



RiskBased
SECURITY

Bring Your Own Internet of Things

BYO-IoT

Carsten Eiram

Chief Research Officer

che@riskbasedsecurity.com / [@CarstenEiram](https://twitter.com/CarstenEiram)

Jake Kouns

Chief Information Security Officer

jake@riskbasedsecurity.com / [@jkouns](https://twitter.com/jkouns)

Community offerings:



OSVDB



MY PRIVACY AUDIT



DATA LOSS db
open security foundation



SECore .info beta

Commercial offerings:



VulnDB Risk Based Security



Cyber Risk Analytics



YOUR CISO



What's IoT?



“I could be wrong, but I'm fairly sure the phrase 'Internet of Things' started life as the title of a presentation I made at Procter & Gamble in 1999.”

Kevin Ashton



WOOPTY DOO BASIL



**BUT WHAT DOES IT ALL
MEAN**

memegenerator.net

“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

<http://www.techopedia.com/definition/28247/internet-of-things-iot>

“The Internet of Things (IoT) is the **network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.**”

- Gartner

<http://www.gartner.com/it-glossary/internet-of-things/>

“The Internet of Things (IoT) is the **network of physical objects or "things" embedded with electronics, software, sensors and connectivity** to enable it to achieve greater value and service by **exchanging data with the manufacturer, operator and/or other connected devices.**

Each thing is uniquely identifiable through its embedded computing system but is **able to interoperate within the existing Internet infrastructure.**”

- Wikipedia

http://en.wikipedia.org/wiki/Internet_of_Things

“The fact that I was probably the first person to say "Internet of Things" doesn't give me any right to control how others use the phrase. But what I meant, and still mean, is this: Today computers - and, therefore, the Internet - are almost wholly dependent on human beings for information.

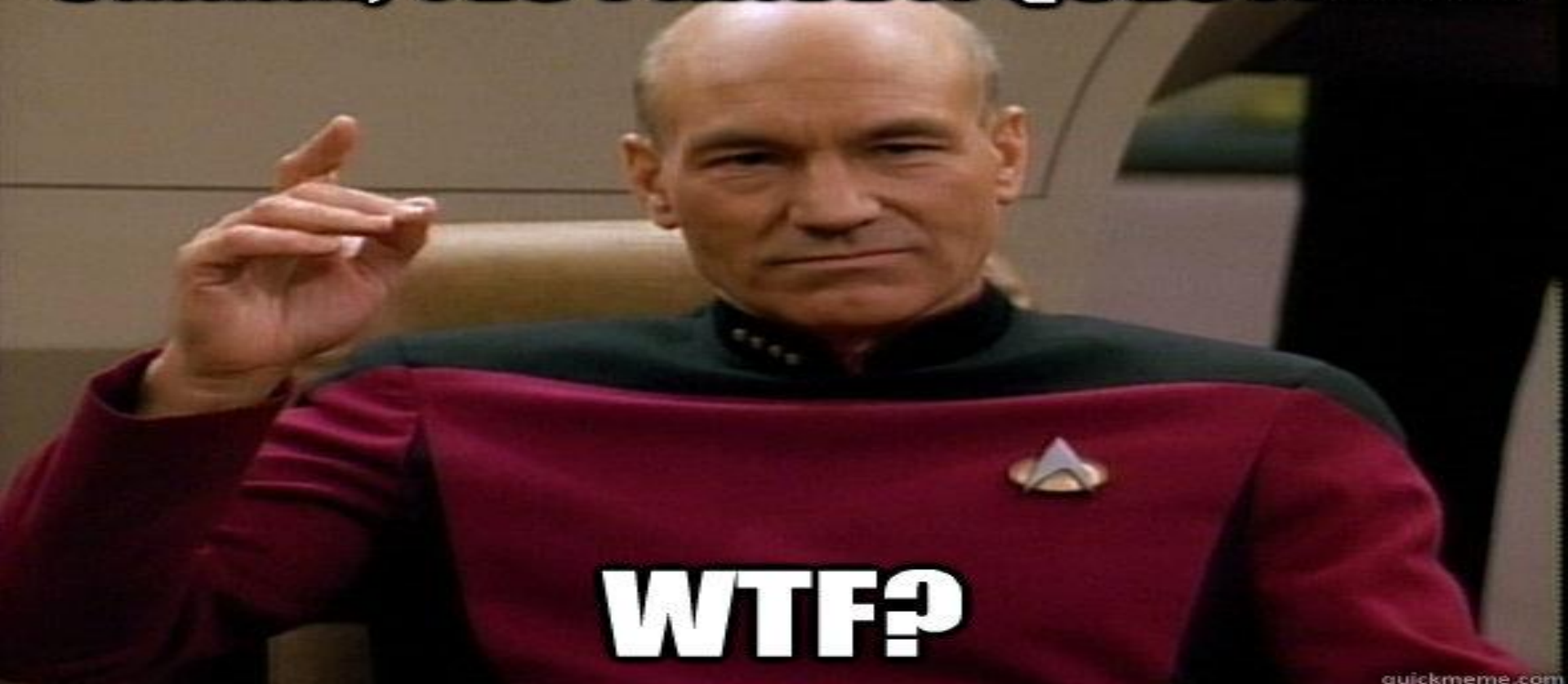
If we had **computers** that knew everything there was to know about things - **using data they gathered without any help from us** - we would be able to track and count everything.

