Cybersecurity and the Internet of Things

Christopher Biedermann
Emitel sp. z o.o., Poland
Department of Information Systems
Warsaw University of Technology

Abstract

Purpose/Thesis: The purpose of this paper is to use a recent cyber-attack to highlight the current state of readiness of Internet of Things (IoT) technologies with regard to security vulnerabilities as well as fundamental – in the author's opinion – changes that will need to take place within these industries and technologies to mitigate the overall cybersecurity risk.
Approach/Methods: The analysis of the findings from numerous existing published security studies.
Results and conclusions: The following conclusions were reached: (1) in the world becoming more and more interconnected through the web enabled devices (IoT devices), new forms of security threats have been developed; (2) at present IoT devices introduce a high level of vulnerability; (3) many of these risks may be mitigated with already existing technologies; (4) however, due to the fragmented and heterogeneous nature of the IoT devices, the implementation of even basic levels of security is more challenging than in the case of traditional Internet connected devices (e.g. personal computers); (5) the industry needs to face and address three key issues that will in turn help to mitigate the unique security threats posed by IoT devices, namely: the drive towards open standards, the industry cooperation and consolidation, and the improvement of consumer awareness.
Originality/Value: The value of the research is to highlight the security issues related to the Internet of Things and propose solutions that must be implemented to increase the level of security awareness within the IoT environment.

Keywords

Cybersecurity. Denial of Service Attack. Internet Security. Internet of Things.

Received: 21 November 2016. Reviewed: 27 December 2016. Accepted: 30 December 2016.

1. Introduction

In recent years, news of cyber-attacks has become relatively common place in the popular press. Consumers have learned to understand risks associated with surfing the net on their personal computers or smart phones, and in many cases have started to take increased precautions to minimize this risk. As Internet based technology however, has become more and more ubiquitous with connected devices now utilized in many more situations from wearable health trackers to industrial automation, the risk of cyber-attacks has expanded to these new connected devices. The idea that home monitoring cameras or smart TV's could be used to drive a large scale cyber-attack was not generally discussed in the popular media and was not generally considered by most users as a high risk area. The public perception of this however began to change in October 2016, when the press was full of news regarding a massive cyber-attack utilizing Internet connected devices. Although security

weaknesses of these Internet connected devices have been exploited in the past, the scale of this attack was unique in that it utilized millions of simple common place Internet connected devices to launch a coordinated attack and thus garnering space in the headlines.

These devices operate in realm of what is commonly called the Internet of Things (IoT), which broadly refers to all these devices and supporting platforms all connected through the Internet. The devices have changed many aspects of our daily lives and are expected to drive innovation across many industries over the upcoming years. Everyday objects are being combined through the Internet with each other and powerful applications in the cloud to transform the way we work live and play. As highlighted however with this case, these benefits do not come without new challenges, with security being one of the most significant. The potential of exploiting security weakness of IoT devices has certainly been on the radar of industry experts, and within profession literature much discussion as already taken place around it, however very little actual coordinated industry action has taken place to address these concerns.

The purpose of this paper is to use the October 2016 IoT attacks to provide a brief overview of the state of the industry today with regard to cybersecurity and IoT devices. Using the above attack as an example the paper will attempt to better highlight the challenges facing society as IoT connected devices become more and more prevalent. By looking to outline what is the IoT and how it operates, together with how attack of this sort can be executed, a proposal of what changes will take place in the industry is proposed. As such the paper will initially describe the IoT, the attack and address how such an attack could happen, then discuss what measures could limit the ability to launch such an attack and finally predict what effect this could have on the expected development of IoT technologies.

2. Background

2.1. The Internet of Things (IoT)

As noted above the Internet of Things or IoT, is a broad term used to refer to the growing universe of connected devices such as sensors, video cameras, remote meters, medical devices and broad list of consumer devices. The expansion of these connected devices promises to impact a multitude of aspects of how we work, live and plays. These devices are expected to impact everything from our basic home appliances such as washers and dryers to more complex home energy monitoring and feedback systems and even to how entire cities are managed. Installing sensors, monitors and switches that are all connected to the Internet into these devices, will bring a wealth of information online and into play for cloud based control and analysis. In addition to home uses, consumers will face more and more Internet connected devices that are imbedded in our cars and road infrastructure such as roads and lights. Outside of homes other industries are becoming increasingly connected. By design then these devices will all be interconnected with each and with the Internet overall allowing for unprecedented levels of information sharing.

