IoT Security

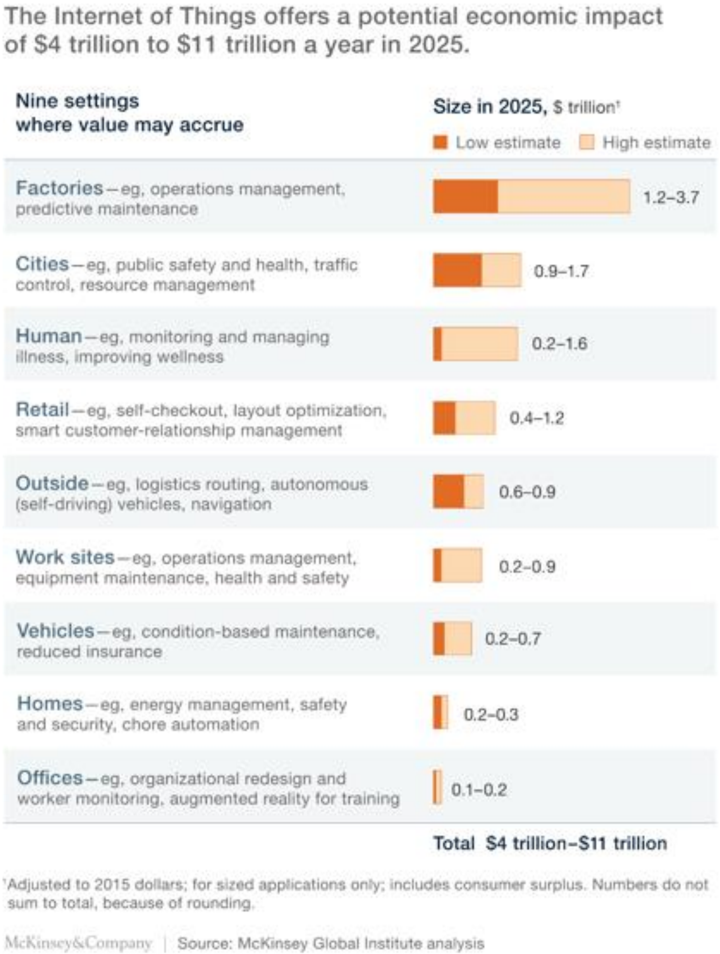
Industry Landscape

Hima Devisetti, Vijay Eranti, Dina McKinney, Serge Maskalik,
Venkata Nandanavanam, Geoffrey Perez, Jeff Pierce

THE INTERNET OF INSECURE THINGS

IoT Potential Impact

Exact estimates vary, but general consensus is yearly economic impact will be in trillions by 2025 (**$4-11 Trillion annually**)

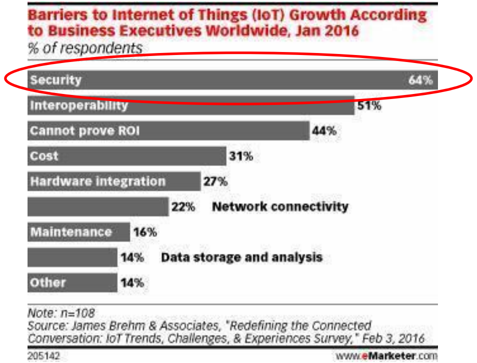


The Internet of Things offers a potential economic impact of $4 trillion to $11 trillion a year in 2025.

[1] Adjusted to 2015 dollars; for sized applications only; includes consumer surplus. Numbers do not sum to total, because of rounding.

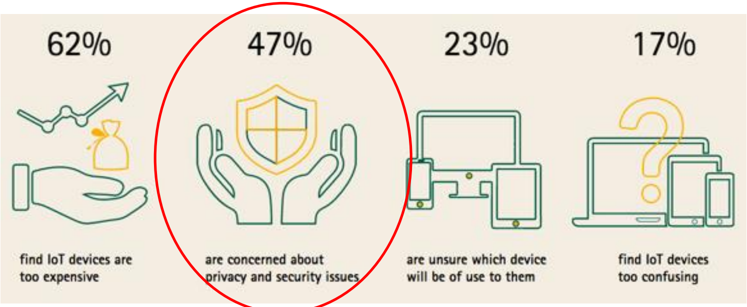
McKinsey&Company | Source: McKinsey Global Institute analysis

