ASA

Annie Searle & Associates LLC

Research Note

The Harmonious Blend of Policy and Technology: The Need for an IoT Compliance Framework

Andy Herman

April 2017

Keywords: cybersecurity, Internet of Things, compliance, security framework

Abstract: This paper discusses the rising concerns associated with the Internet of Things, and the lack of a comprehensive cybersecurity compliance framework. The rising number of internet-connected devices has created increasing number of cybersecurity risks, as network of devices are hijacked for malicious purposes.

The first "networked device" was demonstrated in 1990 at the Interop Networking Conference where MIT researcher John Romkey and Simon Hackett presented an "Internet Toaster," where the researchers could control the settings of the toaster through a connection made through the internet.[1] It took another decade for these networked devices to become a popular trend and Kevin Ashton coined the term "Internet of Things."[2] Since then, the number of connected devices has rapidly increased. Strategy Analytics forecasts that the 1.4 devices per person average at the end of 2014 will nearly quadruple to 4.3 devices per person in the next few years, predicting over 33 billion connected devices by 2020.[3] There are many benefits to the connected devices - simplicity of installation and use; convenience and automation of daily tasks; potential for increased productivity and efficiency; and even new avenues for innovation. Though there are many advantages, the rapid increase of connected devices is paralleled by an increase in inherent risks for cybersecurity attacks. As technology continues to develop and improve the way tasks are handled, the development and enforcement of policies will help guide these new technological advances to have a greater positive impact.

The new products purchased today come with less and less documentation. If users are confused on how to set something up, they can typically refer to online searches to find answers. The simplicity of products has reached a point where the term "set-up" is synonymous to "plug in the power and turn it on." A common experience is now to pull things out of boxes and intuitively see exactly how to plug devices in and connect to a PC or mobile phone without referring to the user manual. These natural reactions to technological devices contribute to high risk of breach. Bruce Schneier, author and thought-leader in information security, recently commented about this complacent consumer attitude and lack of concern for security in connected devices by saying that "[t]he owners of those devices don't care. Their devices were cheap to buy, they still work, and they don't even know [the victims of DDoS attacks]. The sellers of those devices don't care: They're now selling newer and better models, and the original buyers only cared about price and features."[4] Though the interest in new technological devices is high, the understanding of what connected devices are is still lacking to many consumers. Per Accenture, 87 percent of the consumer had not heard of the term 'Internet of Things,' prior to the study.[5] With this consumer uncertainty of how devices create an "Internet of Things," hackers can exploit vulnerabilities using fewer resources.

One of the ways that compromised connected devices have been used maliciously has been the recent increase in distributed denial of service (DDoS) attacks. DDoS attacks do not take personal identifiable information from consumers but they can be nuisances to victims. Connected devices have been used to conduct DDoS attacks by using an army of infected devices and computers known as "botnets" that can be remotely controlled by the attacker to send traffic to a single target. By sending traffic to a single target by a large number of bots, you can overload the system and crash the system. To create a botnet, attackers spread the malware through clickable links on websites, emails, and social media. When people click on links that contain the malware, their computers become compromised and can be part of the botnet without detection. The MIRAI malware, which was responsible for creating disruptions to Dyn, is the latest example of the use of connected devices to DDoS an Internet service provider server.[6] The MIRAI malware has roughly 100,000 connected devices in its' botnet army and is expanding as infected devices conduct wide-ranging scans of IP addresses, with the intent of "locat[ing] under-secured IoT devices that can be remotely accessed using brute-force attacks".[7] With more awareness of the malware, hackers have become more creative in its ways to distribute the malware. Recently, MIRAI malware was found to use a new Windows Trojan with the name "Trojan.Mirai.1" which targets Window's PCs. Prior to this new attack vector, the MIRAI malware was mainly attacking Linux OS to scan the user's network for "compromisable Linux-based connected devices".[8] These recent discoveries demonstrate the rapid spread of malware and the constant adjustments that attackers are implementing to avoid detection and increase infection.