The spread of these connected devices is still believed to be in its early stages but is growing rapidly. According to Gartner it is expected that the IoT universe will encompass 20.8 billion devices worldwide by 2020 (Columbus, 2016). In the telecom equipment producer

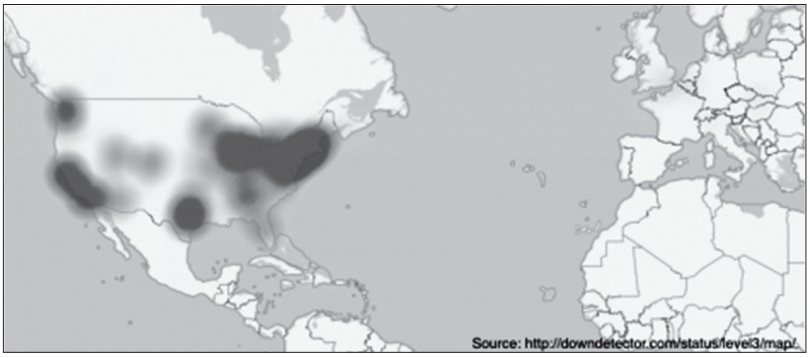
Ericsson's latest Mobility Report (Ericsson, 2016), it was stated that they believe that IoT connections will overtake phone subscriptions by 2018. Along with the rapid growth of IoT devices and technologies comes unique challenges. One of the biggest challenges facing the further expansion of IoT technologies is addressing the unique security challenges that they present. The Internet of Things is a blend of many technologies, all of which have their own traditional security and privacy flaws and in many cases the technologies have not had time to consider to full security risks. Compounding this challenge is the vast number and diversity of participants operating in the IoT sphere from hardware producers to systems designers, each developing platforms based upon their own needs and requirements with little regard for integration with the myriad of other devices connected to the web. For example, as noted in a recent Harvard Business Review article (Rezendes et al., 2016), it is estimated that 85% of the American critical infrastructure (electric grid, gas and oil pipelines, bridges and tunnels) are in the private sector where cybersecurity is fragmented with no consistent systems to ensure sharing of cybersecurity data and standards. The new IoT technologies will require the industry as well as consumers to review what it means to be sure from a cybersecurity perspective.

2.2. October DDoS Attack

A noted in the introduction the recent cyberattack will be used as an example to illustrate how these weaknesses can be exploited. On October 16, 2016 an unknown group launched an attack on the domain name server (DNS) service managed by Dyn, a company not generally well known to the public but one that provides backbone support many household names. By blocking the services that this company provided, more than 80 major websites including Twitter, Amazon, Netflix were adversely affected. A DNS service, in general, is a global database that translates domain names to Internet addresses that are used by computers to talk to each other. This allows consumers to type in well recognized names such as "www.amazon.com", rather than having to type in actual service addresses and understand anything about how these pages are routed along the Internet. The sites that were impacted utilized the managed DNS service from Dyn to facilitate the connections of visitors to their websites. Thus by launching an attack on the Dyn servers, the attackers effectively took down a large cross section of commercial web pages (See Fig.1).

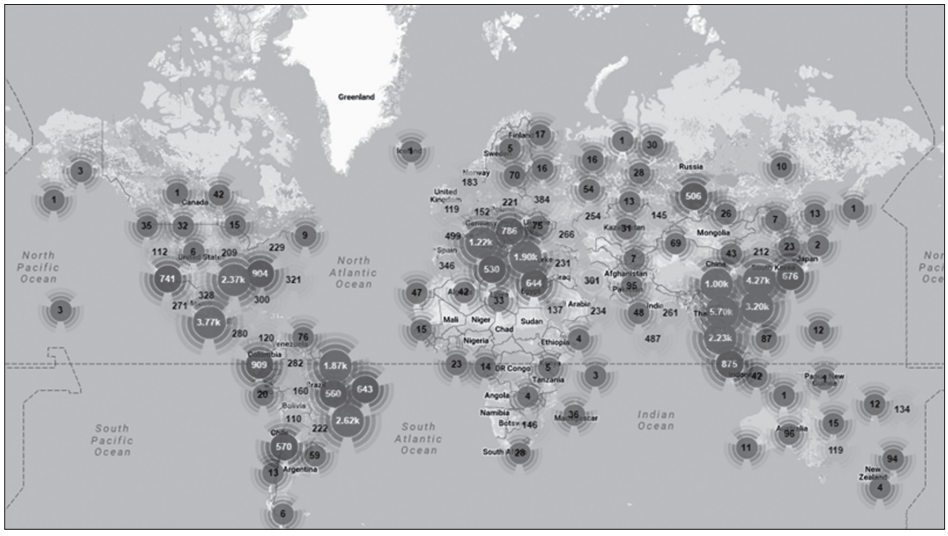
The type of attack that was used was a form of a Denial of Service (DoS) attack, which is when an attack on a machine or network is flooded by a large volume of superfluous requests. The impact of these requests is to over-load the resources, making it unavailable to users for its intended purposes. In this case the attack was a specific form of a DoS attack called a Distributed DoS (DDoS) attack. This is one where these requests are sent by multiple and in many cases geographically distributed machines from across the globe. DDoS attacks have become more common places over the last years, however prior to this October attack, these distributed requests were typically sent by hijacked PC's and computers that were infected with software called botnets. A botnet is defined as a collection of Internet-connected user computers infected by malicious software that allows the computers to be controlled remotely by an operator to perform automated tasks, such as stealing information or launching attacks on other computers. The unique aspect of this attack was that in this case, the compromised devices were not typical computers and home PC's but rather lower level unprotected IoT devices such as cameras and smart TV's.

