IoT Security: Part 2
November 20, 2016

M. R. Pamidi, Ph. D. Editor-in-Chief
Matt Pamidi Creator
IT Newswire

Executive Summary

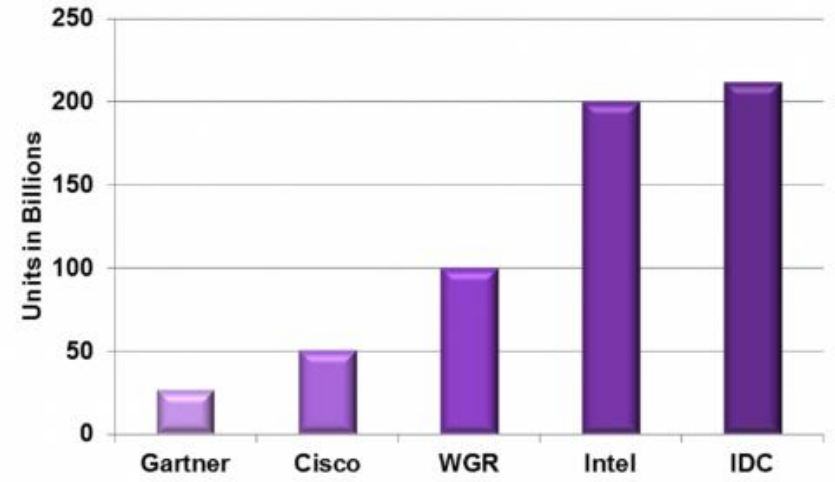
With the rapid growth of the Internet of Things and billions of devices expected to be interconnected worldwide over the next decade, security and privacy are increasingly at risk. This has (i) led traditional security hardware and software vendors to refresh their products to meet the scalability requirements in a highly heterogeneous environment of diverse devices, and (ii) given birth to a new kind of startups focusing exclusively on IoT security.

This report, a follow-on to an earlier report published this year, examines the IoT threat vectors, security market size, vendor landscape, and future trends.

1. Introduction

Because of its explosive growth, the IoT is becoming an increasingly attractive target for cybercriminals and hackers. More connected devices attract more attack vectors and more possibilities for hackers to target the innocent. Recent hackers' attacks, State-sponsored or individuals', on IoT devices by 'bot-herders' involving hundreds of thousands of Internet-connected devices like cameras, baby monitors, and home routers to launch massive DDoS attacks reflect IoT's fragility and are just the beginning of challenges that lie ahead for vendors. Unless the industry moves fast to address rising security concerns and stop overselling their products with little or no attention paid to security, we'll soon be facing inevitable, large-scale disasters. This is as a result of the sheer expected phenomenal growth of IoT devices over the next four years (Figure 1 and Table 1).

Figure 1. Forecasts for Connected Devices/Source Nodes in 2020[1]



[1] Device definitions vary by company

Table 1. IoT Devices Growth Forecast[2]

Year	2003	2010	2015	2020
World Population (billion)	6.3	6.8	7.2	7.8
Connected Devices (billion)	0.5	12.5	25	50
Connected Devices per Person	0.08	1.84	3.47	6.58

[2]Various sources

As we have noted before, unfortunately, many vendors have security as an add-on, afterthought feature, instead of building it from the ground up. Figure 2 illustrates major IoT security challenges.

Figure 2. IoT Security Challenges

2. IoT Security Basics

There are three basic categories of IoT applications:

- Mobile or desktop apps that control IoT devices
- IoT firmware and embedded apps
- Apps on open IoT platforms, e. g., apps built for Apple Watch.

There are four major threat areas:

- Improper or unsafe operation of devices
- Theft of confidential data, private user information, or application-related intellectual property
- Fraud and unauthorized access to payment processing channels
- Damage to your brand image and deterioration of customer, prospect, and partner trust.

Before attempting to find solutions to IoT security problems, with billions of devices active in this scenario, it behooves security vendors to answer some fundamental questions:

1. What is the connectivity model?
2. Who owns the device?
3. What is running on it?
4. Where is it located?
5. How is it protected?
6. How are attacks detected?
7. What is the recovery mechanism?

