RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

SESSION ID: CSV-F02

Bring Your Own Internet of Things: BYO-IoT

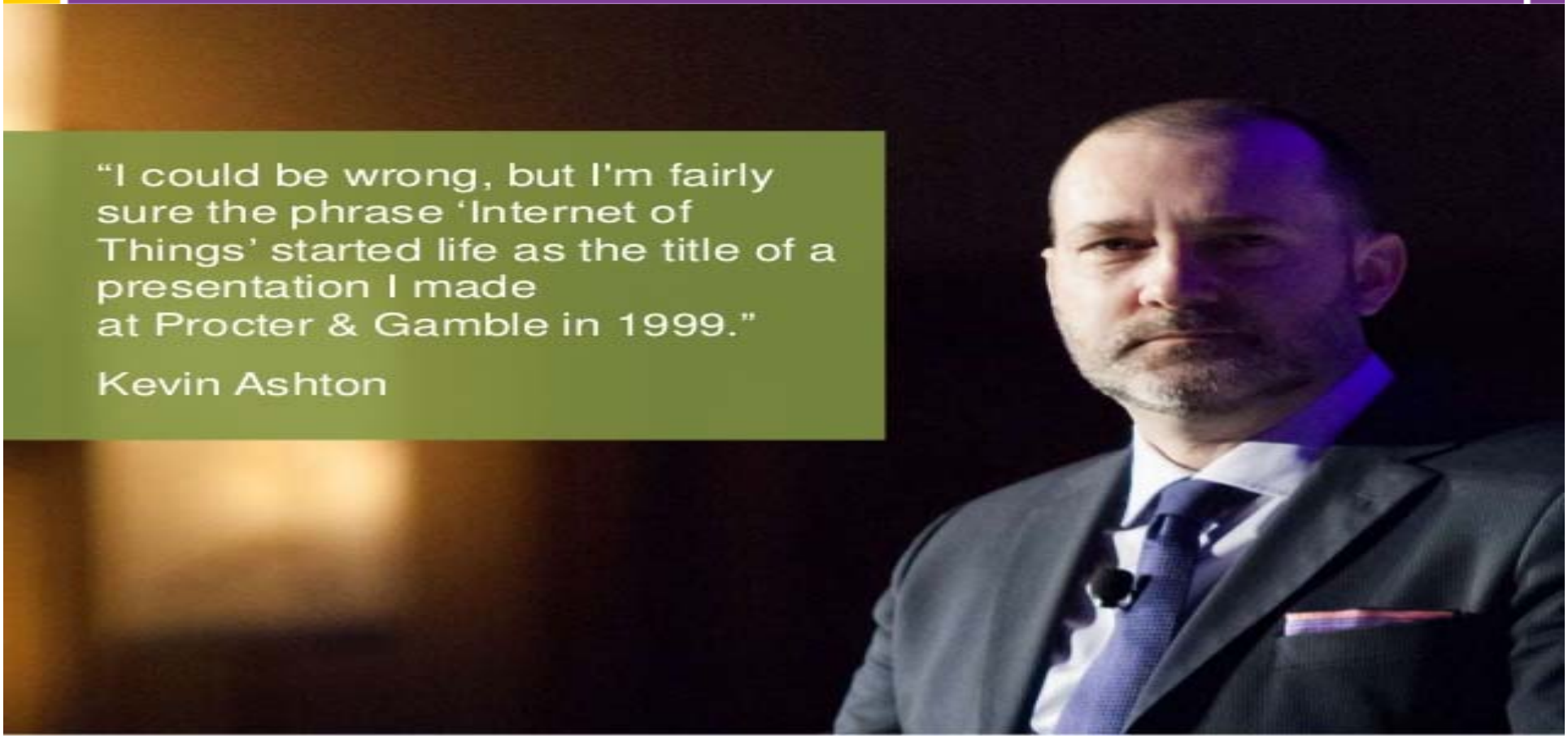
Carsten Eiram
Chief Research Officer
Risk Based Security
@carsteneiram

Jake Kouns
CISO
Risk Based Security
@jkouns

Agenda

- What is IoT?
- What's the Problem?
- What's the Attack Surface?
- IoT Security – Current State
- Response and Actions

Internet of Things – Who Came Up With It?



Internet of Things – Definition?

Internet of Things – Definition (Techopedia.com)

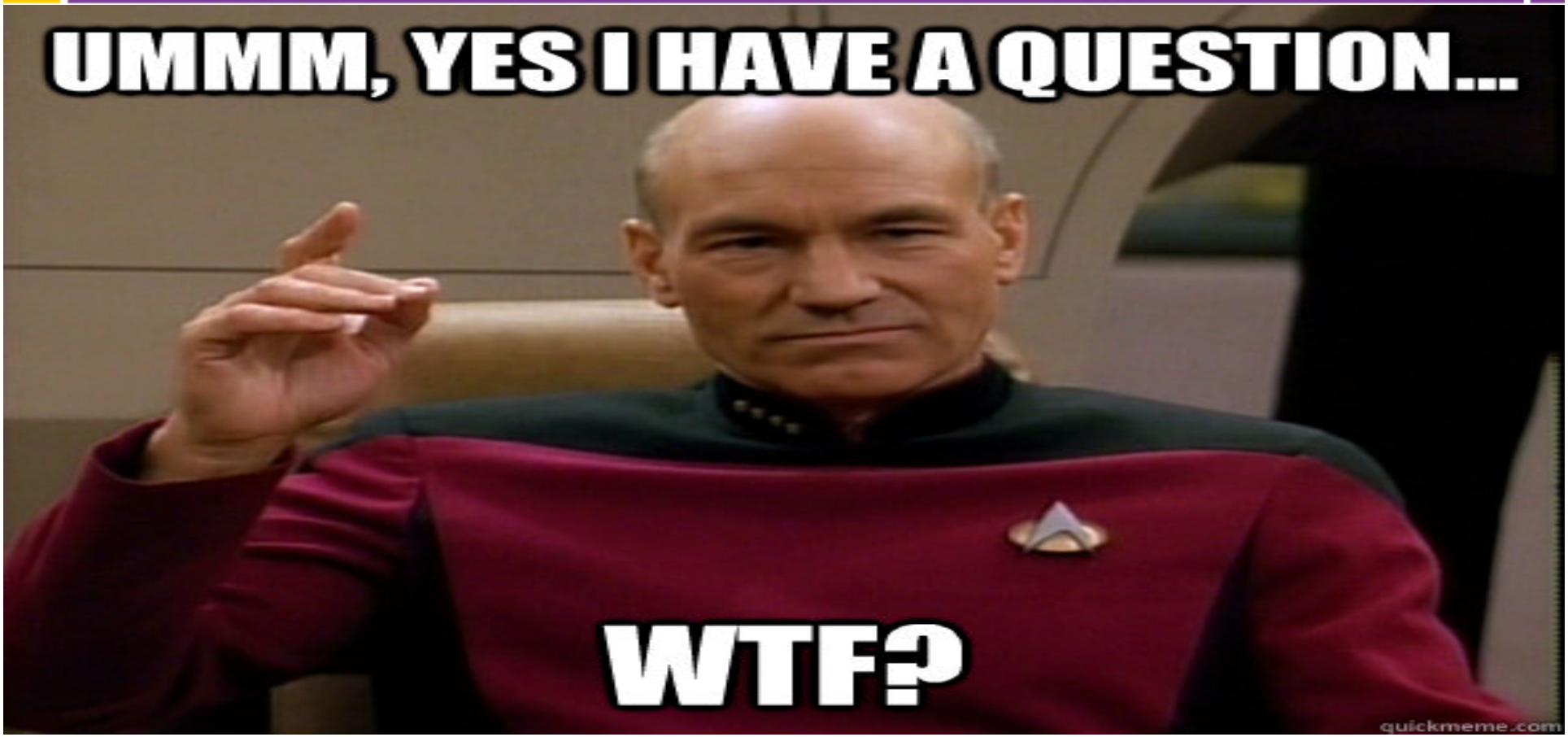
"The Internet of Things (IoT) is a computing concept that describes a future where everyday physical objects will be connected to the Internet and be able to identify themselves to other devices. The term is closely identified with RFID as the method of communication, although it also may include other sensor technologies, wireless technologies or QR codes.

