The Internet of Things (IoT) – Removing the Human Element

Robert Martin

East Carolina University

Target Publication: www.infosecwriters.com

Table of Contents

Abstract

This paper focuses on the IT security challenges facing the Internet of Things (IoT). An isaca.org article describes the Internet of Things as, “a scenario in which objects, animals or people are provided with unique identifiers and the ability to automatically transfer data over a network without requiring human-to-human or human-to-computer interaction” (Gonzalez & Djurica, 2015). Additionally, this paper outlines the security risks and impacts associated with removing human intervention from the Internet of Things. The four components of the Internet of Things discussed in this paper are the “things” themselves, the data, the communication network, and the computing systems. The purpose of this paper is to show the underlying security risks associated with interconnecting people, data, and devices via the Internet, without human controls.

The Internet of Things (IoT) – Removing the Human Element

Gartner reports "that 4.9 billion connected things will be in use in 2015, up 30 percent from 2014, and will reach 25 billion by 2020" (Gartner, 2014). These "4.9 billion things" are currently producing, exchanging, analyzing, and collected information but lack human intervention. What this means is that IT professionals must begin to rapidly dissect the security risks associated with connecting personal and corporate devices containing sensitive data to the Internet without human intervention or oversight. With the Internet of Things (IoT), the boundaries of what individuals, businesses, and governments must secure are yet undefined; in fact all industry verticals could be adversely affected by the IoT. These security risks must be realized and proactive action plans must be put in place to preserve the confidentiality, integrity, and availability of all of those devices and the data contained within them. The purpose of this paper is to outline the risks involved with the IoT, map those risks to regulatory and industry standards, and provide some security methods to mitigate those risks.

Literature Review

The Internet of Things presents security professionals with three questions. First, what is the scope of the Internet of Things? Second, what are the privacy, legal, and regulatory risks associated with the Internet of Things? Third, what proactive IT security measures must be put in to place to mitigate these issues?

Maras (2015) outlines four points that support this paper. The first point is that "the Internet of Things (IoT) creates new security risks that device manufacturers and application developers have not anticipated." The second point is that "devices that have become part of the IoT enable the storage, analysis, monitoring, and sharing of vast quantities of data with other networked devices and users." The third point is "users' privacy is threatened because of their limited control and choice over the collection, retention, and distribution of their data." The fourth point is "the inadequate legal framework regulating the Internet of Things" (Maras, 2015).

Gonzalez and Djurica (2015) list the three principle components of the Internet of Things that support this paper. These components are the things themselves, the communications network, and the computing systems. The things themselves "represent the devices or sensors with the ability to capture or produce data, and the time to create an effect on the environment in which they have some influence." The communication network is the medium that connects all of the things. The computing systems are responsible for processing and using the "data received and/or transmitted by the things, with, in most cases, a minimal computational capability." The authors outline the opportunities as well as the risks associated with the Internet of Things (Gonzalez & Djurica, 2015).

In a recent Trend Micro article, the company echoes a Public Service Announcement from the Federal Bureau of Investigations that supports this paper by outlining the devices and verticals in the scope of the Internet of Things. Some of those verticals include smart homes, smart devices, automotive systems, and public utilities. The article also recommends some proactive measures to augment security of IoT against threats (Trend Micro, 2015).

Gartner is a leading technology research and advisory company. The statistics reported by Gartner advocate the need for awareness and decisive action. Gartner reported that "the Internet of Things has become a powerful force for business transformation, and its disruptive impact will be felt across all industries and all areas of society." Gartner details that "the IoT will bring into the digital security architecture dozens of new platform options, hundreds of variations on hybrid IT/IoT integration, new standards per industry, and a new view of an application" (Gartner, 2014).

