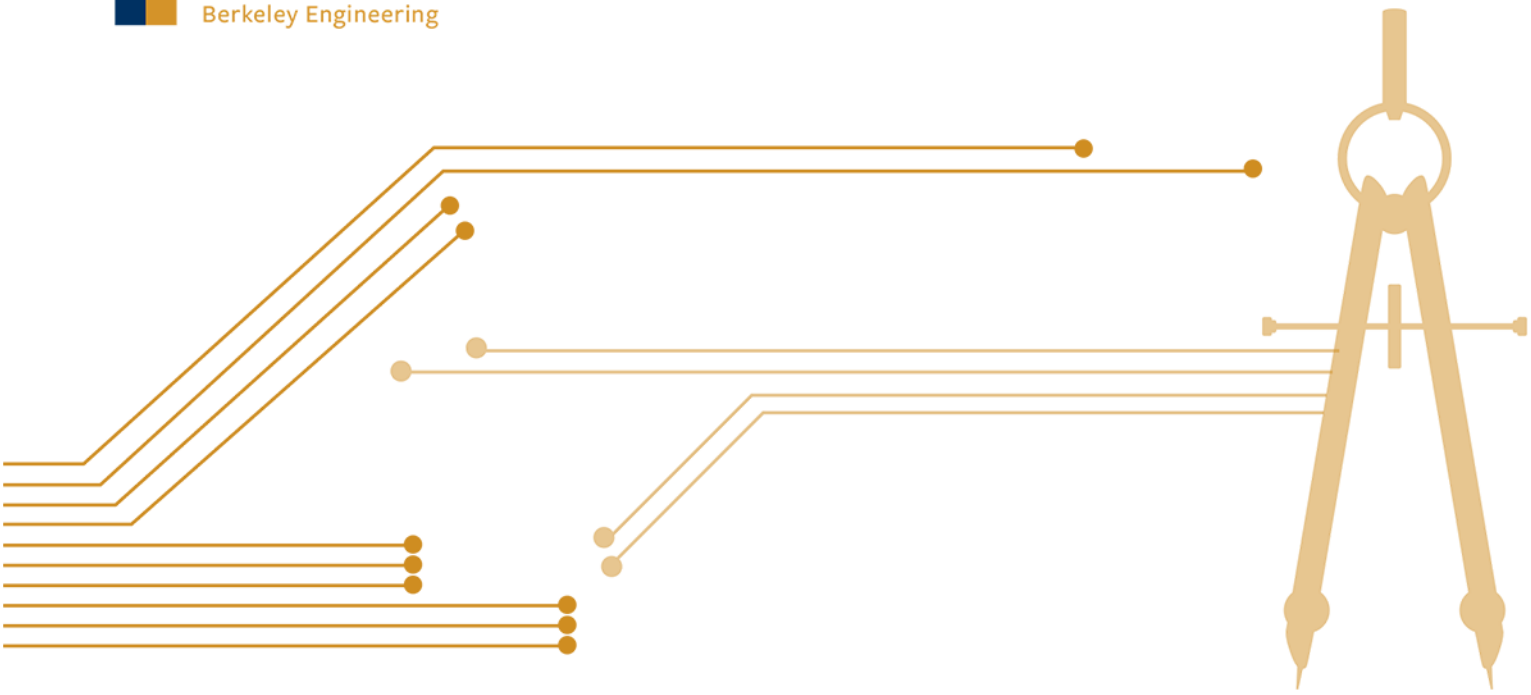
Pantas and Ting
Sutardja Center
for Entrepreneurship & Technology
Berkeley Engineering



2016 ELPP – IoT Security

- Vijay Kumar Eranti
- Serge Maskalik
- Jeffrey Pierce
- Dina McKinney
- Hima Devisetti
- Venkata Nandanavanam
- Geoffrey Perez

Berkeley
UNIVERSITY OF CALIFORNIA

Introduction

IoT has the potential to be one of the great new frontiers for innovation and technological growth. As the infrastructure and technology grow to support the possibilities of a connected world, we will soon see examples of IoT integrated throughout our daily lives. Where once electricity was new and still being understood, and is now taken for granted as ubiquitous and commonplace, IoT will become accepted as an integral part of how we work and live.

The IoT space is still in its infancy and the projected growth and impact of this this technology for businesses, consumers, and society is set to shake up the foundation of traditional institutions an industries.

Estimates for the impact of IoT on the global economy range from four to eleven trillion dollars in the next decade.

Our bottom-up analysis for the applications we size estimates that the IoT has a total potential economic impact of $3.9 trillion to $11.1 trillion a year by 2025. At the top end, that level of value—including the consumer surplus—would be equivalent to about 11 percent of the world economy. (James Manyika, 2015)

One of the fastest growing segments of the IoT space is security. With the enormous increase in available data and the possibility of misuse, security and privacy concerns are increasingly coming to the forefront of the IoT discussion. Proving solutions to address security problems will be a significant area of investment for businesses looking to reap the rewards of a connected world.

"The global IoT security products market was valued at US$ 7.8 Bn in 2014 and is expected to increase at a CAGR of 16.5% during the forecast period (2015 -2020). Enhancement in end-user experience and data security are the basic factors propelling growth of this market currently. ... Meanwhile, the software segment in the global IoT security products market was valued at US$ 3.9 Bn in 2014 and is anticipated to register a CAGR of 17.2% during the forecast period." (futuremarketinsights.com, 2015)

"The Internet of Things (IoT) security market is driven due to rising security concerns in the critical infrastructures and strict government regulations and is expected to grow from USD 7.90 Billion in 2016 to USD 36.95 Billion by 2021 at a Compound Annual Growth Rate (CAGR) of 36.1%. The year 2015 has been considered as the base year for the study, while the market size forecast is from 2016 to 2021." (marketsandmarkets.com, 2016)

Many of the same security issues exist with current Internet technologies. Businesses are keenly aware that security is an important component to the growth of this burgeoning space. There are opportunities to capitalize on the mounting concerns about security in the IoT space. The Internet of Things is poised to add trillions of dollars to the annual GDP in the next few years. However, realizing that potential impact requires addressing security, which is one of the primary barriers to adoption.