We need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves, in all its random glory. **RFID and sensor technology enable computers to observe, identify and understand the world - without the limitations of human-entered data.**”

- Kevin Ashton

<http://www.rfidjournal.com/articles/view?4986>

UMMM, YES I HAVE A QUESTION...



WTF?

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)



NOT JUST SECURITY , THE RIGHT SECURITY

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



NOT JUST SECURITY , THE RIGHT SECURITY

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 – Examples (Retail)



NOT JUST SECURITY, THE RIGHT SECURITY

Internet of Things – Examples (Environmental)



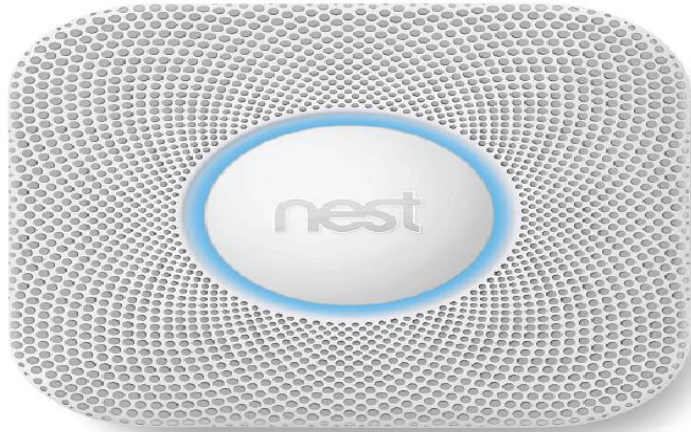
NOT JUST SECURITY , THE RIGHT SECURITY

Internet of Things – Examples (Your Network?)



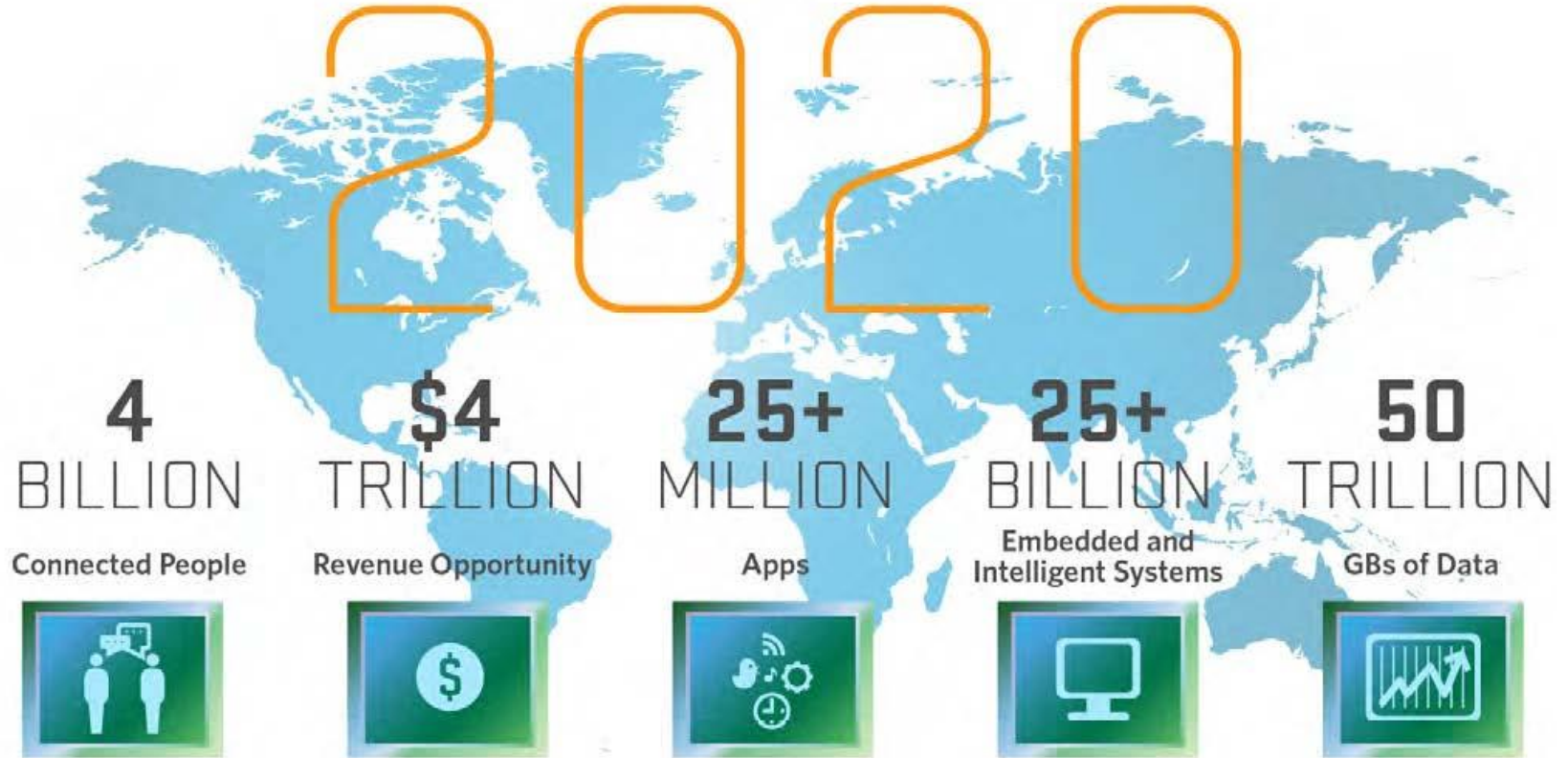
NOT JUST SECURITY , THE RIGHT SECURITY

Internet of Things – Examples (Your Network?)