Rahmatian (2014) proposes using hardware-based intrusion detection systems in order to detect malware in, or illegal modification to, embedded systems. This research emphasizes that "embedded devices are handling data of increasing value, such as consumer banking credentials or stock market information." The author also states that the manufactured devices are security risks because the software platforms are open-source "with high levels of off-device connectivity that enable the consumer to download any third-party applications." Mobile phones have embedded security devices; however, "they can be bypassed with little effort using reprogramming tools" (Rahmatian, 2014). This research lends credibility to this paper by demonstrating that hardware-based intrusion detection systems can be a viable remediation method to help defend against hackers.

The Internet of Things (IoT)

The center of the device connected to the Internet of Things is the embedded system. An embedded system is defined as "a dedicated computer system designed for one or two specific functions." This embedded system is part "of a complete device system that includes hardware, such as electrical and mechanical components." The embedded system is not "engineered to manage a wide range of processing tasks" like a typical computer. Designers of embedded controllers focus on optimizing "size, cost, power consumption, reliability and performance" (Techopedia, n.d.). Security is an afterthought with these systems, with attackers taking advantage of their lack of built-in security. This lack of built-in security is creating a new set of global risk and privacy problems for manufacturers and users of these systems.

Security and Privacy Implications

With the functionality advancements of new smart mobile devices, users now have the ability to monitor and control home security systems, operate their automobiles, monitor their health, and much more. This mix of data about the "user and target" produced by these smart devices is being stored, processed, and read by other users without human intervention. This convenience "comes at a cost, namely security." Manufactures are primarily focused on productivity and functionality. "Most IoT devices were built without security in mind." Device engineers are leaving in security vulnerabilities like backdoors and hardcoded passwords that can be exploited. The new attack surface is creating a new set of unrealized risks. "With more objects being connected to the Internet and the creation of new types of critical infrastructure, we can expect to see (more) targeted attacks on existing and emerging infrastructures, including new forms of blackmailing and extortion schemes (e.g., ransomware for smart cars or smart homes),

data theft, physical injury and possible death, and new types of botnets." The data contained in these devices can include personal, corporate, medical, and/or financial information. As more and more IoT devices are connected to the Internet, more security issues are being discovered. "If security issues are widespread within an IoT device that has been identified as vulnerable, class action and product liability lawsuits could be brought against IoT device manufacturers by affected customers." The author recommends that IoT infrastructure be resilient to cyberattacks (Maras, 2015). So what verticals are being affected by the IoT?

IoT Verticals

Some of the verticals that are being affected by the Internet of Things include Industrial Control Systems, healthcare, and the private sector. Each of these verticals is becoming increasingly dependent on embedded systems in order to operate, but these systems are not safe from attack.

Industrial Control Systems are designed to "allow operators to monitor and control industrial processes, including those in the oil and gas, nuclear, power transmission and distribution, manufacturing, chemical, and other industries." Industrial Control Systems can be found in technologies that run the Power Grid, regulate energy used in a building, or manage the processes in an industrial plant (Bielski, 2014). "As more and more embedded devices are exposed to the Internet because of driving forces like the Internet of Things (IoT) and remotely-controlled industrial systems, the number of targets is increasing all the time" (Haughn & Rouse, 2015). In a recent usatoday.com article, it was reported that "the branch of the Department of Homeland Security that monitors cyberthreats received reports of 151 'cyber incidents' related to the energy industry in 2013 — up from 111 in 2012 and 31 in 2011" (Reilly, 2015). An example

of these attacks is an "unnamed public utility that was recently breached by a sophisticated threat actor who gained unauthorized access to its control system network." The attackers were able to gain access through a vulnerability "found in the software used by the utility to administer the control system assets." These control system assets "were accessible through its Internet facing hosts" (Brocklehurst, 2014). These embedded systems will come under the scrutiny of industry standards like the Critical Infrastructure Protection (CIP) standards enforced by the North American Electric Reliability Corporation (NERC) (NERC, n.d.).

