Securing The Internet of Things:

Enhancing Security Protocols for Personal Devices

by

Esmeralda Alvarado Michaca

Submitted to the Board of Mathematics and Computer Science

School of Natural and Social Sciences

In partial fulfillment of the requirements

for the degree of Bachelor of Arts

Purchase College

State University of New York

May 2019

Sponsor: David Jameson

Second Reader: Lee Tusman

TABLE OF CONTENTS

ABSTRACT …….2

INTRODUCTION …….2

CHAPTER ONE ……3

1. 1 THE INTERNET OF THINGS…….3
1. 2 TCP/IP: A BRIEF HISTORY ……..……4
1. 3 TCP/IP & IOT: FUNCTIONALITY & SECURITY WEAKNESSES……5
    1.3.1 TCP/IP FUNCTIONALITY FOR IOT……5
    1.3.2 IPv4 and IPv6……..7
    1.3.3 TCP/IP SECURITY WEAKNESSES……9

CHAPTER TWO ……..13

2.1 BOTNETS AND DDOS…….13
    2.1.1 DDoS CONSEQUENCES……14

CHAPTER THREE ……16

3.1 IOT COMPANY SECURITY STANDARDS & CONSUMER SOLUTIONS……16

CONCLUSION……..…18

BIBLIOGRAPHY ……..19

ABSTRACT

This essay covers the Internet of Things (IoT), its use of the TCP/IP networking model, and the security issues that come with TCP/IP, company security standards, and customer security habits that hinder the overall security of IoT devices. It will cover an overview of how TCP/IP works and what vulnerabilities it has, the consequences of these vulnerabilities, and consumer side solutions.

INTRODUCTION

Technology has always been key in mankind's survival and evolution, shaping and helping society as a whole. Now, our technology has evolved from fire and the wheel to smartphones and watches that monitor your health. Everything in our world is becoming increasingly digital as the internet becomes more integrated into our daily lives. This world of digital objects is called the Internet of Things (IoT). As the Internet of Things grows however, we become more prone to vulnerabilities due to weak security in these devices.

One of the largest problems to arise from these weaknesses is a type of cyber attack known as Distributed Denial of Service (DDoS). This type of attack takes advantage of IoT security weaknesses to flood the resources of its target, which can range from an enterprise or an individual. This can cause millions of dollars in damages to the companies, and the manipulation of IoT devices in these attacks means sensitive consumer data is compromised in the process.

In order for security of IoT devices to improve there must be a better understanding of how these devices work, not only at the consumer level but at the production level with the companies that make them. Cybersecurity is important to consider in product manufacturing, but it is not being

prioritized as much as it should, making IoT devices increasingly vulnerable as technology, and malware, continue to evolve. This, along with the amount of security information the average consumer has, or rather doesn't have, makes IoT devices incredibly susceptible to attacks. This is to say that, while perfect security may not be inevitable, it is possible to better secure our IoT devices, mitigate cyber-attacks, and improve overall protection of sensitive data.

CHAPTER ONE

1.1 THE INTERNET OF THINGS

The Internet of Things (IoT) can be defined as the network of everyday appliances and devices -such as doorbell cameras, smart locks, learning thermostats, or fitbits, to name a few - equipped with computer chips and sensors that collect and transmit data through the internet.**[1]** In 1992, the Internet of Things did not yet exist, as the only device that fit the description was the home computer. Around the early 2000's the laptop -- a smaller, portable version of the home computer -- became available to the public. It would not be until years later that the inception of IoT would come about, circa 2009**[2]**. Since then, the world of devices we define as IoT, has grown considerably.

The prevalence of digital technology is constantly increasing and Internet of Things technology has come with benefits. One prominent solution IoT has brought is an improvement in medical care. For example, there are devices that track vital data which is then transferred to people, like patients or doctors, about critical parts such as irregularities in heart rate or high blood pressure via mobile apps and other linked devices**[3]**. However, while IoT brings us quick solutions, the downside of the Internet of Things is the little to no security that comes with most IoT devices. As

we become more connected to the internet, so do our devices, making it harder to keep confidential information out of the hands of hackers and other unauthorized users**[4]**. To understand the security risks of IoT devices, we will review the structure of the typical IoT device as well as TCP/IP protocol, the data transfer protocol on which most devices operate.

1.2 TCP/IP: A BRIEF HISTORY

TCP/IP, which stands for Transmission Control Protocol/ Internet Protocol, is a data transfer protocol used by modern data networks. TCP/IP is the most widely used networking protocol and came to fruition as a result of ARPAnet.

