Consumer and Industrial IoT Security

Gregory Boykin

East Carolina University

Target Publication: Infosecwriters

Target Publication URL: https://www.infosecwriters.com

Abstract

With the rapid expansion of internet access globally, Internet of Things (IoT) technologies have exploded onto the market, offering many connected and convenient devices to consumers and industry alike. With the proliferation of devices already connected and the increasing popularity of those devices, this trend in IoT growth will only continue to increase. The ongoing development and evolution of IoT devices has the potential to shape and benefit many industries, including agriculture, education, health care, automotive, and environmental. However, the improvement offered by these devices comes accompanied by potential security threats. These devices are a growing surface which cyber attackers can exploit, leading to exposure of business and consumer data. This risk is compounded by the interconnectedness and interaction between these new gadgets and often driven by a rush to market, which is itself a response to eager consumer and industrial buyers wanting more connected devices expanding convenience and automation. This paper will review the literature to look at the history and current state of the IoT in the marketplace. Possible emerging trends, benefits and concerns such as security will be addressed in relation to the growth of IoT. The paper will conclude with recommendations on how the developing IoT markets can thrive and garner increased device security, protecting the data being stored and accessed.

Keywords: Internet of Things, IoT, security, infosec, data

Introduction

The growth of the internet and desire for connectivity have resulted in an increasing number of internet-linked devices being developed and brought to market. These devices are shaping how businesses operate and consumers live, ushering in new conveniences in functionality and information access with the click of a button or a spoken word. Connected appliances, lighting, thermostats, safety devices, environmental monitoring devices and countless others are being used by both business and consumer alike in growing numbers. This has been foreseen by many, such as Gartner Inc., which predicted IoT devices will number 14.2 billion this year and grow to 25 billion by 2021 (Gartner, 2018). These connected devices, commonly known as the Internet of Things (IoT), are being used more than ever—almost any device can now be connected and interfaced to a local area network or the internet. However, the growth of the IoT industry is accompanied by vast quantities of data, both in motion and at rest, and consideration must be given on how to secure the IoT devices that collect and transmit such data. Manufacturers, developers and consumers who purchase IoT devices need to consider the critical role security measures play in protecting data processed and collected by them. As the IoT market continues to grow, attention to security standards and practices will help to protect business and consumer data and encourage continued growth in the worldwide IoT market.

What is the Internet of Things?

The Internet of Things (IoT) is the term commonly used to refer to the many devices throughout the globe which are connected to the internet or local area networks which can collect, transmit and share data. These connected devices also typically contain some sort of sensing mechanism and can communicate with other smart devices or the cloud (Lee & Shin, 2019). As the growth in the IoT market reflects, almost any device can be connected, controlled,

or monitored using network connectivity. The term “Internet of Things” was originally coined in 1999 by Kevin Ashton, who believed IoT had the potential to change the world, allowing the internet to reach devices and permeate all aspects of our lives (Qin, et al., 2016). Likewise, the term Industrial Internet of Things (IIoT) has been used to specifically refer to devices used to enhance manufacturing or industrial processes. Typically, IIoT deployments are much larger in scale than normal IoT, sometimes numbering hundreds or thousands of interconnected endpoints (Gold, 2018). Since Kevin Ashton’s original prediction, two decades have seen internet-connected device usage soar worldwide. Market research firm IDC has predicted IoT will continue to grow to an explosive $1.7 trillion market, up from $655.8 billion in 2014 (Ray, 2016). Similarly, McKinsey Global Institute predicts that IoT applications will have a potential economic impact of $3.9 trillion to $11.1 trillion a year by 2025 (Attaran, 2017). These trends indicate the impact and benefit consumers and industry are finding through incorporating IoT devices in their businesses and lives.

Consumer and industrial IoT devices have grown in popularity in the last decade due to the automation and convenience added to a variety of applications and environments. Some of the areas which are seeing a high rate of adoption of IoT include home automation, logistics, agriculture, industrial controls, security and automotive. Consumers have looked to IoT devices to potentially improve their homes, making life easier, more comfortable and more convenient (Lee M. , 2019). As a result, more and more consumers are adopting lighting systems, watches, televisions, appliances, locks and cameras in home environments. These devices utilize small wired and wireless local area networks connected to the internet, allowing for communication between local devices and internet-based services. Industry is following a similar path, with businesses seeking ways to improve the work environment through various methods, including

automation. IoT-connected devices allow for control and monitoring of industrial equipment such as factory machines, meters, actuators, electrical distribution automation devices, and supervisory control and data acquisition systems (Son, Jha, Kumar, Chatterjee, & Khari, 2019). Adoption and use of these IoT devices allow for environmental monitoring, predictive failure, energy consumption tracking, HVAC controls, connected robotics and safety monitoring, all benefiting overall operations in a variety of industrial settings. As additional devices and use case scenarios are developed, continued adoption will benefit both the consumer and industry.

