Internet of Things (IoT) Security in Consumer Devices

Mark E. Turner

East Carolina University

Abstract

In the past 5 years, the Internet of Things (IoT) has exploded onto the computing world and changed markets with it. No market has been changed more than the consumer market. As a result, consumers have enjoyed huge improvements to their everyday lives. While IoT has provided many benefits, it has also brought many challenges with it. The most significant of these challenges is how these devices have impacted consumer network security. Because of the competing platforms and technologies of consumer IoT devices, security methods for each have resulted in different strategies. The author will focus on the most prevalent security methods used on consumer IoT devices today and how they are implemented.

The purpose of this paper is to provide simplified understanding and analysis of the most common methods of securing consumer IoT devices available today. A literature review of current IoT standards and terms will be provided from relevant industry sources. Various international journals and standards were reviewed, with the intent of determining which IoT security methods were most effective. An overview of security characteristics for each method will be reviewed along with best practice configurations. Any potential challenges occurring from these practices will be further explored and documented. Finally, these security methods will be compared and analyzed for better understanding.

Keywords: Internet of Things, IoT, Security, Consumer

Internet of Things (IoT) Security in Consumer Devices

In the past five years, the Internet of Things (IoT) has exploded onto the computing world and changed markets with it. Both the enterprise and consumer markets have received nothing short of a deluge of products and services. Many of the services provided require the use of manufacturer devices to access them. Devices targeted towards enterprise markets have been quickly deployed into existing corporate infrastructure. Deployment has been facilitated by the testing and configuration provided by very large Information Technology (IT) departments. IT departments obviously retain the necessary expertise and skills to accomplish this goal. Unfortunately, consumer markets and the devices that are directed towards it do not have users with this degree of skill and knowledge.

This lack of understanding of IoT devices by users does not dissuade manufacturers from continuing to market new devices and services. A constant flow of new services and more simplified designer devices constantly promises new experiences. Data from Statista (2018) predicts that consumer IoT spending will rival enterprise spending by 2020. As a result, no market has been changed more by IoT than the consumer market. Services are allowing consumers to interact with their friends and family in real-time. Personal data is now platform agnostic and can be virtually accessed anywhere in the world. Consumers have enjoyed huge improvements to their everyday lives. While IoT has provided many benefits, it has also brought many challenges with it.

Service providers consistently find that a lack of user understanding is their greatest hurdle. The increased network configuration requirements to deploy these devices overwhelms many consumers. Users increasingly creating misconfigured and insecure networks. Yet, users are still demanding security along with improved functionality from devices. The problem is

further compounded for manufacturers by a lack of security and software development standards. Colakovic & Hadzialic (2018) tells us that competing platforms and technologies fragment solutions even further. The impact that IoT devices have made on network security because of these challenges threatens further consumer adoption of devices. To provide secure devices and relevant services, manufacturers and providers must devise new security methods outside of consumer control. Therefore, it is imperative that providers and manufacturers understand these security methods in order to deploy them effectively.

The purpose of this paper is to provide simplified understanding and analysis of the most common methods of securing consumer IoT devices available today. A literature review of current IoT standards and terms will be provided from relevant industry sources. Various international journals and standards were reviewed, with the intent of determining which IoT security methods were most effective. An overview of security characteristics for each method will be reviewed along with best practice configurations. Any potential challenges occurring from these practices will be further explored and documented. Finally, these security methods will be compared and analyzed for better understanding.

Visual designs of these practices were created to explain the characteristics of methods where appropriate. When applicable combinations of methods are displayed to align with Defense in Depth security theory. Age of all resources including journals, articles, and referential literature were limited to a period of three years. This choice was made to provide an analysis of only current and relevant methods. This paper is intended for an audience of typical security professionals seeking information on IoT security theory for consumer devices. By examining these trends, the author hopes to provide a stronger insight and understanding of IoT security for consumer devices and to promote a refined understanding of the topic.