Fig. 1. Map of areas DDoS attack in October 2016 (Hamblen, 2016)



In order to execute this attack a malicious piece of software, a botnet called Mirai was used. Based upon information published by Imperva Incapsula (Zeifman et al., 2016), a security firm who analyses such attacks, the IP addresses of Mirai-infected devices were spotted in 164 countries worldwide (See Fig. 2). As further analyzed and described by Imperva Incapsula, the Mirai botnet was and still is specifically targeted to attack IoT devices to launch DDoS attacks from commands issued from a command and control server. This botnet was designed to find easy targets by performing an automated scan of Internet addresses to locate poorly secured devices that could be readily accessed using easy to find login credentials. The software was then able to break in and install itself on these devices by using a crude form of hacking, referred to as the brute force technique.

Fig. 2. Geo-locations of all Mirai-infected devices uncovered so far (Zeifman et al., 2016)



In an analysis completed by Zscaler (Desai, 2016), a cloud based information security company, the devices that were most vulnerable and therefore most likely hijacked were home security systems, home monitoring cameras and smart TVs. Common security

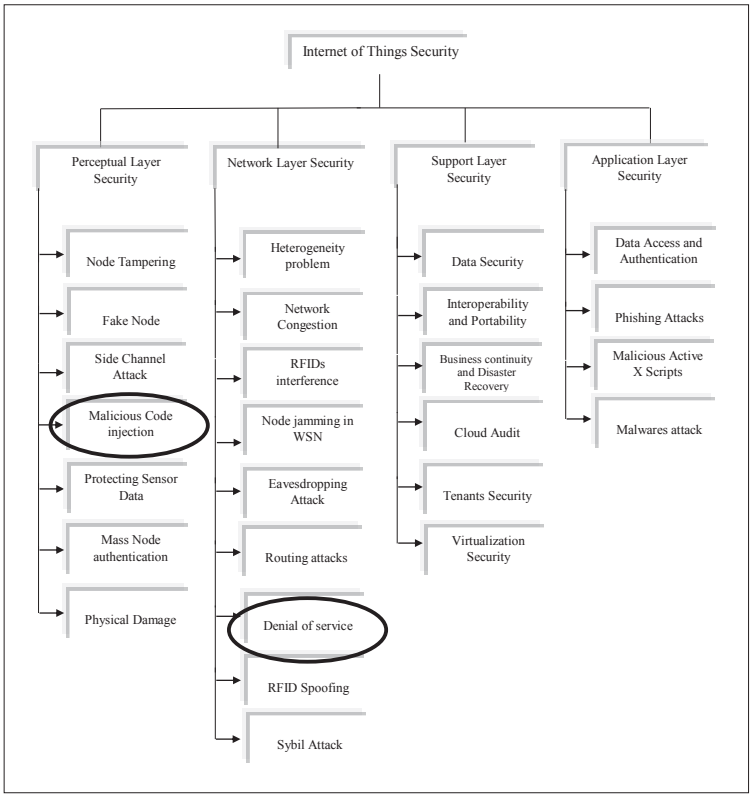
weaknesses found in these devices included weak login controls often using a predefined password and unencrypted communication.

The speculation in the industry is that we have not yet seen the last of the Mirai botnet, given how widespread its infection is estimated. It should be noted that in early November 2016 a large infrastructure provider in Liberia was also knocked offline through an attack from this same botnet.

2.3. Other Threat Examples

Although the focus of this paper thus far has been on this type of DDoS attack it should be highlighted that this attack is only one of many security weakness already identified related to IoT devices. The technology is also susceptible to a myriad of other security weaknesses. In an August 2016 paper published in the *International Journal of Computer Science and Information Security*, the authors map out numerous types of security threats that the IoT system may be susceptible too (Inayat et al., 2016). Figure 3 reproduced from this paper is included to give a flavor for the scale and complexity of IoT security risk that exist, with a DoS type of attack (highlighted in orange) being just one branch of this tree.

Fig. 3. IoT Security and Threats Summary (Inayat et al., 2016, 458)



With so many potential threats to IoT devices and given that all IoT devices are in a sense interconnected, a weak link in any one device can put many other devices and networks in the chain at risk. The exploitation of a security threat on one type of device can in effect threaten an entire system of devices. To highlight this and provide an additional interesting example another vulnerability namely, "malicious code injection" (the blue circle in Fig. 3), we can look at a recent study done by Weizmann Institute of Science in Israel (Ronen et al. 1). In this paper the group demonstrated how an IoT worm could take down the entire lighting for an entire city by exploiting weakness in the wireless connectivity of Phillips Hue smart lamps. As described in the paper

> the worm spreads by jumping directly from one lamp to its neighbors, using only their built-in ZigBee wireless connectivity and their physical proximity. The attack can start by plugging in a single infected bulb anywhere in the city, and then catastrophically spread everywhere within minutes, enabling the attacker to turn all the city lights on or off, permanently brick them, or exploit them in a massive DDOS attack (Ronen et al., n.d.,1).