In the late 1960s, the United States Department of Defense had become concerned with the security and efficacy of their computer systems. The problem was that they had computer systems of machines from different manufacturers and each system's protocols were made specific to their respective corporation which only allowed networking with other systems from the same company; this was an attempt by the manufacturers to lock consumers into their own system in order to get rid of competition. This was an obstacle for security and functionality, especially since the United States' concern was large-scale nuclear attacks, due to tensions with foreign powers at the time. Operating during a potential shut-down from an attack was important, and the Department of Defense wanted all their computer systems to be able to share data across a common network**[5]**.

In order to achieve such a goal, the United States Department of Defense's Advanced Research Projects Agency (ARPA) was assigned to design this network. The main priority of the network was that it would be decentralized with no single point of failure, as this would make networking between computers easier as well as more secure. This new network was called ARPAnet, and its protocols would go on to provide the basis for TCP/IP protocol. The following

section will cover TCP/IP protocol, its layers, and how they work together to transfer data over a network.

1.3 TCP/IP: FUNCTIONALITY & SECURITY WEAKNESSES

1.3.1 TCP/IP:FUNCTIONALITY

Comprised of two protocols, TCP and IP, the TCP/IP protocol is the collection of protocols, named a protocol suite, that dictate how systems should communicate and transfer data from one system to another**[5]**. The TCP/IP model is made up of four layers: a practical and condensed implementation of the seven layer Open Systems Interconnection (OSI) model. The OSI Model is a conceptual layout which breaks down how networking works and was originally the base model for designing protocols.

TCP/IP Model is now the most popular model to use but is largely based on the OSI Model. Each layer is responsible for fulfilling its corresponding role and communicating with the layers above it and below it in order to successfully transfer data successfully**[6]**. We will briefly review of each layer of the TCP/IP model, what layers of the OSI Model they are based on, and how they function.

TCP/IP Model	OSI Model
APPLICATION	Application
	Session
	Presentation
TRANSPORT	Transport
INTERNET	Network
NETWORK	Data Link
	Physical

2.1.1.A Layers of TCP/IP Model vs Layers of OSI Model**[6]**

The Application Layer takes the responsibilities of the the OSI's Application, Presentation, and Session layers. It is in charge of focusing on "process-to process communication across an IP network and provides a firm communication interface and end-user services"**[7]**. This layer is concerned with interacting with the user and provides full end-user access to a variety of shared network services and has the responsibility of error handling and recovery, data flow over a network, and full network flow**[7]**. Essentially, the Application Layer is designed to send and receive data while being user-friendly.

The Transport Layer's responsibility is "end-to-end communication over a network. It provides logical communication between application processes running on different hosts within a layered architecture of protocols and other network components"**[8]**. The Transport Layer is vital for data integrity, which ensures that the data transmitted is the same data that is received. Packets of data that have not been received by the target machine are resent and Transport Layer checks for these failures in order to resend the necessary packets**[8]**.

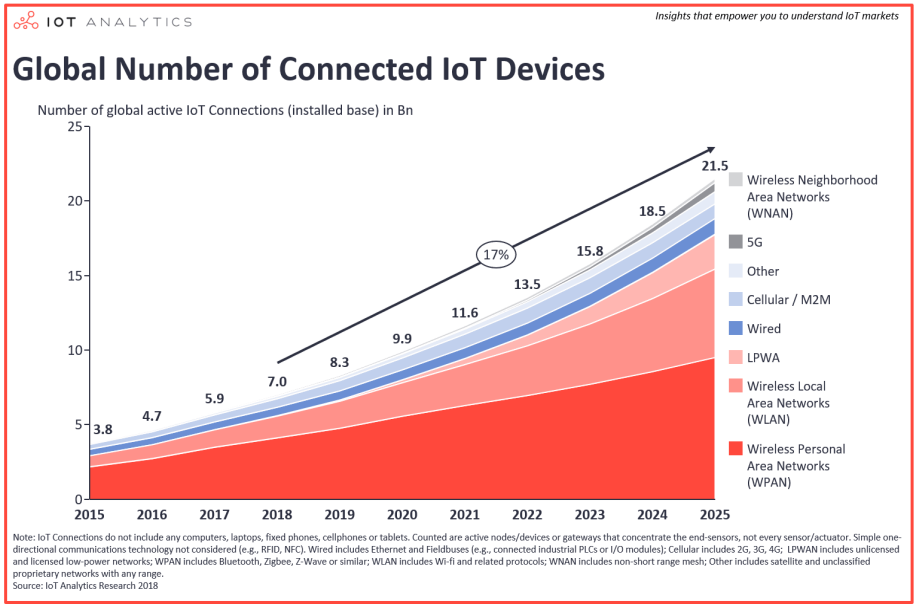
The Internet Layer is tasked with the objective to "[accept and deliver] packets for the network"[6]. This layer is where the IP (Internet Protocol) part of TCP/IP resides. IP protocol is in charge of packet forwarding, routing, and addressing[9]. This means that it is responsible for requesting and sending packets from the transport layer and must know to which machine it is sending the packet. Note that Internet Protocol is important in this layer because Internet Protocol is "the convention which helps two distinctive system elements to speak with each other" **[10]**. TCP/IP's Internet Layer currently uses Internet Protocol version 4 (IPv4) but is slowly transitioning to Internet Protocol version 6 (IPv6).