Literature Review

IoT is defined as being a collection of “things”. These things are made up of various types of devices and software. Each of these is interconnected by a web of networks available through the Internet. Sombir & Solanki (2018) go further by explaining that these devices are composed of sensors and are consistently collecting and reporting data on these networks. When we review the advantages of IoT, we can review that these benefits are important as shown in Table 1. While there are many more uses for IoT we are concerned with the consumer applications of this technology. Widespread applications of this technology continue to grow as developers enhance and push the boundaries of how the technology is applied.

Internet of Things in Review

Advantages of IoT	Applications of IoT
Efficient Resource Utilization	*Health Care Applications*
Increased Automation	*Smart Home Control*
Saves Time	*Personal Wearables*
Improved Security	*Transportation*

Table 1 – Internet of Things in Review

As IoT devices provide benefits, it is important to understand how the technology is divided and managed. Colakovic & Hadzialic (2018) describes a division of four domains titled as Application, Middleware, Networking, and Object. Each domain is tied to a specific control area and is displayed in Figure 1. As you can see the Application domain is where the software and programs that deliver services to users via the other domains exist. The Middleware domain includes the platforms that are used to manage these applications such as Software Developed Networks (SDN) or cloud-based platforms. The Networking Domain follows with the infrastructure networking devices that are used to connect to the final domain. This is the Object

Domain and it contains the endpoint devices which the user interfaces with. By understanding what occurs at each of the Functional Domains, we can better understand how to better secure them.

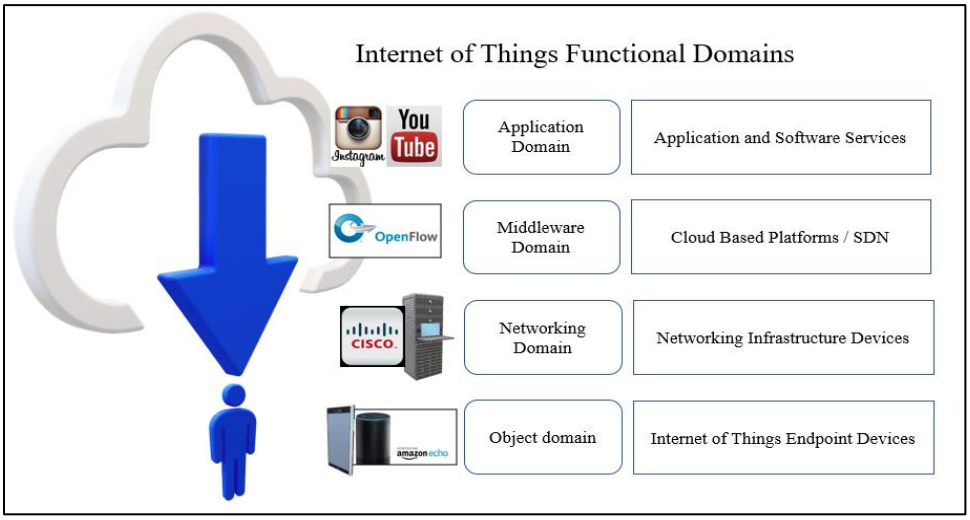

Figure 1 – IoT Functional Domains

The Application domain is software driven and is susceptible to attacks based off errors in code or unknown errors that can be exploited to gain access by an attacker. Consistently evaluating errors and event logs can provide significant mitigation to these issues. As always malware will be an issue as well, but this is again usually a failure of the application code or the underlying technologies that the application uses to provide services.

Often the middleware domain is susceptible to various types of Denial of Service (DoS) attacks and exploited infrastructure of the SDN. Consistently patching hardware systems and integrated operating systems will provide a significant lead on an attacker. Utilization of an effective Intrusion Detection System (IDS) and a Firewall appliance combined with effective and traditional security controls is advised at this domain level.

Oddly enough the Networking domain is similar in many of the same needs and requirements as the Middleware domain. Whereas the SDN is more application than hardware the networking domain is more hardware than application, but it leans on the intelligent and dynamic fluidity provided by the SDN. Integrating these domains together effectively provides and extremely valuable infrastructure and core system. As with any physical hardware physical access to the devices in this domain should always be restricted and asset management is critical.

