A literature review of Internet of Things security

Blair Urish
Kansas State University
College of Engineering
Department of Computer Science

Dr. William Hsu
Professor
Department of Computer Science

May 4, 2017

Abstract

The Internet of Things (IoT) is a rapidly growing industry with lots of potential for innovation. Due to this rapid growth, it is important that the security risks IoT devices face are properly identified and addressed. In the literature, numerous security risks have been identified in every layer of the IoT architecture. These risks include distributed denial of service, unauthorized access, and many others. In order to mitigate these risks the literature has suggested tailoring existing protocols to the constrained hardware found in the IoT. These protocols include Datagram Transport Layer Security (DTLS) and the Host Identity Protocol (HIP). In the literature, several extensions to DTLS and HIP were proposed. The literature generally found that HIP outperformed DTLS. However, a gap was identified in the research due to some authors not comparing their results to the protocols without optimization. This results in the optimizations being hard to compare. Governments are also considering taking action to ensure the security of the IoT. In the European Union, a labeling requirement for devices has been proposed. In the U.S., the FTC has only recommended general cyber security legislation and would prefer that the industry remain self-regulating. Currently, the FTC is under new leadership so it is not yet clear when or if any action will be taken.

Contents

List of Figures

Introduction

This section will discuss background information regarding the security of the Internet of Things, give a brief overview of the current research, describe the specific purpose of this report, and briefly outline the overall structure of the report.

Historical Background

By 2020, it is expected that there will be 25 billion Internet of Things (IoT) devices connected to the Internet. (Martínez, Mejía, and Muñoz, 2016). With so many devices, it is important that manufacturers take security very seriously. In September 2016, a security researcher named Brian Krebs had his website temporarily taken down due to a distributed denial of service attack. The attacker used thousands of malware-infected IoT devices and sent 600 gigabits per second of traffic to Krebs' blog. (Krebs, 2016b). The malware, called Mirai, infected IoT devices with poor security. An analysis showed that the devices were mainly CCTV cameras, DVRs, and routers. (Herzberg, Bekerman, and Zeifman, 2016).

A few months later, in December 2016, SEC Consult discovered a backdoor in Sony IPELA Engine IP Cameras that allowed for full remote access over the Internet. (SEC Consult, 2016). The backdoor could allow an attacker to install malicious code on the device. At the time of the disclosure, there were at least 4,250 devices at risk. (Krebs, 2016a). Owners of the affected devices must manually update them to be safe from potential attack. No malware has targeted these devices yet, but it is possible that may change in the future if the owners do not update their devices. Overall, these two incidents are just a few examples of the problems with IoT security.

Overview of Current Research

The literature outlines security risks in all layers of the Internet of Things architecture. (Xiaohui, 2013; Zhao and Ge, 2013; Suo, Wan, Zou, and Liu, 2012). There is some debate as to which layers need the most attention for future research. Some argue that risks in the perception layer present the greatest risk. (Zhao and Ge, 2013). Others argue that security at the perception layer is of a lower priority. (Kozlov, Veijalainen, and Ali, 2012).

As for security standards, the Constrained Application Protocol suggests the use of Datagram Transport Layer Security (DTLS). However, this introduces a large amount of overhead. (Capossele, Cervo, Cicco, and Petrioli, 2015). Other literature has considered the use of the Host Identity Protocol (HIP) instead. (Garcia-Morchon et al., 2013). The literature found that HIP has less overhead when compared to DTLS. Some literature has even proposed extensions to HIP that would further reduce overhead (Hummen, Wirtz, Ziegeldorf, Hiller, and Wehrle, 2013).

Purpose of the Research

The purpose of this literature review is to synthesize the existing research regarding the security risks, standards, and government action into one report. There are many different points of view in the literature about which areas of the IoT are most at risk. There is also conflict in the literature regarding which standards should be used and how they should be implemented. With this literature review, all of this debate will be collected into one report which will make it easier for future research to be done. Below are the specific research questions that this report aims to answer:

- What types of security risks do IoT devices face today?
- What types of security standards has the literature proposed?
- Are there any government standards in place or are there any being considered?

