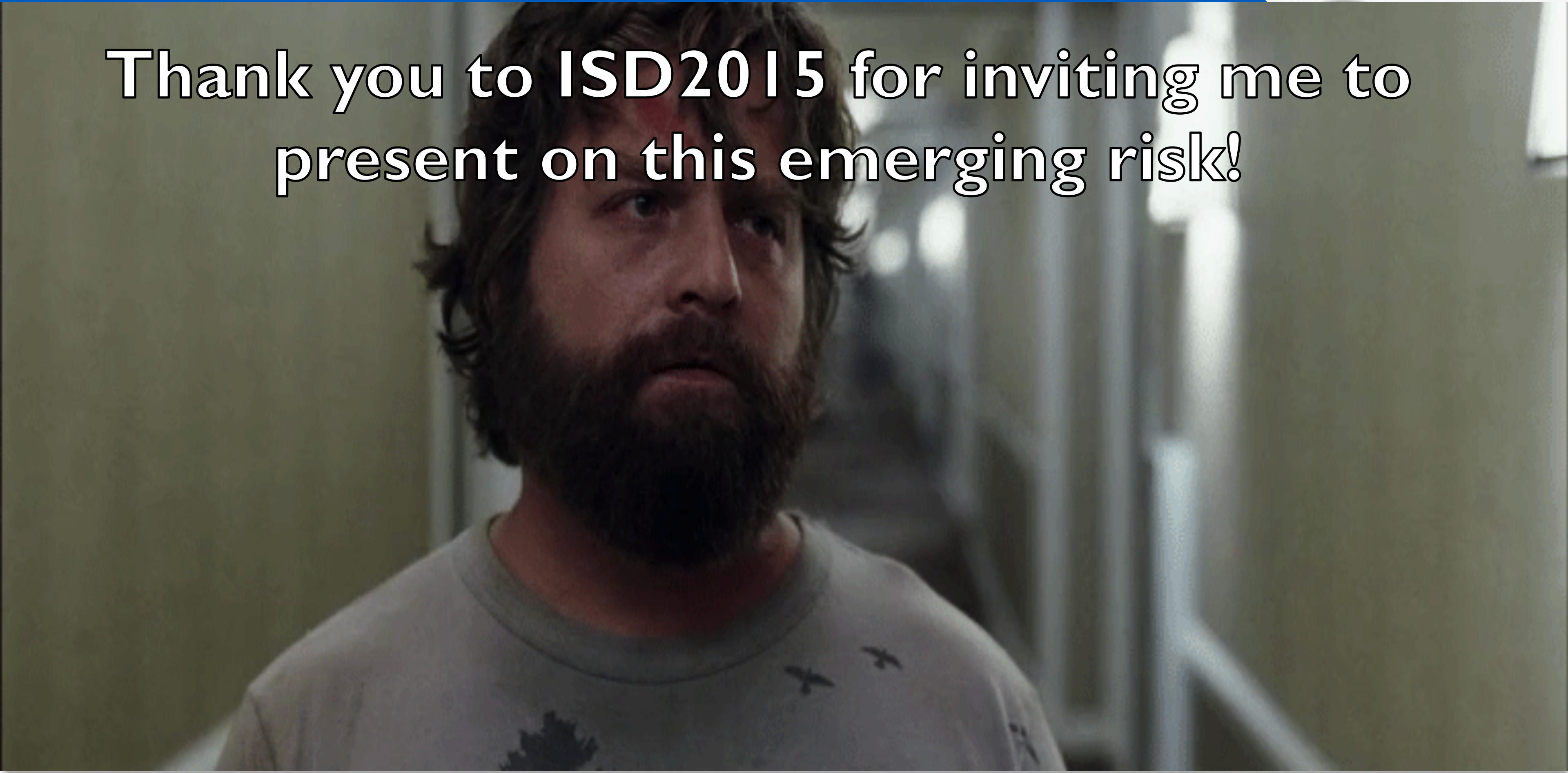
Implement proper network segmentation for all IoT devices where possible

- Allows for reduction of attack surface
- Improves incident response ability when devices are clearly identified

Internet of Things – Conclusion

- IoT is already in your network and expect it to be insecure.
- Start talking with your executives / IT personnel about the issues and conduct proper risk assessments.
- Ensure you incorporate your incident response program to include IoT products and vendors.
- Work with vendors and pick products that demonstrate they care about security!

Thank you!



Thank you to ISD2015 for inviting me to present on this emerging risk!

Internet of Things – Questions?

RiskBased SECURITY

RiskBased SECURITY

Internet of Things Gone Wild

Carsten Eiram

Chief Research Officer

che@riskbasedsecurity.com / @CarstenEiram