Finally, the Object domain which is an Endpoint specific domain, the critical points at this layer are Authentication and Authorization. This is essential when these hardware devices are on the front lines in the sense that they are directly front facing to the user. Whereas the backplane of the upper-layer domains is protected by a small army of IT professionals, the primary baston of defense is the user. It is their responsibility to insure they limit access to the device. Because of the nature of packet sniffers and social engineering this domain is highly susceptible to these types of attacks. As with all IoT devices the primary point of access to the internet is often a wireless network and the security of these devices is only as strong as the security of the network.

Because of the collective nature of what IoT does with Personally Identifiable Information (PII) it is important to draw a balance between security and privacy. This is best explained by understanding that if users allow providers to have access to everything they are better prepared to secure it. Unfortunately, because of the nature of PII this is difficult to gain. Ghorbani & Ahmadzadegan (2017) tells us that users are not willing to put their security at risk, yet they still demand privacy for their data. Ghorbani & Ahmadzadegan (2017) also show us there are several challenges including Implementation, Privacy, Network Infrastructure, Quality of Service (QoS), Security Threats, Authentication and Authorization, and many others.

Hislop (2018) references the need for IoT implementation in a company at all levels. He also points out that failing to address these challenges properly can lead to a costly mistake. How we manage these challenges will directly impact a company and their ability to respond to customer needs. To put it succinctly, you must pay into the IoT system in order to receive benefits from the system. This requires substantial investment throughout the entire deployment process and beyond. Therefore, it is equally important to appreciate the limitations of IoT devices as well as the advantages.

The complexity of the IoT system is infinitely scalable and is based directly on the needs of the developer and the user. Yang, Wu, Yin, Li, & Zhao (2017) state that the real limitation of IoT devices is tied to its low cost and small form factor. Because of the shortened battery life associated with small, low cost devices the devices often are required to be powered by a wired connection. This is compounded by the nature of most IoT devices being tied to some form of wireless technology. Which forces the device to fall back on the security of the local wireless network gateway. When IoT devices are designed they are often built around some type of low-cost motherboard and Computer Processing Unit (CPU). Low processing power limitations remove many security remedies and deny the use of many security encryption algorithms.

The static nature of IoT devices makes the platform easy to develop for, but it presents a unique security issue. Operating systems on these devices are often very small and located on some type of flash memory. As with the larger computer operating systems in the world, software updates are of significant value. They allow for increased functionality as well as patches for bugs and security issues. Dennis (2018) points out that each type of software will require the need for software fixes as vulnerabilities in the software are discovered or with the technologies that the software is built upon. Because of the nature of how these updates and

patches are deployed, security must be a major concern. An insecure update system whether it is wired or Over the Air (OTA) must be secured and not made easily available to an attacker.

Finally, as explained earlier the most difficult challenge is user-based challenges. There is a plethora of potential issues that a user with limited networking knowledge can create simply by not protecting their home wireless network with some type of encryption. Nearly all IoT devices are connected to the internet as referenced in the usage rates in Figure 2 below. With IoT devices requiring an always-on connection, this presents a deeper threat to typical users. Sruoginis & Shane (2016) have provided data from a study that show that over half of the US population owns a Smart TV that is constantly connected to the internet.

A very large attack surface is created when the user fails to implement effective network security onto their home wireless network. For this reason, Makhdoom, Abolhasan, Lipman, Liu, & Ni (2018) explains that one of the biggest threats is the consumer themselves. Now that we have covered the basics of IoT and the advantages and challenges as well, we must now turn our attention to the security issues we have discovered.