Importance of Security to IoT

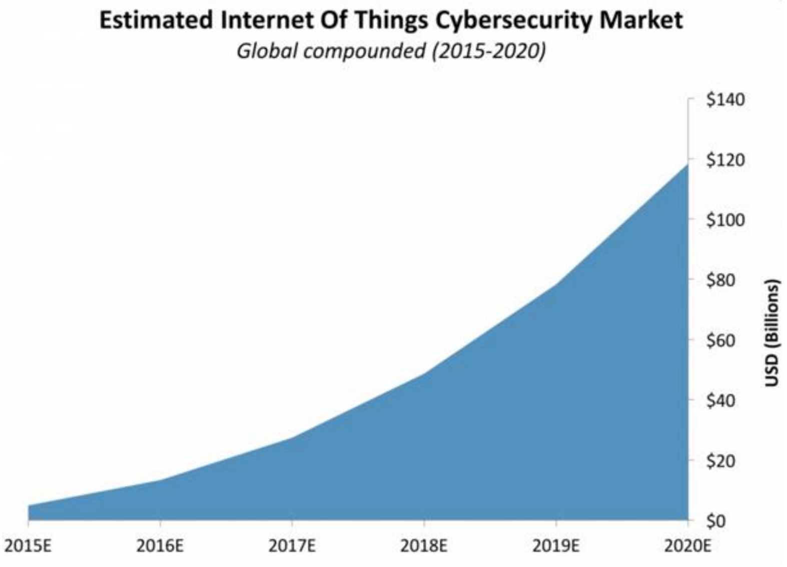

Barriers to Internet of Things (IoT) Growth According to Business Executives Worldwide, Jan 2016

% of respondents

Note: n=108
Source: James Brehm & Associates, "Redefining the Connected Conversation: IoT Trends, Challenges, & Experiences Survey," Feb 3, 2016
205142 www.eMarketer.com



Accenture 2016 Survey on Barriers to Consumer IoT Adoption

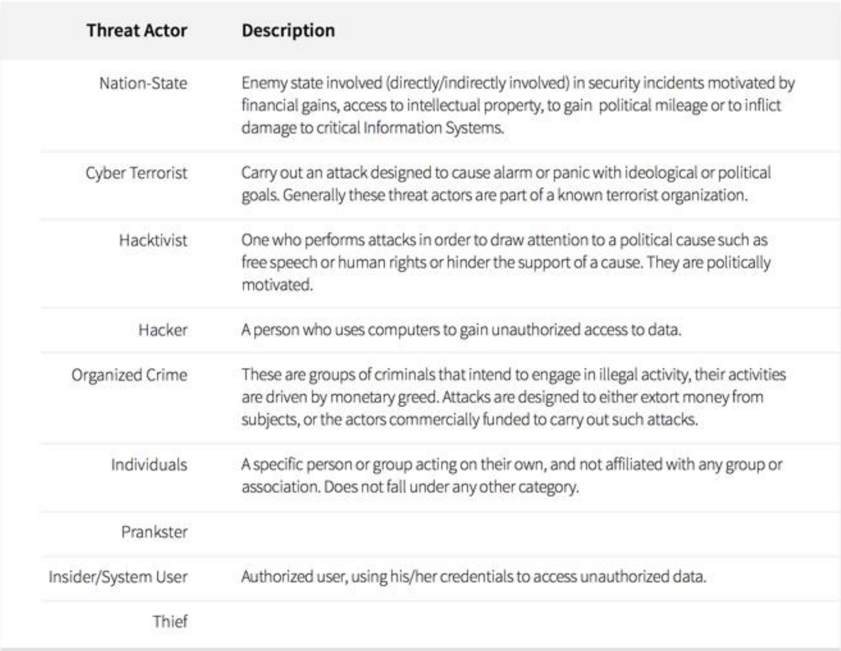

Estimated Internet Of Things Cybersecurity Market

Global compounded (2015-2020)

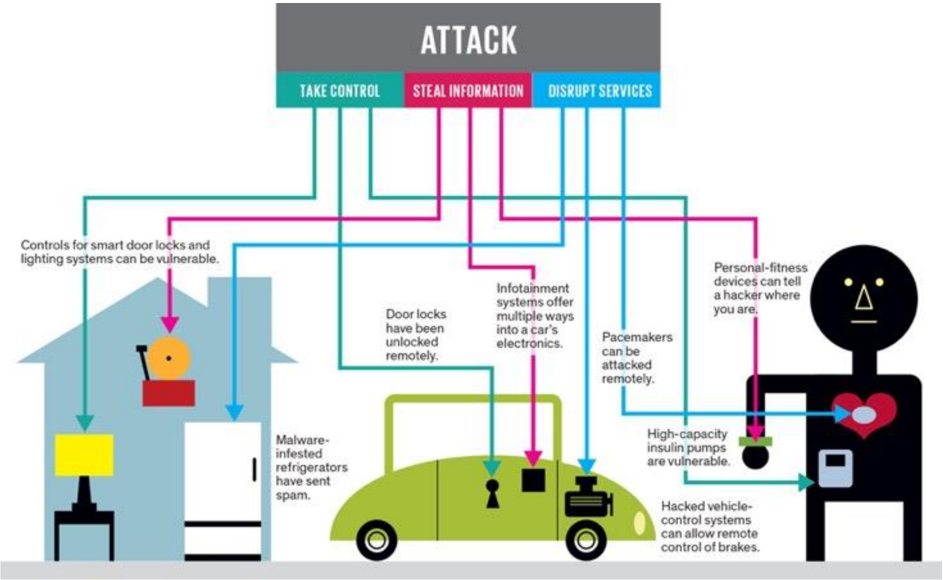
Security is both a barrier to widespread adoption…