The IoT is significant because an object that can represent itself digitally becomes something greater than the object by itself. No longer does the object relate just to you, but is now connected to surrounding objects and database data. When many objects act in unison, they are known as having "ambient intelligence.""

"The Internet of Things is a difficult concept to define precisely."

- Techopedia.com

Internet of Things – So, What Is it?



Internet of Things – Definition (Conclusion)

1. Needs to be networked / connected
2. Some capability of sensing and decision making without human interaction/control

Many products have the word ”Smart” in their name or to describe its function

Internet of Things – Examples (Everyday Life)

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.

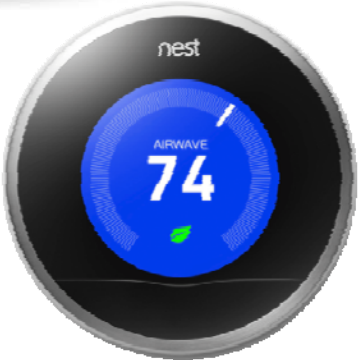
Internet of Things – Process

Internet of Things – Examples (Retail)

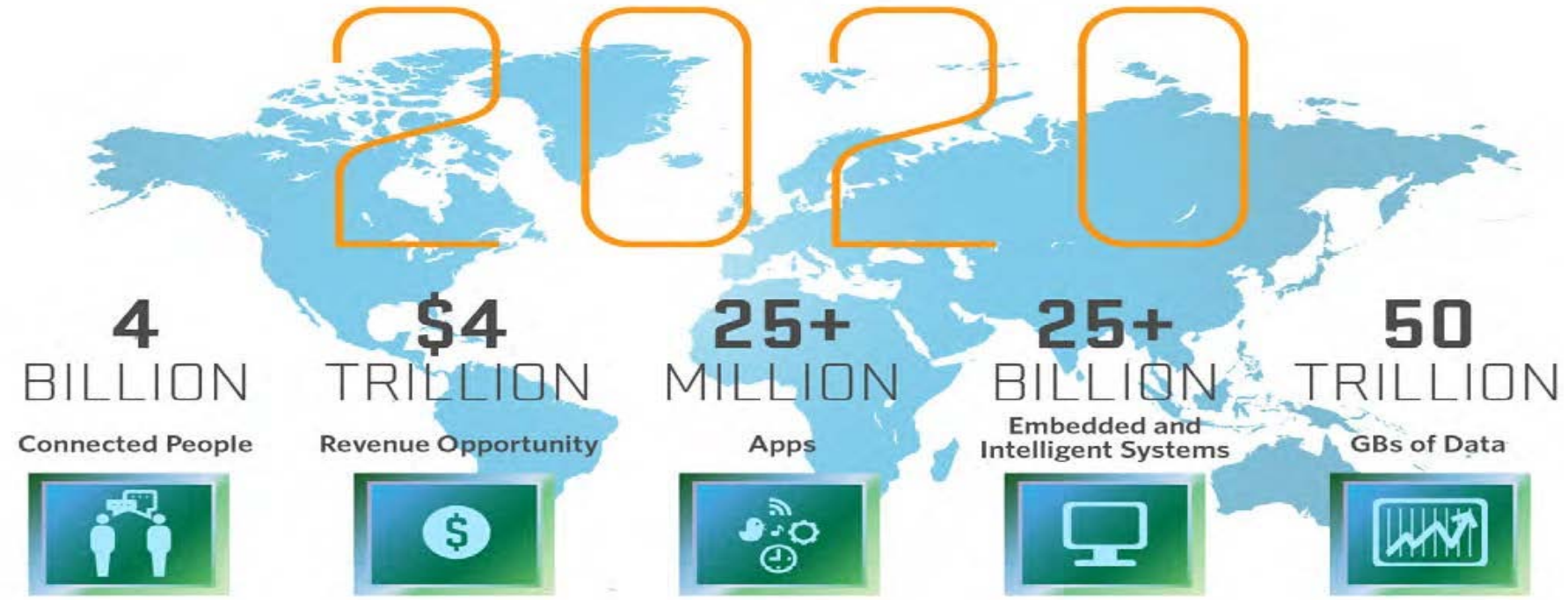
Internet of Things – Examples (Environmental)

Internet of Things – Examples (Your Network?)

Internet of Things – Examples (Your Network?)



Internet of Things – Why Should You Care?



Source: Mario Morales, IDC

Internet of Things – Why Should You Care?

- The analyst firm Gartner says that by 2020 there will be over 26 billion connected devices… that's a lot of connections (some even estimate this number to be much higher, over 100 billion).

- "We expect the number of connected objects to reach 50bn by 2020 (2.7% of things in the world)" - Cisco

http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/
http://newsroom.cisco.com/feature-content?type=webcontent&articleId=1208342

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!

RiskBased SECURITY

What's The Problem?

Internet of Things – What About YOUR Network?

Internet of Things – What About YOUR Network?

STAMFORD, Conn., May 1, 2013

View All Press Releases

Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes

Enterprises That Offer Only Corporate-Liable Programs Will Soon Be the Exception

BYOD circa 2018 will challenge enterprise IT

No tech vendor will be safe from consumerization, according to Gartner. Companies will have to prepare for multiple vendors and a possible PC market crash.