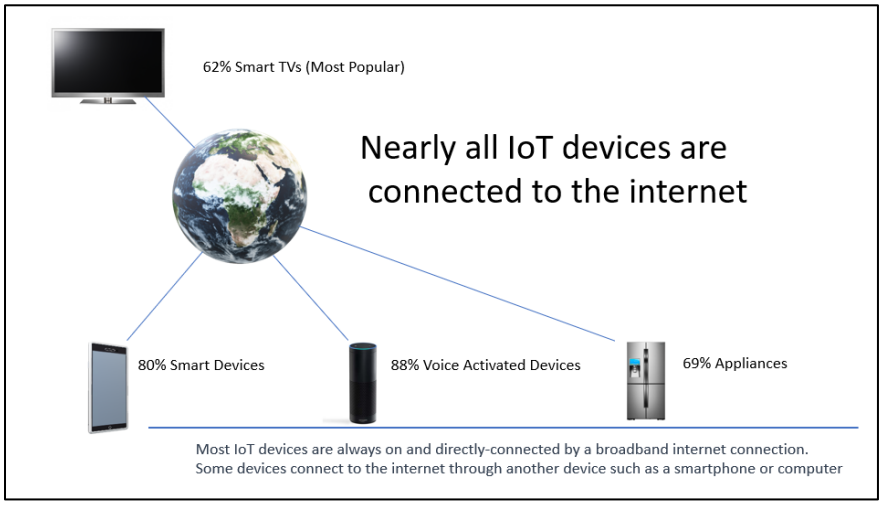

Figure 2 – IoT Device Statistics

Discussion

After reviewing the information in this literature review it is important now to determine what are the commonly used and popular security methods for implementation on IoT networks. From my analysis there are five primary methodology. These address the issues of always-connected devices with software deficiencies, data and privacy security, local-based and cloud-based network hardening, insecure IoT devices with low hardware resources, and intrusion and malware detection.

Using the IoT Functional Domains model from earlier we will apply security methodologies to each domain with the intent of securing each further. These new IoT Functional Security Domains can be reviewed in Figure 3. Notice how we have placed a new security technology at each domain level with the intent of providing layered security across all securing all domains at each level. Notice that we have added Blockchain PKI Encryption, Secure SDN, Distributed Intrusion Detection System (IDS), Edge/Fog Computing, and OTA Updates/Patch Management.

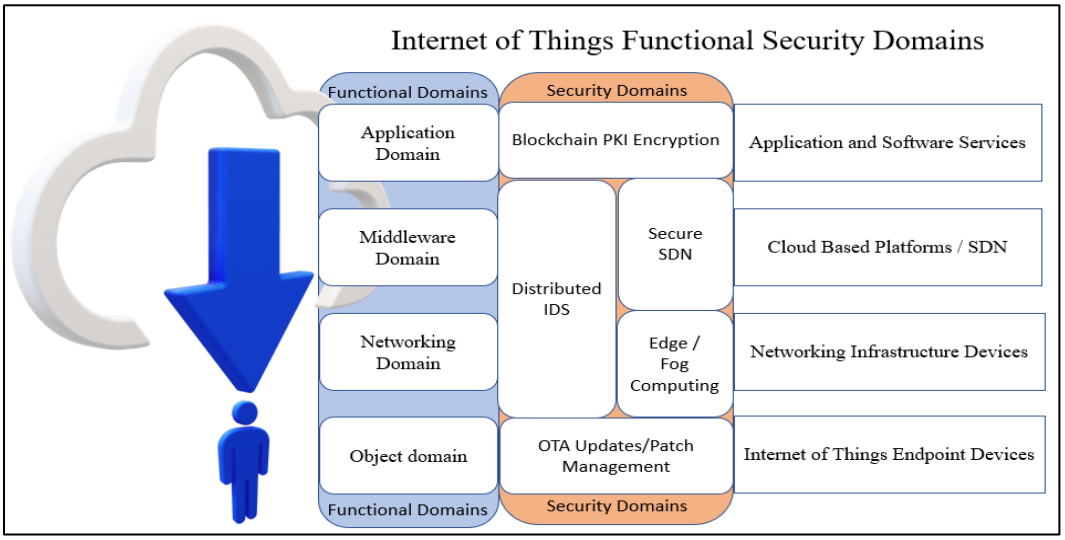

Figure 3 – IoT Functional Security Domains

Distributed IDS

Network intrusions are extremely difficult to come back and return to a sense of normalcy. It is this reason that computer security specialists prefer to prevent the intrusion before it happens. To that end computer security specialists employ the use of Intrusion Detection Systems to prevent this from happening. Kumar & Venugopalan (2017) explain that an IDS simply is designed to identify unauthorized access and then to effectively respond to the malicious activities. These attacks are detected at times and at others it is not. How these events are recorded is what makes the IDS effective or not.