… and a Growing Market in its own right.

IoT Security Threat Types



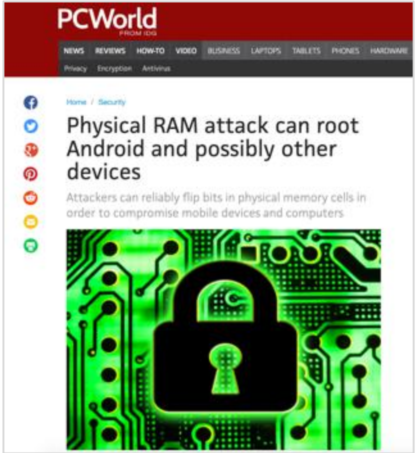
Threat Actor	Description
Nation-State	Enemy state involved (directly/indirectly involved) in security incidents motivated by financial gains, access to intellectual property, to gain political mileage or to inflict damage to critical Information Systems.
Cyber Terrorist	Carry out an attack designed to cause alarm or panic with ideological or political goals. Generally these threat actors are part of a known terrorist organization.
Hacktivist	One who performs attacks in order to draw attention to a political cause such as free speech or human rights or hinder the support of a cause. They are politically motivated.
Hacker	A person who uses computers to gain unauthorized access to data.
Organized Crime	These are groups of criminals that intend to engage in illegal activity, their activities are driven by monetary greed. Attacks are designed to either extort money from subjects, or the actors commercially funded to carry out such attacks.
Individuals	A specific person or group acting on their own, and not affiliated with any group or association. Does not fall under any other category.
Prankster	
Insider/System User	Authorized user, using his/her credentials to access unauthorized data.
Thief	



ATTACK
TAKE CONTROL
STEAL INFORMATION
DISRUPT SERVICES
Controls for smart door locks and lighting systems can be vulnerable.
Door locks have been unlocked remotely.
Infotainment systems offer multiple ways into a car's electronics.
Personal-fitness devices can tell a hacker where you are.
Pacemakers can be attacked remotely.
Malware-infested refrigerators have sent spam.
High-capacity insulin pumps are vulnerable.
Hacked vehicle-control systems can allow remote control of brakes.

IoT Security Threat Vectors

Device Level	Recent Issue	Relevant Companies
Silicon	Row hammer	intel ARTIK Infineon ARM

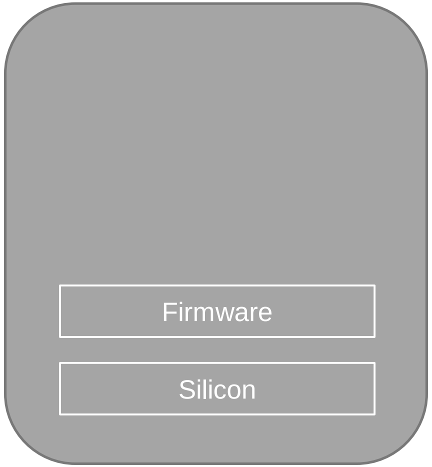


Physical RAM attack can root Android and possibly other devices

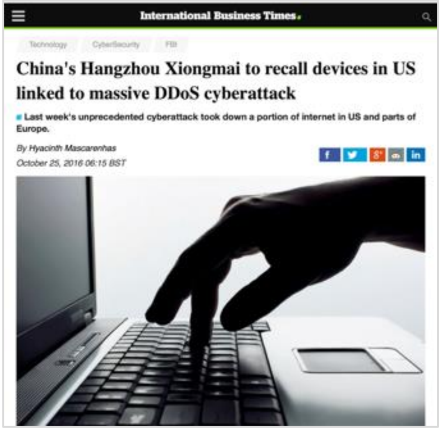
Attackers can reliably flip bits in physical memory cells in order to compromise mobile devices and computers

October 24th

IoT Security Threat Vectors



Device Level	Recent Issue	Relevant Companies
Firmware	Dyn DDoS	MOCANA escrypt Embedded Security
Silicon	Row hammer	intel ARTIK Infineon ARM