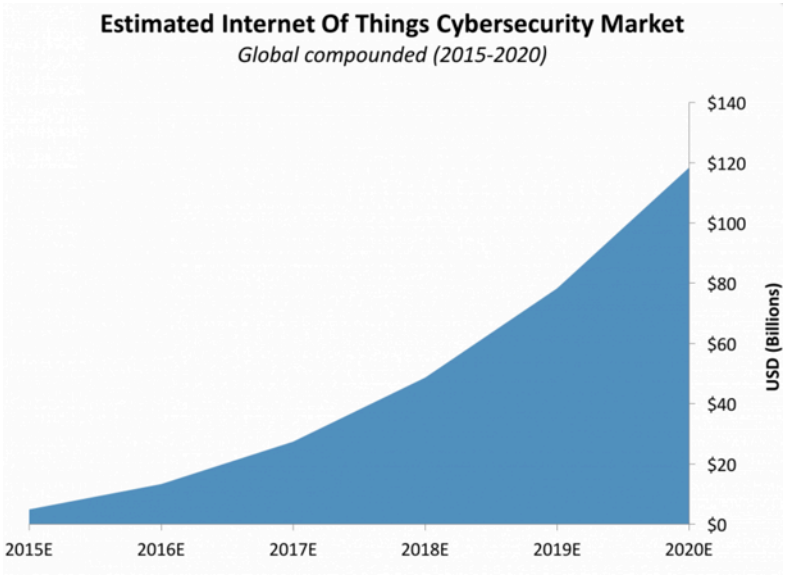


Figure 1: Estimated size of the IoT Security market (Source: Business Insider Intelligence Estimates 2015)

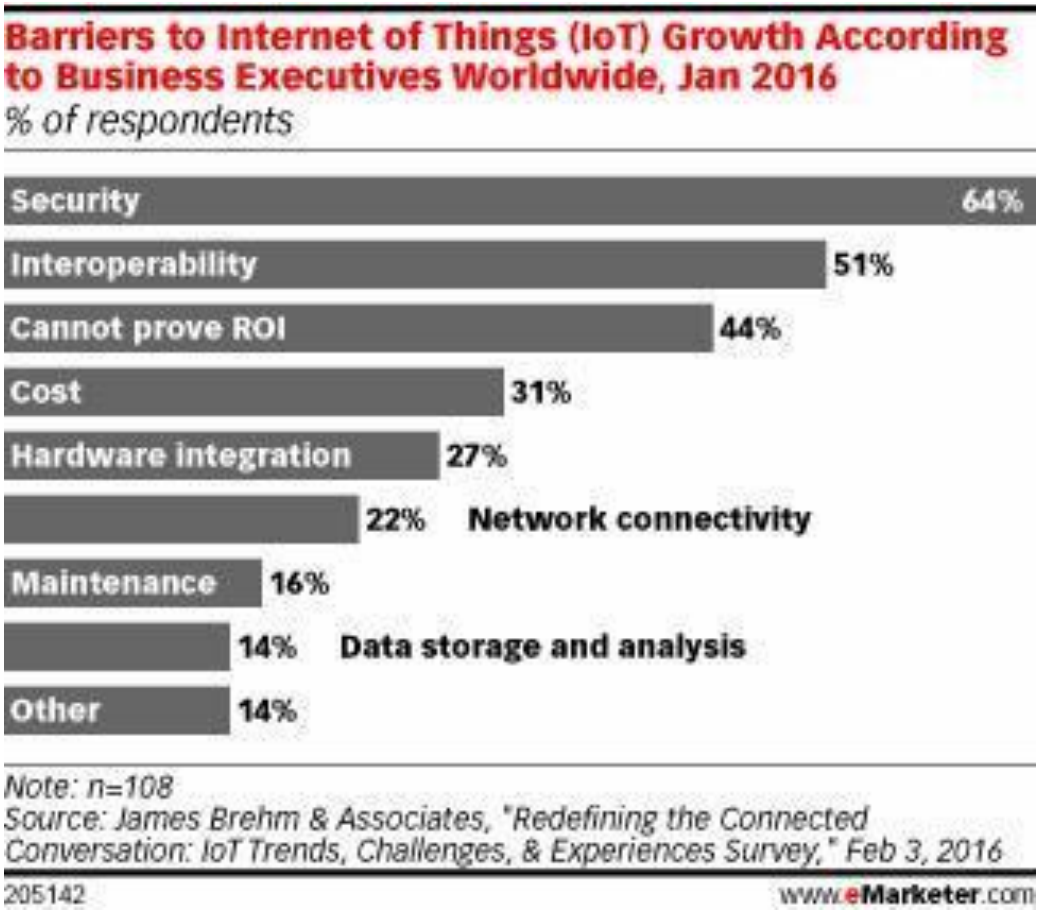


Figure 2: Business perception of IoT barriers

Looking at security as just a challenge to be overcome, however, is only part of the story: IoT security is a large potential business in its own right. If companies stand to gain trillions from IoT offerings, they are likely willing to pay billions to address security concerns. Last year Business Insider estimated that the IoT cybersecurity market could grow to $120 billion per year by 2020.

IoT Security Threat Types

IoT faces a variety of security threats with widely different capabilities. At one of the spectrum security threats include nation-states (who might attack a country's electrical grid it to cripple it in a war or electronic voting machines to influence an election…) who possess considerable resources, both personnel and material. On the other hand

are “script kiddies or other unskilled individuals who can re-use existing attacks but are unable to create their own exploits. Despite the variety of actors, most attacks have one of three basic goals: to take control of affected devices (for example, to unlock doors), to steal information (such as corporate secrets), or to disrupt services (such as your autonomous vehicle).