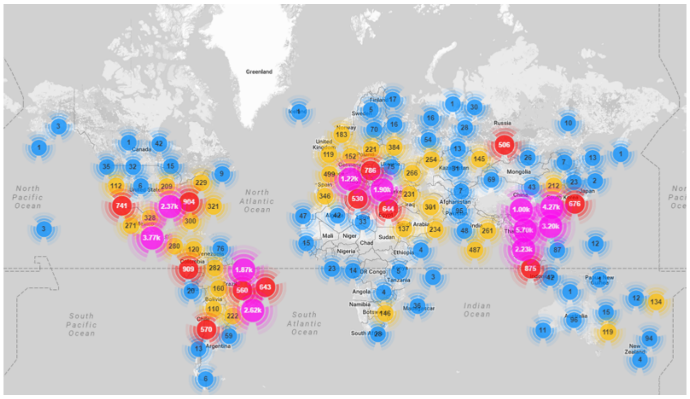


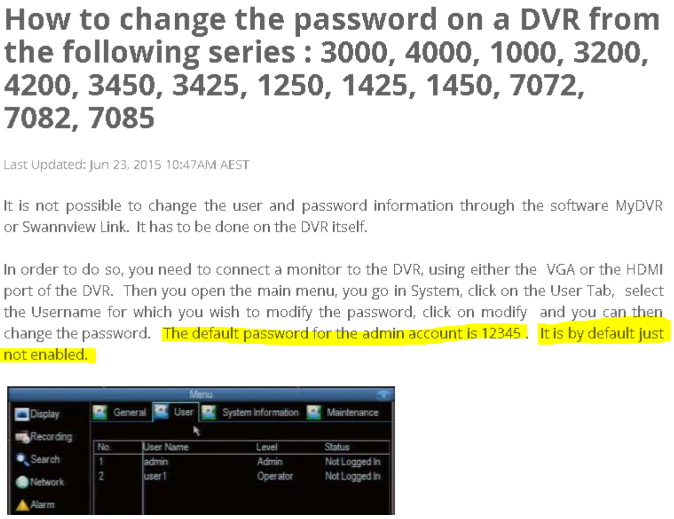
Figure 1: Geographic representation of where Mirai-infected devices are. (Bekerman et al, 2016)

The main reason why connected devices have helped hackers exploit this effective method of attack is that the devices themselves are shipped out from their manufacturers with default security settings. Default passwords are set on devices to reduce the complications of creating random passwords for each device being produced. Manufacturers and developers provide the option to consumers to change the default settings to something more secure to prevent the hassle of implementing random passwords on the thousands of products that they are manufacturing. A common example of this would be wireless routers: consumers have become more aware of setting passwords on their wireless routers to prevent others from using it without your permission. To help contribute to the increased awareness of the risk of not changing passwords and developing an awareness of cybersecurity, it is important that regulations be put in place to oversee products before they reach the consumer. This would ensure that consumers not follow old habits, forced to become more vigilant in their cybersecurity awareness.

Recently, there has been a huge push for security policy firms to research and publish guidelines to help companies become more aware of the security issues associated with IoT devices and guidelines to help mitigate some of these problems. The National Institute of Standards and Technology (NIST) published NIST 800-160: Systems Security Engineering, to provide guidance to software engineers to build secure systems.[9] Other groups like the Open Web Application Security Project (OWASP) group has created a working group "designed 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."[10] The increase in attention and research into connected devices is critical especially because of the impact that connected devices have on our lives. In fact, connected devices are slowly becoming a larger part of our daily routine that it should be considered one of the critical infrastructures in the U.S. Treating these devices as a critical infrastructure would help create a defensive mindset. Imagine attackers compromising healthcare connected devices and remotely shutting off all devices. Furthermore, think about what would happen if compromised connected devices can be traced back to a power plant and the attackers decide to DDoS servers in power plants. Manufacturers of connected devices must be regulated to provide security to this critical component of our infrastructure. There are many potential solutions that policies can help enforce, though these rules and regulations must blend with technology to create the most effective defense. First, connected device manufacturers should require users to reset default device passwords the first time a consumer turns on a device. This standard must be incorporated into software development requirements. In addition, there should be an international effort by groups that are conducting research into best practices to create a framework that manufacturers would want to become certified in to show that the products that they are selling are secure - like PCI compliance for the payment card industry.

Enforce Password Reset when Consumers Start their Device

Many connected devices such as refrigerators and thermostats often do not have a user-friendly interface. Some devices require connecting devices right out of the box to an application on a mobile phone. Others will allow users to simply select an "express set-up" to help with ease of use. Providing consumers fewer hassles is always one of the targets that manufacturers strive to achieve. In the pursuit of providing consumers with the most simple and user-friendly experience in using these new technological devices, manufacturers have resorted to setting default passwords to avoid the hassle of having to change the passwords for users.