International Business Times

China's Hangzhou Xiongmai to recall devices in US linked to massive DDoS cyberattack

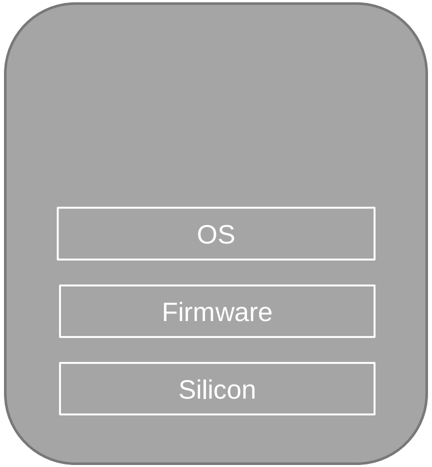
Last week's unprecedented cyberattack took down a portion of internet in US and parts of Europe.

By Hyacinth Mascarenhas

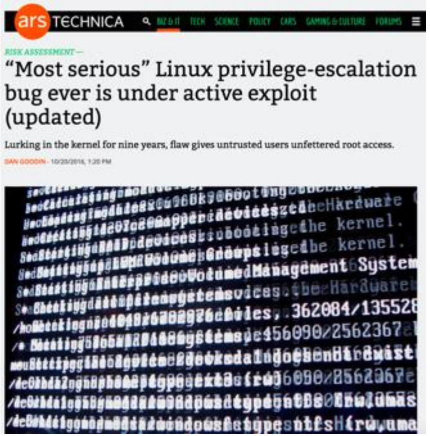
October 25, 2016 06:15 BST

October 24th

IoT Security Threat Vectors



Device Level	Recent Issue	Relevant Companies
OS	Linux kernel	gemalto WIND RIVER Symantec LYNX SOFTWARE TECHNOLOGIES
Firmware	Dyn DDoS	MOCANA escrypt Embedded Security
Silicon	Row hammer	intel ARTIK infineon ARM



RISK ASSESSMENT —

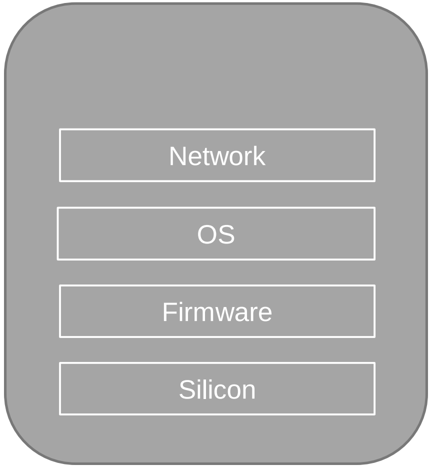
"Most serious" Linux privilege-escalation bug ever is under active exploit (updated)

Lurking in the kernel for nine years, flaw gives untrusted users unfettered root access.

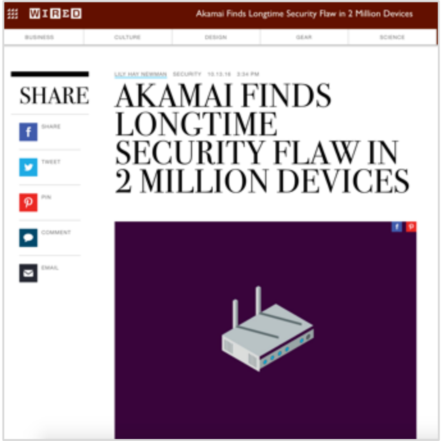
DAN GOODIN - 10/20/2016, 1:20 PM

October 20th
"Dirty Cow"
(race condition)

IoT Security Threat Vectors



Device Level	Recent Issue	Relevant Companies
Network	SSHowDowN	CENTRI, digicert, SECURE RF, Rubicon
OS	Linux kernel	gemalto, WIND RIVER, Symantec, LYNX SOFTWARE
Firmware	Dyn DDoS	MOCANA, escrypt
Silicon	Row hammer	intel, ARTIK, infineon, ARM