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	

Figure 3: IoT Threat Actors - Security Guidance for Early Adopters of the Internet of Things – April 2015

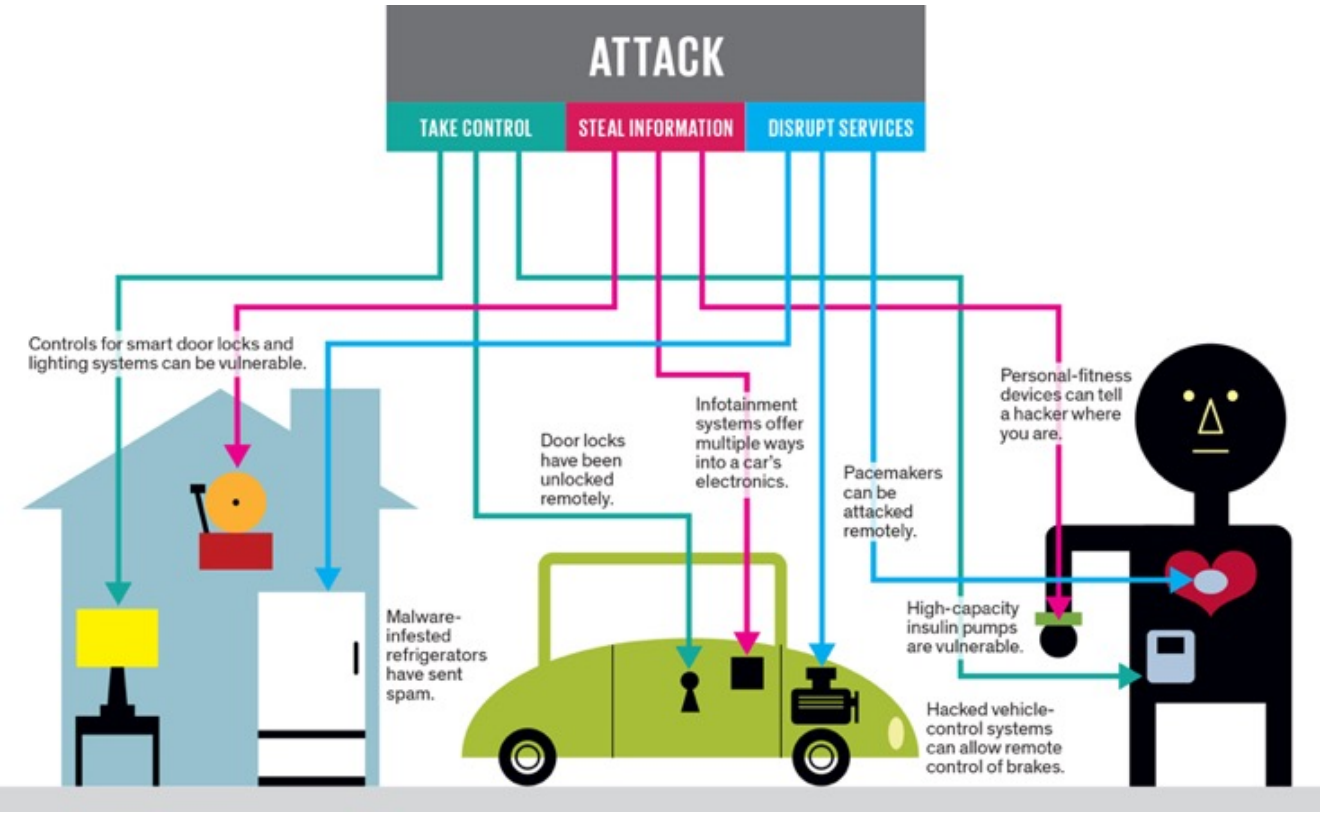


Figure 4: Types of IoT attacks

IoT Security Threat Vectors

To build a secure IoT offering, a company needs to start with the security of individual devices. And even a simple device has multiple levels that need to be secured.

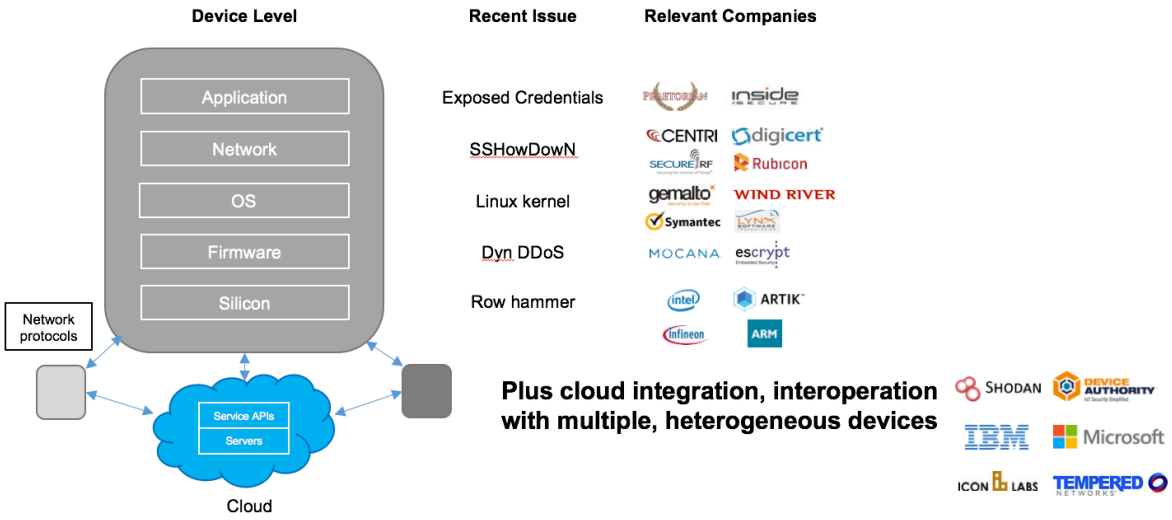


Figure 5: IoT components, issues, and relevant companies

Silicon

At the lowest level, securing a device requires securing its hardware components: its "silicon". A device cannot be secure if software on the device can manipulate the execution of arbitrary code on the device or access arbitrary data. But achieving that security is non-trivial, as can be observed by attacks such as the recent "Row hammer" attack, which allows arbitrary software to manipulate the contents of memory to achieve root access.