The Network Layer combines the OSI model's Data Link and Physical Layer. " It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission

of data **[11]**. This means that this layer allows data to be sent via hardware; packets can be sent over mediums in the physical world like copper wire, fiber optic cables, wifi, or ethernet **[12]**.

1.3.2 IPv4 and IPv6

IPv4 was first created in 1980 and provides the logical connection between network devices by providing identification for each device**[13]**. IPv4 uses 32 bit addresses for communication, meaning that it has an address space of 2^{32}. This number, 2^{32}, signifies the 4,294,967,296 possible IP addresses IPv4 is able to create for devices that want to connect to the internet. In 1980, this was considered sufficient and at a first glance 2^{32} is such a large number that the average person can assume this could still be sufficient today. However, because of the drastic increase in IoT devices and the fact that IoT continue to grow, IPv4 is no longer adequate.



1.3.2.A Global Number of Connected IoT Devices (consumer side and company side)**[14]**

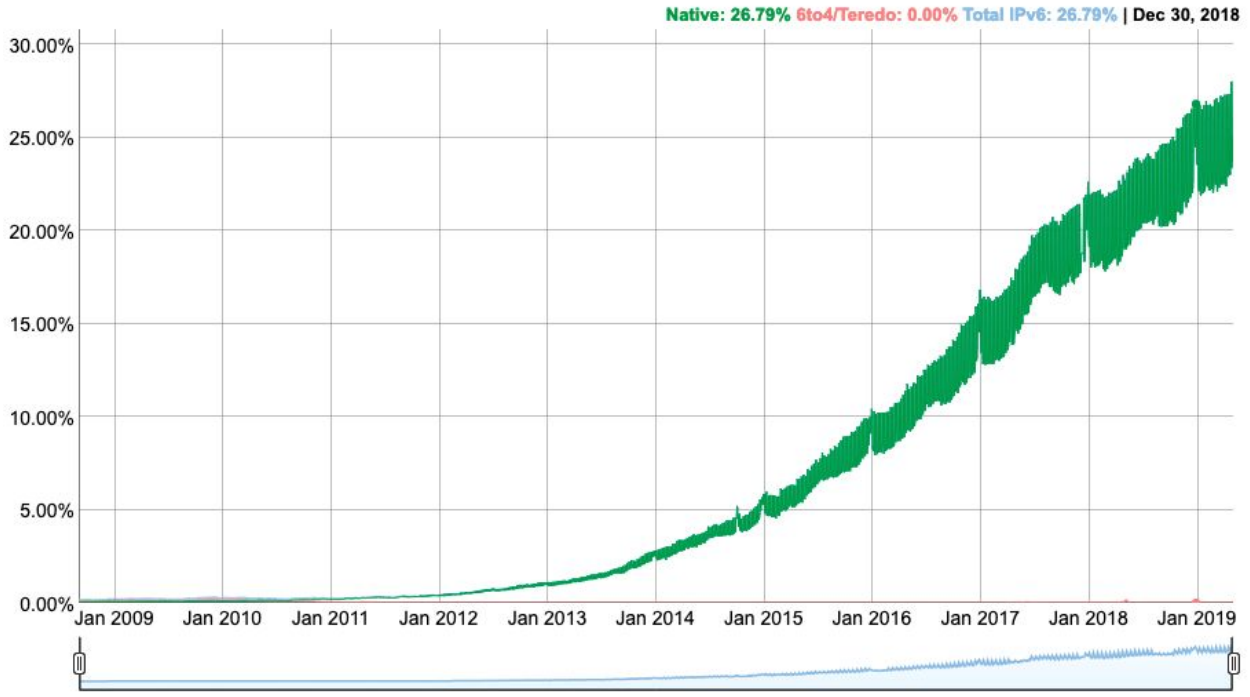
Image 1.3.2A shows the current number of IoT devices and predictions for IoT growth. With this growth rate, it is clear to see that IPv4 is definitely not going to be enough for each device to have its own identification, inevitably leading to IPv4 address exhaustion, where there will not be enough addresses for the amount of devices trying to access the internet at one time. One solution that has allowed IPv4 to mitigate exhaustion issues is Network Address Translation (NAT) **[15]**.

NAT has delayed the problem by allowing many devices to use a single IP address. What this means is that with NAT a single device, "such as a router, [is able to act as] an agent between the Internet (or "public network") and a local (or "private") network. This means that only a single, unique IP address is required to represent an entire group of computers"**[15]**.