Structure of the Report

The report will first cover the methods used to gather the relevant research. Next, the report will discuss the security risks for current IoT devices. Then, the report will synthesize the research being done to develop new security standards and protocols. After that, the report will discuss current and future government standards for IoT security. Finally, the findings of the report will be summarized in the conclusion section.

Methodology

To create the report, information from academic journals and conference proceedings were used. These articles were found in databases such as Scopus, IEEE, and the ACM. Search terms such as "Internet of Things" and "security" were used to locate relevant articles in the databases. Web sources from industry leaders were used to provide background information surrounding the topic.

Security Risks for IoT Devices

This section will discuss the security risks faced by current IoT devices. The section will use the three main layers of the IoT architecture to break down the risks. Before the risks at each layer are discussed, the IoT architecture will be formally defined. After that, the risks found in the perception layer, network layer, and application layer will be discussed.

Defining the IoT Architecture

The literature generally breaks the IoT architecture down into three layers: perception, network, and application. (Zhao and Ge, 2013; Xiaohui, 2013). Some literature adds additional layers to further narrow down the purpose of each layer. (Granjal, Monteiro, and Silva, 2015; Kozlov et al., 2012; Suo et al., 2012). However, for the purposes of this report,

three layers will be sufficient. The perception layer generally includes the devices that allow an IoT device to interact with the physical world. A temperature sensor would be an example of a perception layer device. The network layer includes devices that allow the perception layer and application layer to interact through the Internet. Traditional network hardware is included in this layer. Finally, the application layer is defined as the software that allows end users to control and retrieve data from the perception layer devices. Below is a figure that gives more examples of devices that are commonly found at each layer.

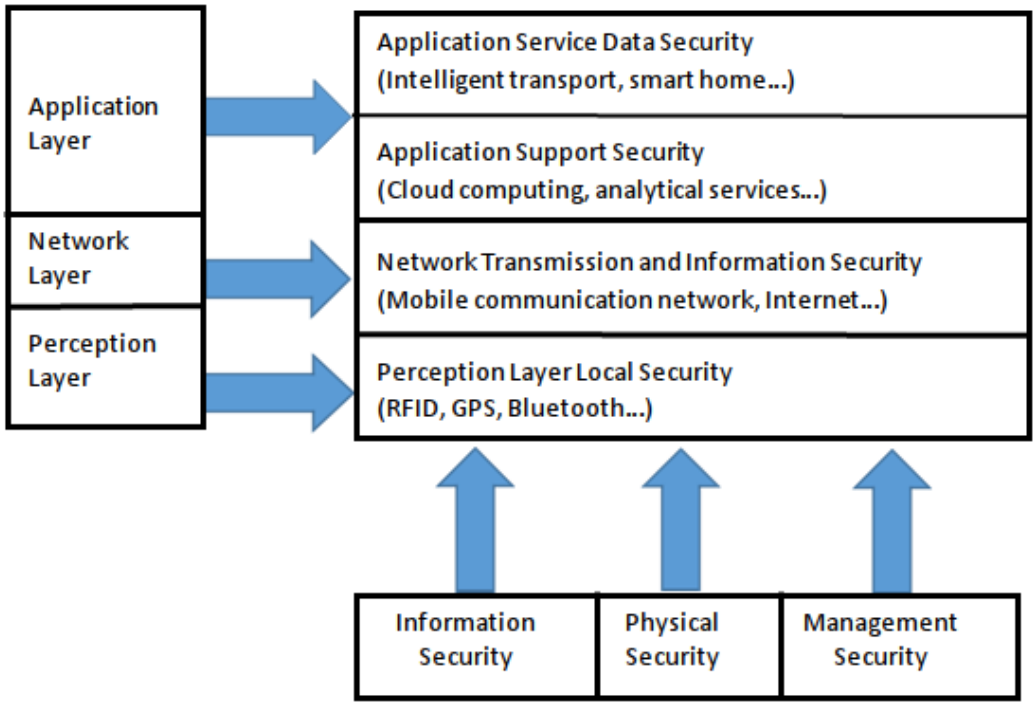

Figure 1: Internet of Things Architecture (adapted from Zhao and Ge, 2013)