Intrusions on a network have a specific pattern that they take. There is first reconnaissance, then target assessment, followed by an exploit that is used. From this point there is usually some type of malware used to further inhibit the target and provide an easier access for the attacker. A single IDS is traditionally deployed on a network edge near the firewall and then place the sensor on the outside of the firewall. Obviously this allows for a single point of failure and can create an issue if an attacker has gotten access to the network. Therefore, security specialists utilize the Distributed IDS.

As we discovered earlier the Middleware and Networking domains are highly susceptible to attacks and require a significant amount of protection. A distributed IDS is a simple concept of placing multiple IDS devices and sensors on a network. From this network of interconnected sensors and devices, if an attacker manages to get past one point in the network then at best they will be likely identified by another IDS. At the very least this network of logged and monitoring sensors can provide forensic information to prevent future attacks.

Gajewski, Batalla, Mastorakis, & Mavromoustakis (2017) have proposed a unique solution which involve placing IDS devices to protect home consumer devices. Their proposal is that the security of Consumer Smart homes should be provided by the ISP. By placing an IDS in a gateway provided by the ISP combined with a Network Intrusion detection System (NIDS) on the ISP level network, they hope to protect these networks far more efficiently. To better understand this principle, review Figure 4 below. Notice that the lack of NIDS and Host Based Intrusion Detection System (HIDS) provides an increased attack surface for the consumer devices.

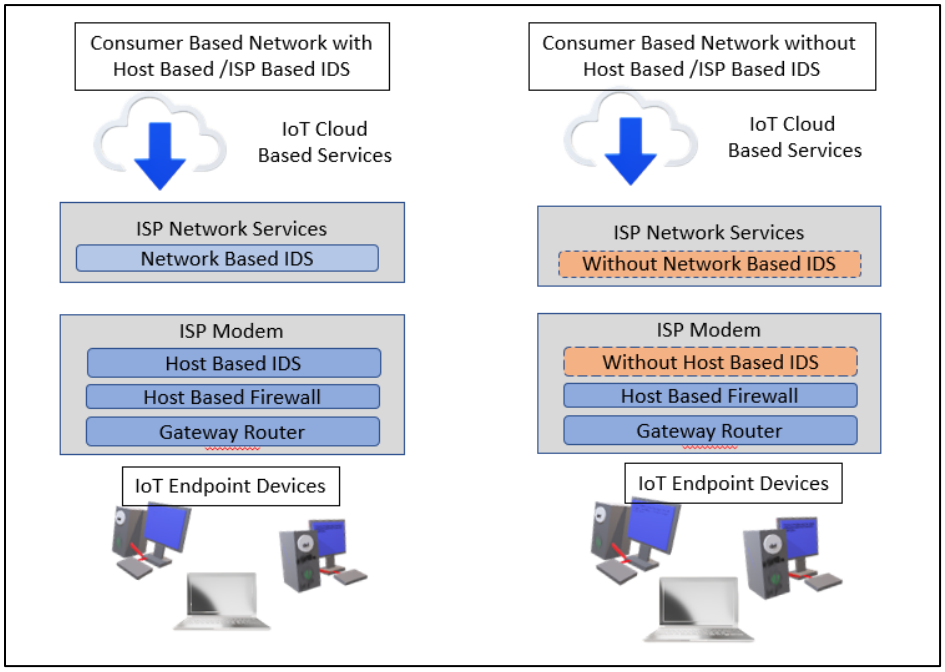

Figure 4 – IDS Deployment

IT is highly advisable to include a NIDS and a HIDS on networks. These devices are the front line of defense against network intrusion attacks. Placing these on SDN and Fog Computing Edge networks will provide an even stronger defense for these hybrid networks. This will be covered in later sections.