RiskBased SECURITY

Internet of Things – IoT IS Coming!

Gartner estimates the IoT will see 26 billion units installed by 2020 – channelling huge volumes of data traffic into datacentres

CIOs beware, IoT is coming

May 13, 2015 | By Fred Donovan

SHARE

Email

42 Tweet

4 Share

0

Editor's Corner:

The Internet of Things revolution is under way, and CIOs need to consider ways to incorporate IoT devices, apps and platforms into their company. [click to tweet]

Fred Donovan

Azmi Jafarey, CIO at Ipswitch, offers some areas for CIOs to consider when contemplating an IoT deployment, in a *Computerworld* article.

"At the business level there will be two imperatives. For those manufacturing physical goods, there will be the pressure for 'smart everything'-- what should be measured and why, how the data should be used and when, and how such sensors can be made virtually invisible," Jafarey wrote.

Internet of Things – How Is This Different?

Even more Shadow IT, where unexpected

BI/PD (Bodily Injury, Property Damage) - People can get hurt, and property can be damaged

Real world impact - no longer 1s and 0s

Internet of Things – What's In The News?

NEWS ANALYSIS

DHS investigates 24 potentially deadly cyber flaws in medical devices

Credit: Steve Winton

DHS is investigating 24 cases of potentially deadly cybersecurity flaws in medical devices and hospital equipment.

MORE LIKE THIS

Feds pressed to protect wireless medica devices from hackers

Brute-force cyberattacks against critical infrastructu energy industry,...

FDA asks hackers to expos holes in medical devices, b many researchers fear...

on IDG Answers

How serious of a security threat is the "B bug?"

Internet of Things – What's In The News?

CAR HACKED ON 60 MINUTES

Internet of Things – What's In The News?

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 Not Just In Your Garage

Internet of Things – IoT Connected

GM is making your car a rolling Wi-Fi hotspot

2 Comments / 398 Shares / 90 Tweets / Stumble / @ Email More +

Your car can become a rolling Wi-Fi hotspot with new technology General Motors (GM) is introducing with its 2015 models. On a family road trip, for instance, each member who isn't driving could watch a different movie, play games or check email because the system can stream to as many as seven devices.

TESLA'S OVER-THE-AIR FIX: BEST EXAMPLE YET OF THE INTERNET OF THINGS?

Internet of Things – Tripwire Study

tripwire

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-

RiskBased SECURITY

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

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

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

Internet of Things – Tripwire Key Findings

Remote workers have an average of 11 IoT devices on their home networks

24% have already connected at least one of these to their enterprise networks

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

Internet of Things – Is There An Impact?

Internet of Things – 3rd Party Breaches

TARGET

HVAC Vendor Confirms Link to Target Data Breach

BY STEPHANIE MLOT FEBRUARY 7, 2014 03:40PM EST 0 COMMENTS

A Pennsylvania company confirmed that the Target hackers stole network credentials from its network.

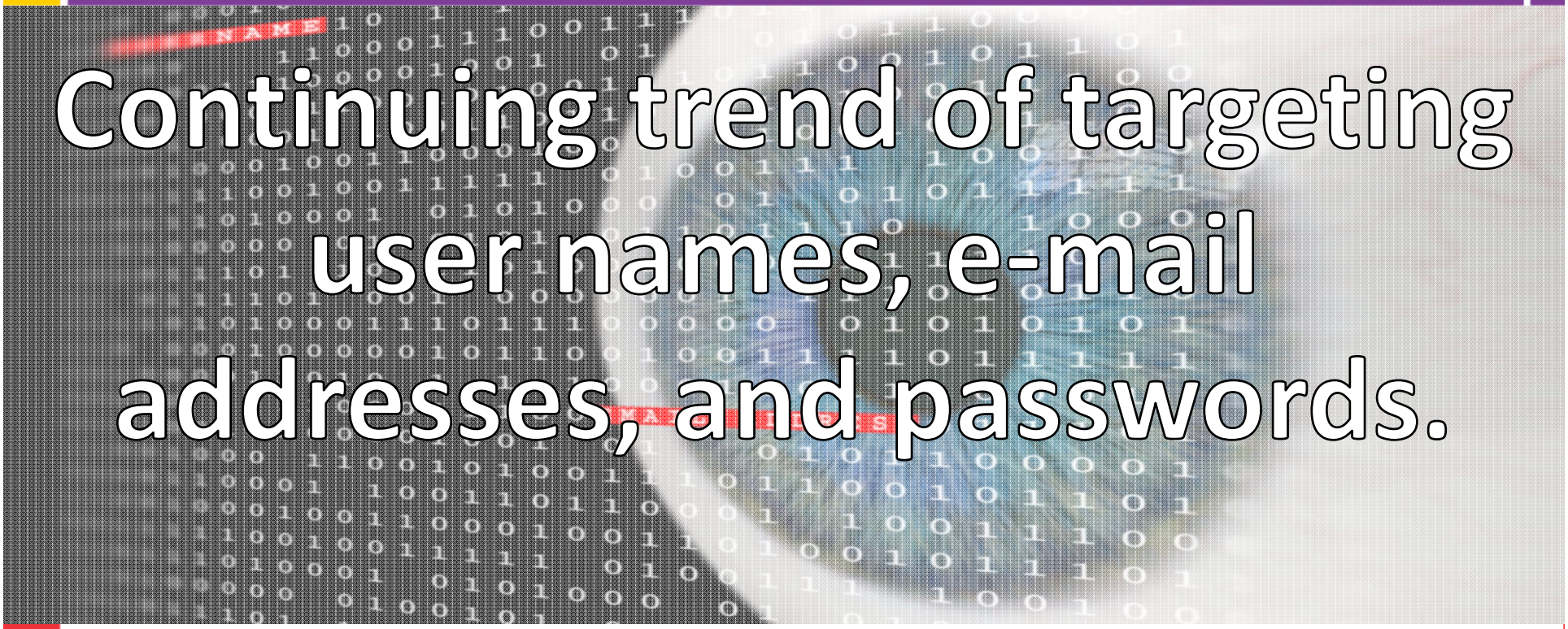
89 SHARES

Almost two months after Target reported a massive data breach that put the personal data of up to 70 million shoppers at risk, more details have emerged about how the hackers gained access to the retailer's systems.

As first reported by security blogger Brian Krebs, hackers broke into Target's network using credentials stolen from a third-party vendor—Sharpsburg, Penn.-based Fazio Mechanical Services.

On Friday, owner and president Ross E. Fazio confirmed that his company, a refrigeration and HVAC systems maker, was "a victim of a sophisticated cyber attack operation."