Security Risks in the Perception Layer

In the perception layer, devices are commonly found in public with minimal physical security. The literature states that there is a risk of an attacker physically modifying a device at this layer. (Zhao and Ge, 2013; Xiaohui, 2013; Suo et al., 2012). Devices in the perception layer, for the most part, are not very powerful. The devices use processors that prioritize efficiency and cost over speed. Due to this limitation, they are often unable to use the same security mechanisms found in traditional computers. (Suo et al., 2012; Granjal et al., 2015; Xiaohui, 2013). Even traditional attack methods used to target conventional computers could be used against the IoT. (Zhao and Ge, 2013). Attacks such as distributed denial of service (DDoS) could disrupt sensors from communicating with the devices that receive the gathered information. Devices in the perception layer are also susceptible to malware, as shown by the recent Mirai botnet which infected thousands of IoT devices. (Herzberg et al., 2016).

Security Risks in the Network Layer

Many of the security risks in the network layer are already well-known, because they also apply to traditional computing platforms. (Zhao and Ge, 2013; Xiaohui, 2013). According to Zhao and Ge, the security implementations found in the network layer are fairly complete, but the risks should not be ignored. Zhao and Ge also found that the most common threats found in the network layer include man-in-the-middle attacks, illegal access due to insufficient authentication measures, and information eavesdropping. These types of attacks put the privacy of users at risk because most of the information being transmitted is from the physical world.

Security Risks in the Application Layer

Like the network layer, many of the security risks present in the layer are also found on traditional computing platforms. The literature outlines risks such as software vulnerabilities and insecure authentication methods. (Zhao and Ge, 2013; Suo et al., 2012). Just like with traditional platforms, mistakes by programmers that introduce vulnerabilities like buffer overflow are still common with IoT software. (Zhao and Ge, 2013; Xiaohui, 2013). For authentication, the developers must ensure that users are only allowed to access data they need. IoT devices commonly collect sensitive information that could violate the privacy of the public if it got into the wrong hands. (Zhang, Cho, and Shieh, 2015).

IoT Security Protocol Standardization

This section will first outline the need for a standardized suite of protocols to ensure security for the IoT. It will then evaluate various protocols that have been proposed and outline any debate found in the literature. The protocols that will be discussed include the Constrained Application Protocol (CoAP), Datagram Transport Layer Security (DTLS), and the Host Identity Protocol (HIP).

The Need for Standardization

Many of the protocols required to ensure security for the IoT already exist but most IoT devices are not powerful enough to use them. (Keoh, Kumar, and Tschofenig, 2014; Granjal et al., 2015; Garcia-Morchon et al., 2013). Currently, standardization efforts are underway by the Institute for Electrical and Electronics Engineers (IEEE) and the Internet Engineering Task Force (IETF). One project by the IETF is the Constrained Application Protocol (CoAP). CoAP is a protocol similar to HTTP that allows devices to make requests and receive responses. (Keoh et al., 2014; Capossele et al., 2015). The most commonly used protocol used to secure CoAP is Datagram Transport Layer Security (DTLS). (Keoh et al., 2014; Garcia-Morchon et al., 2013). Some literature proposes the use of the Host Identity Protocol (HIP) as an alternative to DTLS. (Hummen et al., 2013; Garcia-Morchon et al., 2013). The conflict in the literature on this issue alone shows the need for standardization. As pointed out by Koeh et. al, the reason for the success of the HyperText Transfer Protocol (HTTP) has been the completely standardized protocol suite.

For the Internet of Things to have a successful and secure future, the industry must agree on a standardized security suite.

The Constrained Application Protocol

The IETF decided that a new protocol was necessary to allow devices with limited resources to communicate efficiently. A working group was formed which came up with the idea for the Constrained Application Protocol (CoAP). The protocol allows devices to send and receive messages in a way similar to HTTP. (Keoh et al., 2014; Capossele et al., 2015). A universal resource identifier (URI) is used to make requests to destination devices and to receive responses. In the figure below, a basic CoAP request and response is displayed. The client makes a "GET" request to the server at the location identified by the URI. In the "GET" request, the client requests the contents of "temp." The server acknowledges the request with an "ACK" and sends the requested content back to the client.