Blockchain Encryption

One of the biggest threats that IoT devices encounter is the lack of secure data transmission. This can occur at any time in the data stream. The biggest protection against unauthorized access to data thereby nullifying the confidentiality standard of information security is encryption. Traditional computers will use an encryption standard such as Public Key Infrastructure (PKI) to protect data transmissions. This is simply the issuance of a digital certificate to create a secret key thereby allowing other public keys to be created from it. Public keys can be verified against the Private Key to determine identity and to authorize access to data traffic. Because this structure is considerably taxing on resource constrained devices like IoT devices other systems have been proposed. Singla & Bertino (2018) have discovered that there are blockchain based PKI solutions being created. From their research they have explained that this will be highly effective, but it is still in its infancy.

One of the newer and exciting techniques is the use of lightweight cryptographic algorithms. Qasaimeh, Al-Qassas, & Tedmori (2018) describe this as a solution to IoT encryption difficulties at the local level. Currently any encryption and decryption processes are managed through the use of cloud services to offload the processing form the devices. IoT devices are like a terminal computer system similar to a Chromebook. Whereas the operating system and all software management occur in the cloud.

Blockchain based encryption is a much lower impact on low resource devices and can provide very impressive returns if used correctly. Unfortunately, this technology solution is not readily available for deployment and will need more time to be effectively tested. Any of these authentication and authorization systems will benefit the Application domain as moving these services to the Object domain will decrease resource utilization. Khan & Salah (2018) explain

that because of the nature of blockchains and their decentralized and distributed processing of encryption algorithms, this can be a serious risk to implement this encryption. They recommend that this technology be effectively deployed so as not to have it disrupt networks or expose them to critical risks.

OTA Updates and Patch Management

Currently the state of IoT is still much like the Old West in regard to regular security updates. Additionally, these very security updates are often insecure themselves. Because of the lack of standards for management of these important updates, the entire ecosystem continues to draw more negative attention. Once consumers have made the decision that IoT is insecure and unable to protect their data, mainstream adoption of the technology will become a dream.

Leiba, Yitzchak, Bitton, Nadler, & Shabtai (2018) studied the security updates and software patching of IoT devices and discovered several startling facts. For reasons, mostly attached to a lack of standards, security updates are not being provided on a regular basis. They have proposed a decentralized and incentivized IoT delivery system. While this is a hopeful and novel approach, without some type of governmental regulation of device manufacturers, security updates will continue to be an option.

Because of the nature of the Object domain and the expense of devices, they are often not replaced as often as newer and more secure solutions come out. The best strategy to manage this is to simply purchase consumer devices from well-known manufacturers who have a long track record of strong standards of customer service. Companies that are simply not established and recognizable should be avoided at all costs. Using secure and strong passwords to manage the various ecosystems of devices will provide effective protection as well.

Fog / Mobile Edge Computing

When the concept of the cloud was first introduced many professionals had difficulty understanding how the concept was related to the real world. As cloud computing and virtualization has matured, the concept of the Fog was introduced. Cisco Systems defines Fog computing as being the network devices that connect the cloud to end devices. While this is accurate, there are some misconceptions that the devices located are considered to be backplane devices. Whereas in reality they are often front facing and directly connected to customers.

Roman, Lopez, & Mambo (2018) explain that Fog Computing is similar to Mobile Edge computing. Where Fog Computing connects to customers, Mobile Edge networks connect to mobile device provider customers. Roman et al. (2018) suggests that the utilization of mesh networks composed of IDS devices will provide more effective on these edge networks. Remember that the Networking domain requires hardware protections and it is at this domain that we would deploy these mesh networks and to provide more effective edge management. To better explain and to help visualize this concept refer to Figure 5 below. Notice how the