Figure 6: PCWorld Oct 24

While securing hardware is difficult, most of the core chip manufacturers (such as Intel, ARM, and Samsung) are now competing to distinguish themselves through secure hardware offerings.

Firmware

One level up from a device's hardware is its firmware, its lowest-level control software. Securing a device's firmware is critical, because unlike a device's operating system it is often impossible to update a device's firmware. Low cost providers that baked passwords into firmware were at the root of the recent DDos attack against Dyn.

Figure 7: IBT Oct 25

Companies like Mocana and Escrypt are trying to provide secure firmware as a component to IoT device makers.

Operating System

Figure 8: Ars Technica Oct 20

While operating systems tend to be easier to update than firmware, they're also a lot more complex. Many devices use Linux as a low-cost and powerful operating system, yet despite years of experience and its fundamental openness people are still identifying new security exploits for it. Dirty COW (*Dirty copy-on-write*) is a sample security vulnerability that affects all Linux-based operating systems, including Android. It is a local privilege escalation bug that exploits a race condition in the implementation of the copy-on-write mechanism. The bug has been lurking in the Linux kernel since 2007 and has been actively exploited at least since October 2016.

A number of companies, such as Gemalto, Intel's Wind River, and Lynx, provide secure operating systems to device makers. Others, such as Symantec, provide services that help monitor and secure operating systems provided by other entities.

Network

Figure 9: Wired Oct 13

In addition to computation, communication is the other core component of an IoT device. And the networking stack is a common source of security flaws, such as weaknesses in SSH implementations. SSHowDowN exploits vulnerability in OpenSSH that is 12 years old, and yet IoT devices still ship with the flaw unpatched.

Companies like Centri, SecureRF, and Rubicon offer secure network stack implementations, while other companies such as DigiCert offer digital certificate solutions that address endpoint authentication.

Application

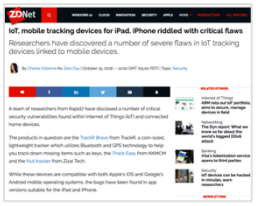


Figure 10: ZDNet Oct 25

Even if a device's own hardware and software is secure, the particular application or applications that run on that device may introduce their own security flaws. Common

flaws arise from applications storing data insecurely on a device or failing to properly secure and authenticate network connections.

Securing applications is difficult because each application is different, but companies like Praetorian and Inside Secure provide consulting, design, and analysis services to help makers build secure applications.

Cloud + Multiple, Heterogeneous Devices
Of course, in the Internet of Things, securing a single device is insufficient. Devices communicate with each other and with the cloud, meaning that IoT providers also need to worry about the security of network protocols and devices, their cloud infrastructure, and their cloud APIs.

In addition to established companies like IBM and Microsoft, start-ups like Icon Labs and Tempered Networks provide offerings that help companies secure their cloud components and manage their device collections.

Further research: https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf

Security Approaches
Securing devices and their communication with other devices and services focuses on preventing security issues, but it's only one part of how companies need to approach securing the Internet of Things. Prevention largely focuses on companies creating IoT devices and services. However, prevention can be challenging: the devices involved are often resource constrained so that they can't handle complex security solutions, they often need to last an order of magnitude longer than traditional computing devices (for example, 20 years instead of 2 years), and updating them with new software is difficult, if not impossible.

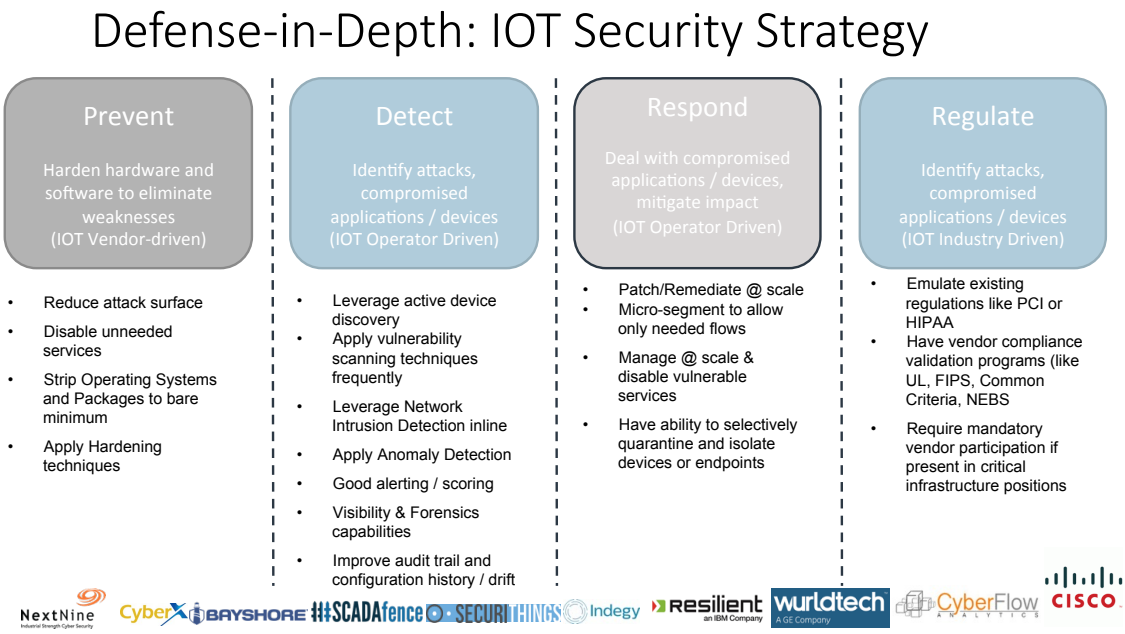


Figure 11: Approaches to IoT security include Prevention, Detection, and Responding

To address these limitations, companies also focus on detecting attacks or compromised devices and responding appropriately. Numerous IT and IoT companies, both bigger players like GE, Wurldtech, and Cisco and smaller start-ups like Indegy and CyberFlow Analytics, offer solutions to IoT operators (those that purchase, assemble, and operate an IoT installation) that allow them to monitor the operation of their IoT installations and detect potential issues. Other companies, like Resilient Systems, CyberX, and NextNine, offer solutions that help operators respond to detected issues and handle compromised devices.