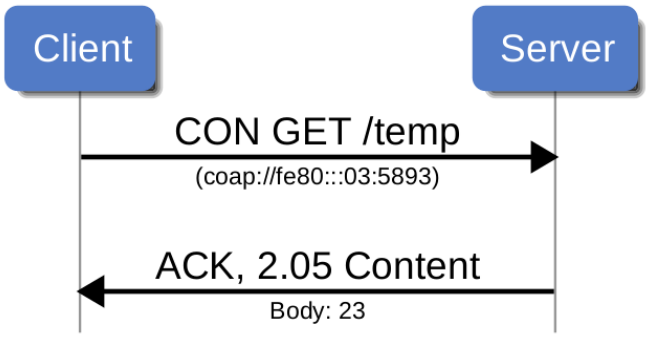

Figure 2: A Basic CoAP Interaction (Capossele, Cervo, Cicco, and Petrioli, 2015)

The major question currently in the literature is how this protocol should be secured. The subsections that follow will discuss various ways of securing the Constrained Application Protocol.

Datagram Transport Layer Security

This section will begin by discussing the findings of Garcia-Morchon et. al. regarding the viability of Datagram Transport Layer Security (DTLS) for securing CoAP messages. To start with, DTLS is simply TLS over the UDP protocol instead of TCP. The CoAP recommends using DTLS in place of any other method. Some literature argues that DTLS is the best suited protocol to secure CoAP. (Keoh et al., 2014). However, one major issue with DTLS is that it was designed for traditional networks. (Capossele et al., 2015). Since IoT devices generally run on constrained hardware, it is necessary for the protocol to be specifically tailored for the IoT. The IETF has created a working group called "DTLS In Constrained Environment", whose goal is to come up with a DTLS implementation that is usable with the IoT. (Keoh et al., 2014).

In a report by Garcia-Morchon et al., the authors analyzed the performance of DTLS using

a custom application running on a Redbee Econotag. The device was used to simulate a real world IoT device. The authors found that DTLS used a significant amount of memory due to the amount of messages sent. The authors also found that DTLS does not perform well in a network with high packet loss.

The work of Garcia-Morchon et al. demonstrates the need for additional changes to enable DTLS to work with the IoT. Capossele, Cervo, De Cicco, and Petrioli released a report outlining their optimized DTLS implementation. For their work, they used a MagoNode to simulate the presence of an IoT device. The specifications of the test device were similar to the one used by Garcia-Morchon et al., but with 16 KB of RAM instead of 128 KB. In order to make DTLS functional on their test device, the authors optimized modular arithmetic on large integers using their own assembly code. The authors also created their own ECC library to further optimize the cryptographic functions. The authors analyzed the results by separating their optimizations in order to see which ones had the greatest impact on performance. In the table below, one can see which optimization was performed, the time the operation took, the energy used, and the increase in ROM usage.

Scalar Multiplication			
Optimization	Time	Energy	ROM
base	13487 ms	190.17 mJ	/
assembly	13057 ms	184.1 mJ	2318 B
curve opt.	12591 ms	177.53 mJ	578 B
proj. coord.	3896 ms	54.93 mJ	1994 B
all	976 ms	13.76 mJ	4890 B
all + IBPV	135 ms	1.9 mJ	5852 B

Figure 3: Scalar Multiplication Time Comparison (Capossele, Cervo, Cicco, and Petrioli, 2015)

As one can see from the figure, the optimizations together provide a large increase in performance when doing scalar multiplication, but at the expense of more ROM usage. The authors also analyzed how their optimizations improved the performance and energy usage when doing cryptographic functions. The figure below shows their results.

	base (ms/mJ)	all (ms/mJ)	all + IBPV (ms/mJ)
ECDSA sign	13635 / 192.25	1045 / 14.73	150 / 2.11
ECDSA verify	27476 / 387.41	1076 / 15.17	1076 / 15.17
ECDH	26974 / 380.33	1952 / 27.52	1111 / 15,67

Figure 4: Overhead and Energy Consumption After Optimization (Capossele, Cervo, Cicco, and Petrioli, 2015)

Overall, the optimizations proposed by Capossele et. al. address the major problem preventing DTLS from being adopted with the IoT: its efficiency. However, other literature suggests that the Host Identity Protocol may be a better option. This protocol will be discussed in the next section.