2.4. Implications

Denial of service attacks utilizing computers or PC's can be traced by to the 1990's and are still common place today. As reported by a recent survey done by AT&T:

> The first documented denial-of-service attack over the Internet occurred in February 2000. (...) DDoS attacks have since become common, with 73% of global survey respondents reporting at least one DDoS-related issue in the past year (AT&T, 2016, 10).

The survey additionally noted that

> More than 90% of attacks logged by AT&T are known attacks or their variants – not zero-day attacks (e.g. new forms of attacks) (AT&T, 2016, 24).

These examples clearly highlight the challenges faced today combating these attacks utilizing more powerful devices such as desktop PC's which translate into a much greater challenges when dealing with less sophisticated IoT devices.

These challenges will get further amplified as IoT devices become more ubiquitous and at the same time take on more critical functionality (e.g. critical medical sensors, self-driving cars). As noted in the same AT&T survey,

> AT&T has recorded a 3.198% increase in IoT vulnerability scans over the past three years" (AT&T, 2016, 14),

highlighting again the increasing importance that IoT security will play in the coming years.

The implications of the recent attack are twofold, in the first case it demonstrates in a much more public manner that warnings that have been issued to date are in fact warranted and thus highlights the critical vulnerability of IoT devices. However a second implication is to raise the awareness of the risk now in what are still the early stages of IoT development and thereby to ensure that steps are taken sooner rather than later to improve the security profile. As noted by the US President Barack Obama shortly after the attack, we now face the challenge of

> how do we continue to get all the benefits of being in cyberspace but protect our finances, protect our privacy. What is true is that we are all connected. We're all wired now (Hamblen, 2016).

This attack then has raised the overall level of awareness of the public that the specter that furthers such attacks will most likely come, and that action is needed by designers and producers of these devices, regulatory bodies as well as consumers.

3. Minimum Level Security Enhancements

As highlighted by these attacks, the baseline level of protection on many IoT devices are far from adequate. In a survey completed by the IoT security foundation (Seals, 2016), it was estimated that less than 10% of IoT devices in the market are designed with adequate security.

There are already in existence a number of basic security enhancements that can be implemented with minimal changes utilizing existing tried and tested methods. These basic enhancements would simply be implementing solutions that have been tried and tested on existing web platforms for the mitigation of the risk of such attacks. These fixes range from better password control and use of encryption technologies to firewall protection or use of gateway controls. Outlined below is an overview of some these measures as well limitations.

3.1. Improve Login Control

One of the primary factors that allowed this attack to occur was the fact that many simple consumer IoT devices come preconfigured with a standard username and password that is often times not changed by the user prior to use. In some cases the passwords to the devices were even hard-coded in the device, making them impossible to change. These default usernames are often easy to determine and in many cases can simply be looked up on the Internet.

A clear simply fix for this would be educating users to create new custom logins as part of the activation process before the device could be used. Another simple fix that could be implemented by industry would be a limit on login attempts or longer delays between log-ins in order to thwart brute force attacks. Although this fix would most likely not go far enough in the long term, as it will just be a matter of time until this a more sophisticated attack takes place that can override this, it would provide a vast improvement to the current security situation.

The key challenged here is simply providing for the urgency of the device manufactures to execute these changes as well as education on the part of consumers as to their importance. Given the fragmented industry with a high degree of cost competition on many of these devices, getting a concerted action within the industry as structured today, without regulatory pressure is a clear challenge.

3.2. Utilize Existing Encryption Techniques and Enhanced Device Protection

In many cases, and especially with home devices, basic encryption systems are not yet implemented on a consistent basis leaving exposed the ability to not only extract confidential information but also to highjack the machines by issuing direct remote instructions (as

with the Mirai attack). The current multitude of IoT devices and specifically those that are used in home and consumer applications do not always make use of these encryption techniques in a consistent manner. There are available encryptions techniques such as AES and RSA that have proven to be quite effective and secure and in many cases could be used to significantly increase the level of security. Other existing encryption methods include the use of public keys systems that ensure that only authentic code from a trusted source is allowed to run on the device. Similar to the prior point, the challenge are inherent in the nature of the industry, fragmented with a high level of cost competition. Thus the impetus for change will also need to come from other sources such as regulating bodies and a more educated consumer base.