WIRED — Akamai Finds Longtime Security Flaw in 2 Million Devices

BUSINESS CULTURE DESIGN GEAR SCIENCE

LILY HAY NEWMAN SECURITY 10.13.16 3:34 PM

SHARE

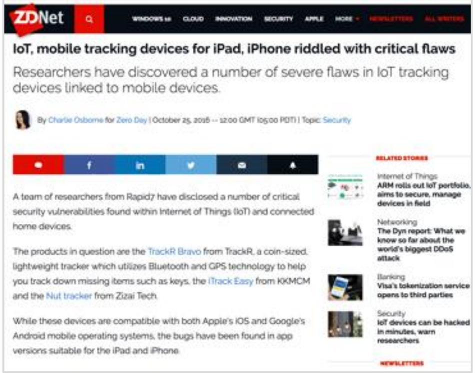
SHARE TWEET PIN COMMENT EMAIL

AKAMAI FINDS LONGTIME SECURITY FLAW IN 2 MILLION DEVICES

October 13th

IoT Security Threat Vectors

Device Level	Recent Issue	Relevant Companies
Application	Exposed Credentials	PRAETORIAN inside SECURE
Network	SSHowDowN	CENTRI digicert SECURERF Securing the Internet of Things Rubicon
OS	Linux kernel	gemalto security to be free WIND RIVER Symantec LYNX SOFTWARE TECHNOLOGIES
Firmware	Dyn DDoS	MOCANA escrypt Embedded Security
Silicon	Row hammer	intel ARTIK Infineon ARM



IoT, mobile tracking devices for iPad, iPhone riddled with critical flaws

Researchers have discovered a number of severe flaws in IoT tracking devices linked to mobile devices.

By Charlie Osborne for Zero Day | October 25, 2016 -- 12:00 GMT (05:00 PDT) | Topic: Security

A team of researchers from Rapid7 have disclosed a number of critical security vulnerabilities found within Internet of Things (IoT) and connected home devices.

The products in question are the TrackR Bravo from TrackR, a coin-sized, lightweight tracker which utilizes Bluetooth and GPS technology to help you track down missing items such as keys, the iTrack Easy from KKMCM and the Nut tracker from Zizai Tech.

While these devices are compatible with both Apple's iOS and Google's Android mobile operating systems, the bugs have been found in app versions suitable for the iPad and iPhone.

RELATED STORIES

Internet of Things
ARM rolls out IoT portfolio, aims to secure, manage devices in field

Networking
The Dyn report: What we know so far about the world's biggest DDoS attack

Banking
Visa's tokenization service opens to third parties

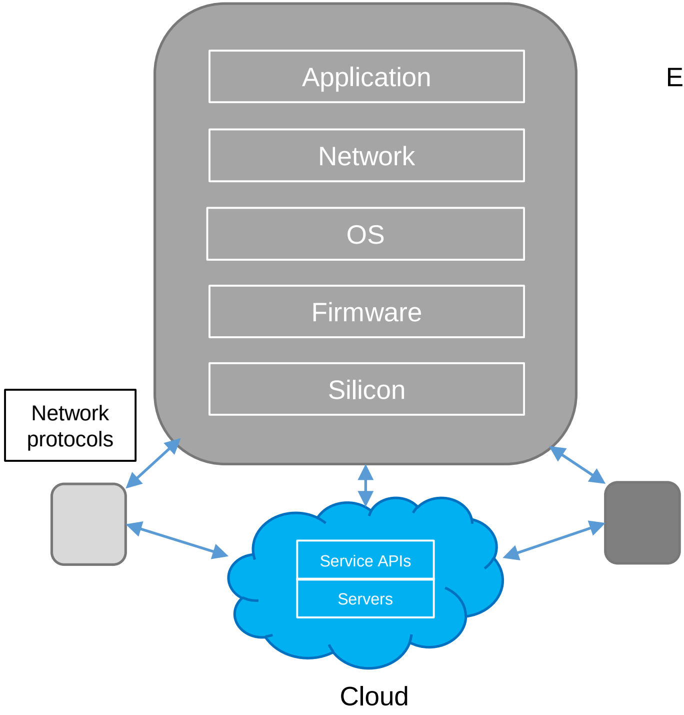
Security
IoT devices can be hacked in minutes, warn researchers

NEWSLETTERS

October 25th

IoT Security Threat Vectors

Device Level



Recent Issue

Exposed Credentials

SSHowDowN

Linux kernel

Dyn DDoS

Row hammer

Relevant Companies

PRAETORIAN inside SECURE

CENTRI digicert

SECURE RF Rubicon

gemalto WIND RIVER

Symantec LYNX SOFTWARE TECHNOLOGIES

MOCANA escrypt

intel ARTIK

Infineon ARM

Plus cloud integration, interoperation with multiple, heterogeneous devices

SHODAN DEVICE AUTHORITY

IBM Microsoft

ICON LABS TEMPERED NETWORKS

Security Approaches

Prevent

Harden hardware and software to eliminate weaknesses

Detect

Identify attacks, compromised applications / devices

Respond

Deal with compromised applications / devices, mitigate impact

- Most relevant for Makers: creators of IoT devices and services

- Prevention can be challenging for IoT
  - Resource constrained devices in large numbers
  - Devices may last order of magnitude longer (20-30 vs. 2-3 years)
  - Limited update capabilities