Defense in Depth

There a number of analogies to be drawn from what has happened in the datacenter/IT space in the context of addressing the attack vectors that are prominent in the IOT space now – technologies at various levels already exist to address majority of the issues. Vendors can significantly improve the security posture of the solutions by hardening their applications and operating systems, removing and shutting down the unnecessary services, applying security scanning and penetration

testing in their quality assurance cycles, and leverage 3rd party security assessment vendors to close gaps prior to shipment of new devices.

Industrial and consumer customers of IOT can benefit from detection capabilities available in IT space today if applied against IOT area. Examples would be discovery-based inventory solutions with scanning to determine security patching levels and vulnerability state of the devices. Inline network-based anomaly-detection and intrusion prevention techniques can be applied to wired/wireless networks aggregating IOT and centralized alerting/monitoring and configuration audit trail mechanisms can be applied to increase visibility of the IOT implementations to further decrease awareness of potential issues and decrease the remediation times for security events.

From response and remediation perspective, having central management delivered as SaaS for industrial IOT solutions is a possibility, but not likely in the heterogeneous consumer environments. In enterprise space, mass-patching solutions exists to provide comprehensive distribution and installation of security fixes – this can be applied to IOT at scale to insure latest fixes are deployed to devices rapidly and timely.

It would also be interesting to do a further study across vendors and devices to see if a positive security model can be applied where only the needed communication flows are allowed in the IOT wired/wireless networks and the rest of the unneeded communications paths are micro-segmented and turned off by default. In homogenous stacks, this would be a possibility.

Further research: https://inform.tmforum.org/sponsored-feature/2014/09/defense-depth-breadth-securing-internet-things/

Business Landscape

The Internet of Things is comprised of a wildly diverse range of device types- from small to large, from simple to complex – from consumer gadgets to sophisticated systems found in DoD, utility and industrial/manufacturing systems. Now part of the expanding web connected network – Internet of Things, embedded devices are very different from standard PCs or other consumer devices. These

industrial operational assets are commonly fixed function devices designed specifically to perform a specialized task. Many of them use a specialized operating system such as VxWorks, MQX or INTEGRITY, or a stripped down version of Linux. Installing new software on the system in the field either requires a specialized upgrade process or is simply not supported. In most cases, these devices are optimized to minimize processing cycles and memory usage and do not have extra processing resources available to support traditional security mechanisms.
As a result, standard PC security solutions won't solve the challenges of embedded devices. In fact, given the specialized nature of embedded systems, PC security solutions won't even run on most embedded devices. There are many companies that are working on providing security in IoT landscape. Some of the companies include:

- Azeti Networks AG
- Intel
- Sypris
- ZingBox
- Shodan
- **Certified Security Solutions** : Enterprise digital identity
  Certified Security Solutions (CSS) (https://www.css-security.com/) is a cyber security company that builds and supports platforms to enable secure commerce for global businesses connected to the Internet. CMS enterprise certificate lifecycle management and VerdeTTo™ IoT identity security platforms simplify the design, deployment, monitoring and management of trusted digital identities, making authentication scalable, flexible and affordable.

- **Symantec**:
  Symantec (https://www.symantec.com/) expands security portfolio with new Embedded Critical System Protection, designed to defend IoT devices against zero-day attacks, and signs ATM manufacturer Wincor Nixdorf as one of the early adopters. To further fuel innovation in IoT security, Symantec recently announced a partnership with Frost Data Capital to incubate early-stage startups with funding, resources and expertise. Frost Data Capital underpins the incubator with seasoned

entrepreneurs, proven innovation methodology and process, and deep expertise in big data analytics, IoT, industrials and healthcare. These startup companies will have the opportunity to collaborate with Symantec to solve the most complex challenges shaping tomorrow's threat landscape.

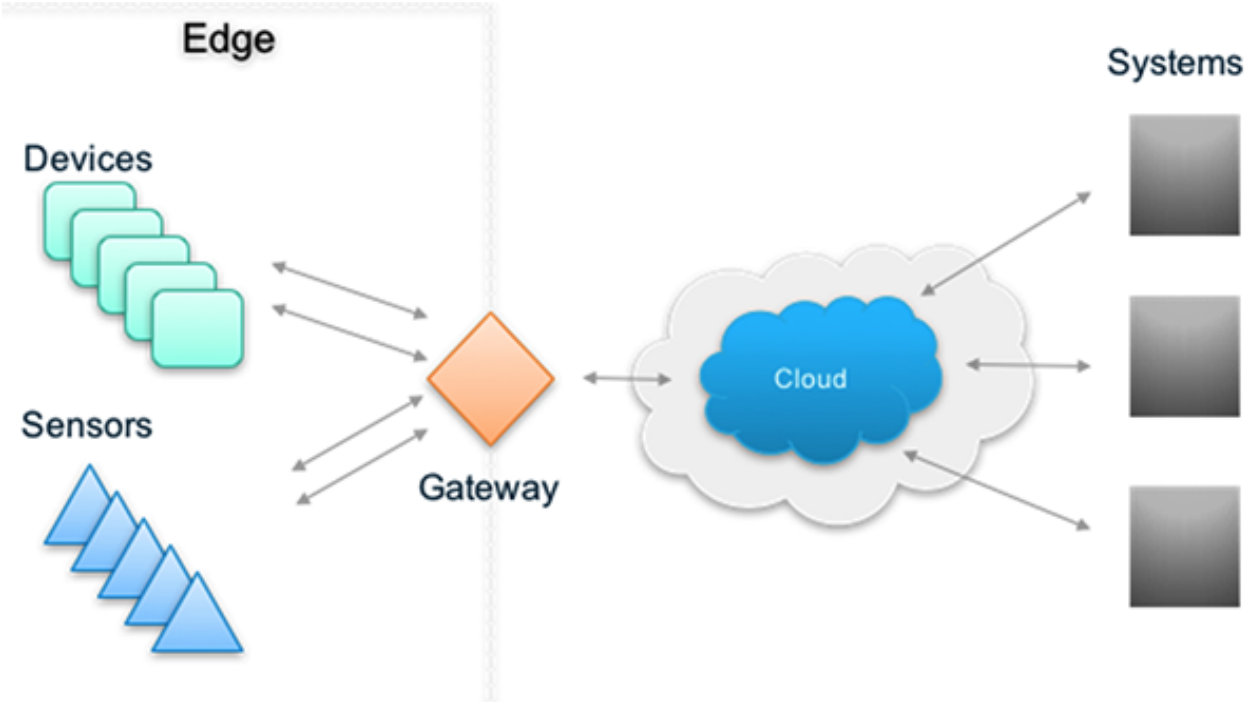
- **SecureThings**:
  SecuriThings (http://securithings.com/) is a User and Entity Behavioral Analytics (UEBA) solution for IoT. It monitors users and the IoT devices themselves. It uses machine learning security algorithms adapted for IoT to identify and mitigate threats. And it's simple to add to any IoT application, because it's pre-integrated with leading IoT platforms.