NOT JUST SECURITY, THE RIGHT SECURITY

Internet of Things – Why Should You Care?



Source: Mario Morales, IDC

NOT JUST SECURITY , THE RIGHT SECURITY

- 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>

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!**

What's The Problem?





BYOD

BRING YOUR OWN DEVICE

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.

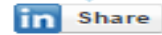
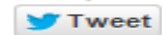
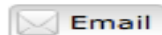


Gartner estimates the IoT will see 26 billion units installed by 2020 – channelling huge volumes of data traffic into datacentres


CIOs beware, IoT is coming

May 13, 2015 | By Fred Donovan

SHARE



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](#)]

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.



Fred Donovan

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

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 medical devices from hackers



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



FDA asks hackers to expose holes in medical devices, but many researchers fear...

on IDG Answers →

How serious of a security threat is the “Bug?”

GAIN ENTERPRISE VISIBILITY.

USE CONTEXT TO DRIVE ACTION.



60 MINUTES

[EPISODES](#) - [OVERTIME](#) - [TOPICS](#) - [THE](#)



CAR HACKED ON 60 MINUTES

NOT JUST SECURITY, THE RIGHT SECURITY



U.S. Edition

News Video TV Opinions More...

New York City, NY 64° Sign in

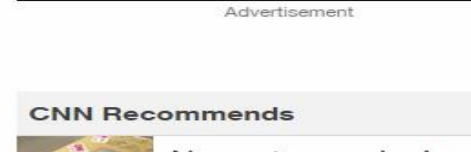
Search CNN

U.S. World Politics Tech Health Entertainment Living Travel Money Sports

Watch Live

FBI: Hacker claimed to have taken over flight's engine controls

By **Evan Perez**, CNN Updated 9:19 PM ET, Mon May 18, 2015



[Dailydave] Junk Hacking Must Stop!

Dave Aitel [dave at immunityinc.com](mailto:dave@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.

A large, yellow diamond-shaped sign with a black border, mounted on a post. The sign has the words "CHANGE" and "AHEAD" written in large, bold, black, sans-serif capital letters, stacked vertically. The background behind the sign is a clear blue sky with some light clouds.

**CHANGE
AHEAD**

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?



[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-](http://www.tripwire.com/register/enterprise-)

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/>

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

Less than $\frac{1}{4}$ of IT professionals are **confident** in the secure configuration of common IoT devices on enterprise networks

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

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

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/>

THE INTERNET OF THINGS & KICKSTARTER A perfect match?



NUMBER OF CAMPAIGNS BY YEARS



Internet of Things – Kickstarter & Indiegogo



Rank	Company	Description	Amount raised	Campaign end	Crowdfunding site
1	Pebble	Smart watch	\$10,266,845	May/2012	Kickstarter
2	OUYA	Cloud video game platform	\$8,596,474	Aug/2012	Kickstarter
3	The Dash	Smart earphones	\$3,390,551	Mar/2014	Kickstarter
4	Scio	Molecular sensor	\$2,762,571	Jun/2014	Kickstarter
5	Oculus Rift	3D headset	\$2,437,429	Sep/2012	Kickstarter
6	Sense	Pillow/room sensor	\$2,364,765	Aug/2014	Kickstarter
7	Canary	Home security device	\$1,961,663	Aug/2013	Indiegogo
8	Anova Precision Cooker	Smart cooker	\$1,811,321	Jun/2014	Kickstarter
9	JIBO	Social robot	\$1,781,437	Sep/2014*	Indiegogo
10	Scanadu Scout	Sensor packed device	\$1,662,187	Jul/2013	Indiegogo

- **Crowdfunding:**
 - Lots of innovation is happening, which is great, but its happening in some cases under-funded
 - Quick go-to-market is important
 - Features win out over security
 - Devices still will end up in the enterprise

Internet of Things – Is There An Impact?



NOT JUST SECURITY , THE RIGHT SECURITY



NEWS / OPINIONS / FEATURES / DEALS / HOW-TO / BUSINESS / VIDEO / SUBSCRIBE

ALL REVIEWS ▼ LAPTOPS / TABLETS / PHONES / APPS / SOFTWARE / SECURITY

Home / Reviews / Networking / Security / HVAC Vendor Confirms Link to Target Data Breach

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.

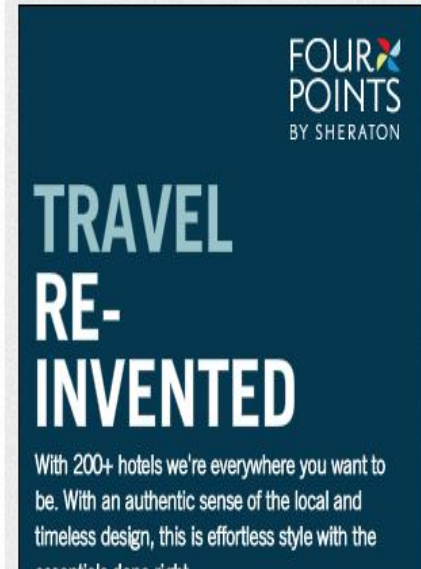
On Friday, owner and president Ross E. Fazio confirmed that his company, a refrigeration and HVAC systems maker, was "a victim of a sophisticated cyber attack operation."

