Chapter 7
Hidden Dangers of Internet of Things

Martha Daniel

Overview

Computer security has evolved over the past 25 years as innovative technologies embrace wireless telecommunication integrating information and data and connecting the world globally. I can remember in the early 1990s the announcement that the "Super Highway" was coming with the prediction that it was going to significantly change the way we do business, the way we live, and the way we work.

Now today over 25 years later the "Superhighway" opened avenues and roads thrusting information and connecting our world globally. In reality, this revolutionary technology created a "new world" a domain we call "the Internet". Within this "new world", we have been existing without global policies, rules or regulations, treaties to guide collaborations and protection. Every country has embraced this "new world" and within each country they have declared jurisdictions and territories which are hosting and housing public, private and federal information and data.

The increased volume of information and data being introduced into this "new world" also introduces serious demands for protection and computer security. Today, we are challenged with protecting this information from those who desire to take it and capitalize upon it through theft, corruption, and fraud. The goodness of this innovation far outweighs it negatives; however over the past years the "bad guys and gals" have increased their presence which has now required us to focus on computer security and protection which today is called, Cybersecurity.

The worldwide problem we face today with the internet is—how do we keep the "bad guys and gals, other countries, and terrorist from taking the information and data from this "new world" to specifically corrupt and destroy the world we live in today.

M. Daniel (✉)

D.A. Christofferson (ed.), *Women in Security*, Women in Engineering and Science, https://doi.org/10.1007/978-3-319-57795-1_7

The increasing number of devices that are interconnecting us worldwide and more and more innovation of the utilization of these devices in a wireless environment is driving the need for Cybersecurity and governance. Unethical practices, malicious attacks on data, and corruption have already started Cyber wars. There are so many unknowns, threats, and vulnerabilities associated with the internet today and yet we are now moving towards an advanced age of information now called "The Internet of Things—IoT".

We have so much more work to do with "the Internet" and now with "the Internet of Things-IoT" we are challenged with more hidden unknowns and uncertainties that will surely impact the world we now live. My company, IMRI has been a significant player in the technology industry through the dynamic evolution of technology since 1992, and we are no strangers to Cybersecurity. Our Cybersecurity Division, Cytellix, www.cytellix.com, has been engaged in the protection of the internet worldwide now since 2007 and currently offers a Managed Services Subscription service offering that protects information and data providing real time continuous monitoring of networks bringing complete visibility of all assets and devices residing on your networks, and bringing unique intelligence from threat feeds which identifies and profiles "bad guys and gals—any intruders" who attempt to maliciously attack your company's public or private information. Whether the company is a large entity or small business, we have proven, tested, operational, and affordable services and solutions that bring winning results and outcomes in the war against Cyber intrusions.

This chapter will focus on the "Hidden Unknowns of the Internet of Things". After reading it, you will better understand the challenges that our world now faces as we expand beyond "the internet" to now, "the Internet of Things".

What Really Is the Internet of Things: IoT?

Internet of Things, IoT, refers to internet-connected devices which can interact with other connected devices or objects over a network. IoT is a network of physical and sometimes virtual platforms with IP (Internet Protocol) addresses to enable internet connectivity. These platforms use built-in technology to interact and communicate with other Internet-enabled systems. Besides common computing devices such as laptops, desktops, tablets and smartphones; you can connect other objects with IP (Internet Protocol) addresses to the Internet.

Household appliances, baby monitors, smart locks, smart TVs, wearables, utility devices and other devices with built-in computing systems can be connected to the internet. Electronic appliances, alarm clocks, speaker systems, security systems, thermostats, vehicles, light bulbs, refrigerators, pacemakers and others can have computing systems embedded in them. These devices are known as smart or connected devices. Each device or platform has an identifier, IP address, that can allow specific objects to transfer data through the internet.

The IoT is presently a high volume emerging technology in today's world. According to Gartner, by 2020, suppliers of IoT products and services will generate a revenue increase of over $300 billion. They also expect about 20.8 billion IoT devices. This excludes tablets, smartphones, and computers. IDC, on the other hand, predict a $7.1 trillion growth from $1.9 trillion in the worldwide market regarding IoT solutions in 2020. They expect 28.1 billion devices excluding tablets, smartphones, and computers. IHS Markit professionals predict about 30.7 billion IoT devices by 2020. Regardless of which estimate is on target, we anticipate over 20 billion interconnected devices in the next 3 years.

