IoT Security: An Oxymoron or a Tautology?

June 16, 2016

M. R. Pamidi, Ph. D.
Editor-in-Chief
and
Keith Brown
Managing Editor
IT Newswire

Executive Summary

With the explosive growth of the Internet of Things (IoT), digitally connected devices are intruding every aspect of our lives—bodies, cars, homes, and offices. But every IoT device is vulnerable to hackers and, with the increasing adoption of IPV6 and exponential growth of devices, expected to exceed 50 billion by 2020, the situation will only get worse. This paper discusses current state of the art in IoT security (or lack thereof) and delves into what the future might hold.

1. Introduction

There are tomes of material available on the IoT market growth forecast. *Forbes* has published a good compilation here and we don't intend to reproduce it here. Suffice it to say, IoT is improving our lives in many ways in being able to do things we could never do before. But every good thing has a downside: It 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. 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 an inevitable disaster.

Unfortunately, many vendors have security as an add-on, afterthought feature, instead of building it from the ground up. If IoT is a cake, security should be baked in like eggs, not schmeared on as icing. In fact, in July 2014 HP Labs did a study of 10 popular IoT devices and found that the security was shockingly bad. The researchers studied 10 devices, looking at the end-to-end security capabilities of these devices including privacy protection, authorization, encryption, user interface protection, and code security. They found that 70% of the devices had at least one major vulnerability! By the time they completed their study, the researchers identified over 250 vulnerabilities, an average of 25 security vulnerabilities per device. Security was clearly an afterthought – or worse – for these devices.

2. Recent Attacks

This section cites some recent attacks on numerous IoT devices, mostly to demonstrate how vulnerable these are, despite vendors' claims they were secure.

2.1 Baby Monitors

In the past few years, hackers have targeted baby monitors to scream at toddlers and to curse out their parents, turning them into spy cams. Last year, a hacker put live feeds from a thousand baby monitors onto a site titled, "Big Brother is Watching You." Hackers also took over Foscam, a Chinese-made camera, in a home, and published photos of their living room, kitchen, and bedrooms. Most of these hackers have no ill intentions, but just want to expose the vulnerabilities of these devices and the callous attitude of manufacturers towards privacy and security.

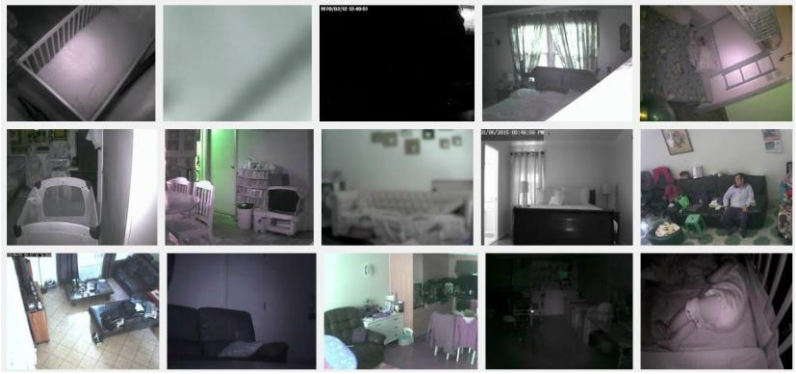

Figure 1. Images captured on the now-defunct Spycam site.

2.2 Automobiles

Last year, well-intentioned hackers targeted a Jeep Cherokee with software that let them send commands through the Jeep's entertainment system to its dashboard functions, steering, brakes, and transmission, from a laptop. Remotely controlling these functions, the hackers were able to send the Jeep to a ditch.

Figure 2. Jeep Cherokee in a ditch

2.3 Toilets

Trustwave, a security firm, hacked a Satis toilet, which is controlled via an Android app, demonstrating that the smart toilet can be easily taken over. The app's Bluetooth PIN was hard-coded to the not-very-secure "0000". "An attacker could simply download the 'My Satis' application and use it to cause the toilet to repeatedly flush, raising the water usage and therefore utility cost to its owner," Trustwave's researchers said. "Attackers could cause the unit to unexpectedly open/close the lid, activate bidet or air-dry functions, causing discomfort or distress to user," researchers warned. No s&*%!

2.4 Hotels

Hackers have also targeted hotel-reservation systems and, in many cases, checked out paying no bills. This is especially true in Black Hat and DefCon conferences held every year in Las Vegas where hackers are not evil-minded crooks, but just expose how vulnerable our IT systems are. In fact, an attendee from a Las Vegas casino (who shall remain anonymous) we chatted with at the IoT World said some of the Las Vegas casinos *invite* hackers to break into their wireless networks just to discover the weak spots in their IT infrastructure!

3. IoT Security: What's is being done?

This is a pretty serious topic because there are multiple threat vectors, but how are they being addressed?

3.1 The Skeptics

To say there are folks who are skeptical about IoT security is an understatement. The most common arguments extended by them are: There are/will be billions of IoT devices from tens of thousands of manufactures from around the world with a multitude of hardware architecture, software, operating systems (mostly embedded and probably

open source), firmware…how can anyone promise security in such a morass? It's like the 7 billion people on earth expected to be speaking the same language! Remember Esperanto?

We believe they have a valid argument. In this whole scheme of IoT, what is a 'thing'? A Barbie Doll, a smart fridge from Samsung, a smart car from Germany or Japan, a smart toothbrush, a tracking scope (Figure 3), an umbrella, a water bottle, egg tray, or tampon—don't laugh, even the conservative *The Wall Street Journal* talks about it (Figure 4)? They ALL are vulnerable and denying it is just plain humbug. Unfortunately, many IoT device vendors are still in denial ("I'm secure"), ignorant ("I don't know"), or apathetic ("I don't care"), and have a lackadaisical attitude about the whole security issue and a superficial awareness of the threat vectors.