Internet of Things – 3rd Party Breaches



Internet of Things – 3rd Party Breaches

Home Depot hackers used vendor log-on to steal data, e-mails

Michael Winter, USA TODAY 8:57 a.m. EST November 7, 2014

RiskBased SECURITY

RSAConference2016

Internet of Things – 3rd Party Breaches

Not just a few 3rd party breaches...

In 2015 alone:

Source: Cyber Risk Analytics (www.cyberriskanalytics.com)

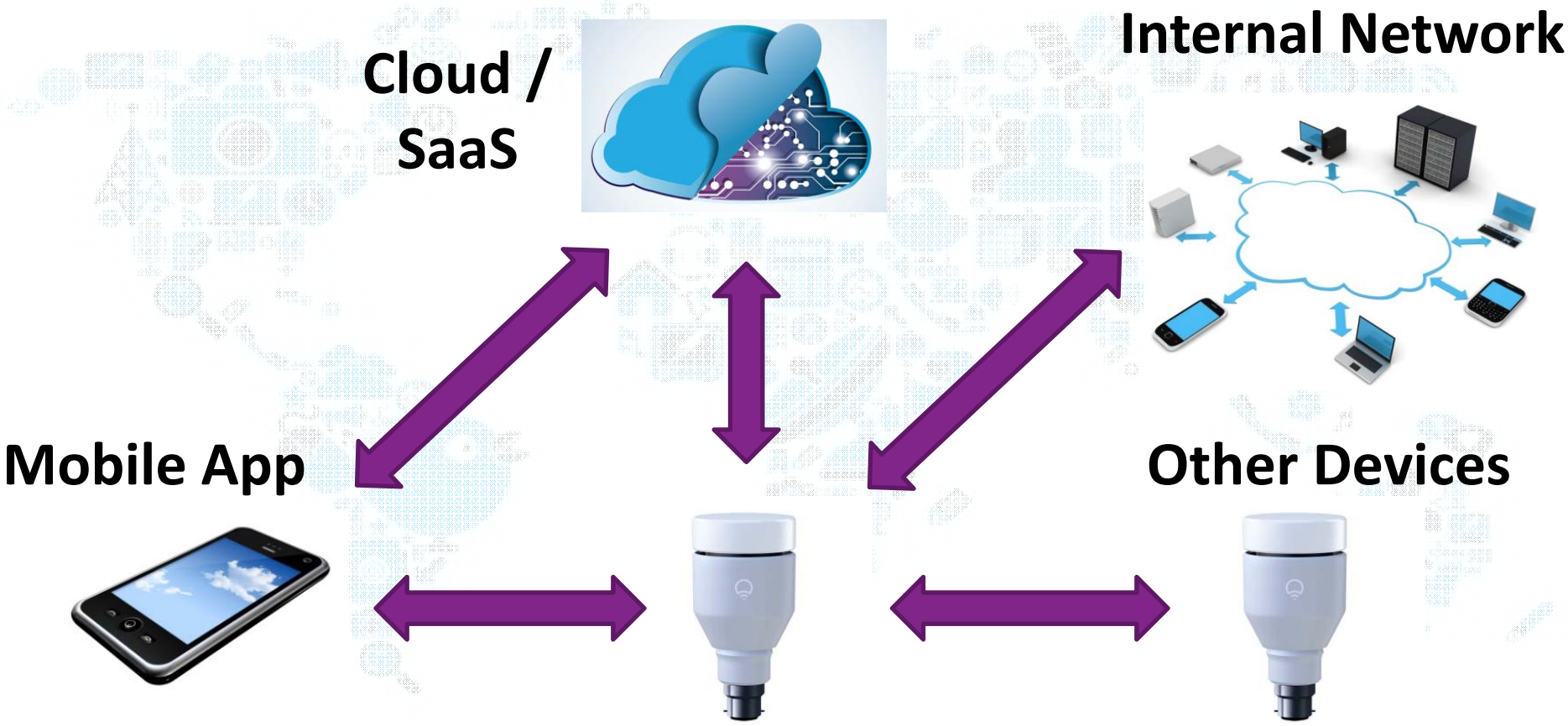
Internet of Things – More Shadow IT With IoT!

SHADOW IT

COMING TO A DEPARTMENT NEAR YOU.

What's The Attack Surface?

Internet of Things - Communication



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

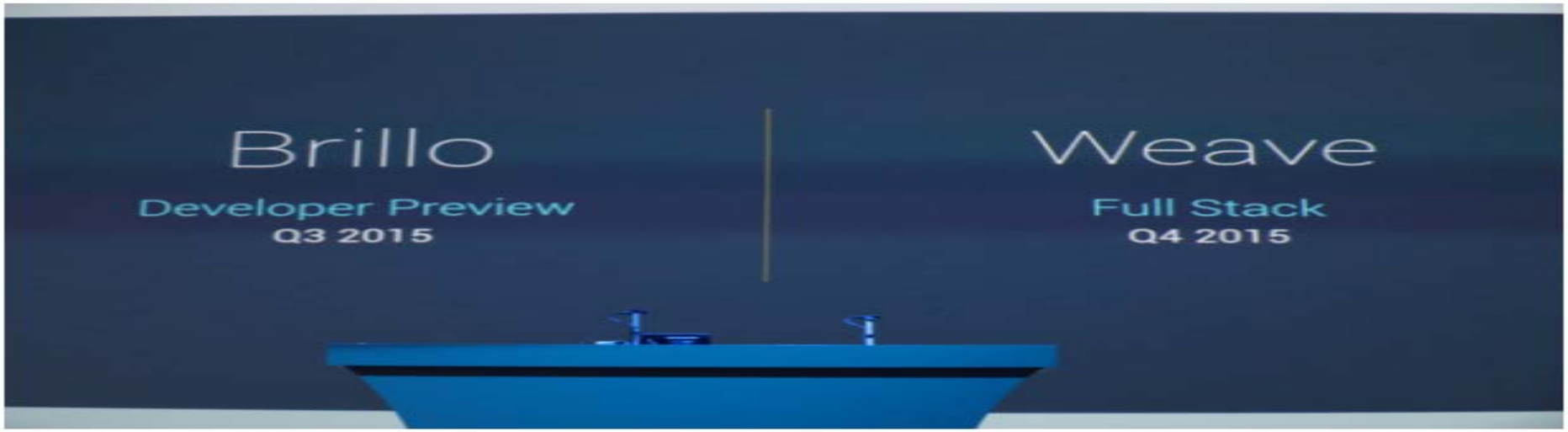
During a wireless assessment of a client's WiFi network, InGuardians sniffed for **ZigBee, Z-wave, and other 900 MHz traffic common** for IoT devices

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

Internet of Things – Google!