- **Device Authority**: Security Automation for Internet of Things
  Device Authority (http://www.deviceauthority.com/) provides simple, innovative solutions to address the challenges of securing the Internet of Things (IoT). IoT brings new security challenges introduced by the scale and pace of adoption, as well as the physical consequences of compromised security. These challenges cannot be effectively addressed by traditional Information Technology (IT) security solutions. The Device Authority IoT security platform is purpose-built to address these challenges through automated device provisioning, credential management, secure updates and policy-driven data encryption. The IoT promises countless efficiencies, increased competitiveness, improved customer service and even brand new market opportunities. However, deploying strong security is hard and always has been. Deploying strong IoT security is even harder. According to Gartner, by 2020, around 25% of all identified security breaches will involve IoT. To address this, Device Authority introduces a new paradigm of IoT Security Automation that accelerates and simplifies the deployment of strong IoT security. Advanced, policy driven security automation is critical for industrial, healthcare, transportation and other large scale security sensitive IoT environments. Their patented dynamic key technology provides the essential device-based trust anchor for IoT devices, enabling policy-driven provisioning,

access control and data protection for mission-critical IoT applications and services.

- **Bastille**: Security for the Internet of Radios
  Bastille (https://www.bastille.net/)is the first company to enable enterprise security teams to assess and mitigate the risk associated with the growing Internet of Radios. Bastille's software and security sensors bring visibility to devices emitting radio signals (Wi-Fi, cellular, wireless dongles and other IoT communications) in the installed organization's airspace. Bastille's technology scans the entire radio spectrum, identifying devices on frequencies from 60MHz to 6 GHz. This data is then gathered and stored, and mapped so that companies can understand what devices are transmitting data, and from where in their corporate airspace. This provides improved situational awareness of potential cyber threats and post-event forensic analysis.

Following are some of the companies that are working on providing security in IoT landscape at each of the following layers (shown in the picture below):



Company	Edge	Gateway	Application	Network	Datacenter /Cloud
ARM					
Cisco					
Dell					
Fujitsu					
Google					
Hitachi					
Intel					
Microsoft					
Nokia					
Oracle					
Siemens					

Startups

Company	Edge	Gateway	Application	Network	Datacenter /Cloud
Bastille					
Bayshore					
CyberX Labs					
Icon Labs					
Indegy					
Lynx Software Technologies					
NextNine					
Nozomi Networks					
Rubicon Labs					
SecureRF					
Tempered Networks					

Challenge: Heterogeneity

The types of security threats and the approaches to providing security are similar across IT and IoT, but securing IoT is significantly more complex. One reason is that IoT has to deal with significantly more heterogeneity. Not only do makers and operators need to address multiple levels of threats, they have to do it across a much wider variety of devices. And because security is only as strong as its weakest link, mixing multiple components and devices that may not have been explicitly designed to work with each other makes providing secure offerings much harder.

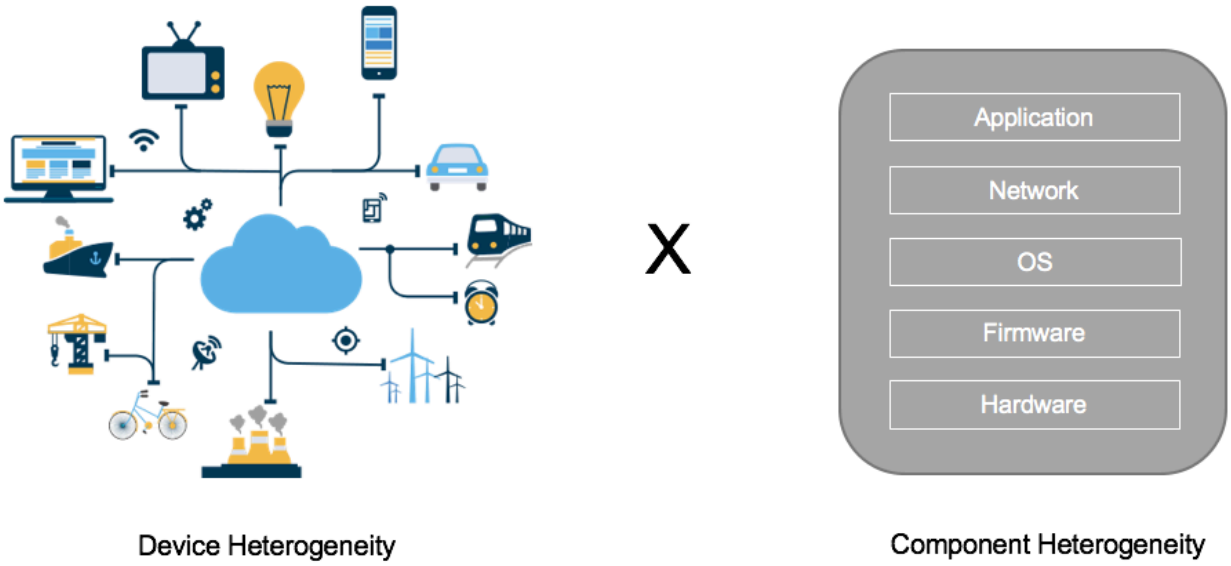
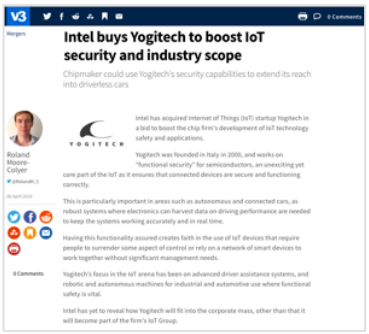