How to change the password on a DVR from the following series : 3000, 4000, 1000, 3200, 4200, 3450, 3425, 1250, 1425, 1450, 7072, 7082, 7085

Last Updated: Jun 23, 2015 10:47AM AEST

It is not possible to change the user and password information through the software MyDVR or Swannview Link. It has to be done on the DVR itself.

In order to do so, you need to connect a monitor to the DVR, using either the VGA or the HDMI port of the DVR. Then you open the main menu, you go in System, click on the User Tab, select the Username for which you wish to modify the password, click on modify and you can then change the password. The default password for the admin account is 12345. It is by default just not enabled.

No.	User Name	Level	Status
1	admin	Admin	Not Logged In
2	user1	Operator	Not Logged In

Figure 2: Swann DVR Support Webpage showing the default password. (support.swann.com)

A simple search online for default passwords on connected DVR devices showed the webpage showing the DVR series number along with the default password and (vague) instructions on how to change and enable the passwords (Figure 2). The U.S. Computer Emergency Readiness Team (US-CERT) has issued an alert (TA13-175A) to address the risk and impact of not changing passwords. US-CERT has identified that “attackers can easily obtain default passwords and identify internet-connected target systems” and that exposed systems can be identified using “search engines like Shodan” to conduct their attacks on vulnerable systems.[11] One simple solution to decreasing the attack surface in connected devices would be to prompt consumers to reset their password after an initial start or factory reset. This would force consumers to reset default passwords to prevent systems being open to attacks by hackers.

International Effort to Create Internet of Things Security Framework Certification

Compliance to international frameworks and attainment of certifications by businesses are mainly done to show the customers that the business is providing the best standard of products and services. The most common and well-known certification is the Payment Card Industry Data Security Standard (PCI-DSS) certification which is a “widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information.”[12] Businesses will seek to become PCI-DSS compliant for their own benefits to prevent data compromise of sensitive financial information of customers, but also customers who have an understanding of PCI compliance will want to see that the business that they are interacting with is PCI-DSS compliant to have a sense of confidence that their data will be secure.

Like the credit card industry, there is a need for an increase in emphasis for manufacturers of connected devices to show that the devices that they are producing is compliant with international standards as a secure device. A consumer who buys a closed-circuit television expects that there are security controls in place to prevent potential hackers from watching them and their family. The domains for the proposed Internet of Things Compliance Framework should incorporate the common families and domains as seen in established frameworks such as the NIST 800-53 Rev 4: Security and Privacy Controls and the NIST Cybersecurity Framework. Alongside these domains, the working group should refer to research by well-known vulnerabilities research groups like OWASP to determine what are some of the greatest concerns. The "OWASP Top IoT Vulnerabilities," published in 2014, cite insecure web interface and insufficient authentication/authorization at the top of the list for vulnerabilities in connected devices.[13] Using the research that is continuously being conducted on the possible points of weakness, a security compliance framework should be created and implemented across the industry.

Recently, the IoT Security Foundation released the "IoT Security Compliance Framework." This framework divides the compliance into different compliance classes that focus on security objectives for confidentiality, integrity, and availability. This framework works more like a checklist that asks the questions of whether the manufacturer or consumer has met the list of requirements on their compliance framework. Upon analysis of this specific framework, the requirements are vague and do not focus on connected devices but rather the business practices. For example, Requirement 2.3.1.4 states, "the company follows industry standard cyber security recommendations (e.g. UK Cyber Essentials, NIST Cybersecurity Framework, etc.)."[14] Merely asking whether the manufacturer is implementing other cyber security recommendations does not provide clear expectations of a strong security posture. The difference between checklists and frameworks is that checklists often creates a sense of complacency by the organization using it because the certificate can be attained by showing how the company meets each requirement whereas frameworks tend to have procedures and guidelines to help guide and interpret the business to be at its desired security posture.

Despite some need for revision and improvement, the efforts by the IoT Security Foundation should serve as a model for the international community to contribute in the efforts of regulating and controlling the security of connected devices. As connected devices increase in its impact on daily lives, it is only a matter of time before connected devices are considered a critical infrastructure of the U.S. and across the world.

But Wait… Compliance Does Not Equal Security

Though creating frameworks and promoting compliance is beneficial in creating an awareness and a security-first attitude, compliance does not equal security. Former CEO of Target Gregg Steinhafel said "Target was certified as meeting the standard for the payment card industry in September 2013. Nonetheless, we suffered a data breach."[15] Security professionals will all agree that compliance to a set of rules or a framework is not enough. While the frameworks illustrate a set of rules and procedures that professionals have agreed upon as best practice, without an investment in blending the policy and the technology, data breaches can never be completed prevented.