The healthcare industry is also under siege by hackers. Hackers are attacking hospitals to steal electronic health records (EHR). These records contain valuable data such as administrative and billing data, which can include a person's full name, maiden name, social security number, email address, spouse's contact information, patient demographics, medications, and address (HealthIT.gov, n.d.). The U.S. Food and Drug Administration issued a safety communication through fda.gov outlining the cybersecurity risks associated with medical devices that contain configurable embedded computer systems. The FDA has become aware that as a result of embedded system vulnerabilities, healthcare organizations "can be vulnerable to cybersecurity breaches." The FDA warns that "as medical devices are increasingly interconnected, via the Internet, hospital networks, other medical device, and smartphones, there is an increased risk of cybersecurity breaches, which could affect how a medical device operates." These connected devices could be "disabled by malware." The patient data contained within these devices could be altered or stolen. These device security issues could be a result of the "failure to provide timely security software updates and patches to medical devices and networks and to address related vulnerabilities in older medical device models (legacy devices)." These security issues could also be a result of "security vulnerabilities in off-the-shelf software designed to prevent

unauthorized device or network access, such as plain-text or no authentication, hard-coded passwords, documented service accounts in service manuals, and poor coding/SQL injection" (U.S. Food and Drug Administration, 2013). According to bloomberg.com, "a rise in cyber attacks against doctors and hospitals is costing the U.S. health-care system $6 billion a year as organized criminals who once targeted retailers and financial firms increasingly go after medical records" (Pettypiece, 2015). These healthcare embedded system vulnerabilities are certain to come under examination of the watchful eye of healthcare standards like HIPAA and HITECH. These standards were put in to "protecting the privacy and security of certain health information" (U.S. Department of Health & Human Services, n.d.).

The private sector is also not immune to the vulnerabilities associated with embedded systems. These systems exist in Internet of Things devices such as wearable smart devices, smart homes, smart phones, and smart automobiles. According to Don Bailey, CEO of Lab Mouse Security, "the number one issue is identity. We will have all of these unmanned devices that aren't going to be monitored by anybody." Cellular communications are assumed to be safe; however, "each provider of software and hardware often presume they're all secure, and no one has any real control over the security of the entire system" (Hulme, 2014). Consumers also assume the vehicles we drive are safe as well, but they are not. According to a recent wired.com article, two WIRED security researchers were able to wirelessly hack a Jeep; the author "was driving, taking over dashboard functions, steering, transmission and brakes." As a result of that data, "Chrysler announced that it's issuing a formal recall for 1.4 million vehicles that may be affected by a hackable software vulnerability in Chrysler's Uconnect dashboard computers." The Jeep Cherokee was hacked from 10 miles away from the researcher's basement (Greenberg, 2015). The private sector is governed by many regulatory bodies or groups, like the Federal

Communications Commission (FCC), which governs "cellular telephones; paging; personal communications services (PCS); public safety; and other commercial and private communications services (FCC, n.d.). The Chrysler Jeep hack recalls are certain to gain the attention of the National Highway Traffic Safety Administration (NHTSA). The NHTSA is "charged with regulating safety standards in the auto industry and transportation" (NHTSA, n.d.).

Remediation

Because of the tremendous growth and complexities of the IoT across all industry verticals, securing these devices and the network to which they are connected is a complex issue that must be addressed. Remediating these security issues should begin with the device itself, move to the network to which it is attached, and then to the person or entity to whom it belongs.

A starting point for securing these devices is the device itself. "Security is not even considered during the architecture and design of IoT devices." Manufactures of smart devices are simply not building in security. The security of the device is left to the consumer. However, efforts to secure devices are already in motion. After the successful hack of the Chrysler Jeep, "U.S. senators reacted quickly, proposing new legislation on the same day the news broke that would require the US National Highway Traffic Safety Administration (NHTSA) to set standards to ensure that all wireless access points of a vehicle are secured and built with technology to detect and stop a hack in real time." This new legislation "includes rules to force car companies to make customers aware of the data collected about them and their use of the car." For smart home devices, U.S. lawmakers "are looking to adopt new laws to secure these gadgets."