Figure 13: IoT heterogeneity is the combination of both device and component heterogeneity

Trends in IoT Security: Acquisitions

Examination of current offerings in the IoT security space and the ongoing challenges faced by IoT makers and operators, several trends are apparent. First, particularly in the industrial IoT, operators are looking for single-provider solutions that reduce the heterogeneity of installations and thus hopefully increase their security. In response, many of the large players (particular established IT security players) are acquiring smaller companies in order to increase their ability to provide "one stop shopping" IoT security solutions. Cisco's acquisition of Jasper, Intel's purchase of Yogitech, and Qualcomm's purchase of NXP are all in part intended to allow those companies to improve their IoT security offerings.

$1.4 billion acquisition



Undisclosed acquisition price

$47 billion acquisition

This consolidation is likely to increase, as other companies will feel the pressure to provide comparative offerings and will thus need to make acquisitions of their own. Larger players are also well positioned to make these acquisitions because of their larger cash balances, which allows them to consider both large and small companies as potential purchases.

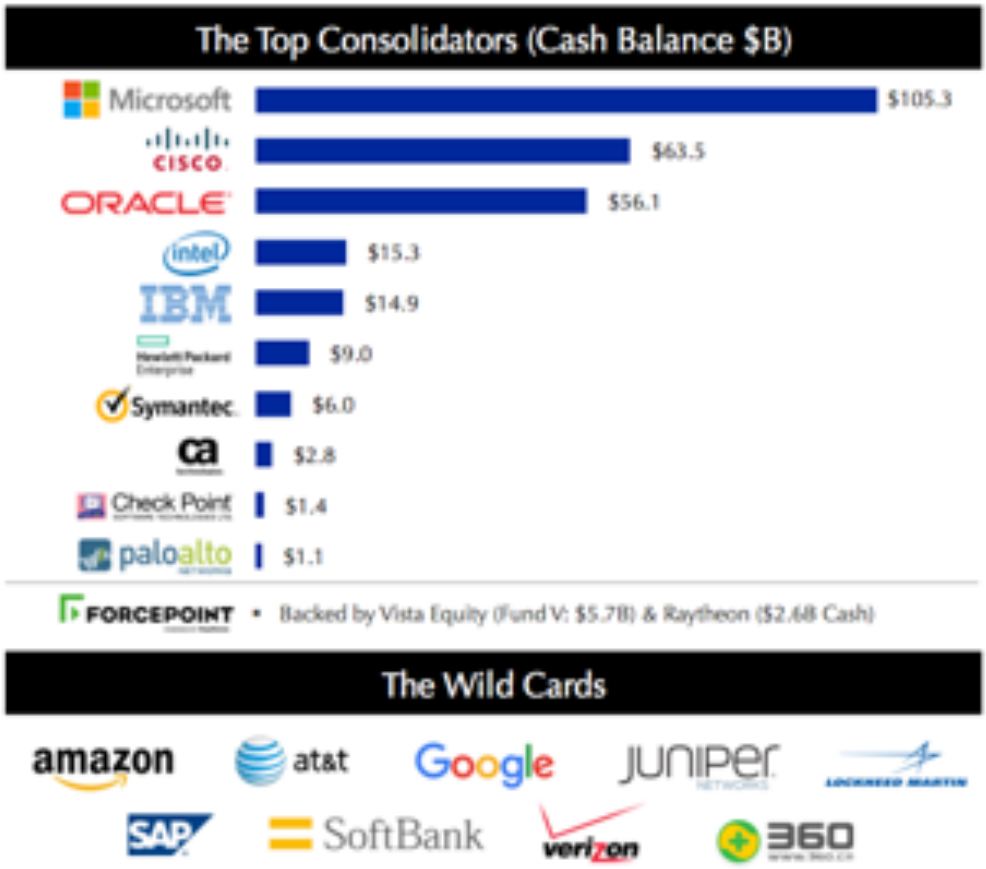


Figure 15: Cash balance of top consolidators (Source - Momentum Partners 2016)

Challenge: Cost

In addition, cost is much more of a consideration for IoT. Spending tens of dollars to secure a device that costs thousands of dollars may be acceptable, but spending that same amount of money to secure a light bulb, a light switch, or a door lock is clearly not. As a result, consumer IoT security tends to either ignored or provided as cheaply as possible.

Complicating the matter is that consumers typically consider just the short-term cost of IoT devices: their purchase cost. But the real cost of those devices may be their long-term cost when they fail: a $50 smart lock that can be easily hacked, allowing thieves to steal your valuables, will end up a lot more expensive than $50. And while manufacturers may focus on the short-term costs of manufacturing a device, IoT devices are more likely to fall under product liability laws than IT devices, leaving their creators subject to substantial lawsuits in the long

term. And both of those cases ignore the costs to 3rd parties, as in recent cases where hacked IoT devices have participated in DDoS attacks.