- Most relevant for Operators: purchasers of IoT devices and services

wurldtech A GE Company

CISCO

Resilient an IBM Company

SCADAfence

BAYSHORE

CyberX

SECURITHINGS

Indegy

NextNine Industrial Strength Cyber Security

CyberFlow ANALYTICS

Defense-in-Depth: IOT Security Strategy

Prevent

Harden hardware and software to eliminate weaknesses
(IOT Vendor-driven)

- Reduce attack surface
- Disable unneeded services
- Strip Operating Systems and Packages to bare minimum
- Apply Hardening techniques

Detect

Identify attacks, compromised applications / devices
(IOT Operator Driven)

- Leverage active device discovery
- Apply vulnerability scanning techniques frequently
- Leverage Network Intrusion Detection inline
- Apply Anomaly Detection
- Good alerting / scoring
- Visibility & Forensics capabilities
- Improve audit trail and configuration history / drift

Respond

Deal with compromised applications / devices, mitigate impact
(IOT Operator Driven)

- Patch/Remediate @ scale
- Micro-segment to allow only needed flows
- Manage @ scale & disable vulnerable services
- Have ability to selectively quarantine and isolate devices or endpoints

Regulate

Identify attacks, compromised applications / devices
(IOT Industry Driven)

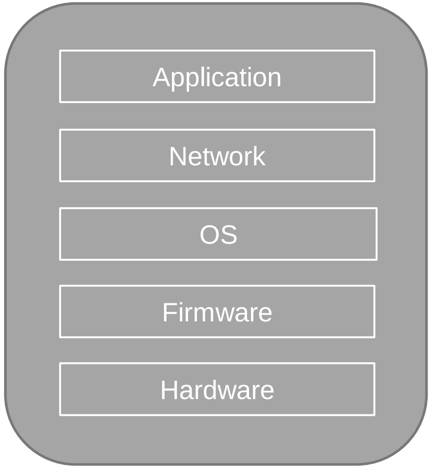
- Emulate existing regulations like PCI or HIPAA
- Have vendor compliance validation programs (like UL, FIPS, Common Criteria, NEBS
- Require mandatory vendor participation if present in critical infrastructure positions

NextNine Industrial Strength Cyber Security · CyberX · BAYSHORE · SCADAfence · SECURITHINGS · Indegy · Resilient an IBM Company · wurldtech A GE Company · CyberFlow ANALYTICS · CISCO

Challenge: Heterogeneity

Device Heterogeneity

X



Application

Network

OS

Firmware

Hardware

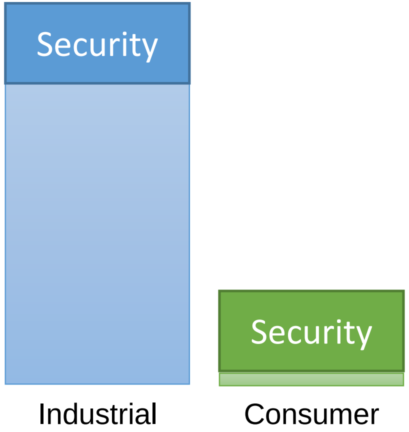
Component Heterogeneity

Security is only as strong as it’s weakest link; mixing many hardware and software components complicates security.

Challenge: Cost

Relative Impact

$50 for security on $2,000 of equipment: workable.



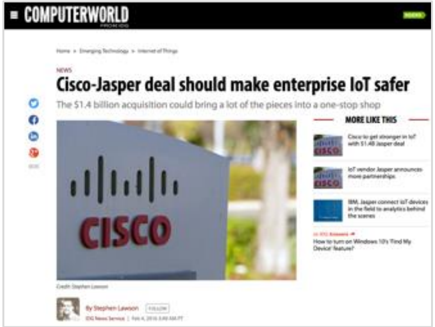
$50 for security on a $5 lightbulb: impractical.

Who bears the cost

	Short-term	Long-term
Consumer	Purchase	Failure
Manufacturer	Make	Liability
3rd Party		DDoS

Trends in IoT Security: Acquisitions

- Companies making acquisitions to increase coverage of the security stack
  - Driven in part by belief that single-provider systems are more secure than heterogeneous offerings
- Likely to pressure other large players to make similar acquisitions



COMPUTERWORLD

Home » Emerging Technology » Internet of Things

NEWS

Cisco-Jasper deal should make enterprise IoT safer

The $1.4 billion acquisition could bring a lot of the pieces into a one-stop shop

MORE LIKE THIS

Cisco to get stronger in IoT with $1.4B Jasper deal

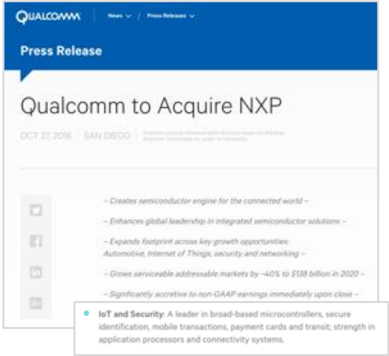
IoT vendor Jasper announces more partnerships

IBM, Jasper connect IoT devices in the field to analytics behind the scenes

How to turn on Windows 10's 'Find My Device' feature?