Traditional security solutions that addressed transition from closed networks to enterprise IT networks to the public Internet may no longer be adequate. Traditional enterprise IT had to deal with scalability and security issues with mostly known entities. In the world of IoT, these issues are magnified by orders of magnitudes—dealing with billions of devices from tens of thousands of unknown entities. As we become increasingly reliant on intelligent,

interconnected devices in every aspect of our lives, how do we protect potentially billions of them from intrusions and interference that could compromise personal privacy or threaten public safety?

Security is of paramount importance for the safe and reliable operation of IoT connected devices because it is the foundational enabler of IoT. But the question arises as to how best to implement security in IoT at the device, network, and system levels. Network firewalls and protocols manage the high-level traffic through the Internet, but how do we protect deeply embedded endpoint devices that usually have a very specific, defined mission with limited resources available to accomplish it? There seems to be a general consensus that some entirely new, revolutionary security solution will emerge that is uniquely tailored to IoT. But, our challenge is to compress 25+ years of security evolution into the tight timeframe in which next-generation devices will have to be delivered to market.

Unfortunately, there is no "silver bullet" that can effectively mitigate every possible cyber-threat. However, the tried-and-true IT security controls that have evolved over the past 25+ years can be just as effective for IoT—provided we can adapt them to the unique constraints of the embedded devices that will increasingly comprise networks of the future.

Bastille, an Atlanta, GA.-based startup, goes beyond IoT threats and lists Top 10 Internet of Radios (IoR) Vulnerabilities.

1. Rogue Cell Towers ('Stingrays', 'IMSI Catchers')
2. Rogue Wi-Fi Hotspots
3. Bluetooth Data Exfiltration (tethering)
4. Eavesdropping/Surveillance Devices (e. g. conference room bugs)
5. Vulnerable Wireless Peripherals (mice/keyboard)
6. Unapproved Cellular Device Presence
7. Unapproved Wireless Cameras
8. Vulnerable Wireless Building Controls
9. Unapproved IoT Emitters
10. Vulnerable Building Alarm Systems

After all, IoR is the combination of mobile, wireless, bring your own device (BYOD), and IoT devices operating within the radio frequency (RF) spectrum.

3. Cybersecurity Aspects

There are various aspects of cybersecurity, as listed below.

3.1 Behavioral Detection

Detecting abnormal behavior in organizations in order to identify threats and manage risks from cyber-attacks.

3.2 Cloud Security

Solutions for enterprises looking for secure application delivery across private, public, and hybrid clouds.

3.3 Continuous Network Visibility

Solutions for visualizing network activity and responding to cyber-attacks in real time.

3.4 Deception Security

Identify and proactively deceive and disrupt attackers before they can cause harm.

3.5 IoT/IIoT Security

Security for automobiles and industrial control systems used across critical infrastructures, including energy, water utilities, petrochemical plants, manufacturing facilities, etc.

3.6 Mobile Security

Enterprise mobile threat protection for Android and iOS devices.

3.7 Network and Endpoint Security

Protecting enterprise computer networks from vulnerabilities that arise as a result of remotely bridging users' laptops, tablets, and other electronic devices ("endpoints").

3.8 Quantum Encryption

Encrypted wireless and data communications technology that relies on the science underlying quantum mechanics.

3.9 Risk Remediation

Solutions for pinpointing vulnerabilities in technologies, people, and processes with recommendations on how to effectively fill security gaps.

3.10 Threat Intelligence

Targeted malicious activities on the deep Web to uncover potential threats and thwart attacks.