Continuing trend of
targeting user names, e-
mail addresses, and
passwords.



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

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



FOUR POINTS
BY SHERATON

TRAVEL RE- INVENTED

With 200+ hotels we're everywhere you want to be. With an authentic sense of the local and timeless design, this is effortless style with the essentials done right.

Not just a few 3rd party breaches...



Number of Incidents

2,030



Number of Records

1,127,511,501



Avg Records Lost Per Breach

555,424

In 2014 alone:



Number of Incidents

325



Number of Records

410,445,549



Avg Records Lost Per Breach

1,262,909

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

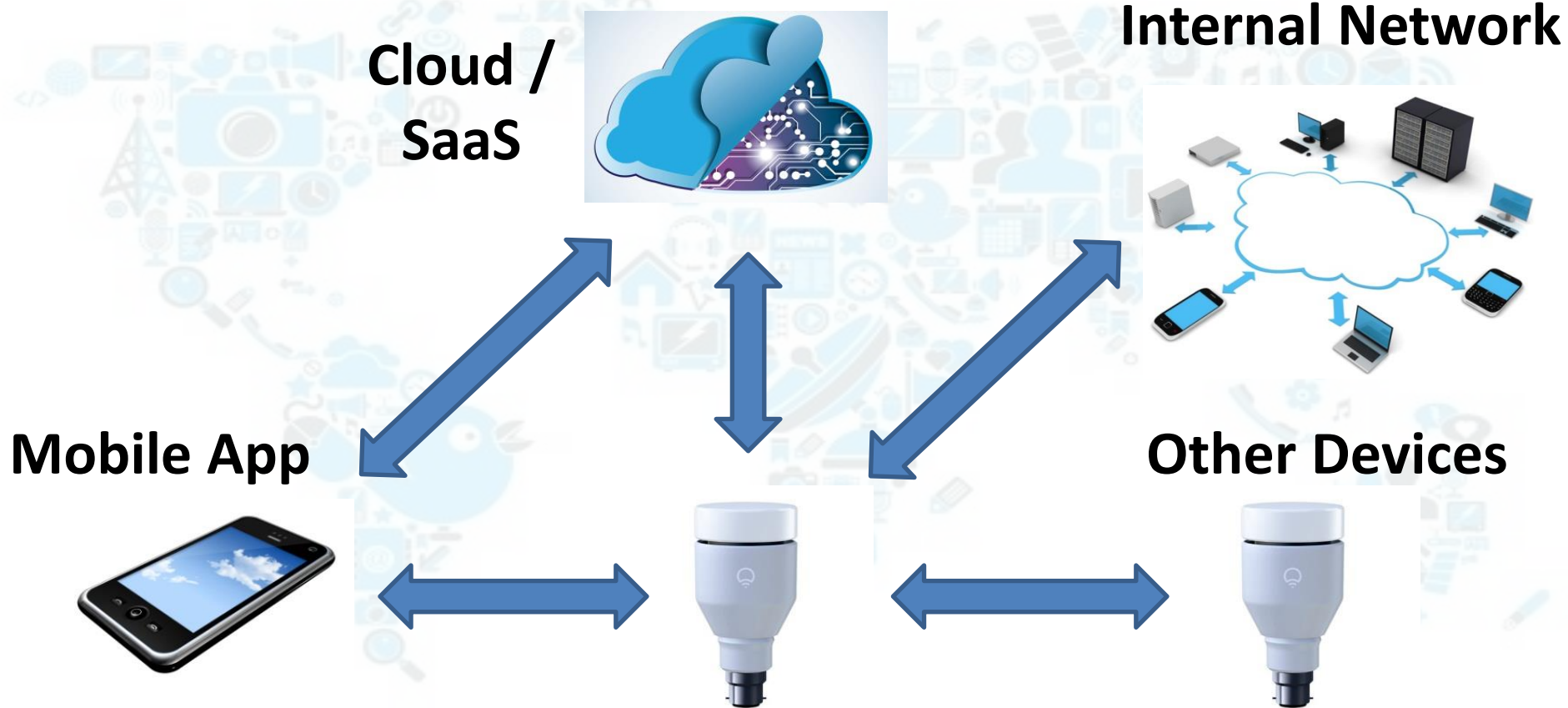


SHADOW IT

COMING TO A DEPARTMENT
NEAR YOU.

What's The Attack Surface?





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

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

- 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?

- 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?

Enterprise IoT

BYOD (BYO-IoT) / Cross-contamination

Remote workers

IoT Security

Current State



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.