3.3. Use of Automated Device Updates

Another measure of security that has proven effective with devices such as personal computers and phones would be to allow devices to get automatic updates. As for example with Microsoft Windows, or IOS which are used to patch security weaknesses as they are detected or to imbed more sophisticated encryption systems and adaptability. As security flaws become identified the automatic update of the operating platforms of these devices could implement on the fly fixes for them. This fixes however may require processing capacity on the device that is currently available, especially in the case of simple one function sensors.

3.4. Use of Anti-Virus/Malware Software

A measure commonly used with personal computers, servers and other higher level computing devices is the installation of protective software, such as anti-virus programs. The use of such measures however is vastly more complicated in the realm of IoT given the sheer number of potential devices and the lower computing power inherent with them. However, certain hybrid solutions have already become available whereby a connected computer scans all devices on the network to determine which ones are vulnerable to threats. For example, Rapid7, an Internet security company following the Mirai attack released a scanner designed to search users' networks and find common IoT devices with default usernames and passwords.

3.5. Firewall Protection and Gateway Controlling

An inherent problem in some of the above fixes is the limited processing overhead that some of these devices contain. A basic web connected on/off switch or video camera, by design is constructed with minimal overhead in part to ensure lower energy consumption. Thus a more involved solution would include the separation of the devices from the direct interaction with the broader Internet through some form of a central gatekeeper. This central gatekeeper would be designed with enough overhead to allow for the execution of the multiple security solutions such as those mentioned above. By managing the data flow of the many IoT devices in a more consolidated manner defenses to attacks could be elevated to a higher level in the structure which has better ability to react to such attacks. Software to detect and eliminate viruses and malware would be significantly easier to maintain and

update on one central machine rather than across a larger group of smaller heterogeneous devices. This benefit comes from not only the sharing of threat resources but the ability to put in place higher processing capacity machines between the device and the web. The execution of this solution however inherently requires a much higher degree of industry cooperation and standardization for communication protocols, some of the key limitations further discussed in the next section.

4. Core Issues and Current Limitations

As highlighted, even these relatively simpler changes face greater challenges in the IoT environment due to a number of factors. One of the first notable issues is related to the lower level of processing overhead available in many IoT devices. Compounding this concern is the overall lack of standards at present in the IoT universe with a large number of hardware producers each developing systems based upon their own needs, which do not necessarily factor in coordination with those from other producers. Finally, one of the more critical points is a relatively low level of consumer awareness around the risks associated with typical IoT devices and sensors.

4.1. Processing Overhead

The inherent low processing overhead of end IoT devices represents one of the key development challenges. Many of these devices are by design meant to be low overhead and lower power consumption devices. Price is also a big factor, and the more overhead there is the greater the final consumer price of the device. This in turn limits the amount of sophisticated protection that could be built into the devices. A tradeoff therefore exists, between efficiency and cost of the device, which is crucial as we continue to rollout a large numbers of simple single function devices, on one hand, and higher computing power overheads to allow for more sophisticated security schemes on the other. As noted in the prior section this could be addressed partially through a central gatekeeper, however this solution is hampered by a lack of standards needed for effective communication.

4.2. Lack of Standards

Therefore a key critical overriding issue is related to the ability to implement these changes with a very low degree of industry standardization. This refers to both definitions and certifications as to what are the minimum security level required, as well as a lack of technical standards and protocols that allow the effective communication between devices from different producers. For example, in order to effectively execute a gateway controlling mechanism as mentioned in the last section, the myriad of devices need to be able to "talk to each other" in an effective manner. This in turn requires standardization of communication protocols which today does not exist across the industry. Thus an IoT thermostat system from Nest and a home appliance controller from Samsung would need to be able to communicate both with each other and another third party gatekeeper. This unfortunately does not work in practice today, due to a lack of a common language, e.g. communications standards and protocols.

4.3. Fragmentation of the Industry

With fragmented and diverse market of many thousands of producers of IoT devices and the focus on low cost devices, there are significant barriers to incentivize many these changes. Given the fragmentation and heterogeneous nature of the devices, at present it is even difficult to answer the basic question as to how many IoT connected devices are in service let alone provide a more transparent system to control them. This in turn then makes standardization initiatives as described above move much slower or not at all in many cases.

4.4. Consumer Awareness

Finally, last but certainly not least is an inadequate level of awareness of consumers regarding the vulnerabilities of these connected devices. At the time of the October attack the average consumer was most likely not aware that their home Internet connected cameras could be hijacked to execute a coordinated attack with other devices. Since the attack, the level of awareness may have been raised but is still not at the level required. Consumer will need to be a key drive to demand device producers to factor in enhanced security controls on the products they sell. In a fragmented industry, consumers will need use their buying power to put pressure on manufacturers to address security risk. Additionally consumers need to take responsibility on themselves to adhere to basic level actions such as changing password from default ones before putting these devices on line.