Fuel for Growth

IoT market growth has been exponential in both the consumer and industrial markets. Several key factors have served as driving forces for IoT growth in a variety of scenarios. From a consumer standpoint, convenience and access to modern amenities are often important reasons for adoption. IoT devices often offer easy accessibility and control of physical objects and systems found in the home, which directly impacts the lives of the users and thus encourages consumer adoption (Mehta, Bansal, Mohit, & Banerjee, 2018). Correspondingly, in industrial environments, automation, monitoring and control are critical factors in successful operations. Development of intelligent production sites and systems through IoT technology is a highly-discussed topic in industry (Wortmann & Flüchter, 2015). If the addition of IoT brings more efficiency and higher production, the resulting higher profits will serve to drive adoption.

Another very influential factor for IoT's rapid expansion is the growth of wireless networking. Although wired network connectivity is used on many IoT devices, wireless connectivity expanded the reach and lowered the cost of deployment. Whether in a consumer's home or on the industrial factory floor, wireless connectivity allows for IoT devices to be placed anywhere wireless connectivity is available, thus eliminating additional costs associated with

wired networks. Both cellular and Wi-Fi wireless technologies are readily available, simple to connect to and widely adopted throughout the globe. In addition to cellular and Wi-Fi, other wireless communication standards such as Bluetooth low energy (BLE), Zigbee, SIGFOX and LoRaWAN are also being used for IoT connectivity (Mosin, 2018). New and existing wireless standards are in a continual state of development and improvement, consequently building a large infrastructure for the connection of IoT devices. Such expansion of wireless connectivity, especially the imminent release of Wi-Fi 6 and 5G, will continue to encourage healthy IoT growth. With the expanding bandwidth and coverage of cellular 5G, Ericcson forecasts the number of cellular IoT connections to reach over 4 billion by 2024 (Ericcson, 2019). Continued expansion of wireless network technology will correlate closely with the sustained growth of the IoT market.

Additionally, growth in the interconnectivity of IoT devices has encouraged the market's continued expansion. Cost reductions in the hardware and software required for adding connectivity and sensors to devices has enabled developers and manufacturers to expand the scope of what devices can be connected and used across the IoT landscape. Not only are IoT devices able to connect to local systems, but developments over the last decade have enabled connectivity and data sharing between devices as well as to cloud-based systems and devices. This has led to the functions of one product being further enhanced if it is connected to related products as part of a product system (Wortmann & Flüchter, 2015). Expanding connectivity options between IoT devices allows for extended convenience and efficiency for both the consumer and industry through data sharing and elaborate systems which base actions of one IoT device on sensor or collected data of another. These types of systems also allow for large-scale data collection, which provides historical analysis and trends, proving beneficial in the use and

management of IoT devices and the systems they support. These types of changes and the continued innovations in wireless technology simplify the adoption of IoT devices and will continue to encourage their usage by consumers and industry in years to come.

Security Concerns

The IoT and its supporting landscape are flourishing, but this means related security concerns are also becoming more widespread. In the past, cybersecurity concerns were confined to a range of known devices, including desktop computers, laptops and phones. However, as trends indicate, the IoT amplifies the scope and scale of products and services that are being connected and can become potential targets for cyberattacks (Tanczer, Steenmans, Elsden, Blackstock, & Carr, 2018). As referenced earlier, the number of IoT devices currently in use is staggering—and will continue to rise. Collectively, they present a growing attack surface to exploit across consumer and industry markets. This increasing IoT attack surface is made more vulnerable by the "always on" nature of IoT devices. Most connected IoT devices have low power consumption and are designed to operate continually, only entering sleep states as needed. The number, connectivity and complexity means more parts, more interactions and more design mistakes which in turn extend the attack surface for the growing number of always-on devices (Mahmoodi, Reiter, Viehl, Bringmann, & Rosenstiel, 2018).

The number of devices correlates with the increasing amounts of data collected. As both consumers and industry continue use of IoT devices, large quantities of data will be generated and pass through the various IoT systems. This data becomes a prime target for cyber criminals. This highlights a key concern for those adopting IoT technologies: the risk of data exposure if systems or devices are compromised. Due to the overwhelming popularity and functionality of IoT devices, security is frequently neglected by both manufacturers and implementors, leaving

consumers and businesses vulnerable to attack. As the literature and secondary research shows, as more IoT connectivity is seen in homes and businesses, increased exposure is possible, thus validating the importance of addressing security concerns and truly gaining advantage from the implementation of IoT (Ramsoomair & Kolb, 2018).

The need for increased focus on security for IoT devices and systems is illustrated by the abundance of incidents involving IoT devices being compromised or exploited. Many existing exploits in differing markets have been used to compromise IoT systems. In one example, an IoT smart toy, the CloudPets brand teddy bear, was found to be exploitable and remotely accessible; in addition, customer records were left exposed in an improperly-secured cloud database (Franceschi-Bicchierai, 2017). Similarly, the notable security software company Rapid 7 conducted a case study on baby monitors and vulnerabilities. This study revealed several vulnerabilities in which the IoT devices were accessible directly and the cloud storage utilized by them was accessible without authentication (Rapid7, 2015). Another risk was revealed when the FDA issued a warning that implantable cardiac devices used by St. Jude Medical were potentially vulnerable. These devices were found to be exploitable, allowing modification of functionality through programming commands (US Food and Drug Administration, 2017). Another incident involving IoT and the underlying security of its implementation involved a researcher's study of traffic light systems used in 40 states throughout the US. Research on 100 traffic lights in Michigan revealed improperly configured IoT devices using unsecured wireless networks, allowing these systems to be accessed and controlled (Priff, 2014). As a final example from the automotive industry, several manufacturers' IoT implementations were also discovered to be vulnerable. Several cases were documented in which models from BMW, Audi, Toyota and Tesla were subject to the exploitation of the controller area network (CAN) of

the vehicle; this allowed control of ignition, locks, screens and braking systems (McGoogan, 2016) (Solon, 2016). As seen with these examples of successful exploits, IoT devices pose serious security concerns. Although these vulnerabilities were often corrected, such incidents highlight the potential compromises IoT devices may face if security is not considered in the design and implementation of connected systems.

Another security issue associated with IoT devices involves how they can be compromised and used by malware on larger scales. Numerous malware variants form BotNets which leverage IoT devices like cameras and routers to conduct distributed denial of service (DDoS) attacks (Gurunath, Agarwal, Nandi, & Samanta, 2018). One such example which leverages known IoT vulnerabilities is Tsunami or Kaiten which has been actively targeting IoT devices (Barnett, 2018) (Seals, 2016). These malware variants are internet relay chat (IRC) controlled versions which have been used to successfully conduct DDoS attacks using compromised IoT devices. Similarly, a variant of the Tsunami/Kaiten malware named Mirai has been utilized to exploit vulnerable IoT devices. Mirai was able to successfully infect IoT devices running on ARC processors; these devices were then used to participate in a DDoS attack which often utilized up to 400,000 simultaneously infected IoT endpoints (Kolias, Kambourakis, Stavrou, & Voas, 2017). Mirai-based attacks targeted the website of well-known security expert Brian Krebs and sites such as Twitter, Netflix, Reddit and GitHub, causing outages which lasted several hours (Williams, 2016). Attacks such as these have great impact—and often financial consequences for businesses. Once such example surrounds a Mirai BotNet DDoS attack against the DNS company Dyn. Due to the attack, Dyn lost nearly 8% of its customers (Weagle, 2017). Impacts such as these reinforce the need to focus on security for the IoT.

Securing the Internet of Things

Security will play a critical role in protecting the growing IoT. Both consumers and businesses are looking for the connectivity and automation that IoT offers but also want those same devices secure, protecting private information and collected data (Khan, Aalsalem, Khan, & Arshad, 2019). Many steps can be taken in order to secure IoT devices and systems, but basic steps are often overlooked, leaving devices and networks exposed to cyberattacks. A first critical step for IoT device protection is to update the default security credentials so that a unique and standards-conforming password is in place. Additionally, checking default settings should include attention given to unused services; ideally, only necessary services should be running. Also, software and firmware updates should be reviewed and installed to patch any discovered vulnerabilities. In large-scale environments, best practices should be observed when deploying IoT devices, including network segmentation in order to isolate sensitive network zones. The devices being deployed should be from reputable manufacturers who are implementing current security methods such as public key infrastructure or emerging technology such as blockchain. These manufacturers often will continue support of IoT devices, delivering updates and firmware to improve performance and increase security. Additionally, IoT devices should be placed in secure areas in order to limit physical access. Finally, intrusion detection and prevention systems (IDPS) should be configured in order to detect possible intrusions and exploitation attempts of IoT devices on the network.