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

Hacking Insulin Pumps And Other Medical Devices From Black Hat

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

**HOW THIEVES CAN HACK AND
DISABLE YOUR HOME ALARM
SYSTEM**

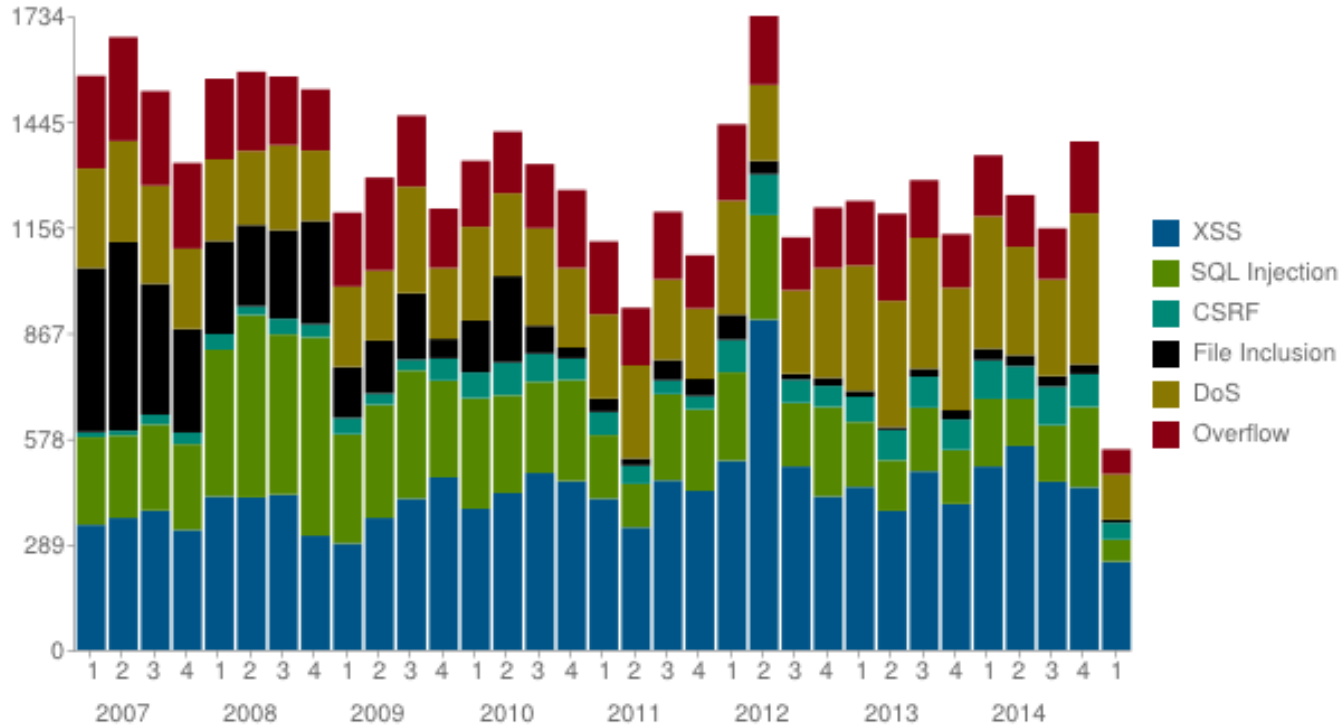
Why so relatively few critical vulnerabilities?

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

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

Internet of Things – State of Security

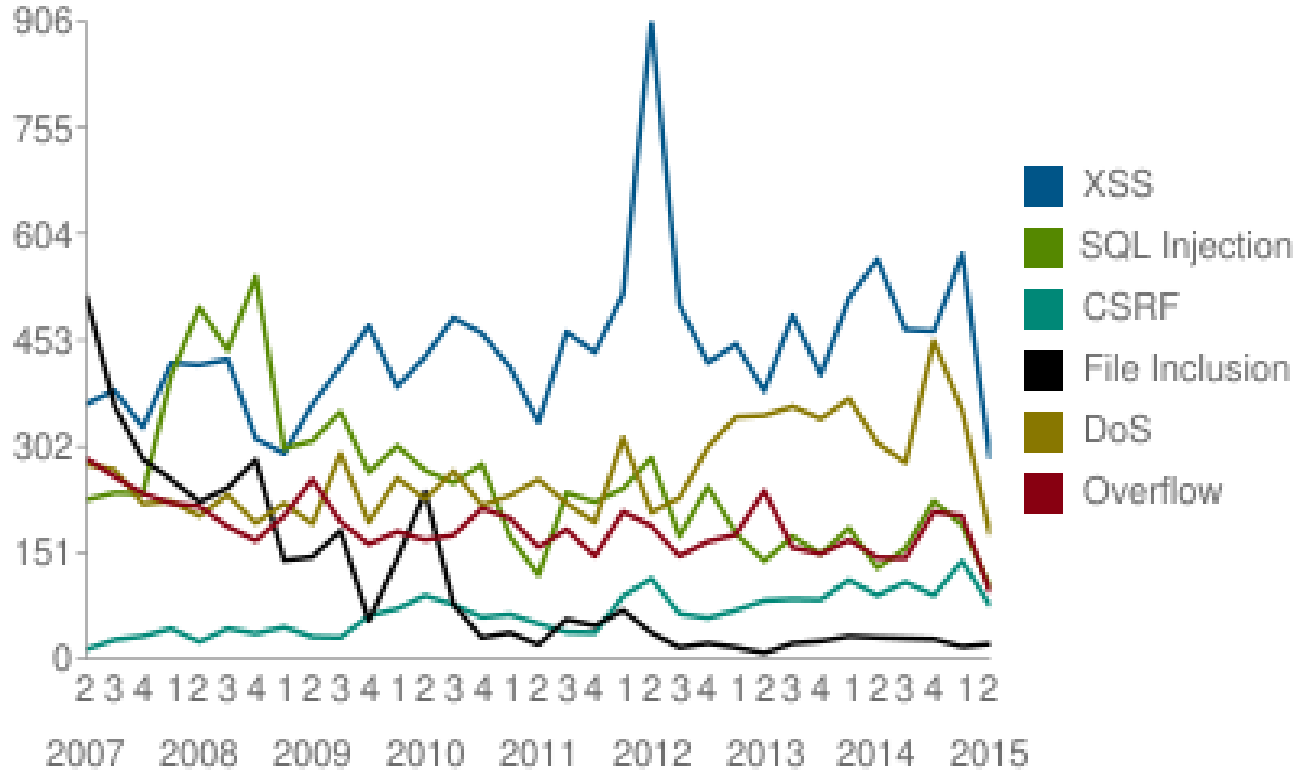
Vulnerabilities in OSVDB by Quarter by Type