5. Expected Industry Changes

Therefore in order for a more concerted and significant effort to improve cybersecurity in the IoT connected world a number of more structure changes within the industry will need to take place. As noted above even simpler tried and tested security defenses are inherently more challenging in the IoT realm. Outlined below is a summary of certain fundamental factors and changes that need to take place to drive the security environment.

5.1. Drive for Open Standards

The lack of standardization has become one of the hotter topics of the IoT world. This issue is reflected not only in the need to develop standards and norms from a security perspective but as well from an overall technological development perspective. The existing protocols and models do not effectually meet the needs of the IoT and the lack of overall standards is a hindrance for development of more effective security. Without standards the execution of fixes discussed in section four, will be difficult to implement. In particular the implementation of any form of common gateway controlling devices to provide a buffer for lower level IoT devices from multiple manufactures is next to impossible. In addition to simply having standards, the standards need to be open. Given the heterogeneous nature of devices, the security requirements, attack vulnerabilities and computing overhead available for security vary widely between these devices. Simple sensor devices generating

a one number standard output only will require a different set of abilities, than a more sophisticated device engaging in two way communication. Open standards will allow for the ability develop and customize the protocols as new needs arise as well as allowing for a degree of customization when required, structured however upon a clear backbone of defined standards.

Impetus is already starting to develop, and should be expected to continue with combined calls to action from consumers, regulators as well as industry group. Many of the Internet setting standard groups such as, The Internet Architecture Board (IAB), the IETF, and the Internet Research Task Force (IRTF) have ongoing projects to address different aspects of the IoT and IoT security. Additionally regulatory agencies are working with industry groups to address issues of interoperability, communication protocols and security. For example, following the October attack, the U.S. Commerce Departments and the National Telecommunications and Information Administration (NTIA) initiated a process to

> develop a broad, shared definition or set of definitions around security upgradability for consumer IoT, as well as strategies for communicating the security features of IoT devices to consumers. One initial step will be to explore and map out the many dimensions of security upgradability and patching for the relevant systems and applications (NTIA, 2016).

Other highlights include a workshop held in October 2016 by the Internet Architecture Board (IAB) to address

> concerns about the status of software/firmware updates for Internet of Things (IoT) devices. IoT devices, which have a reputation for being insecure at the time when they are manufactured, are often expected to stay active in the field for 10+ years and operate unattended with Internet connectivity (IAB, 2016).

A key take away from this meeting includes the agreement that a form of standardized secure updating process is required, with feedback being solicited a present to determine how best to address this need.

On last example of this from the industry group, the Institute of Electrical and Electronics Engineers (IEEE) which has begun to issue standards that address security elements applicable to the Internet of Things (Grau, 2016). These include a standard for Public-Key cryptography, encryption of data on fixed and removable storage devices, the security of printers, copiers and similar devices, as well as security of Media Access Control (MAC).

5.2. Industry Cooperation and Ultimately Consolidation

Although there are no industry standards in place today, the actual companies building IoT devices must start and be proactive and help lead the drive for standards. A gradual cooperation among key industry players is therefore expected. Critical for effective response to security threats to IoT devices is much greater cooperation and sharing of information amongst device producers. In contrast to more established technologies such as the PC market, the number of companies involved in the production of IoT related devices is immense. Not only are the number of companies operating in this segment large but also diverse, encompassing software and hardware vendors, end to end providers as well as connectivity providers. This makes the effective communication and sharing of threat

data extremely difficult. Nonetheless it appears that the larger players are beginning now to gradually implement this. This is expected to take place not only through a gradual development of industry standards but also more critically an actual consolidation of the numbers of companies operating in the market. Thus industry consolidation is both unavoidable and necessary. As an example to this, in November 2016, one month after the attack on the Dyn services mentioned earlier, Dyn was purchased by Oracle, one of the world largest IT providers, for $600 million (Lunden, 2016).

Other segments of the industry have already begun to take some unified action with regard to standards. As in the case of the companies operating in the electrical power infrastructure and industrial automation markets, who have begun to cooperate through the International Electrotechnical Commission (IEC) and have set out security requirements for equipment operating within the North American power grid. This standard (known as IEC-62443), is a security standard for industrial automation and control systems that creates a baseline that device manufactures must meet when developing their products. This will allow devices that meet these standards to be sold with a stamp of certification. As time goes on, it is expected that other industry group will create their own set of sub-industry standards specific to their needs which can then be merged across industries to create baseline standards for all devices.

Furthermore beyond simply developing open common standards the industry will need to develop a system to increase common awareness of attacks. This can be achieved through information sharing or common security monitoring systems to jointly detect intrusion. At a minimum a more rigorous forum for information sharing on timely basis among the industry will be for the common good of all participants. A consequence of this increased cooperation among IoT device manufactures is another factor that will contribute to the eventual consolidation of the device producer market.