IPv6, on the other hand, was created in the late 1990s in order to accommodate the growing amount of IoT devices. Instead of IPv4's 32 bit addressing, IPv6 uses 128 bit addressing. This means that IPv6 can create up to 340 duodecillion possible IP addresses. That's more than enough IP addresses for every grain of sand on earth, and will likely be enough IP addresses for every IoT device for a significantly longer time than IPv4.

However, even though IPv6 is more efficient than IPv4 and has many security improvements, IPv6 is still not used everywhere. Most websites and applications already run on IPv4 and changing to IPv6 is expensive, meaning most companies are not willing to change over to IPv6 since it will cost them more time, resources, and money. Internet Service Providers (ISPs) have stuck to money-saving solutions for IPv4 address exhaustion such as NAT, that allow IPv4 to continue to function.

Despite this, IPv6 is still growing in use online as some websites have started to use both IPv4 with its solutions alongside IPv6. This will help with IPv4 address exhaustion and aide in the transition to IPv6. As of December 30, 2018, 26% of the internet is IPv6 capable, and continues to grow.



Google Statistics on IPv6 adoption (https://www.google.com/intl/en/ipv6/statistics.html)

1.3.3 TCP/IP SECURITY WEAKNESSES

While TCP/IP is one of the most popular forms of networking, it is still susceptible to cyber attacks through weaknesses in the protocols at each layer. Even with the transition from IPv4 to IPv6 in an attempt to make networking more efficient, there have already been cyber attacks on IPv6. One of the most popular types of attacks has become Distributed Denial of Service (DDoS) and has taken advantage of security weaknesses of IoT devices. A DDoS attack is defined as an incident in which a network of computers floods an online resource with high levels of unwanted traffic so that it is inaccessible to legitimate service requests**[16]**.

DDoS attacks take advantage of of Application Layer Protocols by attempting to disrupt any transactions occurring on a network. Any attack on the Application Layer appears as legitimate traffic but its aim to is debilitate services that aid in collecting information. The table below shows the type of DDoS attacks that take advantage of Application Layer protocols and what they do.

APPLICATION LAYER DDoS ATTACKS [17] [18] [19]	
Type of Attack	**What it does**
HTTP/HTTPS Flooding	Botnet is used to send overwhelming amount of HTTP GET or POST requests. Requests appear real to server or application.
FTP Flooding	Influx of SYN requests are sent to FTP server to overwhelm server and use up its resources
Telnet DDoS	Takes advantage of Telnet software flaws.
Mail Bomb	Massive amount of e-mail is sent to a specific person or system. Large amount of e-mail can fill up target's disk space or server.
SQL Slammer	Computer worm that scans for vulnerable systems on the internet. Constant, aggressive scanning can overload networks and slow traffic
DNS Flood	Floods CPU with User Data Protocol (UDP) requests from botnet

Transport Layer-based DDoS attacks are focused on volume. The table below describes how each attack is able to overwhelm its target through flooding it and depleting resources.

TRANSPORT LAYER DDoS ATTACKS [17]	
Type of Attack	**What it does**
SYN Flooding	Influx of SYN requests are sent to use up server resources, causing a system to become unresponsive.**[16]**
UDP Flooding	Large UDP packets are sent to single destination or random ports to overwhelm target
TCP Null Flooding	Floods target using packets of data with missing flags, used in scanning the packet, causing them to be invalid. Overwhelms system in port scanning.

DDoS attacks Internet Layer through TCP/IP protocol vulnerabilities, mostly taking advantage of the Internet Control Message Protocol (ICMP). The table below outlines how vulnerabilities can be taken advantage of.

INTERNET LAYER DDoS ATTACKS [17] [20] [21]	
Type of Attack	**What it does**
Smurf Attack	Large amount of ICMP Echo request packets are sent to overwhelm target.
Fraggle Attack	Similar to Smurf Attack; uses UDP instead of ICMP
Teardrop Attack	Fragmented packets are sent to a target machine, targeting TCP/IP bug in "fragmentation reassembly, the packets overlap one another, crashing the target network device"
ICMP Flooding	Spoofed ICMP packets are sent to target to exhaust resources, degrading server's performance.

DDoS attacks Network Layer and its protocol weaknesses. Many of these attack focus on memory overload or manipulating misconfigured protocols. The table below covers the DDoS attacks that target the Network Layer.

NETWORK LAYER DDoS ATTACKS [23] [24] [25] [26]	
Type of Attack	**What it does**
VLAN Hopping	Attackers take advantage of poor Virtual Local Area Network(VLAN) implementations or misconfigurations which allows the attacker to bypass any security implementations in order to gain access and control of target's traffic.
MAC Flooding	Fills Media Access Control (MAC) address table with fake MAC address/port mappings to overload MAC address memory. Allows attacker to take sensitive data from target network.
DHCP Attack	A Dynamic Host Configuration Protocol (DHCP) server is flooded with DHCP request messages that have spoofed MAC addresses depleting DHCP server's limited IP addressing space.
ARP Spoofing	Fake Address Resolution Protocol (ARP) messages are sent over local area network in order to "[link] an attacker's MAC address with the IP address of a legitimate computer or server on the network [... in order to…] intercept, modify or even stop data in-transit."