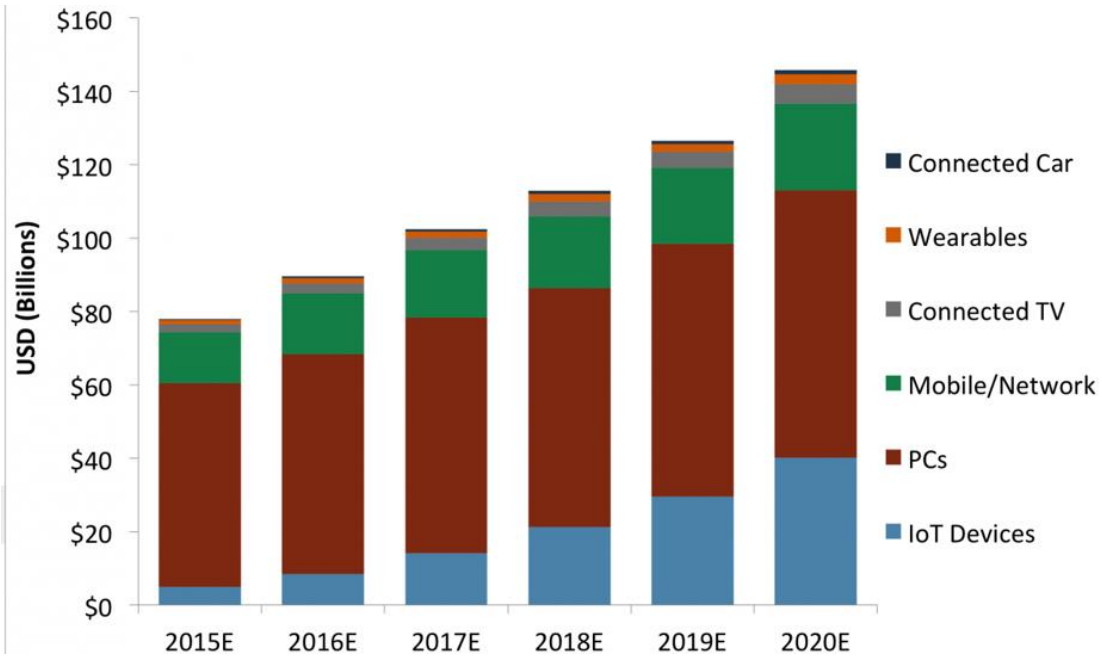
3.11 Website Security

Ability to identify and police malicious website traffic, including malicious bots, and more.

4. Market Scenario

The global IoT security market to grow from just under $5 billion in 2015 to almost $40 billion by 2020. Note, the global cybersecurity market, which includes IoT devices, is forecasted to show an equally robust growth, exceeding $140 billion (Figure 3).

Figure 3. Global Cybersecurity Market Forecast



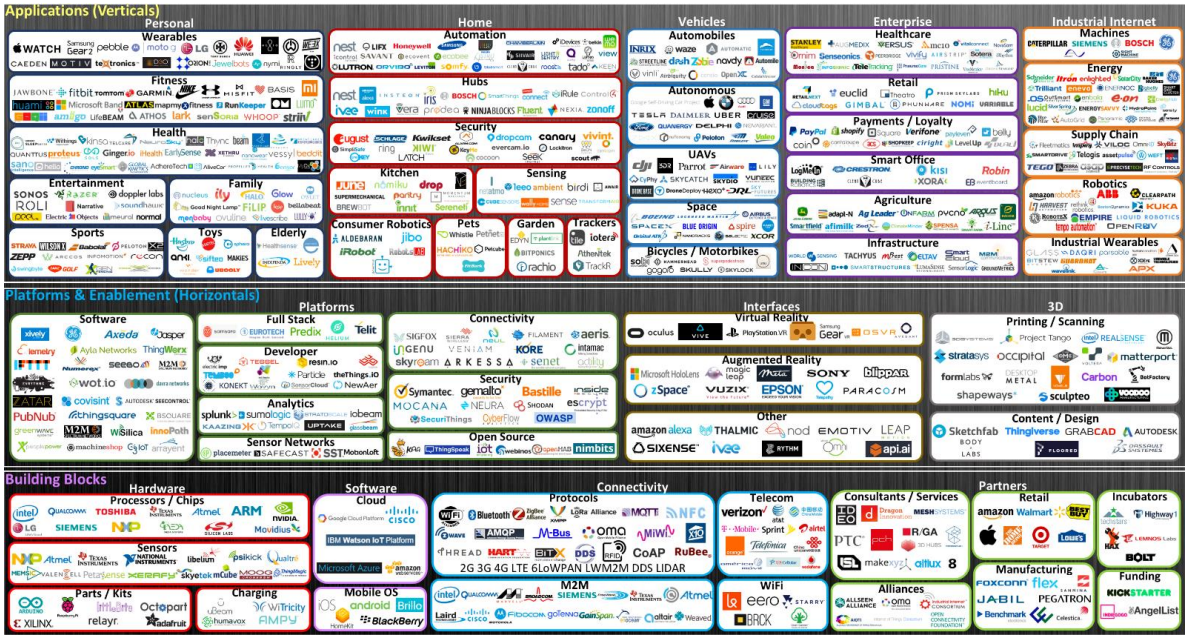
The major inhibitor to a more widespread adoption of IoT is security. Realizing the IoT-related and ancillary economy is expected to reach into the trillion of dollars by 2025, vendors—both established and startups—are investing heavily in improving hardware and software security and privacy in hardware, software, storage, network, and devices.