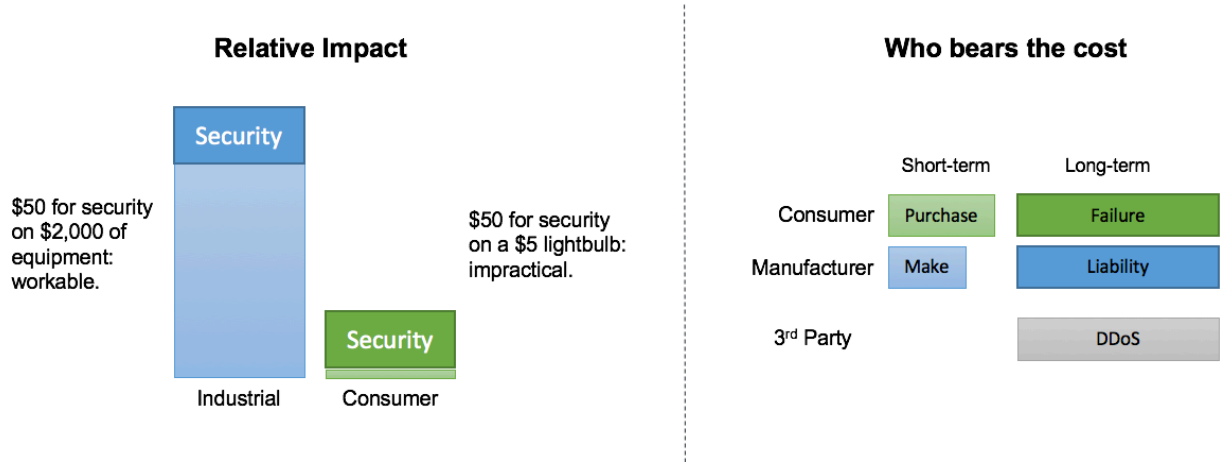


Figure 14: Relative impact of IoT costs and who bears that cost

Trends in IoT Security: Regulations

Regulation is one way to shift long-term cost considerations to the short-term, and there is already evidence of government movement in that direction. The Obama administration, as part of its Cyber security National Action Plan, has actively been working with industry to explore new certification standards. As an analogy, consider how some government regulations require Underwriters Laboratory certification for some electrical products in certain cases. There is a strong likelihood that the government will soon issue regulations that make similar requirements for IoT devices. The Underwriters Laboratory has been actively working with the government to create a Cyber security Assurance certification program for IoT providers.

If regulations do get instituted, they would have a significant impact on demand for different types of offerings. Components that already provide secure components would likely to see increased demand, while more companies will likely enter the space to provide consulting services to help IoT device makers design and implement secure devices. Praetorian is one company that already provides such consulting services and is well positioned to take advantage of increased demand. Existing certification companies such as UL, GE

wurldtech, and ICSA Labs are also ideally positioned to benefit from new security regulations.

Figure 16: Sample IoT companies likely impacted by potential regulation

White Space in IoT Security

Finally, we note that in the consumer space there is significant white space for security offerings that emphasize detecting and responding to security issues. This white space is driven both by the cost consciousness of the consumer space and the relative immaturity of consumer IoT offerings (at least as compared to industrial offerings). However, consumer IoT companies will eventually need to address these approaches, and companies that start to tackle this space early will likely have an advantage.

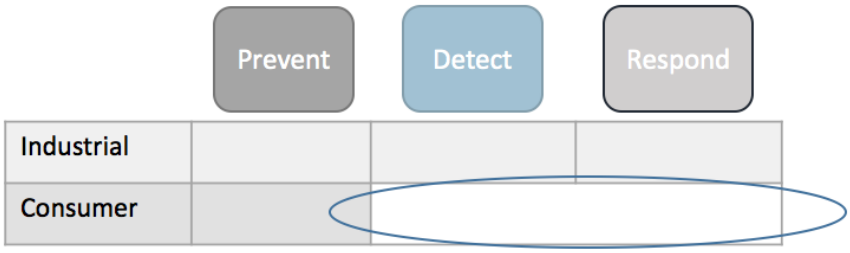
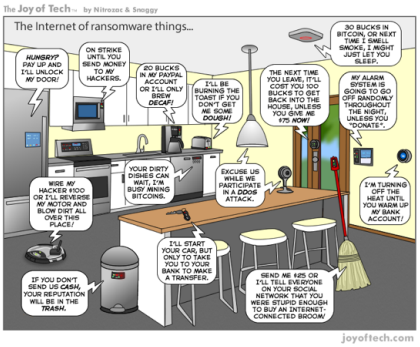


Figure 17: Detection and Response are white space for the Consumer IoT

Summary

The Internet of Things has the potential to have a multi-trillion dollar annual impact in the near future, but only if companies can effectively address security. And while security is a large and complex issue, there are observable trends that how the industry will evolve in the near-term.

IoT Security



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

Related reading:

1. The IOT: Mapping the value beyond the hype : McKinsey Global Institute Analysis
2. Vulnerable IoT devices are changing the cybersecurity landscape : Business Insider Intelligence
3. Security Is a Top Barrier to Internet of Things Growth : Emarketer.com Feb 2016

IOT Security Threat Types
1. Security Guidance for_Early_Adopters_of_the_ Internet_of_Things : Coud Security Alliance
2. Future proofing the connected world : Cloud Security Alliance
3. Security Challenges in the IoT Era – "Internet" & "Things" Coming Together : Equinox blog

Security Approaches
1. Volume-1-Practical- Handbook-and-Reference-Guide- for-the-Working-Cyber- Security-Professional.pdf : Cyberflow analytics and Cisco

IOT Startups/Mergers
1. IoT security M&A, Part 1: Startups tackle early IoT security challenges in key markets
2. 451 Research: IoT security M&A, Part 2
3. Cybersecurity_Market_ Review_Q2_2016