Host Identity Protocol

As mentioned in the previous section, DTLS is not extremely well suited for use with the IoT. An alternative approach proposed by some literature is the use of the Host Identity Protocol (HIP). HIP makes use of public-key cryptography to establish connections. (Hummen et al., 2013; Garcia-Morchon et al., 2013). However, public-key cryptography is an expensive operation on a constrained platform like the IoT. Like DTLS, HIP must be tailored for use with the IoT. This section will discuss two approaches proposed by the literature.

HIP-DEX optimizations proposed by Hummen et al.

In an article by Hummen, Wirtz, Ziegeldorf, Hiller, and Wehrle, the authors analyzed the existing methods of implementing HIP and focused on HIP Diet EXchange (HIP DEX). The first major challenge the authors encountered was the large amount of resources that public-key operations use. When an IoT device is performing a public-key operation, it is often unable to do any of its other tasks. The expensive operations also make it possible for even a single attacker to perform a denial of service attack on the device. In order to address these challenges, the authors proposed the following extensions to HIP DEX: a "comprehensive session resumption mechanism," a "collaborative puzzle-based denial of service protection mechanism," and a "refined retransmission mechanism."

Session Resumption Mechanism

In the session resumption mechanism proposed by the authors, both devices will perform their most expensive protocol operations once during the handshake. If the connection needs to be reestablished, the devices can use the information they have saved to securely resume the session using a lighter weight session resumption handshake. The authors note that this technique could even be used with other protocols, such as DTLS. The technique does introduce some security risks, however. Hummen et al. state that it is possible for an attacker who is eavesdropping on the communications to replay a saved resumption handshake and gain unauthorized access to the network. In order to counteract this risk, a counter is incremented upon each successful session resumption. When the authors evaluated the results of session resumption in isolation, they found that it reduced computational overhead by at least 85.7%.

DoS Protection Improvements

As mentioned previously, the authors proposed improvements to HIP DEX to reduce its vulnerability to denial of service (DoS) attacks. Currently to protect from DoS attacks, HIP

DEX requires a puzzle mechanism to be introduced when a DoS is detected by the device. During normal operation, the puzzle is not used. Hummen et al. note that the mechanisms to detect an attack and to select an appropriate puzzle remain open research issues. In the authors proposal, attacks would be detected by keeping track of the number of public-key operations performed within a specified period. If the limit is exceeded, then a puzzle will be generated for the possible attacker. The authors propose that a high difficulty puzzle be generated for untrusted connections and a low difficulty puzzle for trusted connections. When evaluating the results, the proposed DoS protection was found to successfully protect the IoT device from attack while still allowing legitimate connections to take place.

Retransmission Mechanism

The final extension proposed by the authors was a retransmission mechanism. Currently, the HIP DEX standard specifies an aggressive retransmission strategy for handling the loss of messages. In their report, the authors propose an adaptive retransmission strategy that bases timeout values on the predicted transmission time for the message. However, it is possible that a device may have only received part of a message and a full retransmission is not necessary. To address this, the authors propose the use of pre-fetching message information to delay the retransmission of messages while the remaining parts are still being transmitted. Finally, a new message type proposed by the authors allows the device responding to a message to notify the sender that the message was received. This message would be send before the receiver does any cryptographic processing. When evaluating the results, Hummen et al. found that their retransmission strategy was a significant improvement over both HIP DEX and DTLS. The figure below shows their results and compares the performance to HIP DEX and DTLS. Each protocol is tested with a differing amount of data being lost during the handshake as shown by the loss ratio in the figure.