5. Vendor Landscape

Although the IoT vendor landscape is seeing new entrants every day, vendors offering IoT security still comprise a small number, but growing at a rapid rate. On one hand are traditional IT systems and security vendors—IBM,

Cisco, Intel/McAfee, RSA, Symantec, and Trend Micro—entering the IoT space; on the other are a new breed of startups specifically focused on IoT-related security issues. Figure 4 provides an IoT vendor landscape that includes security vendors. Table 2 provides a sample listing of the startups.

Figure 4. IoT Vendor Landscape 2016



Source: Matt Turck

Table 2. IoT Security Startups to Watch

	Company	Founded	Funding	Leadership	Details
1	Barkly, Boston	2013	$17 million in seed and Series A	Ex-BBN and IBM	A lightweight agent to gather data in the endpoint security space
2	Bastille, Atlanta	2014	$ million from Bessemer Venture Partners	Ex-End Game	Monitoring and analysis pf corporate airspace for IoT devices
3	Bitglass, San José	2013	$35 million from NEA, NVP, and SingTel	Ex-Cisco and Juniper	Safe storage of corporate data in the cloud with AES 256 encryption
4	FinalCode, San José	2014	Digital Arts	Ex-ForeScout	Complex key management in document encryption
5	Ionic Security, Atlanta	2011	KPCB, Meritech Capital, and Google Ventures	Ex-Network Associates and Symantec	Encryption and management of documents using symmetric key encryption
6	Menlo Security, Menlo Park	2013	$35.5 million through Series B from Sutter Hill Ventures, Genera Catalyst *et al.*	Ex-Juniper	Stripping malware from email and Web traffic
7	Niara, Sunnyvale	2013	$29.4 million from Index Ventures, NEA, and Venrock	Ex-Aruba, Juniper, and Netscreen	Analyzes security events and assigns them severity scores and issues alerts.

8	Red Canary, Denver	2014	$2.5 million in seed by Kyrus Tech	Ex-Kyrus	Provides consultants who sort through security alerts to eliminate false positives.
9	Soha Systems, Sunnyvale	2013	$9.76 million from Menlo Ventures, Andreessen Horowitz *et al*.	Ex- Cisco, MobileIron, Nortel, Riverbed	Cloud-based security services, including authentication, authorization, application firewalling, WAN optimization and server load balancing
10	Vera, Palo Alto	2014	$14 million from Battery Ventures	Ex-Cisco	Software imposes encryption on documents that follows them around until a legitimate recipient authenticates to release the decryption keys.

6. Vendor Implementations

As we have emphasized before, security must be built in from the beginning and not added as an afterthought. Some hardware systems vendors have realized this and are doing a decent job of either developing in-house software or acquiring the right companies and integrating them to deliver a complete package. Major chip vendors are also embedding security features at the hardware level, reducing latency and improving performance. The following sections delve into two examples.