Google Announces Brillo and Weave, Android Derivative to Power Internet of Things Devices



Brillo is an underlying operating system for the internet of things devices. It is built with minimal system requirements and supports Wi-Fi, Bluetooth Low Energy, and other connectivity options. A developer preview of it will arrive in Q3 of this year.

The company also announced Weave, the language or standardized communications protocol which will let Brillo-powered devices and other gadgets to talk to one another. A developer preview of it will arrive in Q4 of this year.

Internet of Things – Google!

JANUARY 5 GOOG: 742.58 0.74

First devices that use Google's Brillo and Weave launch at CES 2016

Abner Li - 1 day ago @technacity

CES 2016 GOOGLE CORPORATE

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?

Internet of Things – Three Threat Scenarios

Enterprise IoT

BYOD (BYO-IoT) / Cross-contamination

Remote workers

IoT Security – Current State

Internet of Things – What's In The News?

Stunt Hacking?

Saturday, May 16, 2015

Lets Call Stunt Hacking What it is, Media Whoring.

Lets Call Stunt Hacking What it is, Media Whoring.

by Valsmith

I recently read this article: http://www.foxnews.com/tech/2015/03/17/ground-control-analysts-warn-airplane-communications-systems-vulnerable-to/ and it brought to mind some thoughts that have been percolating for quite a while. Sometime last year I believe Dave Aitel coined the term Stunt Hacking, which I think is a pretty good way to describe it. We often see these media blitzes about someone hacking a car, or an airplane, or some other device. The public who has a limited understanding of the technology, and the media who has a worse understanding, get in a frenzy or outrage, the security company hopes this translates into sales leads, and the researcher hopes this translates into name recognition leading to jobs, raises, conference talks, etc.

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

Hacking Insulin Pumps And Other Medical Devices From Black Hat

HOW THIEVES CAN HACK AND DISABLE YOUR HOME ALARM SYSTEM

Internet of Things – State of Security

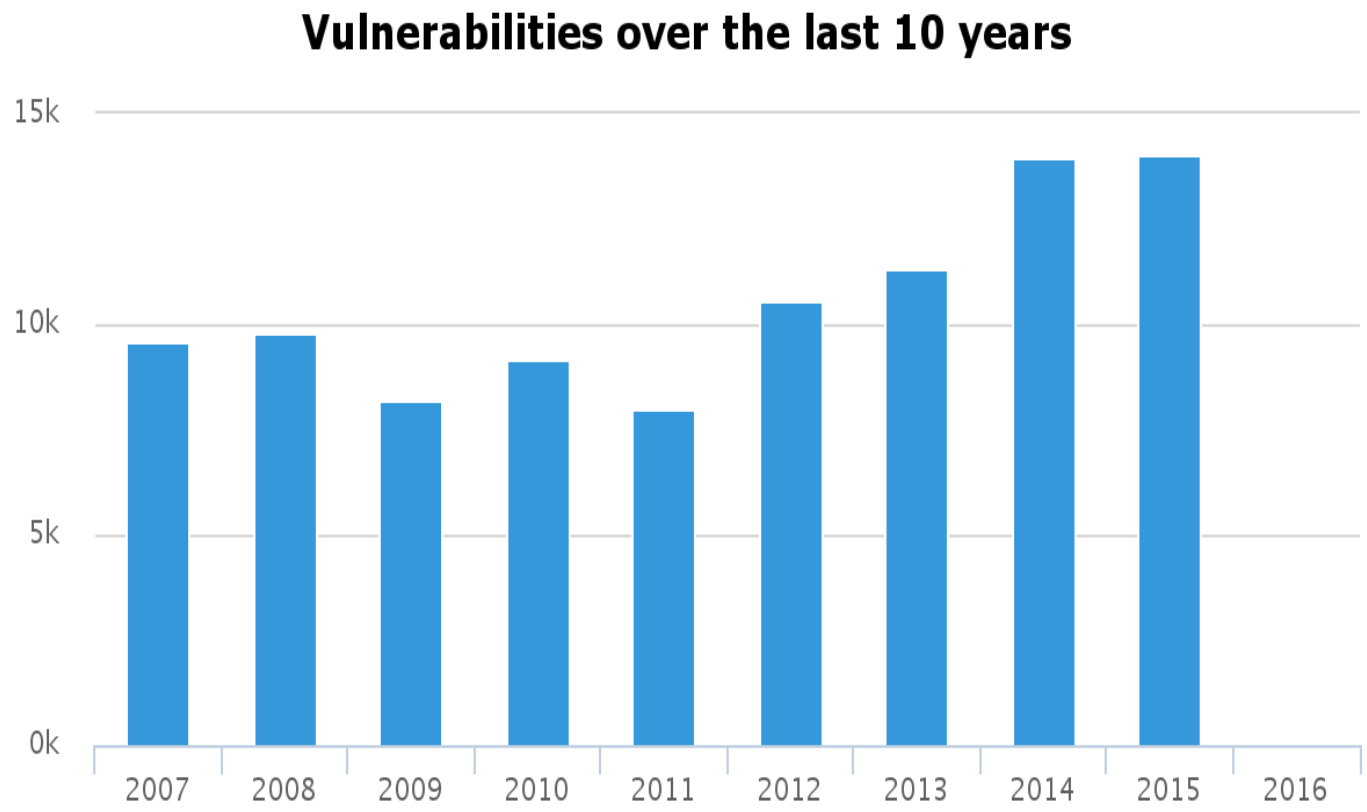
Why so relatively few critical vulnerabilies?

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

Internet of Things – State of 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