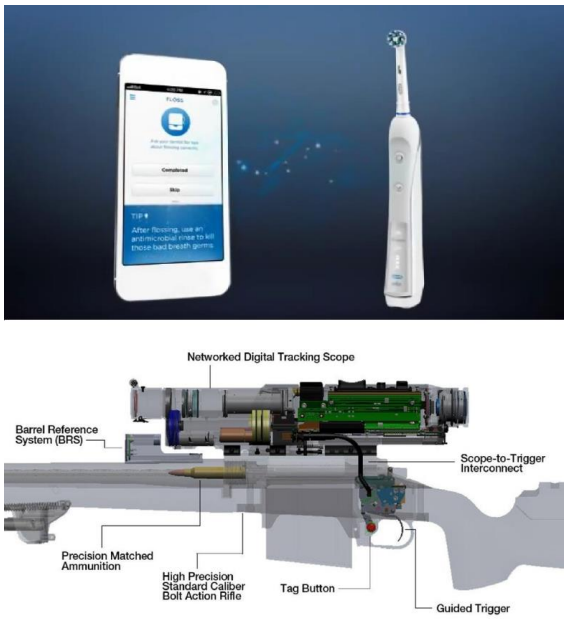

Figure 3. 'Smart' Devices

Figure 4. 'Smart' Paraphernalia

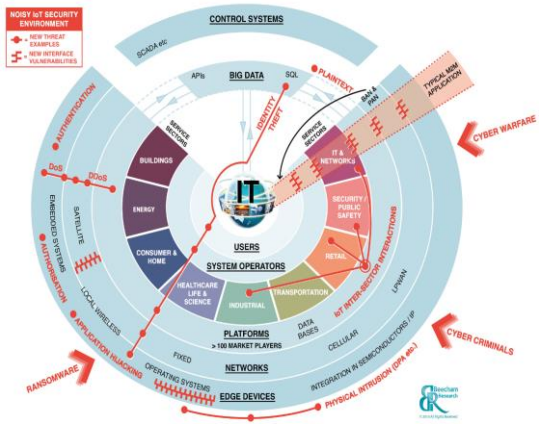

Figure 5. IoT Security Threat Map

3.2 The Do-Gooders

Fortunately, we still have folks who believe the IoT explosion is inevitable and are seriously addressing security issues.

- The U. S. FTC recently (June 2016) warned of security and privacy risks in IoT devices.
- The U. S. FBI has taken note of it and issued a Public Service Announcement in September 2015.
- After the Jeep Cherokee was hacked last year, Fiat Chrysler issued a recall notice for 1.4 million vehicles.
- Microsoft has promised to add BitLocker encryption and Secure Boot technology to the Windows 10 IoT. BitLocker is an encryption technology that can code entire disk volumes, and it has been featured in Windows operating systems since the Vista edition. Secure Boot is a security standard developed by members of the PC industry to help ensure that a PC boots using only software that is trusted by the PC manufacturer. Its implementation can prevent device hijacking.
- A Europe-driven IoT Security Foundation (IoTSF) has been established to respond to the myriad of challenges and concerns over security. Obviously, most of the members of this organization are Europe-based.
- An organization called the Open Web Application Security Project has been established whose scope includes, *inter alia*, "…to help manufacturers, developers, and consumers better understand the security issues associated with the Internet of Things, and to enable users in any context to make better security decisions when building, deploying, or assessing IoT technologies." OWASP has also identified comprehensive IoT attack surface areas (Figure 6).

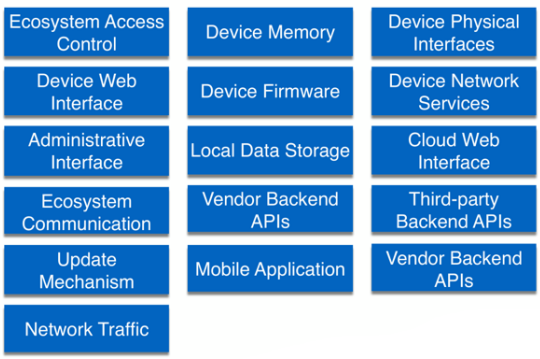

Figure 6. IoT Attack Surface Areas

There is a wide range of standards being developed by the U. S. Government and other professional organizations that are worth a look:

- NERC-CIP security standards were developed for the electric utility industry.

- NIST Cybersecurity Framework is applicable to financial, energy, healthcare, and other critical systems, and is designed to help these industries better protect their information and physical assets from cyberattack.
- In the medical field, the U.S. Food and Drug Administration has provided recommendations to manufacturers for managing cybersecurity risks to better protect patient health and information.
- A number of IEEE standards address security elements applicable to IoT; these include:
  - IEEE P1363, a standard for Public-Key cryptography
  - IEEE P1619 which addresses encryption of data on fixed and removable storage devices
  - IEEE P2600, a standard that addresses security of printers, copiers, and similar devices
  - IEEE 802.1AE and IEEE 802.1X which address Media Access Control (MAC) security.

4. Conclusions

IoT, like any other emerging field, is still in its infancy and experiencing teething problems. There is a lot of hype and hope and, despite all the claims by the vendors and standards bodies, it'll never be 100% secure. This shouldn't surprise anyone: You live in a gated community with a 24x7 security guard, a secure gate to your home, a guard dog, a solid padlocked front door, an integrated security and alarm system, a motion-detector system…each layer of security makes the one below more secure, but nothing makes it 100% secure. The same thing is true of IoT, get over and live with it.