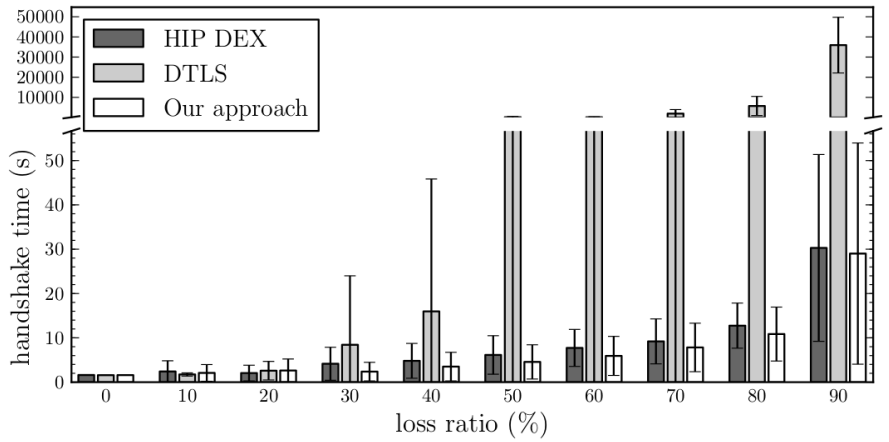

Figure 5: Results of HIP DEX Retransmission Strategy Optimization (Hummen, Wirtz, Ziegeldorf, Hiller, and Wehrle, 2013)

The extensions proposed by Hummen et al. provide a significant increase in performance for HIP DEX for use on constrained platforms like the IoT. However, there are also other

approaches being considered by the literature. To conclude this section, the work of Garcia-Morchon, Keoh, Kumar, Moreno-Sanchez, Vidal-Meca, and Ziegeldorf will be discussed.

HIP-PSK proposition by Garcia-Morchon et al.

In their report, the authors proposed an alternative version of HIP that they called HIP-PSK. Instead of using public-key cryptography, the authors chose to use a pre-shared key (PSK). In their protocol, a more lightweight challenge-based authentication mechanism can be used instead of Diffie-Hellman key exchange. The remainder of the protocol is identical to HIP-DEX. Garcia-Morchon et al. also propose the use of AMIKEY for key management with HIP-PSK and their optimized DTLS implementation. To evaluate the results, the authors compared HIP-PSK to their own optimized version of DTLS. They found that HIP-PSK performed better than DTLS, but DTLS provided better interoperability. The authors did not compare HIP-PSK to HIP-DEX or any other variations.

Conclusions

Overall, the propositions discussed in this section make both HIP and DTLS more viable protocols for use with the IoT. However, there are still gaps in the research that need to be filled in order to choose one protocol to fit in the standardized security suite mentioned earlier. The HIP-PSK proposition by Garcia-Morchon et al. sounds like a very promising solution, however, the authors did not compare their protocol to HIP and DTLS without modification. This makes it harder for researchers studying these protocols to decide if HIP-PSK performs better than the HIP-DEX extensions proposed by Hummen et al., for example. Once gaps like this are filled, the IoT industry will be much closer to coming up with a standardized security stack.

Government Action on IoT Security

This section will first begin by briefly discussing the current government regulations that can be found for Internet of Things devices. After that, the section will discuss future standards and regulations that are being considered. This section will only focus on action from the U.S. government and the European Union.

Current Regulatory Environment

Currently, there are not many regulations or standards governing the manufacturing of IoT devices in both the U.S. and the EU. (Weber, 2010; House Energy and Commerce Committee, 2016). As discussed earlier in the report, there are standards that can help to ensure the security of IoT devices, but manufacturers are not required to follow the standards. In a 2010 report by Weber, some requirements for future legislation are discussed. One of the most important requirements mentioned is that future legislation should be somewhat standardized around the world. Since businesses today do business all

over the world, it is important that they do not have to create separate versions of their devices for sale in countries with different regulations. During a hearing of the U.S. House Energy and Commerce Committee, Representative Walden noted that one of the committee's goals was to make sure that new regulations on the IoT do not hinder innovation in the industry.

Regulatory Proposals

This section will discuss the work being done by the U.S. Federal Trade Commission and the European Union to address the security problems of the Internet of Things.

U.S. Government Proposals

In January 2015, the FTC released a staff report with their findings regarding the security of the IoT. They first discussed the risks to the IoT that they have identified. After that, the FTC report summarized the discussions at their IoT workshop where attendees were able to give their thoughts on the benefits and risks to the IoT. After taking all of their earlier research and discussions into consideration, the FTC staff detailed their findings at the end of the report.