By Stephen Lawson

$1.4 billion



QUALCOMM News / Press Releases

Press Release

Qualcomm to Acquire NXP

OCT 27, 2016 | SAN DIEGO

– Creates semiconductor engine for the connected world –

– Enhances global leadership in integrated semiconductor solutions –

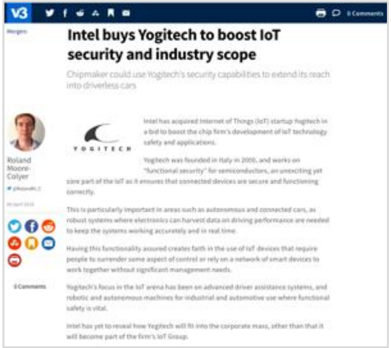
– Expands footprint across key growth opportunities: Automotive, Internet of Things, security and networking –

– Grows serviceable addressable markets by ~40% to $138 billion in 2020 –

– Significantly accretive to non-GAAP earnings immediately upon close –

- **IoT and Security**: A leader in broad-based microcontrollers, secure identification, mobile transactions, payment cards and transit; strength in application processors and connectivity systems.

$47 billion



V3 0 Comments

Mergers

Intel buys Yogitech to boost IoT security and industry scope

Chipmaker could use Yogitech's security capabilities to extend its reach into driverless cars

Roland Moore-Colyer

Intel has acquired Internet of Things (IoT) startup Yogitech in a bid to boost the chip firm's development of IoT technology safety and applications.

Yogitech was founded in Italy in 2000, and works on "functional security" for semiconductors, an unexciting yet core part of the IoT as it ensures that connected devices are secure and functioning correctly.

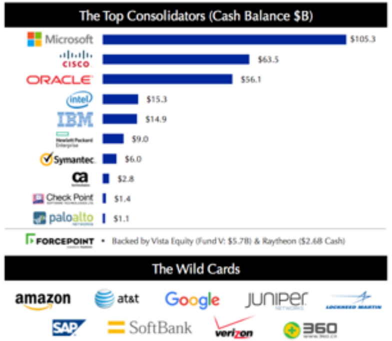
This is particularly important in areas such as autonomous and connected cars, as robust systems where electronics can harvest data on driving performance are needed to keep the systems working accurately and in real time.

Having this functionality assured creates faith in the use of IoT devices that require people to surrender some aspect of control or rely on a network of smart devices to work together without significant management needs.

Yogitech's focus in the IoT arena has been on advanced driver assistance systems, and robotic and autonomous machines for industrial and automotive use where functional safety is vital.

Intel has yet to reveal how Yogitech will fit into the corporate mass, other than that it will become part of the firm's IoT Group.

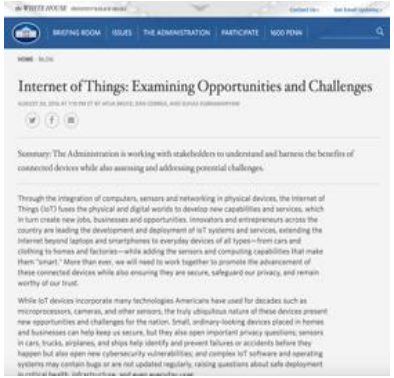
0 Comments



Source: Momentum Partners 2016

Trends in IoT Security: Regulation

- Regulations can shift costs from long-term & 3rd parties to short-term
  - "As part of the Administration's Cybersecurity National Action Plan released earlier this year, the Department of Homeland Security is collaborating with industry partners to develop a Cybersecurity Assurance Program to test and certify networked IoT devices"



Internet of Things: Examining Opportunities and Challenges

AUGUST 30, 2016 AT 7:10 PM ET BY ATUL BAGAI, DAN CORREA, AND SUHAS SUBRAMANYAM

Summary: The Administration is working with stakeholders to understand and harness the benefits of connected devices while also assessing and addressing potential challenges.