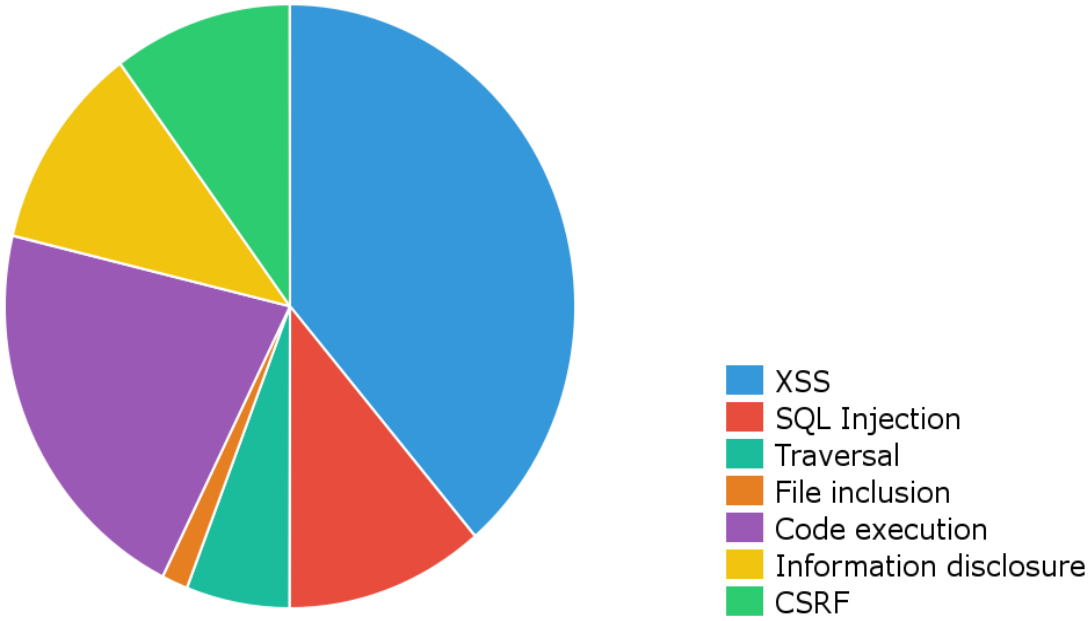


2016*:	*904
2015:	13,995
2014:	13,953
2013:	11,339
2012:	10,544
2011:	7,998
2010:	9,183
2009:	8,194
2008:	9,808
2007:	9,590

Source: VulnDB
*YTD January 29th, 2016

Internet of Things – State of Security

Web Vulnerabilities by Type (2015)



2016*:	*904
2015:	13,995
2014:	13,953
2013:	11,339
2012:	10,544
2011:	7,998
2010:	9,183
2009:	8,194
2008:	9,808
2007:	9,590

Source: VulnDB
*YTD January 29th, 2016

Internet of Things – TRENDnet

ID	Disc Date	CVSS	Title	CVE
129823	2015-11-03	10.0	TRENDnet TPE-4840WS Unspecified SSL Issue	
129632	2015-10-26	10.0	TRENDnet TEW-828DRU Manual Time Settings Unspecified Issue	
129633	2015-10-23	10.0	TRENDnet Multiple Products Unspecified Issue	
128413	2015-10-05	10.0	TRENDnet TEW-812DRU Multiple Unspecified Issues (2.1.2.0)	
127013	2015-09-02	4.3	TRENDnet TV-IP743SIC Unspecified CSRF	
126968	2015-09-02	6.2	TRENDnet TV-IP743SIC WiFi Baby Cam UART Interface Default Hardcoded Credentials	2015-2880
127014	2015-09-02	5.0	TRENDnet TV-IP743SIC Unspecified XSS	
127016	2015-09-02	10.0	TRENDnet TV-IP743SIC Unspecified Buffer Overflow	
127015	2015-09-02	5.0	TRENDnet TV-IP743SIC Unspecified Password Saving Information Disclosure	
127025	2015-09-01	10.0	TRENDnet TEW-812DRU Multiple Unspecified Issues (1.0.15.0)	
126931	2015-08-27	10.0	TRENDnet Multiple Routers WPS PIN Unspecified Issues	
126899	2015-08-27	10.0	TRENDnet TEW-811DRU NetUSB Unspecified Issues	
125950	2015-08-05	3.3	TRENDnet Multiple Routers Insecure Default WPA Key Generation Brute-force Weakness	
123981	2015-06-29	10.0	TRENDnet TEW-812DRU NetUSB Unspecified Issue	
123835	2015-06-26	7.8	TRENDnet TEW-828DRU Unspecified DoS	
123317	2015-06-12	10.0	TRENDnet Multiple Router UPnP miniigd Unspecified Issue	
122324	2015-05-19	10.0	KCodes NetUSB run_init_sbus() Function Computer Name Handling Remote Stack Buffer Overflow	2015-3036
121597	2015-04-30	5.0	TRENDnet TEW-811DRU Unencrypted Backup Configuration File Information Disclosure	
121276	2015-04-24	10.0	Realtek SDK miniigd SOAP Service NewInternalClient Request Handling Remote Code Execution	2014-8361
119932	2015-03-25	10.0	TRENDnet TS-S402 Unspecified Issue	
119523	2015-03-10	10.0	TRENDnet Multiple Product Multiple Unspecified Issues	
118887	2015-02-26	10.0	D-Link / TRENDnet Devices ncc2 Service Unauthenticated Diagnostic Hook Access	
118886	2015-02-26	10.0	D-Link / TRENDnet Devices ncc2 Service ping.ccp String Handling Remote Command Execution	2015-1187

Internet of Things – D-Link

ID	Disc Date	CVSS	Title	CVE
130252	2015-11-14	4.3	D-Link DIR-816L /hedwig.cgi Admin Password Manipulation CSRF	2015-5999
130398	2015-11-13	10.0	D-Link Multiple Products SSDP Packet Handling Remote Command Injection	
130399	2015-11-13	10.0	D-Link Multiple Product /dws/api/Login Remote Buffer Overflow	
130408	2015-11-13	10.0	D-Link DGL5500 /hnap.cgi Remote Buffer Overflow	
130400	2015-11-13	10.0	D-Link Multiple Products /HNAP1/ SOAPACTION Handling Remote Buffer Overflow	
130406	2015-11-13	9.0	D-Link DIR-815 auth_main.cgi Remote Buffer Overflow	
130403	2015-11-13	6.8	D-Link DIR-825 /apply.cgi html_response_page Parameter Path Traversal Remote File Disclosure	
130404	2015-11-13	10.0	D-Link Multiple Products /ping_response.cgi ping_ipaddr Value Handling Remote Buffer Overflow	
130405	2015-11-13	10.0	D-Link Multiple Products /webfa_authentication.cgi Remote Buffer Overflow	
130407	2015-11-13	9.0	D-Link DIR-601 /my_cgi.cgi Remote Command Injection	
130410	2015-11-13	10.0	D-Link Multiple Products /HNAP1/ SOAPACTION Handling Remote Command Injection	
129844	2015-10-28	6.4	D-Link DCS-5222L Unspecified Remote Camera Manipulation	
127428	2015-09-10	2.6	D-Link DI-624 UPnP Protocol Control URL UUID Prediction NAT Bypass Internal Resource Interaction Weakness (Filet-o-Firewall)	
125565	2015-07-28	4.3	D-Link DCS-2103 /vb.htm Multiple Action CSRF	
125566	2015-07-28	5.0	D-Link DCS-2103 /vb.htm tstamplabel Parameter Stored XSS	
124977	2015-07-17	8.3	D-Link Multiple Products /send_log_email.cgi test Parameter Remote Buffer Overflow	
124978	2015-07-17	8.3	D-Link Multiple Products HTTP Cookie Authentication Handling Remote Buffer Overflow	
124310	2015-07-08	7.8	D-Link Multiple Products /cgi-bin/webproc getpage Parameter Absolute Path Traversal Remote File Disclosure	
123501	2015-06-12	10.0	D-Link DSP-W110 HTTP Cookie Handling Limited Remote Command Execution	
123503	2015-06-12	7.5	D-Link DSP-W110 HTTP Request Handling File Upload Remote Code Execution	
123502	2015-06-12	5.0	D-Link DSP-W110 Unauthenticated Remote Information Disclosure Weakness	
122687	2015-05-27	10.0	D-Link Multiple Products Multiple Default Accounts	
122693	2015-05-27	10.0	D-Link Multiple Product check_login() Function Cookie Handling Remote Command Execution	