What Are the Benefits and Significance of IoT?

There are several benefits attached to the revolution of the IoT. These benefits will on daily basis help individuals, businesses, and society as a whole. For individuals, this new concept comes in a lot of forms ranging from safety, health, and everyday automation.

The introduction of IoT into the health care system has proven to be greatly beneficial to both individuals and the society. Hospitals are able to monitor patients vital signs by implementing a chip into individual monitoring devices. These chips provide information to help doctors to determine whether or not a total assessment of the patient is needed. With hospitals struggling on a daily basis to take care of the vast number of patients they have, monitoring each patient's health will allow them to decide who needs attention first. There is a significant cost savings to our healthcare system when we can use automated monitoring as part of preventative techniques.

The Internet of Things can also assist people with their personal safety. ADT, Comcast, AT&T and others provide home security systems that allow individuals to use their phones to monitor and control their home security.

GM's OnStar, Ford's Sync and Chrysler/Dodge's UConnect technologies which are placed in vehicles, provide navigation assistance; allow remote starting and remote locking or unlocking of doors; and detect when a crash occurs and calls 911 automatically. They can also efficiently track any motion of vehicles.

IoT creates an avenue that can help in saving money for people within their homes provided their home appliances can communicate. A smart home is a perfect example of interaction between household appliances and other devices at home. Appliances can be operated in a way whereby energy usage is efficient. The home can provide comfort and convenience based upon the lifestyle of the owners. The garage door opens once the car communicates with it. The homeowner's smartphone unlocks the doors, and the intensity of the home's lighting is set as the user desires. The temperature of the thermostat is adjusted to suit the user's choice. The devices in this home interact with each other to improve the user's lifestyle.

Businesses can equally gain a lot of benefits from the Internet of Things. It can be employed in several different categories which include inventory control, asset

tracking, security, shipping and location, energy conservation, and inventory tracking. Devices are able to communicate their status, location and other pertinent information.

Another benefit of IoT is its ability to track individual consumer behaviors for marketing programs. Each customer is targeted based on the information provided by the device. Marketing programs that use consumer behaviors have been proven to increase business sales and knowledge of demographic trends.

Security Risks of the IoT

The prevalence of objects with digital identifiers that allow them to interact with their environment through the web has become a great concern to security experts. These connected devices are beneficial, but most of them have exploitable vulnerabilities. These devices are not secured, and access to them is rarely restricted. The computing systems embedded in these devices are typically not secured as the design considerations for protection of these objects was not considered. As a result of the insecurity, traffic and access to the smart devices cannot be controlled. This poses a global security risk.

Cyber criminals and unethical hackers can control these smart devices with no more than an internet scan for a manufacturer identifier. Through a basic scan of the internet, a hacker can find a significant distribution of a simple set of devices, such as web cams. With the location identified and the device security flaws understood, the hacker can perform a targeted broad-based attack of the device owner's networks. Recent attacks on the Dyn DNS (Domain Name System) servers, which brought down Amazon, Twitter and Netflix, originated from Mirai botnet infected cameras. Hackers took advantage of IP-based cameras by knowing the device settings and their inherent weaknesses and used tens of millions of smart home devices connected to the internet as weapons in the cyberattack against Dyn.

Users of interconnected devices must be vigilant as long as their devices are connected to the internet. They should be aware of the risks involved in using such devices. Some examples prone to risks include; home security systems, connected cars, smart fridges, smart locks, and smart light bulbs; yes, light bulbs.

The use of smart devices and systems to secure homes has created new security and safety concerns. Smart devices can compromise your privacy. Criminals can take advantage of the weak security of these devices to attack your home network. They can access smart devices, monitor your activities or steal personal data. With the popularity in the use of IoT devices, exposure and risk of cyber attacks on smart homes are on the rise. Most recently, several popular smart home devices including *Nest, Ring, SimpliSafe,* and *SmartThings* were shown to have security flaws that potentially exposed homeowners to all sorts of problems. Also, researchers at the University of Michigan were able to hack into another leading smart home automation system and get the PIN code for a home's front door.