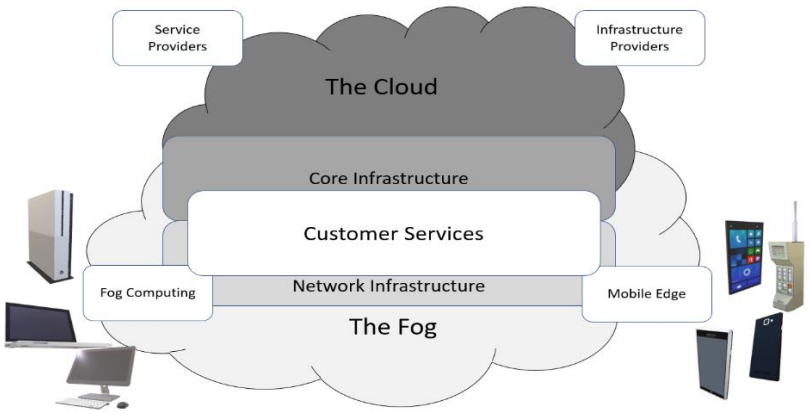

Figure 5 – Fog and Mobile Edge Computing

Software Defined Networks

Software Defined Networks are defined by Rouse (2018) as being "an architecture that aims to make networks agile and flexible." While this may be the case in theory, they often are not as agile as they are intended to be. The main goal of an SDN is to provide a manageable interface for commonly used network administrative duties. By providing a single administrative interface and supplementing it with a software architecture, a Traditional Networking architecture can become far more powerful. Different security components such as firewall appliances and IDS appliances can be integrated into hardware easily. Simply by providing a centralized architecture much like a client/server model in computer systems, the network is made more secure. This technology can provide a significant hardening of the Middleware domain.

As was explained earlier, the Middleware domain is where the SDN resides naturally. As was displayed in Figure 3, the Secure SDN security domain touches both the Application domain as well as the Networking domain. Remember that by working within all three of these domains, the SDN is able to provide more secure management of traffic as well as provide secure data transmissions for IoT devices on the Object domain.

Grigoryan, Liu, Njilla, Kamhoua, & Kwiat (2018) tells us that by providing a bridge to the Network Domain and the Application Domain, an SDN controller can protect IoT devices more effectively. Consequently, Yassein, Abuein, & Alasal (2017) have come to the same conclusion and even go so far as to state that utilizing the SDN can terminate the Traditional Networking model. By allowing the SDN controller to manage packet flow, a layer two switch can be used to route a much more efficiently based on the needs of the network. Combining this with the use of a firewall appliance and by effectively coordinating a Distributed IDS, IoT

devices are more secure. Beecher (2018) explains that through the deployment of these Enterprise-Grade networks using coordinated technologies as described above this will propel the IoT into the mainstream and create new disruptive versions of the technology.

Conclusions and Future Study

As the IoT consumer markets continue to mature the conversation on security will become the primary focus of network managers. Consumer perception is difficult to manage and can be fickle if not encouraged properly. With more information coming out into the current news cycle about possible hacked IoT devices, consumers become warier. Admittedly it is difficult to create security mitigations as fast as new attacks and exploits are discovered. But with issues like a lack of standardization of security updates it is much more difficult to provide this.

Much of the information covered in this paper is easily deployed onto existing consumer IoT networks. While Blockchain PKI encryption is still a way off, the use of Distributed IDS, Secure SDNs, and Fog Computing can provide a more effective security solution if deployed correctly. Press (2017) provides an excellent overview of up and coming technologies and how far on development they are. Press (2017) goes on to explain that the many consumer smart devices have been used to monitor and even spy on consumers. As this information is released into the twenty-four-hour news cycle, it will be more difficult to generate faith with consumers in newer products. It has been the authors hope that some of this information can assist in providing a better understanding of the consumer IoT devices and how best to secure them for use in home networks.

References

Beecher, P. (2018). Enterprise-grade networks: the answer to IoT security challenges. *Network Security*, Vol 2018, Iss 7, Pp 6-9. https://doi.org/10.1016/S1353-4858(18)30067-9

Colakovic, A., Hadzialic, M. (2018). Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. *Computer Networks*, Vol 144, 24 October 2018, pp. 17-39. https://doi.org/10.1016/j.comnet.2018.07.017

Dennis, C. (2018). Why is patch management necessary?. *Network Security*, Volume 2018, Issue 7, pp. 9-13. https://doi.org/10.1016/S1353-4858(18)30068-0

Gajewski, M., Batalla, J.M., Mastorakis, G. (2017). A distributed IDS architecture model for Smart Home systems. *Cluster Computing*, 2017, pp 1-11. https://doi.org/10.1007/s10586-017-1105-z

Ghorbani, H., Ahmadzadegan, H. (2017). Security challenges in internet of things: survey, *2017 IEEE Conference on Wireless Sensors (ICWiSe)*, 2017, pp. 1-6.

doi: 10.1109/ICWISE.2017.8267153

"Global Public IT Cloud Spending, 2014 and 2018." Market Share Reporter. Ed. R. Lazich. 26th ed. Farmington Hills, MI: Gale, 2016. *Business Insights: Global*. Web. 28 Oct. 2018.