5.3. Consumer Education

Finally it is not enough to wait for government bodies or industry group to address this, the impetus must come from the user, the consumer. Ultimately in order for industry changes to take place there must be drive on the part of consumers. Consumers need to demand that the devices they purchase offer a reasonable or acceptable level of security for common use. It cannot be expected that average consumers know the details of security and evaluate whether devices they are purchasing are fully secure. Given all the complexity involved this would be a self-defeating approach to improve IoT security. Thus the earlier the IoT industry overall begins to proactively embrace standards and increase both consumer awareness and comfort of devices the better overall for the industry. A continued stream of news of attacks will drive demand from the consumer side while at the same time increasing the specter of more government involvement. In the United States in November of 2016, the members of Congress began to issue warnings to the Federal Trade Commission (FTC) that the department needs to issue new warnings to consumers and new advice to connected-device manufacturers to address security of IoT connected devices. Two members of Congress, Pallone and Schakowsky asked that the FTC

> immediately use all the tools at its disposal to ensure that manufacturers of IoT devices implement strong security measures to best protect consumers from cyberattacks (Schakowsky, 2016).

Therefore if the industry will ultimately be forced to take further measures under government mandates and the sooner they begin this proactively the less likely that the changes will be mandated by government agencies. Action slowly starting to take place and it can be expected that further changes will be driven by professional industry groups a form of certification along similar lines as the Underwriters Laboratories (UL) or CE safety ratings. These certifications will then provide a standard that the average lay consumer can rely on when making informed purchasing decisions of IoT based products.

6. Conclusion

In summary, the number of Internet connected devices will continue grow at a rapid pace over the upcoming years, enhancing the lives of many people. Together with all the benefits and opportunities that come from these connected devices there are downsides in the form of significant cybersecurity risks. Although many solutions already exist to mitigate these risks, given the nature of these devices, execution will be a significant challenge. Therefore we should expect that the fundamental changes in the industry and technologies as described above will need to take place along with the growth of this technology.

References

AT&T (2016). The CEO's Guide to Navigating the Threat Landscape [online]. *AT&T Cybersecurity Insights*, 4 [22.11.2016], https://www.business.att.com/cybersecurity/docs/vol4-threatlandscape.pdf

Columbus, L. (2016). Roundup Of Internet Of Things Forecasts And Market Estimates [online]. Forbes, 27 November [27.11.2016], http://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#7b0d01844ba5

Denial of Service Attack (2016). In: *Wikipedia, The Free Encyclopedia* [online] [10.11.2016], https://en.wikipedia.org/wiki/Denial-of-service_attack

Desai, D. (2016). IoT Devices in the Enterprise [online]. *Zscaler Corporate Reaserach Blog*, 15 November [20.11.2016], https://www.zscaler.com/blogs/research/iot-devices-enterprise

Ericsson (2016). Internet of Things to Overtake Mobile Phones by 2018: Ericsson Mobility Report [online]. 2016–06-01 press release [11.11.2016], https://www.ericsson.com/news/2016987

Grau, A. (2016). IoT Security Standards – Paving the Way For Customer Confidence [online], *IEEE Standards University*, 29 February [10.11.2016], http://www.standardsuniversity.org/e-magazine/march-2016/iot-security-standards-paving-the-way-for-customer-confidence/

Hamblen, M. (2016). DDoS Attack Shows Dangers of IOT Running Rampant [online], *Computerworld*, 25 October [10.11.2016], http://www.computerworld.com/article/3135285/security/ddos-attack-shows-dangers-of-iot-running-rampant.html

IETF (2016). Internet Engineering Task Force, Workshop on Internet of Things (IoT) Software Update (IOTSU) [online], 8 October [10.11.2016], https://tools.ietf.org/html/draft-farrell-iotsu-workshop-01

Inayat, A.; Sabir, S.; Ullah, Z. (2016). Internet of Things Security, Device Authentication and Access Control: A Review. *International Journal of Computer Science and Information Security*, 14(8), August, 456–466.

Internet Architecture Board (2016). Internet of Things Software Update Workshop (IoTSU) [online] [25.11.2016], https://www.iab.org/activities/workshops/iotsu/

Internet Society (2015). Botnets [online], *Internet Society Policy Briefing*, October 30 [15.11.2016], http://www.internetsociety.org/policybriefs/botnets

Kolkman, O. (2016). Trust Isn't Easy: Drawing an Agenda from Friday's DDoS Attack and the Internet of Things [online], *Internet Society Tech Notes*, 24 October [12.11.2016], https://www.internetsociety.org/blog/tech-matters/2016/10/trust-isnt-easy-drawing-agenda-fridays-ddos-attack-and-internet-things

Lunden. I (2016), Oracle Acquires DNS Provider Dyn, Subject of a Massive DDoS attack in October, [online], *Techcrunch* , 21 November [21.11.2016], https://techcrunch.com/2016/11/21/oracle-acquires-dns-provider-dyn-subject-of-a-massive-ddos-attack-in-october/