Many users are not aware that in addition to the IoT devices, routers can also be exploited. The router connects devices in your home or business. Flaws in routers can make them vulnerable to exploitation by cyber criminals. They can interfere with the functioning, data and network in your home or office once they can control the router.

Car hacking has been on the increase. In 2015, Chrysler announced a recall for 1.4 million vehicles after two researchers demonstrated that they could remotely hijack a Jeep's digital systems over the Internet. While the recall cost Chrysler a lot of money, if those two researchers had exploited the vulnerabilities the way malicious hackers would have done instead of reporting their research to Chrysler, things could have been much worse.

Some devices can be hacked and compromise the safety of users, not just the building they're housed within. Traffic light controls, healthcare services, and industrial systems are at high risks and can cause havoc to safety and emergency response. For example, in October 2016 hundreds of operations, outpatient appointments, and diagnostic procedures were canceled at multiple hospitals in Lincolnshire, England, after a malware hack compromised the National Health Service (NHS) network.

What Can You Do to Protect Your IoT?

You cannot predict cyber attacks, but you can secure your smart devices against them and reduce damages resulting from these attacks. Protecting and managing IoT devices can be a major challenge, especially if you don't know everything that is connected to your networks. You should adopt a situational awareness model of all devices on your network so you have clear knowledge of every asset on the network, their security posture and their communication paths. Knowing about all devices and their cyber posture will help prevent cyber-crimes in the future.

Early detection of threats to connected devices by monitoring in real-time is crucial in the mitigation of security risk posed by these devices. Adoption of a system that prevents intrusion by shutting down the network whenever anomalous traffic to these devices is detected will be helpful. Automated alerts to new devices and behavior changes can inform when criminals may be attacking the network. This monitoring the smart devices environment will help you decide on the best approach to handle an attack and lessen damages if an attack occurs.

Cyber criminals have frustrated owners of smart devices by taking advantage of devices that are using factory default usernames and passwords which make it easy to gain control of these devices. It's important to reset default passwords to be unique and complex.

Security experts have created cryptographic algorithms to help protect identities and control access to sensitive or personal data. Ensure that interactions between interconnected devices are encrypted. Use encryption to store privacy data including

your Wi-Fi password. The use of encryption will protect your connected devices if a hacker gains access to any of the devices.

Regular update of firmware of embedded computer systems and applications can help secure a smart device. Verify that updates are from the OEM (Original Equipment Manufacturer) or developer before applying them.

Conclusion

The Internet of Things no doubt provides several benefits to individuals, business, consumers and ultimately to the society. I am hopeful, that as the evolution of the products and services evolve, the improvements in security will also be seen.

About IMRI

IMRI is an industry-leading provider of cybersecurity, technology, program management, and engineering services for government organizations and commercial enterprises. IMRI is a change integrator that leverages its 25 years of highly-specialized data center expertise to provide its clients with integrated, solution-based programs to help them meet the requirements and challenges of an ever-changing business environment. Working with some of the largest organizations and networks in the world, IMRI operates in 19 states, providing its clients a critical combination of corporate experience, localized expertise, and proven methodologies and tools that integrate seamlessly into any enterprise.

About Cytellix

Cytellix is a privately held cybersecurity consulting firm specializing in comprehensive network intelligence and situational awareness. Powered by Enterprise Situational Intelligence (ESI), Cytellix has the only solution in the industry that can detect known and "unknown" threats in any environment, while providing complete network visibility. A division of Information Management Resources, Inc. (IMRI), Cytellix manages millions of IP addresses for organizations of every size in a wide range of data-rich industries—including government, manufacturing, finance, banking, law, education, healthcare and municipalities—with best-in-class, real-time network scanning technology. In addition to securing network perimeters for the U.S. Army and the Missile Defense Agency, as well as leading corporations such as PricewaterhouseCoopers (PwC), Kaiser Permanente, and the Walt Disney Company, its agentless, scalable solutions are utilized by small- and mid-size companies for

compliance assessments, one-time audits and in preparation for mergers and acquisitions. With a goal to drive business growth by protecting and defending critical enterprise IT infrastructures throughout the world, Cytellix is well on its way to revolutionizing the cybersecurity industry.