CHAPTER TWO

2.1 BOTNETS AND DDOS

In Chapter One, section 1.3.3, we covered the types of DDoS attacks at each layer of TCP/IP. As mentioned previously, a DDoS attack is meant to flood an online resource with high levels of unwanted traffic so that it is inaccessible to legitimate service requests and in order to carry out these large scale attacks, botnets are required**[1]**. In this chapter we will cover motivations for DDoS attacks, what a botnet is and its role in IoT related cyber-attacks.

A botnet is a "collection of internet-connected devices, which may include PCs, servers, mobile devices and Internet of Things devices that are infected and controlled by a common type of malware"("Botnet", Margaret Rouse https://searchsecurity.techtarget.com/definition/botnet). In order to create a botnet, hackers take advantage of IoT devices. Through protocol weaknesses it is possible to corrupt an IoT device; one example of a protocol weakness is IP fragmentation - if a packet is too large it must be fragmented and all fragments must be delivered in order to be reassembled and "before the re-assembly a host must hold partial, fragment datagrams in memory. This opens an opportunity for memory exhaustion attacks**[2]**. Once corrupted, an IoT device becomes part of a botnet. The botnet awaits instructions from a Command & Control server; a computer, usually the hacker's computer, that is used to send commands to the botnet they've created**[3]**. Aside from launching DDoS attacks, botnets can also be used for "stealing private information, exploiting online-banking data, [...] or for spam and phishing emails" (Global Sign, "5 Common Cyber Attacks in the IoT- Threat Alert on a Grand Scale).**[4]** However, we will focus on DDoS, and the ramifications of launched attacks.

2.1.1 DDoS CONSEQUENCES

At the enterprise level, DDoS can affect a company's reputation and financial wellbeing. Any sort of online operations a business may have can come to a halt when attacked via DDoS. The consequence of this is that, because of the overwhelming amount of traffic, real customers trying to reach the website will not be able to. As a result this can damage the reputation of a site and potentially leave customers without an important resource, for example, a news website. Loss of reputation can cause monetary damages in the form of losing consumer trust (and therefore potentially losing future business with those customers), stock prices dropping, mitigation of an attack, recovery of resources, and contractual accountability**[5]**.

On December 32st of 2015, BBC was attacked with what was considered the largest DDoS attack of that time. The website, as well as other services connected to BBC's servers, became unavailable**[6]**. This attack caused one of the largest sources of news to crash and leave people without information on current events, but the damage did not stop there. Once clients realized they could not access the site, they sent emails to BBC to inform the company or complain. This influx of emails also caused the BBC's system to slow down**[7]**. Additionally, once a company is unable to provide their clients with the service they are contractually obligated to provide, known as a Service-Level agreement, clients have the right to ask for compensation**[8]**. If enough clients request this, the company can suffer financially. This adds more financial strain on top of the monetary losses from being attacked, attempting to mitigate the attack, and recovering their systems.

DDoS is such an effective attack that a simple email threatening to launch an attack can cause a company to suffer thousands of dollars in losses, in some instances up to $100,000, to pay off a potential hacker**[9]**. The cost of an actual attack can be much more: it is not clear exactly how

much money a company can lose from an attack as oftentimes, companies do not report attacks to save their reputation. However according to "security software manufacturer Symantec Corp., [...] cybercrime is costing the world $110 billion every year"**[10]**.

As DDoS attacks increase, accessibility to DDoS attack services has also become easier. There are now online services where average people can pay cybercriminals, at a low price, to launch an attack on the target of their choice**[11]**. Depending on the size of the attack, the price for a a DDoS attack can range "from $5 for a 300-second attack to $400 for 24 hours"**[12]**. Motivations for launching an attack are**[13]**:

- **Revenge**: Employees or customers of a company might feel wronged and want revenge
- **Competition**: Companies can launch attacks to interfere with other companies' operations
- **Politics**: radical political organizations can launch attacks based on what they believe is right
- **War**: Countries at war can attack each other on a digital level as opposed to physical
- **Extortion**: threatening to launch an attack can make money quickly and easily

To summarize, DDoS attacks can wreak financial havoc on companies while being extremely lucrative for hackers and affordable for anyone who wishes to launch an attack.