The FTC decided that the risks the IoT faces do not need to be addressed through legislation at this time. Many of the participants at the FTC's workshop shared similar views. One of the attendees stated that "the FTC should be very cautious about proposing regulation of this sector, given its importance to innovation in America." In the report, the FTC also recommended that Congress should enact cyber security legislation that is not specifically targeted at the IoT. The FTC noted that many of the security risks faced by the IoT are similar to traditional computers and that broad legislation would be more effective. No specific policy proposals were given in the report, however.

For some lawmakers, the FTC's current stance is not strong enough. In November 2016, after the large-scale cyber attacks discussed in the introduction of this report, Representatives Frank Pallone and Jan Schakowsky wrote a letter to the FTC Chairwoman Edith Ramirez. In the letter, they asked the FTC to request manufacturers to introduce new security measures like requiring users to change default passwords. They also asked the FTC to alert customers whose devices are at risk of attack.

Others have considered the FTC under Chairwoman Edith Ramirez's leadership to be active in addressing the security risks faced by the IoT. (Roberts, 2016). The workshop and report previously discussed are a few of the contributions the FTC has made to this issue. Under the new administration, however, it is not clear what path the FTC will take. Acting FTC director Maureen Ohlhausen stated in an interview that the FTC is "not primarily a regulator." (Thielman, 2017). In the same interview, Ohlhausen stated that the agency has not taken a position on whether new IoT regulation is necessary.

Overall, the FTC's stance that the IoT should be self-regulating is in sharp contrast to the

European Union, whose proposals will be discussed in the next subsection.

European Union Proposals

The European Commission has been drafting new legislation to address the security of the Internet of Things. (Stupp, 2016). The new rules would require manufacturers to label their devices based on whether the EU has found the device to be secure. This would be similar to how appliances are labeled with their energy efficiency and cars with their fuel efficiency. Many companies are doubting whether labeling is the right approach to solving this problem. (Gardner, 2017). As mentioned in the article by Stephen Gardner, companies would prefer if the system were voluntary. They also note that the labeling criteria would have to evolve quickly because technology is always changing.

If the European Union ends up adopting this proposal, it will provide valuable information to U.S. lawmakers who may be considering similar approaches. As mentioned earlier, however, it will be important that countries do not have regulations that differ significantly. If the EU proposal is found to be successful, the U.S. should adopt something very similar that companies will be able to follow easily without increasing costs.

Conclusion

The main purpose of this paper was to review the literature surrounding the security of the Internet of Things with a focus on the current security risks, security standards, and government regulations. As outlined in the report, the Internet of Things is a growing industry with lots of potential for innovation. However, the industry currently faces many security risks that have already resulted in the disruption of service on many websites. While the literature seems to be in agreement on what the current risks are, there is some debate as to what kind of new standards should be used to mitigate them. Organizations such as the IEEE have been working to come up with new standards that manufacturers can apply to their devices. One of the major challenges these researchers will face is making these standards optimized enough to run on constrained platforms like the IoT. This is a major topic in the literature, with two major protocols that are being considered for use: Datagram Transport Layer Security and the Host Identity Protocol. While either of these standards would provide adequate security for the IoT, manufacturers are not currently required to use either of them. The industry is currently self-regulating. Many governments are considering the legislative options, but a major concern from U.S. lawmakers in particular is that more regulation will stifle innovation in the industry. Lawmakers in the European Union have been more aggressive, proposing a labeling requirement for IoT devices. Overall, researchers and lawmakers will need to work together in order to come up with new ideas for securing the IoT. It is very likely that more security incidents will occur if manufacturers continue to release devices with the security risks mentioned in this report.