2015*:	<u>5,215</u>
2014:	<u>13,527</u>
2013:	<u>11,178</u>
2012:	<u>10,372</u>
2011:	<u>7,921</u>
2010:	<u>9,165</u>
2009:	<u>8,183</u>
2008:	<u>9,806</u>
2007:	<u>9,587</u>
2006:	<u>11,049</u>

Source: OSVDB.org
*YTD May 31st, 2015

Internet of Things – State of Security



2015*:	<u>5,215</u>
2014:	<u>13,527</u>
2013:	<u>11,178</u>
2012:	<u>10,372</u>
2011:	<u>7,921</u>
2010:	<u>9,165</u>
2009:	<u>8,183</u>
2008:	<u>9,806</u>
2007:	<u>9,587</u>
2006:	<u>11,049</u>

Source: OSVDB.org
*YTD May 31st, 2015

ID	Disc Date	CVE	CVSS	Title
121597	2015-04-30		5.0	TRENDnet TEW-811DRU Unencrypted Backup Configuration File Information Disclosure
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
118885	2015-02-26		5.0	D-Link / TRENDnet Devices ncc2 Service fwupgrade.ccp HTTP Request Handling Remote File Creation
118886	2015-02-26	2015-1187	10.0	D-Link / TRENDnet Devices ncc2 Service ping.ccp String Handling Remote Command Execution
107941	2014-06-10		2.1	TRENDnet N300 High Power Easy-N-Range Extender Unspecified Local File Disclosure
117559	2015-01-25	2014-2703	10.0	TRENDnet TN-200 / TN-200T1 /cgi-bin/webfile_mgr.cgi Remote Encoded Path Traversal File Upload / Download
117556	2015-01-25	2014-1628	9.0	TRENDnet TN-200 / TN-200T1 /cgi-bin/system_mgr.cgi Remote Command Execution
117558	2015-01-25	2014-1629	4.3	TRENDnet TN-200 / TN-200T1 Multiple Unspecified CSRF
117561	2015-01-25	2014-1630	9.3	TRENDnet TN-200 / TN-200T1 Authentication Cookie Manipulation Session Hijacking
117562	2015-01-25	2014-2704	5.0	TRENDnet TN-200 / TN-200T1 xml / common Directories Remote Information Disclosure
117557	2015-01-25	2014-1628	9.0	TRENDnet TN-200 / TN-200T1 /cgi-bin/remote_backup.cgi Remote Command Execution
117560	2015-01-25	2014-2703	5.0	TRENDnet TN-200 / TN-200T1 /cgi-bin/folder_tree.cgi Remote Encoded Path Traversal Directory Listing
116248	2014-12-23		10.0	TRENDnet TV-IP310PI / TV-IP311PI Unspecified Unauthorized Access URL Issue
106413	2014-04-29		7.8	TRENDnet TEW-634GRU / TEW-654TR TFTP Service Unauthenticated Remote File Access
115037	2014-11-25	2014-10011	9.3	TRENDnet TV-IP422WN UltraCamX.ocx ActiveX Byte Parsing Stack Buffer Overflow
114410	2014-11-07		10.0	TRENDnet Multiple Cameras Unauthorized Access URL Unspecified Issue
114330	2014-11-06		10.0	TRENDnet Multiple Cameras Unspecified Issues
114355	2014-11-05		4.3	TRENDnet TEW-432BRP Router Unspecified CSRF
115220	2014-10-21		10.0	TRENDnet TPE-2840WS Default Admin Credentials

ID	Disc Date	CVE	CVSS	Title
122679	2015-05-27		5.0	D-Link DNR-326 Widget api.cgi Unauthenticated Access Remote Information Disclosure
122680	2015-05-27		5.0	D-Link DNR-326 wizard mgr.cgi Unauthenticated Access Remote Information Disclosure
122681	2015-05-27		7.8	D-Link Multiple Product et.cgi utelnetd Unauthenticated Access Remote DoS
122682	2015-05-27		5.0	D-Link Multiple Product info.cgi Unauthenticated Access Remote Information Disclosure
122683	2015-05-27		5.0	D-Link Multiple Product Widget api.cgi Unauthenticated Access Remote Information Disclosure
122687	2015-05-27		10.0	D-Link Multiple Products Multiple Default Accounts
122688	2015-05-27		7.9	D-Link Multiple Products Cookie Handling Same Subnet Authentication Bypass
122690	2015-05-27		10.0	D-Link Multiple Products system mgr.cgi cgi set wto() Function Crafted Cookie Authentication Bypass
122691	2015-05-27		10.0	D-Link Multiple Products wizard mgr.cgi cgi set wto() Function Crafted Cookie Authentication Bypass
122685	2015-05-27		5.0	D-Link Multiple Products /xml/info.xml Direct Request Remote Information Disclosure
122692	2015-05-27		10.0	D-Link Multiple Products Unspecified Authentication Bypass
122693	2015-05-27		10.0	D-Link Multiple Product check login() Function Cookie Handling Remote Command Execution
122695	2015-05-27		8.5	D-Link DNR-326 apkg mgr.cgi Unauthenticated Access Remote Issue
122696	2015-05-27		6.4	D-Link Multiple Products system mgr.cgi cgi firmware upload() Function Remote Traversal File Overwrite
122697	2015-05-27		6.4	D-Link Multiple Products file sharing.cgi Command ID 3 Unspecified Remote File Overwrite
122698	2015-05-27		10.0	D-Link Multiple Products system mgr.cgi Multiple Function Remote Command Execution
122684	2015-05-27		10.0	D-Link Multiple Products qdrive.cgi Unauthenticated Access Remote Command Injection
122706	2015-05-27		10.0	D-Link Multiple Products save ajax.php Unauthenticated Remote File Upload
122707	2015-05-27		10.0	D-Link Multiple Products /jquery/uploader/multi_uploadify.php HTTP_HOST Header Manipulation Authentication Bypass
122708	2015-05-27		10.0	D-Link DNS-327L /jquery/uploader/uploadify.php Cookie Handling Authentication Bypass