Attackers, as stated earlier, require botnets to launch DDoS attacks. We know that botnets are comprised of internet connected devices and IoT devices are being used more often in creating botnets. Corrupted devices could potentially be used by hackers if the device collects data that can be easily accessed, such as credit card information or devices that can control things in your home, like garage doors, thermostats, locks, etc.**[14][15]**. For consumers, the average person does not know how to tell if their devices are part of a botnet, or what to do in the event of IoT device corruption. In the following chapter we will cover steps companies have taken so far to improve security and solutions consumers can use to better secure their IoT devices.

CHAPTER THREE

3.1 COMPANY SECURITY STANDARDS & CONSUMER SOLUTIONS

The following chapter will cover company security standards and basic things the average, non-tech savvy consumer can do to better improve their IoT device security and monitor their devices.

Because of the growing concern for IoT security integrity, lawmakers are beginning to take a stance in implementing laws that will help improve the standards for IoT security. "California's new SB 327 law, which will take effect in January 2020, requires all 'connected devices' to have a 'reasonable security feature' "**[1]**. One example covered in the new SB 327 law is that the "preprogrammed password is unique to each device manufactured" **[2]** which would make default settings on IoT devices more secure. This is a step in the right direction since there will be a mandatory minimum for IoT security. However, since security does cost money, it will come as no surprise if companies do their best to provide exactly the minimum and nothing more to mitigate spending.

However, while cutting costs on security might seem like a good idea in the production level, as we have seen in previous chapters, the long term effects can cost a company even more money. One might ask what a company can and should do to improve security. These are some examples best practices for IoT security improvement that companies can follow **[3][4]**:

- Companies can invest in penetration testing, "a simulated cyber attack against [their own] system to check for exploitable vulnerabilities"**[4]**, as this will allow risks and vulnerabilities to show themselves at production level where they can be fixed or improved upon before release.
- Companies can encrypt all data stored in the device, this will improve data security.
- Companies can use authentication schemes to confirm connections can be trusted rather than just connecting to anything.

While there is a lot companies can do to improve IoT security at the production level, consumers also have a responsibility to protect their devices as well as they can. It is important to have some basic knowledge on how to monitor and protect one's devices as it has been estimated that the average IoT device is compromised after being online for 6 minutes. **[5]**The reason for this is that "each hour these devices are tested for vulnerabilities - at least 800 times per hour - with an average of 400 login attempts occurring daily. On average, hackers try to access one IoT device every five minutes and a total of 66 per cent of their attempts end up being successful"**[5].**Since the average consumer is typically not familiar with high-level security implementation, we will look at solutions that are accessible to everyone.

Once you have purchased your device, "visit the manufacturer's website and download any new security patches for known vulnerabilities. Also, without exception, immediately reset any default passwords with secure passwords"**[6]**. If you change the default password you already one step ahead of the average consumer; the next step is to develop secure passwords. Passwords like "[Pet Name][Birth Year]" are short and not secure.

Additionally, if someone has enough information about you, they can figure out your password through social hacking, meaning that they will get to know you and get information out of you personally rather than writing scripts. An example of a good password may be "A+^/r7Wb&uraTSW<". Although it may be difficult to remember at first, having complex passwords that have nothing to do with personal information will go a long way in protecting your devices.

Routers usually come with built-in firewalls that have basic firewall rules. Sometimes it may not be enabled so it is a good idea to "log in to the router per the manufacturer's instructions and confirm that the firewall feature is enabled"**[6]**. Additionally, firewalls can be managed and configured to be more secure. A user can manage and maintain their firewall rules to dictate what devices are allowed to reach which sites**[7]**. This is important as IoT devices can be prevented from accepting requests to reach unfamiliar websites, which can then corrupt them.

Virtual Network Proxies (VPNs) can also provide some level of security. A VPN connects your device to another server in a different location, allowing you to "browse the internet using that computer's internet connection"**[8]**. This type of service grants users more privacy online. While

VPNs are not the best security solution for IoT devices, using a VPN service can help secure PCs by protecting user data.

In the event that a consumer's device has been compromised or the consumer suspects the device has been compromised, there are a few options for what to do. One option is to hard reset a device, which will allow the device to go back to its original factory settings which deletes all data. In this way, even if the device has been compromised, your data is no longer saved onto the device. Once you complete a factory reset you can either change the password to the device to make it more secure, or opt to purchase a newer model with better security. However, security practices should be maintained to minimize the risk of a device being compromised once again**[9]**.

CONCLUSION

Ultimately, security for devices will never be 100% perfect. Improvements will continue to be made and people will continue to test the limits of new standards, updated protocols, and improved architecture. Therefore, while some of the solutions presented may seem obvious, many people overlook these steps, which can in turn contribute to their devices being compromised and become part of a botnet. The more informed the public becomes about securing their own devices and the stricter security standards for companies become, there is a chance that, although DDoS will never be full avoidable, increased responsibility can definitely help reduce attack rates and improve overall security for IoT devices.