Internet of Things – TP-LINK

ID	Disc Date	CVSS	Title	CVE
127536	2015-09-15	10.0	TP-Link NC200/NC220 Cloud Camera Default Hardcoded root Credentials	
125702	2015-07-01	5.0	RIPv1 Protocol Broadcast Request Spoofing Reflection DDoS	
122981	2015-06-08	5.0	TP-LINK TD-W8950ND /dnscfg.cgi Unauthenticated Remote DNS Manipulation	
122324	2015-05-19	10.0	KCodes NetUSB run_init_sbus() Function Computer Name Handling Remote Stack Buffer Overflow	2015-3036
120544	2015-04-10	7.8	TP-LINK Multiple Devices /login/ Remote Path Traversal File Access	2015-3035
116801	2015-01-07	4.3	TP-LINK TL-WR840N Configuration File Importing CSRF	2014-9510
115017	2014-11-24	5.0	TP-LINK TL-WR740N httpd Service PinglframeRpm.htm isNew Parameter Remote DoS	2014-9350
115208	2014-10-30	10.0	TP-LINK M7350 Default Admin Credentials	
112479	2014-10-01	5.0	TP-LINK Multiple Products Cipher Suite Downgrade Weakness	
111915	2014-09-22	7.8	TP-LINK TL-WDR4300 HTTP Header Handling Remote DoS	2014-4728
111914	2014-09-22	4.0	TP-LINK TL-WDR4300 DHCP Hostname Field Stored XSS	2014-4727
111713	2014-09-08	4.3	TP-LINK TL-WR841N / TL-WR841ND /userRpm/LanDhcpServerRpm.htm DHCP Settings Manipulation CSRF	
111709	2014-09-08	5.0	TP-LINK TL-WR841N / TL-WR841ND /userRpm/WlanSecurityRpm.htm pskSecret Parameter Stored XSS	
111715	2014-09-08	4.3	TP-LINK TL-WR841N / TL-WR841ND /userRpm/DateTimeCfgRpm.htm Time Settings Manipulation CSRF	
111707	2014-09-08	5.0	TP-LINK TL-WR340G / TL-WR340GD /userRpm/WlanNetworkRpm.htm ssid Parameter Stored XSS	
111719	2014-09-08	4.3	TP-LINK TL-WR841N / TL-WR841ND /userRpm/WlanSecurityRpm.htm pskSecret Parameter Password Manipulation CSRF	
111758	2014-09-08	5.0	TP-LINK TL-WR841N / TL-WR841ND /userRpm/NoipDdnsRpm.htm Multiple Parameter Stored XSS	
111712	2014-09-08	10.0	TP-LINK Multiple Product Default Admin Credentials	
111706	2014-09-08	5.0	TP-LINK TL-WR340G / TL-WR340GD /userRpm/DomainFilterRpm.htm domain Parameter Stored XSS	
111704	2014-09-08	4.3	TP-LINK TL-WR340G / TL-WR340GD /userRpm/NetworkLanCfgRpm.htm IP Address Manipulation CSRF	
111710	2014-09-08	4.3	TP-LINK TL-WR841N / TL-WR841ND /userRpm/WlanNetworkRpm.htm Multiple Parameter Reflected XSS	
111718	2014-09-08	5.0	TP-LINK TL-WR841N / TL-WR841ND /userRpm/AutoEmailRpm.htm Multiple Parameter Stored XSS	
111714	2014-09-08	4.3	TP-LINK TL-WR841N / TL-WR841ND /userRpm/NoipDdnsRpm.htm Dynamic DNS Settings Manipulation CSRF	

Internet of Things – Everfocus

ID	Disc Date	CVE	CVSS	Title
116603	2015-01-01		9.3	EverFocus EverNet3 ActiveX Control DestroyOcx() Method Uninitialized Value Use Arbitrary Code Execution
116604	2015-01-01		9.3	EverFocus EverNet3 ActiveX Control MoveWindow() Method Uninitialized Value Use Arbitrary Code Execution
116605	2015-01-01		9.3	EverFocus EverNet3 ActiveX Control ProbeDevice() Method Stack Buffer Overflow
116606	2015-01-01		9.3	EverFocus EverNet3 ActiveX Control ReadUnicodeText() Method Stack Buffer Overflow
116607	2015-01-01		9.3	EverFocus EverNet3 ActiveX Control SendHttpRequest() Method Heap Buffer Overflow
116608	2015-01-01		9.3	EverFocus EverNet3 ActiveX Control SendHttpRequest() Method Stack Buffer Overflow
116609	2015-01-01		9.3	EverFocus EverNet3 ActiveX Control SendHttpRequest2() Method Heap Buffer Overflow
116610	2015-01-01		9.3	EverFocus EverNet3 ActiveX Control SendHttpRequestEx() Method Stack Buffer Overflow
116611	2015-01-01		9.3	EverFocus EverNet3 ActiveX Control SendHttpRequestEx() Method Heap Buffer Overflow
116612	2015-01-01		9.3	EverFocus EverNet3 ActiveX Control SendHttpRequestEx() Method szXmlHeader Argument Heap Buffer Overflow
116613	2015-01-01		9.3	EverFocus EverNet3 ActiveX Control SetRegedit() Method szPath Argument Stack Buffer Overflow
116614	2015-01-01		9.3	EverFocus EverNet3 ActiveX Control SetRegedit() Method szValue Argument Stack Buffer Overflow
116615	2015-01-01		9.3	EverFocus EverNet3 ActiveX Control SetROIEraser() Method Arbitrary Code Execution
116616	2015-01-01		9.3	EverFocus EverNet3 ActiveX Control SetUnicodeFontInfo() Method Stack Buffer Overflow
116617	2015-01-01		9.3	EverFocus EverNet3 ActiveX Control String Encoding Routine He
116618	2015-01-01		9.3	EverFocus EverNet3 ActiveX Control Two Methods Uninitialized V
116600	2015-01-01		9.3	EverFocus EPlusOcx ActiveX Control LiveStream() Method Stack
116620	2015-01-01		9.3	EverFocus EverNet3 ActiveX Control CreateAreaLine() Method U
116601	2015-01-01		9.3	EverFocus EPlusOcx ActiveX Control OpenArchive() Function Sta
116602	2015-01-01		9.3	EverFocus EPlusOcx ActiveX Control SendHttpRequest() Method Stack Buffer Overflow
116619	2015-01-01		9.3	EverFocus EverNet3 ActiveX Control CreateObjectSizeGrids() Method Stack Buffer Overflow

21 Vulnerabilities

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]/cgibin/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 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?