Internet of Things – TP-LINK



ID	Disc Date	CVE	CVSS	Title
120544	2015-04-10	2015-3035	7.8	TP-LINK Multiple Devices /login/ Remote Path Traversal File Access
116801	2015-01-07	2014-9510	4.3	TP-LINK TL-WR840N Configuration File Importing CSRF
115017	2014-11-24	2014-9350	5.0	TP-LINK TL-WR740N httpd Service PingIframeRpm.htm isNew Parameter Remote DoS
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
111914	2014-09-22	2014-4727	4.0	TP-LINK TL-WDR4300 DHCP Hostname Field Stored XSS
111915	2014-09-22	2014-4728	7.8	TP-LINK TL-WDR4300 HTTP Header Handling Remote DoS
111713	2014-09-08		4.3	TP-LINK TL-WR841N / TL-WR841ND /userRpm/LanDhcpServerRpm.htm DHCP Settings Manipulation CSRF
111710	2014-09-08		4.3	TP-LINK TL-WR841N / TL-WR841ND /userRpm/WlanNetworkRpm.htm Multiple Parameter Reflected XSS
111709	2014-09-08		5.0	TP-LINK TL-WR841N / TL-WR841ND /userRpm/WlanSecurityRpm.htm pskSecret Parameter Stored XSS
111719	2014-09-08		4.3	TP-LINK TL-WR841N / TL-WR841ND /userRpm/WlanSecurityRpm.htm pskSecret Parameter Password Manipulation CSRF
111718	2014-09-08		5.0	TP-LINK TL-WR841N / TL-WR841ND /userRpm/AutoEmailRpm.htm Multiple Parameter Stored XSS
111717	2014-09-08		4.3	TP-LINK TL-WR841N / TL-WR841ND /userRpm/AutoEmailRpm.htm Mail Settings Manipulation CSRF
111712	2014-09-08		10.0	TP-LINK Multiple Product Default Admin Credentials
111708	2014-09-08		5.0	TP-LINK TL-WR340G / TL-WR340GD /userRpm/WanDynamicIpCfgRpm.htm hostName Parameter Stored XSS
111707	2014-09-08		5.0	TP-LINK TL-WR340G / TL-WR340GD /userRpm/WlanNetworkRpm.htm ssid Parameter Stored XSS
111706	2014-09-08		5.0	TP-LINK TL-WR340G / TL-WR340GD /userRpm/DomainFilterRpm.htm domain Parameter Stored XSS
111705	2014-09-08		5.0	TP-LINK TL-WR340G / TL-WR340GD /userRpm/DynDdnsRpm.htm Multiple Parameter Stored XSS
111704	2014-09-08		4.3	TP-LINK TL-WR340G / TL-WR340GD /userRpm/NetworkLanCfgRpm.htm IP Address Manipulation CSRF
111703	2014-09-08		4.3	TP-LINK TL-WR340G / TL-WR340GD /userRpm/ManageControlRpm.htm Remote Management Settings Manipulation CSRF
109840	2014-08-03		10.0	TP-LINK TL-WR740N Multiple Feature Domain Name Parameters Remote Command Execution
109839	2014-08-03		10.0	TP-LINK TL-WR740N Web Interface Default Admin Credentials