IoT devices like; mobile phones, medical devices, smart grid devices, and wearable fitness monitoring devices are still at risk to hackers. These risks were realized as far back as 2007 “when then-US Vice President Dick Cheney had his doctors disable the wireless connection to his pacemaker because he feared terrorists would hack into it and turn it off to kill him” (Herold, 2015). IoT devices must be equipped with the right security technologies so they can be a functioning part of the security infrastructure. An example of a security technology that manufacturers could include would be antimalware embedded within the device (Herold, 2015).

The network that connects these devices together must also be secured. Setting boundaries for IoT devices is a good starting point for network security. Businesses supporting IoT devices should “establish policies and procedures that clearly describe the boundaries within which IoT devices can be used.” Businesses can also refuse to connect any IoT devices to their network that do not have security and privacy controls built in (Herold, 2015). An example of a built-in security control functioning with a network security control is an embedded system with a hardware-based intrusion detection system. The embedded IDS would have a finite state machine within it so that any deviation from that state machine could be compared and detected. The state machine would contain all of the legal calls defined within. A legal call is an acceptable action carried out by the embedded system. If the embedded system was compromised and the attacker attempted to execute anything outside of those defined parameters, then that action would be flagged as illegal. At that point, action could be taken against that infection in the embedded system by the network-based intrusion detection system (Rahmatian, 2014). Network administrators should also “implement account lockout policies to reduce the risk from brute forcing attempts” using Group Policy and “when remote access is

required, employ secure methods, such as Virtual Private Networks (VPNs)" (Brocklehurst, 2014).

"Many individuals seem to agree that people are the weakest link in security, but not enough effort goes into educating these people" (Harris, 2008). Consumers are concerned about their privacy. "A Pew research study reported that 91 percent of adults care about their privacy, but feel as though they have no control over how their personal information is collected and used by companies" (Herold, 2015). With the Internet of Things, end-users must be educated to the risks and responsibilities assumed when connecting their devices to the Internet.

Some factors end-users and organizations must take into consideration "in order to achieve control and minimize the potential IoT risk" are reducing the collection of personal data, reducing connecting data with individuals, and minimizing and securing data retention. Reducing the collection of personal data focuses on controlling "which data can be exposed to the Internet without an individual's consent." Reducing connecting data with individuals focuses on determining "whether devices or software need personal information or some other data that could be connected with individuals or their private information." Minimizing and securing data retention is done in an effort to eliminate the leak of personal data by instituting best practices, such as encrypting private data sent through a network (Gonzalez & Djurica, 2015). "Ensuring that all end-users are fully aware of the correct usage of devices becomes increasingly important when such devices are interconnecting, as in the world of IoT" (Seaman, 2015).

Conclusion

"It has never been more important for organisations across the globe to work together to ensure that future advancements in technology are carried out safely and securely." The fate of the security of Internet of Things is not set. That "fate we make for ourselves" (Seaman, 2015). Securing these global devices begins with building in security on the embedded system within the device itself. With so many insecure IoT devices currently connected to the Internet, security must also exist at the network level through network-based IDS. As manufactures build in embedded IDS, then those devices will be able to work in tandem with the network-based IDS to improve detection rates and incident response times. The end-user must receive "security awareness training about the safe and secure use of the devices." "Significant threats to data resources come from the end-user perspective, in which users carry out actions that undermine or bypass the security measures employed to protect both the device and the data within it" (Seaman, 2015). To be effective, all of these implementations and corrective measures must remain under the care and watchful eye of well-trained security professionals.