Compliance to frameworks is the foundation for more secure systems. The creation for an

Internet of Things Compliance Framework is a call for the blend of policy and technology. Businesses must be willing to incorporate compliance frameworks to set the first step in motivating consumers to start understanding the changing threat environment. After establishing this baseline, consumers must be more aware of the "default effect" and try to adhere to the using the technology to help create a more secure environment. The 'default effect' by consumers is a psychological effect that reflects a natural acceptance of default settings because of three reasons: "(1) Effort: choosing the default option requires no physical action. (2) Implied endorsement: decision-makers may infer a default has been preselected due to its merit. (3) Defaults may result from reference dependence: the default option may represent a reference point which colors the evaluation of other may represent a reference point which colors the evaluation of other options as gains or losses."[16]

It is understandable that even with the best compliance framework and cooperation by manufacturers of connected devices, consumers must gain a better understanding of why simple controls such as changing default passwords to complicated password lengths are important. This education in cybersecurity is very like what is seen in healthcare. The goal of physicians is to make sure that their patients remain healthy enough so that the patients do not have to come visit them as much. Security professionals are just the same: they strive to create a system that is protected from data breaches so that the business runs smoothly. Physicians follow best practices of preventative medicine by suggesting vaccinations, exercise, and healthy lifestyles to their patients. Security professionals promote "cyber health" by suggesting strong passwords, encryption of hardware, and understanding of basic Internet behavior to the users. Despite the efforts of these professionals, not everyone is 100 percent healthy both in a physical and cybersecurity sense. However, because there are these controls and awareness in place, there is a reduced number of people who become ill and systems being breached. This must be the motivating factor for organizations to adhere to the compliance frameworks for Internet of Things devices. The blend of policy and technology is critical in the formation of a more secure connected device environment.

[1] Noler, C. "Timeline: A Brief History of the Internet of Things (Infographic)". *The Street*. 18 Oct. 2016. Web. 26 Jan. 2017.

[2] Postscapes. "Internet of Things (IoT) History". *Postscapes.com*.

[3] Waring, J. "Number of devices to hit 4.3 per person by 2020 – a report". *Mobile World Live*. 16 Oct. 2014. Web. 26 Jan. 2017.

[4] Schneier, B. "Lessons from the Dyn DDoS Attack". *Security Intelligence*. 1 Nov. 2016. Web. 30 Jan. 2017.

[5] Accenture. "The Internet of Things: The Future of Consumer Adoption". *Accenture Interactive*. 2014. Print. 7 Feb. 2017.

[6] Higgins, K. "DDoS on Dyn Used Malicious TCP, UDP traffic". *Dark Reading*. 26 Oct. 2016. Web. 8 Feb. 2017.

[7] Bekerman, D., Herzberg, B., Zeifman, I. "Breaking down Mirai: An IoT DDoS Botnet Analysis". *Incapsula.com*. 26 Oct. 2016. Web. 8 Feb. 2017

[8] Khandelwal, S. "New Windows Trojan Spreads MIRAI Malware to Have More IoT Devices". *The Hacker News*. 9 Feb. 2017. Web. 21 Feb. 2017.

[9] Block, C. "What does NIST 800-160 Mean for Quantification, FAIR, and IoT?". Linkedin Pulse. 16 Dec. 2016. Web 23 Feb. 2017.

[10] OWASP. "OWASP Internet of Things Project". 15 Feb. 2017. Web. 23 Feb. 2017.

[11] US-CERT. "Alert (TA13-175A): Risks of Default Passwords on the Internet". US-CERT. 7 Oct. 2016. Web 26 Feb. 2017.

[12] Rouse, M. "PCI DSS: Definition". Techtarget.com. May 2009. Web. 26 Feb. 2017.

[13] OWASP. "Top IoT Vulnerabilities". OWASP.com. 18 May 2016. Web. 27 Feb. 2017.

[14] IoT Security Foundation. "IoT Security Compliance Framework". IoT Security Foundation. 6 Dec. 2016 Web 27 Feb. 2017.

[15] Mello, J. "Target Breach Lesson: PCI Compliance isn't enough". *Technewsworld.com*. 18 Mar. 2014. Web. 26 Feb. 2017.

[16] Dinner, I., Goldstein, D., Johnson, E., Liu, K. "Partitioning Default Effects: Why People Choose Not to Choose". *Journal of Experimental Psychology*. Vol. 17. No. 4. 2011.