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

```
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 report available at:

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

No CSRF protection whatsoever

Allows e.g. rebooting device or creating user accounts

`http://[IP]/cgibin/reboot.cgi?action=reboot`

Supports 3 user types:

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

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

`action=add&index=5&username=test&password=test
123&privilege=1`

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

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?

Actions And Response





ACCOUNTABILITY




Kashmir Hill
Forbes Staff

FOLLOW

Welcome to *The Not-So Private Parts* where technology & privacy collide
[full bio](#) →



4
COMMENTS



4 CALLED-OUT

CONFERENCES AND MORE

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

+ Comment Now + Follow Comments

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

Eliminate
reduce
revenue.

Be Certain

LEA



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Contact | Stay C

ABOUT THE FTC

NEWS & EVENTS

ENFORCEMENT

POLICY

TIPS & ADVICE

News & Events » Press Releases » Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to

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."

NOT JUST SECURITY, THE RIGHT SECURITY

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



Chris Clearfield
Subscriber

FOLLOW

I write about the interaction between risk and complex systems.

[full bio](#) →



Comment Now

+ Follow Comments

CONFERENCES AND MORE

Why The FTC Can't Regulate The Internet Of Things

+ Comment Now + Follow Comments

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



Dashboard Trends

Learn tips & tricks for impactful dashboards [eBook]



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Contact | Stay Connected

ABOUT THE FTC

NEWS & EVENTS

ENFORCEMENT

POLICY

TIPS & ADVICE

News & Events » Press Releases » FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks

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,

NOT JUST SECURITY, THE RIGHT SECURITY

H.R.5793 - Cyber Supply Chain Management and Transparency Act of 2014 (Introduced in House - IH)

- To ensure the integrity of any software, **“to verify that the software, firmware, or product does not contain any known security vulnerabilities or defects”** component, and for other purposes.





- 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

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!



Implement proper network segmentation for all IoT devices where possible

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

- Accept devices are going to be connected to the Internet and can be easily accessed
 - Plan for this and ensure the proper security is built 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 feature 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

- 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.

There is a **cost of ownership** with using
3rd party libraries

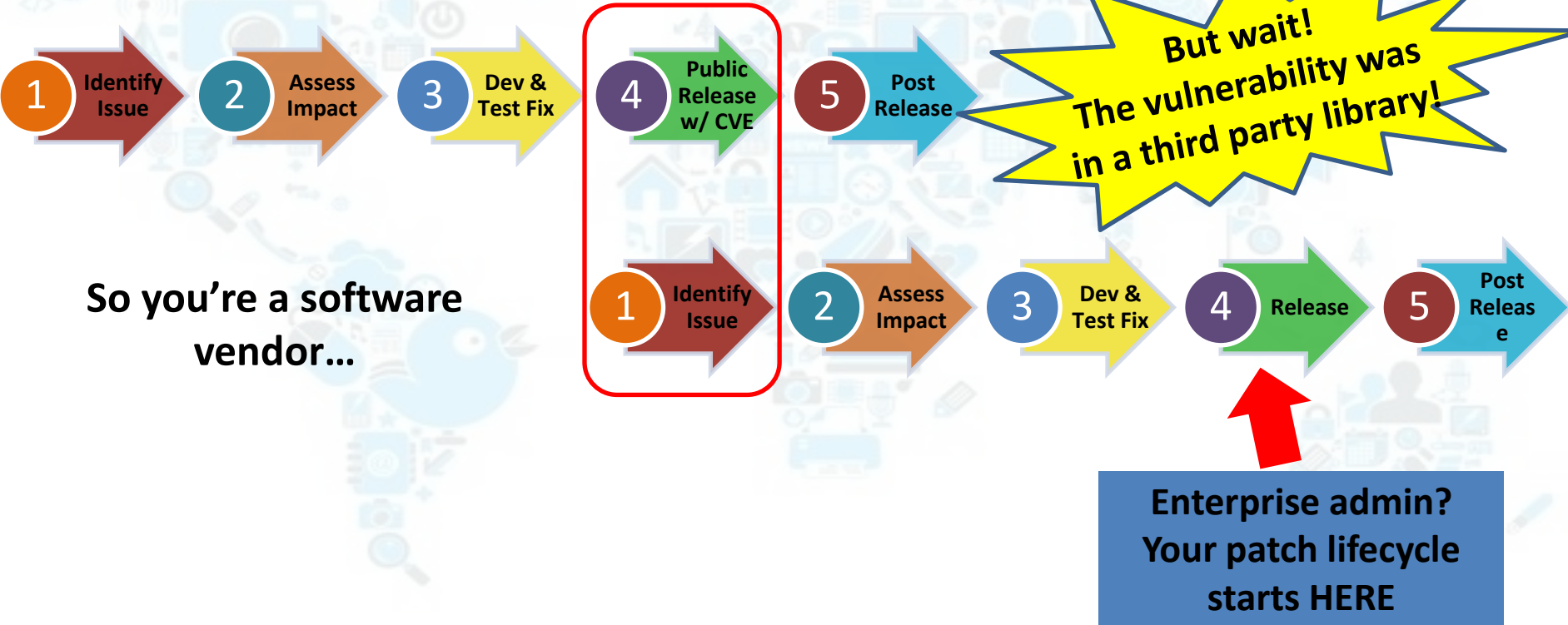
Evaluate **vulnerability trends** in libraries
as part of **selection criteria**

Does the library have **unpatched vulnerabilities?**
End of Life?

Do you have enough **people resources** to handle the expected **vulnerability load**? **Cadence of releases**?

What is your **prioritization model**?

What **early monitoring processes** can you put in place to minimize surprises?



So you're a software vendor...

- IoT is already in your network and more is coming very soon!
- Start talking with your executives about the issues and ensure you are in the loop to conduct the proper risk assessments.
- Inventory IoT and ensure ongoing monitoring
- 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 FIRST for allowing us to present our research on this emerging risk!

NOT JUST SECURITY , THE RIGHT SECURITY





RiskBased
SECURITY

Bring Your Own Internet of Things

BYO-IoT

Carsten Eiram

Chief Research Officer

che@riskbasedsecurity.com / [@CarstenEiram](https://twitter.com/CarstenEiram)

Jake Kouns

Chief Information Security Officer

jake@riskbasedsecurity.com / [@jkouns](https://twitter.com/jkouns)