NTIA (2016). US Department of Commerce, *Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching* [online], 24 October [5.11.2016], https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security

Rezendes, C.; Stephenson, W.D. (2013). Cyber Security in the Internet of Things [online], *Harvard Business Review*, 21 June [26.11.2016], https://hbr.org/2013/06/cyber-security-in-the-internet

Ronen, E.; O'Flynn, C.; Shamir, A.; Weingarten, A.-O. (n.d.). *IoT Goes Nuclear: Creating a ZigBee Chain Reaction* [online], Weizmann Institute of Science [21.11.2016], https://eprint.iacr.org/2016/1047.pdf

Seals, T. (2016). Survey – Less Than 10% of IoT Devices Keep Data Secure [online], *IoT Security Foundation*, June [16.11.2016], https://iotsecurityfoundation.org/survey-less-than-10-of-iot-devices-keep-data-secure/

Schakowsky, P. (2016). Pallone & Schakowsky Urge FTC to Strengthen Security of IoT Devices Following Recent Cyberattack [online], 3 November [28.11.2016], https://schakowsky.house.gov/common/popup/popup.cfm?action=item.print&itemID=3356

Schneier, B. (2014). The Internet of Things Is Wildly Insecure And Often Unpatchable [online], *Wired*, 6 January [20.11.2016], https://www.schneier.com/essays/archives/2014/01/the_internet_of_thin.html

Sheridan, K. (2016). New Free Mirai Scanner Tools Spot Infected, Vulnerable IoT Devices [online], *Dark Reading*, 11 August [16.11.2016], http://www.darkreading.com/perimeter/new-free-mirai-scanner-tools-spot-infected-vulnerable-iot-devices-/d/d-id/1327436

Zeifman, I.; Bekerman, D.; Herzberg, B. (2016). Breaking Down Mirai: An IoT DDoS Botnet Analysis [online], *Imperva Incapsula*, 26 October [23.11.2016], https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

Cyberbezpieczeństwo i Internet Rzeczy

Abstrakt

Cel/Teza: Celem artykułu jest wykorzystanie przykładów niedawnych cyberataków do przedstawienia obecnego stanu przygotowania technologii Internetu Rzeczy (IoT) wobec zagrożeń bezpieczeństwa oraz podkreślenia fundamentalnych, zdaniem autora, zmian, które muszą nastąpić w przemyśle i technologiach IoT, aby zminimalizować ogólne ryzyko związane z cyberbezpieczeństwem.

Koncepcja/Metody badań: Problem przedstawiono w artykule na podstawie analizy i interpretacji wyników badań dotyczących cyberbezpieczeństwa, opublikowanych w licznych studiach i sprawozdaniach.

Wyniki i wnioski: Wnioskami z tej analizy są następujące kluczowe kwestie: (1) w świecie, w którym urządzenia są coraz silniej z sobą powiązane poprzez łącza internetowe (urządzenia IoT, Internetu Rzeczy) powstały nowe formy zagrożenia bezpieczeństwa; (2) obecnie urządzenia te są w dużym stopniu podatne na ataki; (3) istnieją dziś technologie, które można zastosować, aby złagodzić wiele

spośród tych zagrożeń; (4) jednakże, ze względu na rozdrobniony i heterogeniczny charakter urządzeń IoT, zapewnienie nawet podstawowego poziomu bezpieczeństwa jest znacznie większym wyzwaniem niż w przypadku tradycyjnych urządzeń podłączonych do Internetu (np. komputerów osobistych); (5) przemysł musi skierować uwagę na trzy podstawowe zagadnienia, które pomogą zmniejszyć te szczególne zagrożenia bezpieczeństwa stwarzane przez urządzenia IoT, tj.: wykorzystanie otwartych standardów, współpraca i konsolidacja przemysłu, poprawa świadomości konsumentów.
Oryginalność/Wartość poznawcza: Artykuł służy naświetleniu problemów bezpieczeństwa związanych z Internetem Rzeczy oraz zaproponowaniu pewnych rozwiązań, które należy wprowadzić, aby zwiększyć poziom świadomości bezpieczeństwa w środowisku IoT.

Słowa kluczowe

Cyberbezpieczeństwo. Atak DoS. Atak Denial of Service. Bezpieczeństwo Internetu. Internet Rzeczy.

CHRISTOPHER BIEDERMANN is currently a PhD student at the Warsaw University of Technology, Department of Information Systems. Prior to entering into the PhD program he has worked in a number of companies in the technology sector and is currently a management board member at Emitel in Poland. In addition he has received a MBA from the University of Texas-Austin in 1994 and a B.S. from Lehigh University in 1989. His present studies are focused on researching solutions how to develop standardized communication protocols and machine learning principles for the Internet of Things.

Contact to the Author:
cfbieder@hotmail.com
Emitel Sp. z o.o.
ul. Wołoska 22
02–675 Warszawa