Another major step in securing IoT concerns the development and adoption of standards involving the manufacturing and deployment of devices. As with many technologies, standards must be established in order to encourage manufacturers, consumers and industry to follow best practices and adopt the latest security methods. One such standard, released by the ETSI

Technical Committee on Cybersecurity (TC CYBER) in February 2019, was ETSI TS 103 645, which is a standard for cybersecurity in the Internet of Things (ETSI, 2019). Similarly, the Institute of Electrical and Electronics Engineers (IEEE) has also released an approved draft for an Architectural Framework for the Internet of Things (P2413/D0.4.6) standard (IEEE, 2019). These security standards highlight key steps which promote best practices and goals towards securing IoT. Some of the guidelines highlighted in these standards include no longer using default passwords, keeping device software updated, implementation of vulnerability disclosure processes, device usage of secure communications, ensuring software integrity, protecting personal data and securing stored credentials. Continual development of security standards for IoT will help keep devices more secure through the adoption of best practices and new security methods by manufacturers of devices and those who use them.

Conclusion

Once the stuff of science fiction, the IoT is in widespread usage, providing benefits to consumers and businesses alike. In the home, the IoT offers conveniences such as control of lighting and climate systems. In the workplace, the IoT helps streamline processes and increase efficiency via automation and communication between devices. Demand for IoT devices and the variety of emerging technologies applicable to further development of functionality leave the market poised for growth. However, as the Federal Trade Commission (FTC) notes, despite the tangible benefits to consumers and industry, many security concerns exist regarding privacy of connected and embedded devices. The growth of the IoT promises new conveniences, but it also creates new opportunities for unauthorized persons to exploit vulnerabilities (Federal Trade Commission, 2016). The concerns of the FTC are well-founded; there are numerous documented cases of insecure IoT devices becoming liabilities in both consumer and business

settings. The benefits of embracing the IoT come with the responsibility for securing these systems and the data within them. Common-sense best practices such as applying patches and not using default passwords are essential basic security measures often overlooked in IoT deployment, but the development of formal standards promises to help manufacturers, consumers, and industry professionals understand and adopt security methods, decreasing vulnerability to cyberattacks. With proper attention to security, risks can be minimized, and the future of the IoT's growth—both in size and functionality—can be secured.

References

* Attaran, M. (2017). The Internet Of Things: Limitless Opportunities For Business And Society. *Journal of Strategic Innovation and Sustainability, 12*(1), 10-29.

Barnett, R. (2018, September 11). *New Tsunami/Kaiten Variant: Propagation Status*. Retrieved from Akamai Security Intelligence & Threat Researc: https://blogs.akamai.com/sitr/2018/09/new-tsunamikaiten-variant-propagation-status.html

Ericcson. (2019). *Ericsson Mobility Report June 2019.* Stockholm: Fredrik Jejdling.

ETSI. (2019, February). Cyber Security for Consumer Internet of Things. *ETSI TS 103 645*. ETSI.

Federal Trade Commission. (2016). *The Benefits, Challenges, and Potential Roles for the Government in Fostering the.* Bureau of Consumer Protection and Office of Policy Planning.

Franceschi-Bicchierai, L. (2017, February 27). *Internet of Things Teddy Bear Leaked 2 Million Parent and Kids Message Recordings*. Retrieved from www.vice.com: https://www.vice.com/en_us/article/pgwean/internet-of-things-teddy-bear-leaked-2-million-parent-and-kids-message-recordings

Gartner. (2018). Top Strategic IoT Trends and Technologies Through 2023. *Gartner IT Symposium.* Barcelona: Gartner.

Gold, J. (2018, February 2). *What is the Industrial IoT? [And why the stakes are so high]*. Retrieved from www.networkworld.com:

https://www.networkworld.com/article/3243928/what-is-the-industrial-iot-and-why-the-stakes-are-so-high.html

* Gurunath, R., Agarwal, M., Nandi, A., & Samanta, D. (2018). An Overview: Security Issue in IoT Network. *2018 2nd International Conference on I-SMAC* (pp. 104-107). Palladam: IEEE.

IEEE. (2019, March). Approved Draft Standard for an Architectural Framework for the Internet of Things (IoT). (pp. 1-265). IEEE.

Khan, W. Z., Aalsalem, M. Y., Khan, M. K., & Arshad, Q. (2019). Data and Privacy: Getting Consumers to Trust Products Enabled by the Internet of Things. *IEEE Consumer Electronics Magazine, 8*(2), 35-38.