Response and Actions!


ACCOUNTABILITY

Internet of Things – FTC Fines and Penalities

Kashmir Hill
Forbes Staff

FOLLOW

Welcome to The Not-So Private Parts where technology & privacy collide
full bio →

TECH 9/04/2013 @ 4:48PM | 19,681 views

Camera Company That Let Hackers Spy On Naked Customers Ordered By FTC To Get Its Security Act Together

Let's say you bought an Internet-connected camera for your home so you could keep an eye on your baby, or watch your dog while you were at work, or to make sure your home was secure while vacationing. Or maybe you got it for your office to secure your safe or Big Brother your workers. But what if the company that sold you that camera designed it so poorly that anyone with just a modicum of technical savvy could break into it and watch along with you? That's what happened to hundreds of people who bought IP cams from TRENDnet, a company that includes "trust" in its tagline. In January 2012, a blogger revealed a security flaw that let curious users spy on women changing, parents checking on babies, and rooms all over the world worth sticking a camera in. Beyond embarrassment for the company (and its exposed customers) nothing seemed to come of the terrible security mistake... until now. The Federal Trade Commission announced Wednesday that it has ordered TRENDnet to improve the security of its cameras and to warn all of its voyeur-victim customers

Internet of Things – FTC Fines and Penalities

Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy

Hundreds of Camera Feeds for Home Security, Baby Monitoring Were Hacked, Posted Online

FOR RELEASE

September 4, 2013

TAGS: Technology | Bureau of Consumer Protection | Consumer Protection | Privacy and Security | Consumer Privacy | Data Security

A company that markets video cameras designed to allow consumers to monitor their homes remotely has settled Federal Trade Commission charges that its lax security practices exposed the private lives of hundreds of consumers to public viewing on the Internet. This is the agency's first action against a marketer of an everyday product with interconnectivity to the Internet and other mobile devices – commonly referred to as the "Internet of Things."

Internet of Things – FTC – TRENDnet Settlement

TRENDnet is:

- prohibited from **misrepresenting the security of its cameras**
- required to **establish a comprehensive information security program** designed to address security risks that could result in unauthorized access
- **required to obtain third-party assessments** of its security programs every two years for the next 20 years.
- required to **notify customers** of security issues and updates available to correct any flaw

Internet of Things – FTC Fines and Penalities

Chris Clearfield
Subscriber

FOLLOW

I write about the interaction between risk and complex systems.
full bio →

Why The FTC Can't Regulate The Internet Of Things

The "Internet of Things" has become a favored buzzword of consultants and tech journalists. But beware, there be dragons that neither regulators nor privacy advocates can vanquish.

In an early salvo against the manufacturer of a connected device that is part of the Internet of Things, the Federal Trade Commission brought an action against TRENDnet, a developer of web-enabled video cameras that failed to live up to the security claims that the company had made to users: in 2012, hackers found a flaw that exposed users' private video feeds without their knowledge. The settlement imposes a twenty-year security compliance audit program on TRENDnet and potential fines for future violations. Thus, for security vulnerabilities in their connected cameras, TRENDnet joins the likes of Google and Facebook, which are subject to similar settlements and privacy audits for past violations of users' online privacy.

Internet of Things – FTC Recommendations

FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks

Report Recognizes Rapid Growth of Connected Devices Offers Societal Benefits, But Also Risks That Could Undermine Consumer Confidence

FOR RELEASE

January 27, 2015

TAGS: Technology | Bureau of Consumer Protection | Consumer Protection | Privacy and Security | Consumer Privacy | Data Security

In a detailed report on the Internet of Things, released today, the staff of the Federal Trade Commission recommend a series of concrete steps that businesses can take to enhance and protect consumers' privacy and security, as Americans start to reap the benefits from a growing world of Internet-connected devices.

The Internet of Things is already impacting the daily lives of millions of Americans through the adoption of health and fitness monitors, home security devices, connected cars and household appliances, among other applications. Such devices offer the potential for improved health-monitoring, safer highways, and more efficient home energy use,

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 software is in use where including IoT devices
  - Look at outgoing web traffic / logs to see what IoT devices are talking 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 – Don't Only Rely On Vuln Scanning

Most organizations ONLY use scanners for managing vulnerabilities

- Many scanners do not even include IoT checks in their products! Even if they did they can't find some of the issues!
- Even if they did, it is a much longer Time of Exposure than if you truly know your environment (assets) and map to known vulnerabilities
- Use scanners as a catch all and to help uncover configuration issues, but know IoT isn't a focus yet!

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 indentified

Internet of Things – IoT Vendors

- Accept devices are going to be connected to the Internet and can be easily accessed
  - Plan for this and ensure the proper security is in build into the product
- Ensure software / firmware can be updated and actually update it!
  - Do NOT allow “forever day” bugs!
  - Plan for updates, limit the use of embedded components where possible
  - Create an easy to use auto-update features available
- Educate staff on security issues
  - Train developers on secure development
  - Create a process and figure out how to respond when issues are found/reported
  - Create an Incident Response team and disclosure vulnerabilities

Internet of Things – IoT Vendors

- Implement proper logging and audit history for access and usage
- Implement access control for the device, including two factor authentication options.
- Perform source code security audits and product penetration tests
  - Consider creating a bug bounty program to reward reported vulnerabilities in products
- Understand the 3rd party libraries and code used in the product
  - Select secure libraries from the beginning
  - Monitor for 3rd party vulns and correct.

Internet of Things – Actions

1. Start talking with your executives about the issues and ensure you are in the loop to conduct the proper risk assessments.
2. IoT is already in your network and more is coming very soon! Inventory current IoT and ensure ongoing monitoring
3. Ensure you incorporate your incident response program to include IoT products and vendors.
4. Work with vendors and pick products that demonstrate they care about security!

Thank You!


Thanks to RSA for allowing us to present our research on this emerging risk!

Internet of Things – Questions?

RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

SESSION ID: CSV-F02

Bring Your Own Internet of Things: BYO-IoT

Carsten Eiram
Chief Research Officer
Risk Based Security
@carsteneiram

Jake Kouns
CISO
Risk Based Security
@jkouns