6.1 Cisco

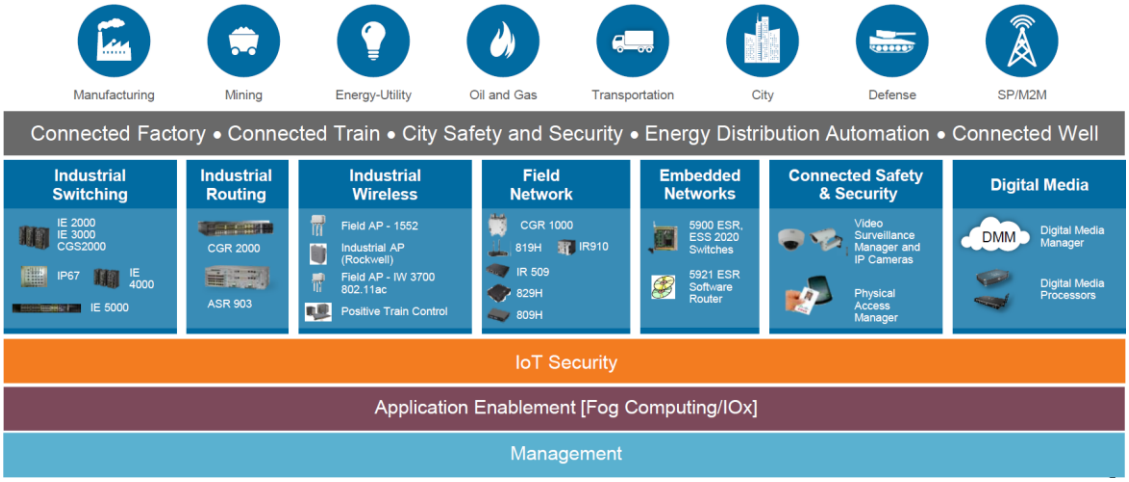
Among the hardware systems vendors, Cisco seems to have the most complete line of security products, although many of them had their pedigree in traditional IT, both in-house developed and obtained through acquisitions—OpenDNS, Neohapsis, Virtuata, Sourcefire, Cognitive Security, ThreatGrid, and CloudLock—to mention a few. This may be due to the fact that Cisco started out as a network products company and network security has always been in its genes.

Cisco's products cover every aspect of IoT security:

- Access Control and Policy
- Advanced Malware Protection
- Email Security
- Firewalls
- Network Security
- Network Security Behavioral Analytics
- Next Generation Intrusion Prevention System
- Security Management
- VPN and Endpoint Security Clients
- Web Security

As can be seen from Figure 5, Cisco addresses security from the ground up and not as an afterthought.