Through the integration of computers, sensors and networking in physical devices, the Internet of Things (IoT) fuses the physical and digital worlds to develop new capabilities and services, which in turn create new jobs, businesses and opportunities. Innovators and entrepreneurs across the country are leading the development and deployment of IoT systems and services, extending the Internet beyond laptops and smartphones to everyday devices of all types—from cars and clothing to homes and factories—while adding the sensors and computing capabilities that make them "smart." More than ever, we will need to work together to promote the advancement of these connected devices while also ensuring they are secure, safeguard our privacy, and remain worthy of our trust.

While IoT devices incorporate many technologies Americans have used for decades such as microprocessors, cameras, and other sensors, the truly ubiquitous nature of these devices present new opportunities and challenges for the nation. Small, ordinary-looking devices placed in homes and businesses can help keep us secure, but they also open important privacy questions; sensors in cars, trucks, airplanes, and ships help identify and prevent failures or accidents before they happen but also open new cybersecurity vulnerabilities; and complex IoT software and operating systems may contain bugs or are not updated regularly, raising questions about safe deployment in critical health, infrastructure, and even everyday uses.

August 30th

- Regulation would substantially impact demand
  - Certified secure components: hardware, firmware, operating systems, etc.
  - Security consulting across design, implementation, and testing
  - Certification services

PRAETORIAN

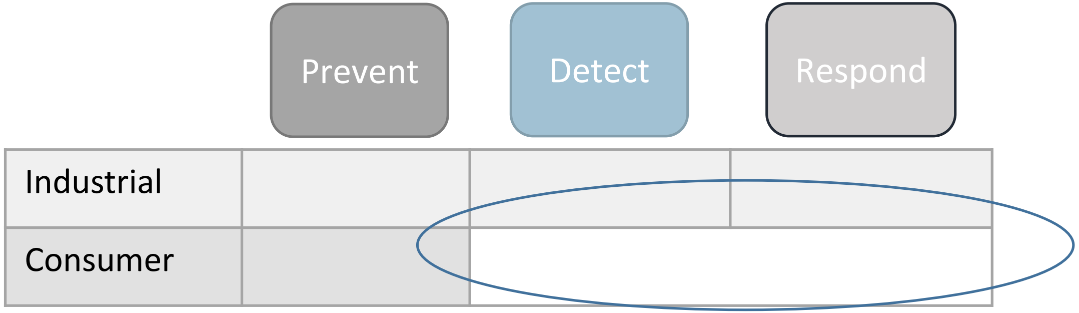
UL

wurldtech A GE Company

achilles

ICSA labs CERTIFIED

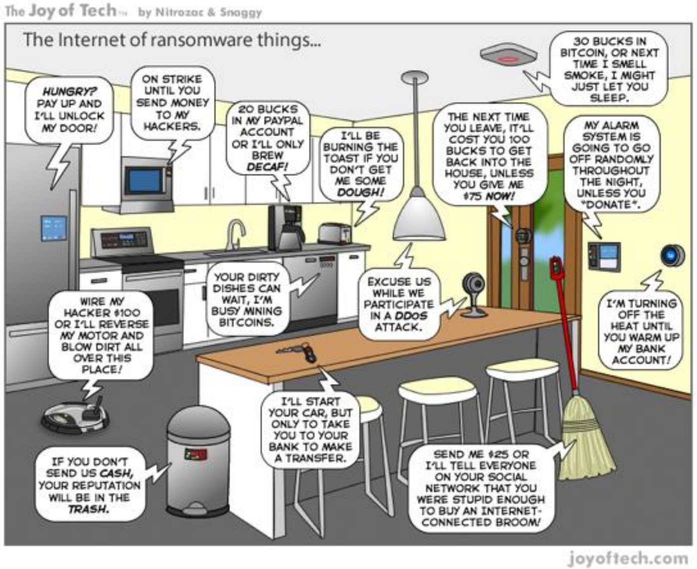
White Space in IoT Security



	Prevent	Detect	Respond
Industrial			
Consumer			

- Offerings must less expensive (and easier to use) than comparable industrial offerings
- Cost consciousness is a significant challenge
- Possibly bundle as part of a upgrade / maintenance / security service

IoT Security


The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
joyoftech.com

IoT's potential impact is in the $ trillions, but realizing that value requires addressing security.

- Acquisition by larger players
- Regulation may increase and shape demand
- White space around detection and response

ZingBox

DEVICE AUTHORITY
IoT Security Simplified

CyberX

PWNIE EXPRESS

ICON LABS
Device Security for the Internet of Things

SECURE RF

Bastille
SECURITY FOR THE INTERNET OF RADIOS

Trillium

BAYSHORE
INDUSTRIAL-STRENGTH CYBERSECURITY

Rubicon

THETARAY

ZITOVAULT

Karamba Security

Indegy

ARGUS
CYBER SECURITY

PFP
CYBERSECURITY

NEXDEFENSE

MOCANA