BIBLIOGRAPHY

CHAPTER ONE

1. *18 Most Popular IoT Devices in 2019 (Only Noteworthy IoT Products)*. https://www.softwaretestinghelp.com/iot-devices/. Accessed 14 May 2019.
2. Behind The Numbers: Growth in the Internet of Things | NCTA — The Internet & Television Association. https://www.ncta.com/whats-new/behind-the-numbers-growth-in-the-internet-of-things-2. Accessed 20 Dec 2018.
3. Internet of Things in Healthcare: Applications, Benefits, and Challenges. https://www.peerbits.com/blog/internet-of-things-healthcare-applications-benefits-and-challenges.html. Accessed 13 Feb 2019.
4. "Internet of Things (IoT): Pros and Cons." KeyInfo, 30 Sept. 2016, https://www.keyinfo.com/pros-and-cons-of-the-internet-of-things-iot/.
5. The TCP/IP Guide - TCP/IP Overview and History. http://www.tcpipguide.com/free/t_TCPIPOverviewandHistory.htm. Accessed 20 Nov 2018.
6. https://docs.oracle.com/cd/E19253-01/816-4554/ipov-10/index.html. Accessed 2 May 2019.
7. "What Is the Application Layer? - Definition from Techopedia." Techopedia.Com, https://www.techopedia.com/definition/6006/application-layer. Accessed 9 April 2019.
8. "What Is the Transport Layer? - Definition from Techopedia." Techopedia.Com, https://www.techopedia.com/definition/9760/transport-layer. Accessed 9 April 2019.
9. "Network Layers Explained: OSI & TCP/IP Models [with Examples]." Plixer, 28 Nov. 2018, https://www.plixer.com/blog/network-monitoring/network-layers-explained/.
10. "The Importance of Internet Protocol." *Eatabbo*, 26 May 2018, https://www.eatabbo.org/technology/the-importance-of-internet-protocol.htm.
11. "Computer Network | TCP/IP Model." GeeksforGeeks, 4 Oct. 2017, https://www.geeksforgeeks.org/computer-network-tcpip-model/. Accessed 10 Oct. 2018
12. "What Is the Physical Layer? - Definition from Techopedia." Techopedia.Com, https://www.techopedia.com/definition/8866/physical-layer. Accessed 13 March 2019.
13. "What Is Internet Protocol Version 4 (IPv4)? - Definition from Techopedia." Techopedia.Com, https://www.techopedia.com/definition/5367/internet-protocol-version-4-ipv4. Accessed 13 March 2019.
14. State of the IoT 2018: Number of IoT Devices Now at 7B – Market Accelerating. https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/.
15. "How Network Address Translation Works." HowStuffWorks, 2 Feb. 2001, https://computer.howstuffworks.com/nat.htm.
16. "The Definition of Ddos." Www.Dictionary.Com, https://www.dictionary.com/browse/ddos. Accessed 16 Oct. 2018.

17. https://pdfs.semanticscholar.org/c787/890383127933d351ec0f449f3e01792485f9.pdf
18. "Types of Attacks - DDoS Part 2." Cloudbric, 26 Jan. 2015, https://www.cloudbric.com/blog/2015/01/types-of-attacks-ddos-2/.
19. Vamosi, Robert. "SQL Slammer: How It Works--Prevent It." ZDNet, https://www.zdnet.com/article/sql-slammer-how-it-works-prevent-it/. Accessed 13 March 2019.
20. What Is a Smurf Attack | DDoS Attack Glossary | Imperva." Learning Center, https://www.imperva.com/learn/application-security/smurf-attack-ddos/. Accessed 5 Jan 2019.
21. https://security.radware.com/ddos-knowledge-center/ddospedia/teardrop-attack/. Accessed 5 Jan 2019.
22. "35 Types of DDoS Attacks (That Hackers Will Use Against You in 2019)." JavaPipe, 13 Jan. 2018, https://javapipe.com/blog/ddos-types/.
23. VLAN Hopping: How to Prevent an Attack. https://www.alienvault.com/blogs/security-essentials/vlan-hopping-and-mitigation. Accessed 2 May 2019.
24. What Is MAC Flooding Attack and How to Prevent MAC Flooding Attack. http://www.omnisecu.com/ccna-security/what-is-mac-flooding-attack-how-to-prevent-mac-flooding-attack.php. Accessed 25 April 2019.
25. DHCP Starvation Attacks and DHCP Spoofing Attacks. http://www.omnisecu.com/ccna-security/dhcp-starvation-attacks-and-dhcp-spoofing-attacks.php. Accessed 4 April 2019.
26. ARP Spoofing | Veracode. https://www.veracode.com/security/arp-spoofing. Accessed 5 Feb. 2019.