References

Capossele, A., Cervo, V., Cicco, G. D., & Petrioli, C. (2015). Security as a CoAP resource: An optimized DTLS implementation for the IoT. In *2015 IEEE International Conference on Communications (ICC)* (pp. 549–554). doi:10.1109/ICC.2015.7248379

Garcia-Morchon, O., Keoh, S. L., Kumar, S., Moreno-Sanchez, P., Vidal-Meca, F., & Ziegeldorf, J. H. (2013). Securing the IP-based Internet of Things with HIP and DTLS. In *Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks* (pp. 119–124). WiSec '13. Budapest, Hungary: ACM. doi:10.1145/2462096.2462117

Gardner, S. (2017). Companies Wary of EU Consumer Cybersecurity Labels Plan. Retrieved from https://www.bna.com/companies-wary-eu-n57982083682/

Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the Internet of Things: A survey of existing protocols and open research issues. *IEEE Communications Surveys Tutorials*, *17*(3), 1294–1312. doi:10.1109/COMST.2015.2388550

Herzberg, B., Bekerman, D., & Zeifman, I. (2016). Breaking down Mirai: An IoT DDoS botnet analysis. Retrieved from https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

House Energy and Commerce Committee. (2016). Understanding the Role of Connected Devices in Recent Cyber Attacks.

Hummen, R., Wirtz, H., Ziegeldorf, J. H., Hiller, J., & Wehrle, K. (2013). Tailoring end-to-end IP security protocols to the Internet of Things. In *2013 21st IEEE International Conference on Network Protocols (ICNP)* (pp. 1–10). doi:10.1109/ICNP.2013.6733571

Keoh, S. L., Kumar, S. S., & Tschofenig, H. (2014). Securing the Internet of Things: A standardization perspective. *IEEE Internet of Things Journal*, *1*(3), 265–275. doi:10.1109/JIOT.2014.2323395

Kozlov, D., Veijalainen, J., & Ali, Y. (2012). Security and privacy threats in IoT architectures. In *Proceedings of the 7th International Conference on Body Area Networks* (pp. 256–262). BodyNets '12. Oslo, Norway: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

Krebs, B. (2016a). Backdoor in Sony IPELA Engine IP Cameras. Retrieved from https://krebsonsecurity.com/2016/12/researchers-find-fresh-fodder-for-iot-attack-cannons

Krebs, B. (2016b). KrebsOnSecurity hit with record DDoS. Retrieved from https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

Martínez, J., Mejía, J., & Muñoz, M. (2016). Security analysis of the Internet of Things: A systematic literature review. In *2016 International Conference on Software Process Improvement (cimps)* (pp. 1–6). doi:10.1109/CIMPS.2016.7802809

Roberts, P. (2016). Lawmakers to FTC: Do Something about Internet of Things Security. Retrieved from https://securityledger.com/2016/11/lawmakers-to-ftc-do-something-about-internet-of-things-security/

SEC Consult. (2016). *Backdoor in Sony IPELA Engine IP Cameras*. Retrieved from http://blog.sec-consult.com/2016/12/backdoor-in-sony-ipela-engine-ip-cameras.html

Stupp, C. (2016). Commission plans cybersecurity rules for internet-connected machines. Retrieved from https://www.euractiv.com/section/innovation-industry/news/commission-plans-cybersecurity-rules-for-internet-connected-machines/

Suo, H., Wan, J., Zou, C., & Liu, J. (2012). Security in the Internet of Things: A review. In *2012 International Conference on Computer Science and Electronics Engineering* (Vol. 3, pp. 648–651). doi:10.1109/ICCSEE.2012.373

Thielman, S. (2017). Acting Federal Trade Commision head: internet of things should self-regulate. Retrieved from https://www.theguardian.com/technology/2017/mar/14/federal-trade-commission-internet-things-regulation

Weber, R. (2010). Internet of Things - new security and privacy challenges. *Computer Law and Security Review*, *26*(1), 23–30. doi:10.1016/j.clsr.2009.11.008

Xiaohui, X. (2013). Study on security problems and key technologies of the Internet of Things. In *2013 International Conference on Computational and Information Sciences* (pp. 407–410). doi:10.1109/ICCIS.2013.114

Zhang, Z.-K., Cho, M. C. Y., & Shieh, S. (2015). Emerging security threats and countermeasures in IoT. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security* (pp. 1–6). ASIA CCS '15. Singapore, Republic of Singapore: ACM. doi:10.1145/2714576.2737091

Zhao, K. & Ge, L. (2013). A survey on the Internet of Things security. In *2013 Ninth International Conference on Computational Intelligence and Security* (pp. 663–667). doi:10.1109/CIS.2013.145