Figure 5. Cisco IoT Portfolio

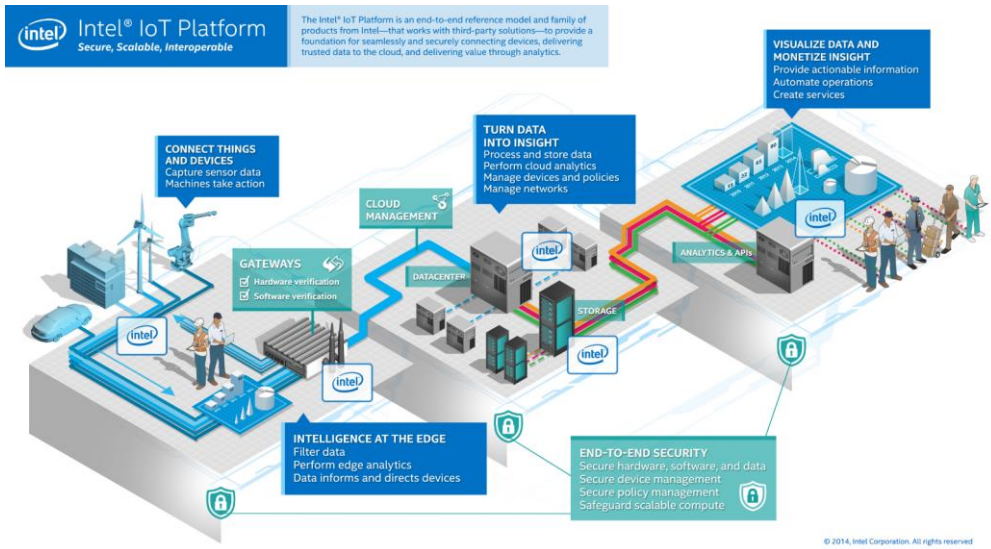


Source: Cisco

6.2 Intel

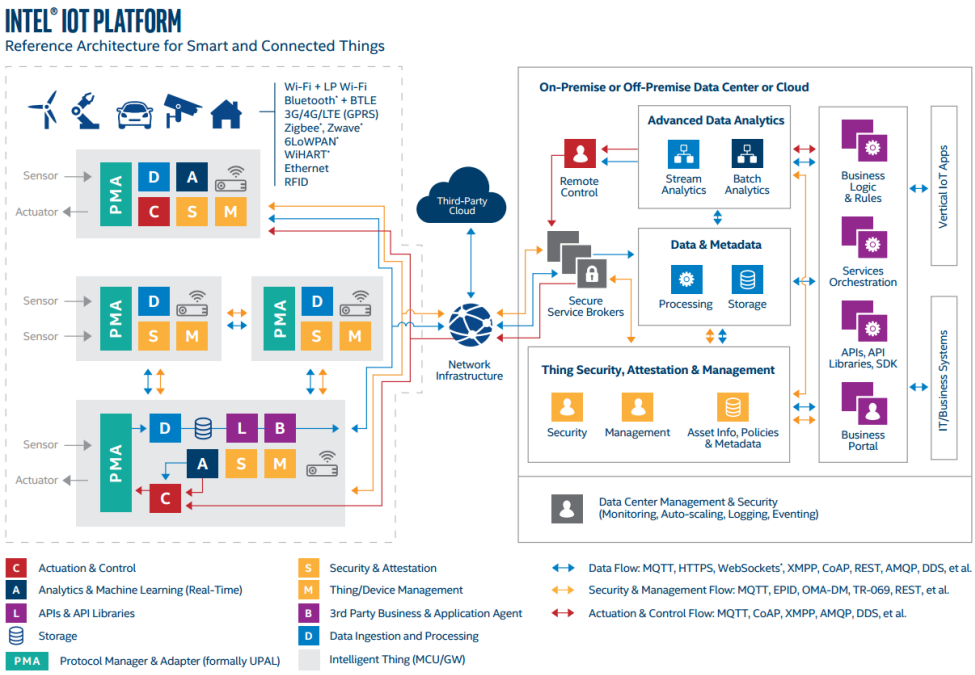
Not to be labeled as just a chip vendor, Intel has built a comprehensive IoT platform (Figures 6 and 7) addressing security based, *inter alia*, on McAfee and Wind River technologies with the goal to protect against attack, to detect compromises, and to remediate or correct after an attack, restoring normal operations. Note, security products are quite prevalent here.

Figure 6. Intel IoT Platform



Source: Intel

Figure 7. Intel IoT Platform Reference Architecture



Source: Intel

7. Conclusions

Traditionally, PCs were the prime targets by hackers to turn them into bots, as many people did not bother with installing anti-malware. But over the last few years, PCs became much more protected and laptops became the new targets. With the proliferation of billions of IoT devices, these are the obvious new targets. Will the IoT world be ever 100% safe and secure? No, but technology improves things:

- In 1921, automobile fatalities in the U. S. per 100 million were 24.09; in 2014 they were 1.08.
- In aviation, the 1970s saw 16,766 deaths; in the 2000s there were 8,318.

People still drive and fly. There *will* be more IoT hacks, some probably even serious; these may only slow down, but not stop, the IoT adoption momentum.