CHAPTER TWO

1. "The Definition of Ddos." *Www.Dictionary.Com*, https://www.dictionary.com/browse/ddos. Accessed 16 Oct. 2018.
2. "Broken Packets: IP Fragmentation Is Flawed." *The Cloudflare Blog*, 18 Aug. 2017, https://blog.cloudflare.com/ip-fragmentation-is-broken/.
3. *Command and Control [C&C] Server - Definition - Trend Micro USA*. https://www.trendmicro.com/vinfo/us/security/definition/command-and-control-server. Accessed 5 Feb. 2019.
4. *5 Common Cyber Attacks in the IoT*. https://www.globalsign.com/en/blog/five-common-cyber-attacks-in-the-iot. Accessed 5 Feb. 2019.
5. Kerravala, Zeus. "Securing the IoT Has Become Business-Critical." *Network World*, 16 Nov. 2018, https://www.networkworld.com/article/3321919/securing-the-iot-has-become-business-critical.html.
6. Knecht, Tobias. *5 Biggest DDoS Attacks Of The Past Decade*. https://www.abusix.com/blog/5-biggest-ddos-attacks-of-the-past-decade. Accessed 12 Jan. 2019.
7. "TeskaLabs Blog · How DDoS Attacks Can Sink Your Business." *TeskaLabs Blog*, https://teskalabs.com/blog/how-ddos-can-sink-your-business. Accessed 5 March 2019.

8. Rana, Omer F., et al. "Managing Violations in Service Level Agreements." *Grid Middleware and Services*, Springer US, 2008, pp. 349–58. *Crossref*, doi:10.1007/978-0-387-78446-5_23.
9. Osborne, Charlie. "How Cybercriminals Earned $100,000 Just by Sending a DDoS Threat Email." *ZDNet*, https://www.zdnet.com/article/empty-armada-ddos-threats-cost-businesses-100000/. Accessed 11 May 2019.
10. Hyman, Paul. "Cybercrime: It's Serious, but Exactly How Serious?" *Communications of the ACM*, vol. 56, no. 3, Mar. 2013, p. 18. *Crossref*, doi:10.1145/2428556.2428563.
11. *The Cost of Launching a DDoS Attack*. https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/. Accessed 11 May 2019.
12. "How Much Costs a DDoS Attack Service? Which Factors Influence the Final Price?" *Security Affairs*, 26 Mar. 2017, https://securityaffairs.co/wordpress/57429/cyber-crime/cost-ddos-attack-service.html.
13. "The 5 Motives for DDoS Attack." *Simplicable*, https://arch.simplicable.com/arch/new/the-5-motives-for-DDoS-attack. Accessed 2 May 2019.
14. "IoT and Payments: Current Market Landscape." *Secure Technology Alliance*, https://www.securetechalliance.org/wp-content/uploads/IoT-Payments-WP-Final-Nov-2017.pdf Accessed 10 Feb 2019
15. *New IoT Security Regulations - Schneier on Security*. https://www.schneier.com/blog/archives/2018/11/new_iot_securit.html. Accessed 20 Jan 2019.

CHAPTER THREE

1. *New IoT Security Regulations - Schneier on Security*. https://www.schneier.com/blog/archives/2018/11/new_iot_securit.html. Accessed 20 Jan 2019.
2. *Bill Text - SB-327 Information Privacy: Connected Devices.* https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327. Accessed 14 May 2019.
3. Kerravala, Zeus. "Securing the IoT Has Become Business-Critical." *Network World*, 16 Nov. 2018, https://www.networkworld.com/article/3321919/securing-the-iot-has-become-business-critical.html.
4. "What Is Penetration Testing | Step-By-Step Process & Methods | Imperva." *Learning Center*, https://www.imperva.com/learn/application-security/penetration-testing/. Accessed 14 May 2019.
5. October 18, Anthony Spadafora, and 2016 Security. "The Average IoT Device Is Compromised after Being Online for 6 Minutes." *IT Pro Portal*, https://www.itproportal.com/news/the-average-iot-device-is-compromised-after-being-online-for-6-minutes/. Accessed 20 April 2019.

6. "Securing Your "Internet of Things" Devices ." ,*Consumer Technology Association,* https://www.justice.gov/criminal-ccips/page/file/984001/download
7. "How to Configure a Firewall in 5 Steps." *SecurityMetrics*, https://www.securitymetrics.com/blog/how-configure-firewall-5-steps. Accessed 14 May 2019.
8. Hoffman, Chris. "What Is a VPN, and Why Would I Need One?" How-To Geek, https://www.howtogeek.com/133680/htg-explains-what-is-a-vpn/. Accessed 14 May 2019.
9. "How to Tell If Your IoT Devices Are Part of a Botnet." NextAdvisor Blog, 15 Dec. 2017, /blog/how-to-tell-if-your-iot-devices-are-part-of-a-botnet/.