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and Other Botnets. *Computer*, *50*(7), 80-84.

* Lee, M. (2019). An Empirical Study of Home IoT Services in South Korea: The Moderating Effect of the Usage Experience. *International Journal of Human - Computer Interaction, 35*(7), 535-547.

* Lee, W., & Shin, S. (2019). An Empirical Study of Consumer Adoption of Internet of Things Services. *International Journal of Engineering and Technology Innovation, 9*(1), 1-11.

* Mahmoodi, Y., Reiter, S., Viehl, A., Bringmann, O., & Rosenstiel, W. (2018). Attack Surface Modeling and Assessment for Penetration Testing of IoT System Designs. *21st Euromicro Conference on Digital System Design (DSD)* (pp. 177-181). Prague: IEEE.

McGoogan, C. (2016, April 25). *BMW, Audi and Toyota cars can be unlocked and started with hacked radios*. Retrieved from www.telegraph.co.uk: https://www.telegraph.co.uk/technology/2016/03/23/hackers-can-unlock-and-start-dozens-of-high-end-cars-through-the/

* Mehta, V., Bansal, P., Mohit, K., & Banerjee, P. (2018). Empowering the Security for Iot-Based Communications in Smart City. *2018 International Conference on Automation and Computational Engineering* (pp. 57-60). Greater Noida: IEEE.

* Mosin, S. (2018). A Model of LoRaWAN Communication in Class A for Design Automation of Wireless Sensor Networks Based on the IoT Paradigm. *2018 IEEE East-West Design & Test Symposium* (pp. 1-6). Kazan: IEEE.

Priff, M. (2014, August 20). *How to get green lights all the way to work: Hackers reveal how simple it is to control traffic lights in major cities using just a laptop*. Retrieved from www.dailymail.co.uk: https://www.dailymail.co.uk/sciencetech/article-2730096/How-green-lights-way-work-Hackers-reveal-simple-control-traffic-lights-major-cities-using-just-laptop.html

* Qin, Y., Z.Shengl, Q., J.G.Falkner, N., Dustdar, S., Wang, H., & V.Vasilakos, A. (2016). When things matter: A survey on data-centric internet of things. *Journal of Network and Computer Applications*, 137-153.

* Ramsoomair, F., & Kolb, E. (2018). Internet Of Things In The Workplace. *i-Manager's Journal on Management, 13*(2), 13-23.

Rapid7. (2015). *HACKING IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities.* Rapid7.

* Ray, P. P. (2016). Creating Values out of Internet of Things: An Industrial Perspective. *Journal of Computer Networks and Communications, 2016*, 1-11.

Seals, T. (2016, March 30). *Kaiten Malware Returns to Threaten IoT*. Retrieved from InfoSecurity Magazine: https://www.infosecurity-magazine.com/news/kaiten-malware-returns-to-threaten/

Solon, O. (2016, September 20). *Team of hackers take remote control of Tesla Model S from 12 miles away*. Retrieved from www.theguardian.com: https://www.theguardian.com/technology/2016/sep/20/tesla-model-s-chinese-hack-remote-control-brakes

Son, L. H., Jha, S., Kumar, R., Chatterjee, J. M., & Khari, M. (2019). Collaborative handshaking approaches between internet of computing and internet of things towards a smart world: a review from 2009–2017. *Telecommunication Systems, 70*(4), 617-634.

Tanczer, L. M., Steenmans, I., Elsden, M., Blackstock, J., & Carr, M. (2018). Emerging risks in the IoT ecosystem: Who's afraid of the big bad smart fridge? *Living in the Internet of Things: Cybersecurity of the IoT* (pp. 1-9). London: IET.

US Food and Drug Administration. (2017, January 9). Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication. *Safety Communications*. FDA.

Weagle, S. (2017, February 21). *Financial Impact of Mirai DDoS Attack on Dyn Revealed in New Data*. Retrieved from www.corero.com: https://www.corero.com/blog/797-financial-impact-of-mirai-ddos-attack-on-dyn-revealed-in-new-data.html

Williams, C. (2016, Octoboer 21). *The Register*. Retrieved from IoT gadgets flooded DNS biz Dyn to take down big name websites: https://www.theregister.co.uk/2016/10/21/dyn_dns_ddos_explained

Wortmann, F., & Flüchter, K. (2015). Internet of Things: Technology and Value Added. *Business & Information Systems Engineering*, *57*(3), 221-224.