Grigoryan, G., Liu, Y., Njilla, L., Kamhoua, C., Kwiat, K. (2018). Enabling Cooperative IoT Security via Software Defined Networks (SDN). *2018 IEEE International Conference on Communications (ICC)*, (2018). DOI:10.1109/ICC.2018.8423017

Hislop, R. (2018). *IoT explained for the CFO*. Cape Town: SyndiGate Media Inc. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/2090135675?accountid=10639

Khan, M. A., Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, Vol 82, 2018, pp. 395-411. https://doi.org/10.1016/j.future.2017.11.022

Kumar, D., Venugopalan, S. (2017). INTRUSION DETECTION SYSTEMS: A REVIEW. *International Journal of Advanced Research in Computer Science*, 8(8) Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1953784901?accountid=10639

Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R., Ni, W. (2018). Anatomy of Threats to The Internet of Things, *IEEE Communications Surveys & Tutorials*,

doi:10.1109/COMST.2018.2874978

Press, G., (2017). *6 Hot Internet of Things (IoT) Security Technologies*, Retrieved from https://www.forbes.com/sites/gilpress/2017/03/20/6-hot-internet-of-things-iot-security-technologies/#24ab77021b49

Qasaimeh, M., Al-Qassas, R., Tedmori, S. (2018). Software randomness analysis and evaluation of lightweight ciphers: the prospective for IoT security. *Multimedia Tools and Applications* (2018) Vol 77, Issue 14, pp 18415-18449. https://doi-org.jproxy.lib.ecu.edu/10.1007/s11042-018-5663-8

Roman, R., Lopez, J., Mambo, M. (2016). Mobile edge computing, Fog et al,: A survey and analysis of security threats and challenges. *Future Generation Computer Systems*, Volume 78, Part 2, January 2018, Pages 680-698. https://doi.org/10.1016/j.future.2016.11.009

Sagirlar, G., Carminati, B., Ferrari, E. (2018). Decentralizing privacy enforcement for Internet of Things smart objects. *Computer Networks*, Vol 143, 9 October 2018, pp 112-125

Singla, A., Bertino, E. (2018). Blockchain-Based PKI Solutions for IoT. *2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)*, 2018, pp. 9-15.

doi: 10.1109/CIC.2018.00-45

Software-defined networking (2018). In TechTarget. Retrieved from https://searchsdn.techtarget.com/definition/software-defined-networking-SDN

Solanki, K., Sombir, D. (2018). LITERATURE REVIEW ON SECURITY OF IOT. *International Journal of Advanced Research in Computer Science*. DOI:9.10.26483/ijarcs.v9i2.5689.

Sruouginis, K., Shane, R. (2016). *The Internet of Things* [PDF Document], Retrieved from iab.com website: https://www.iab.com/wp-content/uploads/2016/12/IAB-Internet-of-Things.pdf

Statista, the Statistics Portal. (2017) *IoT endpoint spending by category worldwide* [Data file]. Retrieved from https://www.statista.com/statistics/485252/iot-endpoint-spending-by-category-worldwide/

Yang, Y., Wu, L., Yin, G., Li, L., Zhao, H. (2017) A Survey on Security and Privacy Issues in Internet-of-Things, *IEEE Internet of Things Journal*, Vol. 4, no. 5, pp 1250-1258.

doi: 10.1109/JIOT.2017.2694844

Yassein, M., Abuein, Q., Alasal,S. (2017). Combining software-defined networking with Internet of Things: Survey on security and performance aspects, *2017 International Conference on Engineering & MIS (ICEMIS)*, Monastir, 2017, pp. 1-7.

doi: 10.1109/ICEMIS.2017.8273027