References

Bielski, J. (2014, November 24). Understanding the Importance of Industrial Control System Security, Interview with Dan Scali, Manager Industrial Control Systems « Threat Research. Retrieved November 28, 2015, from https://www.fireeye.com/blog/threat-research/2014/11/ics_security.html

Brocklehurst, K. (2014, May 21). DHS Confirms U.S. Public Utility's Control System Was Hacked | The State of Security. Retrieved November 29, 2015, from http://www.tripwire.com/state-of-security/incident-detection/dhs-confirms-u-s-public-utilitys-control-system-was-hacked/

FCC. (n.d.). FAQS - Wireless Phones. Retrieved November 29, 2015, from https://www.fcc.gov/encyclopedia/faqs-wireless-phones

Gartner. (2014, November 11). Gartner Says 4.9 Billion Connected. Retrieved November 26, 2015, from http://www.gartner.com/newsroom/id/2905717

*Gonzalez, M. H., & Djurica, J. (2015). Internet of Things offers great opportunities and much risk. *ISACA, 2*, 18-19.

Greenberg, A. (2015, July 24). After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix. Retrieved November 29, 2015, from http://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/

Harris, S. (2008). CISSP exam guide (Fourth ed., p.142). New York: McGraw-Hill.

Haughn, M., & Rouse, M. (2015, February). What is embedded device hacking? - Definition from WhatIs.com. Retrieved November 28, 2015, from http://whatis.techtarget.com/definition/embedded-device-hacking

HealthIT.gov. (n.d.). HealthIT.gov. Retrieved November 29, 2015, from https://www.healthit.gov/providers-professionals/faqs/what-information-does-electronic-health-record-ehr-contain

*Herold, R. (2015). The Criticality of Security in the Internet of Things. ISACA, 6, 18-24. Retrieved November 25, 2015.

Hulme, G. V. (2014, August 4). Black Hat 2014: The challenge of securing embedded devices and IoT on display. Retrieved November 29, 2015, from http://www.csoonline.com/article/2460825/application-security/black-hat-2014-the-challenge-of-securing-embedded-devices-and-iot-on-display.html

*Maras, M. -. (2015). Internet of things: Security and privacy implications. International Data Privacy Law, 5(2), 99-104. doi:10.1093/idpl/ipv004

NERC. (n.d.). Standards. Retrieved November 29, 2015, from http://www.nerc.com/pa/stand/Pages/default.aspx

NHTSA. (n.d.). AllGov - Departments. Retrieved November 29, 2015, from http://www.allgov.com/departments/department-of-transportation-dot/national-highway-traffic-safety-administration?agencyid=7241

Pettypiece, S. (2015, May 7). Rising Cyber Attacks Costing Health System $6 Billion Annually. Retrieved November 29, 2015, from http://www.bloomberg.com/news/articles/2015-05-07/rising-cyber-attacks-costing-health-system-6-billion-annually

*Rahmatian, M. (2014). Intrusion detection for embedded system security (Order No. 3614514). Available from ProQuest Dissertations & Theses Global. (1517984758). Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1517984758?accountid=10639

Reilly, S. (2015, March 24). Bracing for a big power grid attack: 'One is too many' Retrieved November 15, 2015, from http://www.usatoday.com/story/news/2015/03/24/power-grid-physical-and-cyber-attacks-concern-security-experts/24892471/

*Seaman, J. (2015, November). Internet of Things—The Fate We Make for Ourselves. Retrieved December 1, 2015, from http://www.isaca.org/Journal/archives/2015/volume-6/Pages/internet-of-things-the-fate-we-make-for-ourselves.aspx

Techopedia. (n.d.). What is an Embedded System? - Definition from Techopedia. Retrieved November 28, 2015, from https://www.techopedia.com/definition/3636/embedded-system

Trend Micro. (2015, September 17). FBI Warns Public on Dangers of the Internet of Things. Retrieved November 27, 2015, from http://www.trendmicro.com/vinfo/us/security/news/internet-of-things/fbi-warns-public-on-dangers-of-the-internet-of-things

U.S. Department of Health & Human Services. (n.d.). HHS.gov. Retrieved November 29, 2015, from http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

U.S. Food and Drug Administration. (2013, June 13). Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication. Retrieved November 29, 2015, from http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm