Analysis of Vulnerabilities in IOT Devices and the Solutions

Thomas F. Freeman Honors College
Senior Thesis
By
Jimara Thomas
B.S. Computer Science
College of Science, Engineering, and Technology
May 2021

APPROVED BY

Qi Yi 4/16/2021

HONORS FACULTY FELLOW MENTOR **DATE**

Dr. Dianne Jemison Pollard April 18, 2021

DEAN, HONORS COLLEGE **DATE**

TSU
TEXAS SOUTHERN UNIVERSITY
Thomas F. Freeman Honors College

An Analysis of Vulnerabilities in IOT Devices & Solutions

Jimara Thomas, Department of Computer Science, Texas Southern University

Abstract:

This thesis analyzes the insecurities in IOT devices, why these insecurities exist, and solutions to fix these vulnerabilities. IoT (Internet of Things) devices are nonstandard computing devices that connect wirelessly to a network that will transmit data. The amount of IOT devices continues to increase, as the demand for the items increases. It is predicted that there will be about 26 billion IOT devices installed by 2020. They have been improving on the amount of functionality they were previously able to do. For instance, Amazon's Alexa is a speaker that can order items for you from the Amazon website, play your favorite music via Spotify, amazon music, or play music and much more. This requires Alexa to be logged into each one of those accounts to do this. With this information, there is a lot more personal information going in and out of the device. As the demand for the products increases, manufacturers begin to feel the pressure of having to push out products. They feel so much pressure that they skip important features of the IOT devices, including security. This lack of security opens users up to attacks and vulnerabilities from hackers that are trying to steal personal information. Therefore, consumers need to know the steps to take, in order to secure all their information, and the type of attacks and techniques hackers will use to get their private information.

Keywords: Vulnerability - IOT (Internet of Things) – Cyber Security- Hacking-RFID - Wi-fi - Barcode - Bluetooth - Risk - Hardware - Software

Table of Contents

Section Page

List of Tables

List of Figures

Dedication

I dedicate this thesis to my mother. She introduced me to computer science and has loved, supported, and taught me to the best of her ability.

I dedicate this thesis to my person. He has supported me the past 3 years, and even when he knows nothing of the subject, he is still right by my side, supporting me in any way.

I dedicate this thesis to the students and staff of the honors college. They gave me an opportunity to be the best and brightest in the school. They exposed me to so many different subjects, and I have gained memories, learning, and people that I will cherish forever.

I dedicate this thesis to Black women in computer science. Thankful to those that have come before me, and may the ones that come after be successful in every professional aspect of their lives.

Acknowledgements

I would like to acknowledge my faculty mentor, Dr. Yi Qi. She has helped formulate my concepts and articulate my words through every chapter of this thesis. I truly appreciate all of her help.

I would like to acknowledge my group in my capstone project course. We came up with the idea of a vulnerability scanner, and it was a big idea but none of us backed away. We put in a lot of effort, through the pandemic, to deliver a project that was far from finished, but we were proud of it.

Chapter 1: Introduction

The purpose of this thesis is to show the risks within IoT (Internet of Things) devices that are not protected by conventional security measures and to find solutions to combat common IoT vulnerabilities. We will analyze the insecurities in IoT devices, why these insecurities exist, and solutions to the security problems on these devices. We begin by defining IoT devices. IoT devices are nonstandard computing devices that connect wirelessly to a network that will transmit data. These devices connect humans, things, and technology. They are used throughout the world in a multitude of fields, to satisfy different needs. We can use these devices in our private, professional, and public lives. They can be used to collect information and send it and receive information and then act on it. With all these functionalities, the amount of IOT devices continues to increase, and the demand for the items increases. It is predicted that there will be about 26 billion IOT devices installed by 2020. They have been improving the amount of functionality they were previously able to do. For instance, Amazon's Alexa is a speaker that can order items for you from the Amazon website, play your favorite music via Spotify, amazon music, or play music and much more. This requires Alexa to be logged into each one of those accounts to do this. With this information, there is a lot more personal information going in and out of the device. As the demand for the products increases, manufacturers begin to feel the pressure of having to push out products. They feel so much pressure that they skip important features of the IOT devices, including security. As the popularity of IOT devices increase, consumers are put at more of a risk companies try to push out IOT products as soon as possible, so there is an extreme lack of security in IOT devices, and many users are not aware of the potential risk that their information is in and they do not know how to properly protect themselves. So, the vulnerabilities that arise on IOT devices, due to the lack of security resources can be devastating to certain networks. This lack of security opens users up to attacks and vulnerabilities from hackers that are trying to steal personal information. Therefore, consumers need to know the steps to take, to secure all their information, and the type of attacks and techniques hackers will use to get their private information. As a result, it is important to try and find solutions for consumers to protect their sensitive information. We also come up with simple solutions to many common vulnerabilities, and propose a system that will help solve some of these vulnerabilities because this system will allow the insecurities to be detected.

Overview of IOT Devices:

Definition(s) & Differences between IOT & traditional devices:

Many different technical professionals have come together to curate different definitions of Internet of Things (IoT) devices. A basic definition of IoT devices is [things] that are connected to the internet (Viswanathan et. al, 2019). Williams et al. (2017), expands upon this definition by stating that the IoT "has been dubbed as 'the next generation of the Internet'. While definitions vary, the IoT can be described as a combination of technologies, including sensors, actuators, and smart objects with the purpose of connecting "all" things for increased convenience and productivity" (Williams et al., 2017). Stanislav & Beardsley (2015) go a step further to explain that "we can think of a 'Thing' with 'Internet' as simply any device, regardless of size, use, or form factor, that contains a CPU and memory, runs software, and has a network interface which allows it to communicate to other devices, usually as a client, sometimes as a server." Also, these devices have a simple development that includes deployment, monitoring, servicing, managing, updates, and decommissioning. ("Internet Of Things (IoT) Testing", 2020). Thus, it can be seen in Figure 1.1. An example of these devices includes smart cars, smart refrigerators, and smart watches. IoT devices have many benefits including, productivity improvement, predictive analysis, rapid response, reduction of human error, creation of new business opportunities, new capabilities to predict and act, strong monitoring feature, increased customer dialog, fine-tunes services and products, new revenue streams and improvement of control of operation processes. Productivity improvement shows that IoT devices allow the monitoring and control of different processes, which optimizes the different operations that increase productivity and efficiency. The predictive analysis shows that IoT's technologies make it possible to see recurring patterns and contribute to maintenance. The rapid response shows that the data makes it possible to monitor the systems in place in real-time. Reduction of human error means that IoT makes it possible to reduce human errors from repetitive tasks. (Reed, 2019) New business opportunities can be used to uncover business insights and opportunities and reduce operational costs. New capabilities to predict and act is when the device can predict needs before they arise, and act based on insights from the network. Monitoring improvement allows the IoT device to provide the capability to manage a network. The increase of customer dialog allows the IoT device to interact with the customers more often. Fine-tuning of services and products includes businesses being able to improve their products. New revenue streams allow businesses to set up and roll out new products and services. Lastly, improving control of operation processes include the IoT's ability to improve and enhance controls.

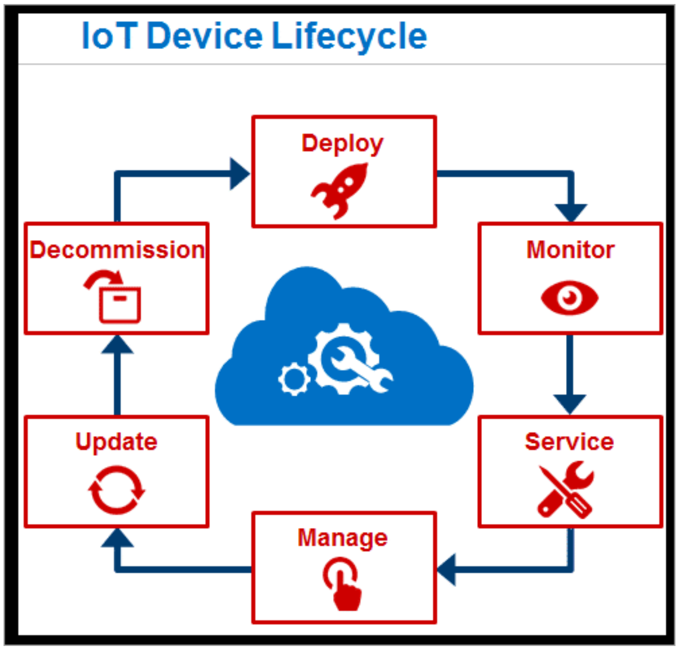
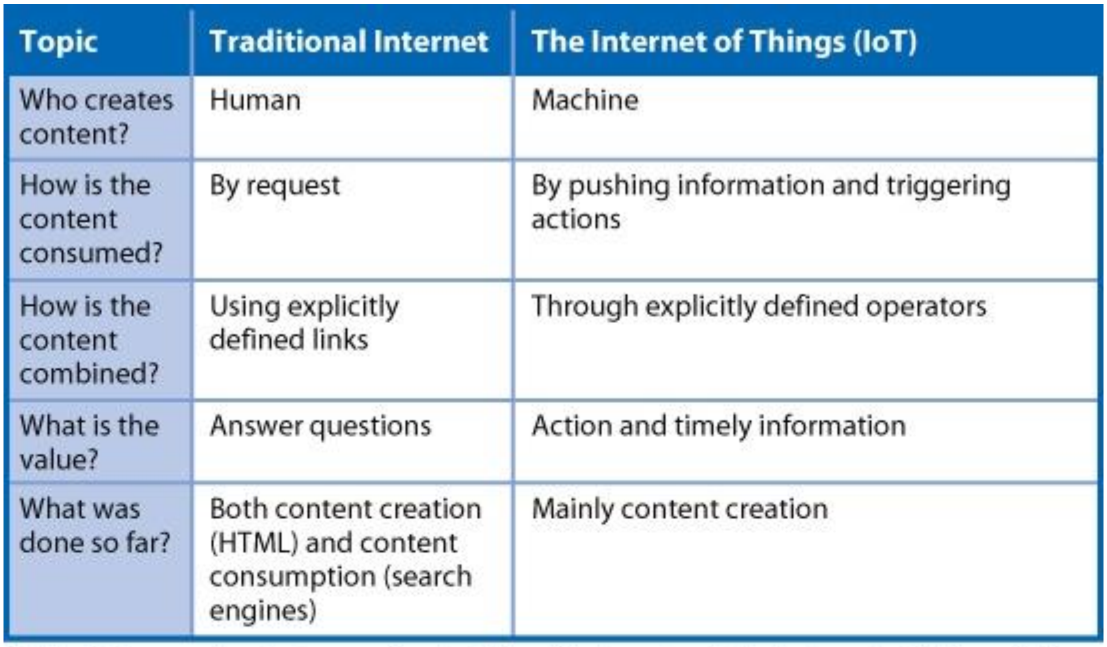


Figure 1.1: The lifecycle of the development of an IoT device.

Source: *All You Need to Know About The IoT (Internet of Things).* TC Global Insights. (2020).

The differences in IOT devices and traditional computers can be seen in their different purposes, and different design. Usually, IoT devices do not resemble traditional computers. They do not have a typical keyboard and mouse interface, and they often have a user interface not centered around a monitor or other text-filled screen (Stanislav & Beardsley, 2015). Also, they are different in how users interact with these devices. Some IoT devices require very limited interaction from users. Once the device has been set up, sensors allow it to generate data autonomously. Other devices foster more interaction with the user by providing a greater variety of access (Williams et al, 2017). For a traditional device to be updated and considered an IoT device, "it must connect to the Internet in any way, and it must integrate with technologies with sensors, actuators, and functional software("Internet Of Things (IoT) Testing", 2020). When these are combined, they create an IoT device. Furthermore, the traditional devices are consumed by request, while the IoT is consumed through pushing the technology as a notification or action when a situation is detected.



Topic	Traditional Internet	The Internet of Things (IoT)
Who creates content?	Human	Machine
How is the content consumed?	By request	By pushing information and triggering actions
How is the content combined?	Using explicitly defined links	Through explicitly defined operators
What is the value?	Answer questions	Action and timely information
What was done so far?	Both content creation (HTML) and content consumption (search engines)	Mainly content creation

Table 1. Comparison between the traditional Internet and the Internet of Things (IoT)

Source: Dr. Opher E (2015). Differences between the IoT and Traditional Internet.

Another key difference is in the value to the consumer. In traditional devices, the value “resides in answering a question that is posed to the consumer” (“Internet Of Things (IoT) Testing”, 2020). Whereas, in IoT devices the value is based on situations and notifications. These differences are listed in Table 1.1.

IoT devices have grown very popular throughout recent years, and recent studies have shown that number is projected to reach 1.5 billion IoT devices with cellular connections in 2022, or around 70 percent of the wide-area category.(“Internet of Things Forecast”, n.d.) Also, a study shows that 86 percent of businesses will increase their spending on IOT devices in 2019, and after. Financially, Opportunities in the IoT, predicts that the markets of IOT devices will double from $235 billion in 2017 to appx. $520 billion in 2021. (Viswanathan et. al, 2019) As far as security, HP's security arm, discovered that about 70% of popular IoT devices can be hacked quite easily. About 48% of U.S. companies using IoT devices have had their networks compromised according to consulting firm Altman Vilandrie & Company. The firm also found that these types of attacks can cause some serious financial and legal damage — up to 13% of the annual revenues of small companies. (M., 2017). According to a 2019 IoT survey, 46 percent of respondents are driven to spend more on IoT technologies for improved security. Better data analytics capabilities and improved daily operational efficiencies are also important drivers behind increasing IoT spending (Vailshery, 2021). Approximately 7.62 billion humans on our planet, but it is projected that by the year 2021 with an increasing graph of IoT devices, there may be around 20 billion IoT smart devices up and running with an increase in the demand of 5g network (Vailshery, 2021). More statistics can be seen in Figure 1.2.

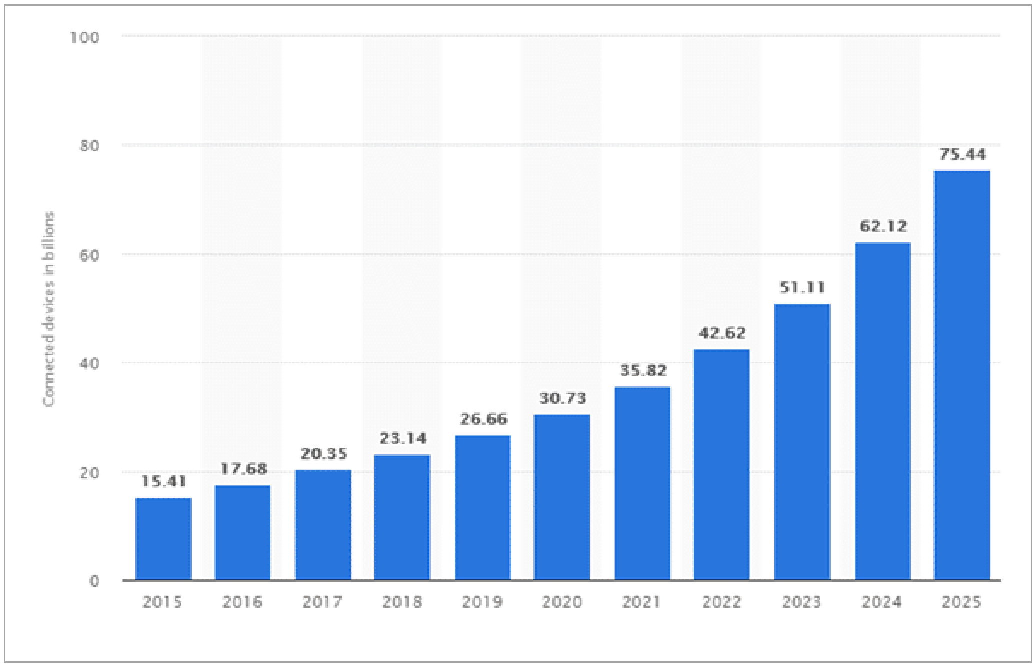


Table 1.2: This table shows how IoT devices will increase from 2015-2025.

Source: Statista Research Department. *Internet of Things - number of connected devices worldwide 2015-2025.* (2016).

How IOT Devices Work and Connect:

IOT devices have many ways of connecting to different devices and one another. This section will examine the different ways IOT devices can connect to other technologies via the Internet.

1. Radio Frequency Identification Devise (RDFID):

Radio Frequency Identification is a form of technology that uses radio frequencies to transmit data. It is used to automatically identify an object and capture data about that object that has been stored in a small microchip tag and is attached to the object. This happens using RFID tags that can be deployed in specific spots. The RFID tag has a built-in antenna that communicates to a scanning device that reads the data remotely. The data is then transferred from the scanning device to the enterprise application software that houses the data. Each RFID tag has its own unique identifying number. There are two kinds of RFID tags, including active tags and passive tags. Active tags have an internal power supply, while passive tags do not have an internal power supply. The tags communicate with an RFID reader (Suresh et al, 2014). This can be used to record and control the movement of assets and personnel.

2. Wireless Fidelity (Wi-fi):

Wi-fi is a wireless connection that can be used to send/receive data, signals, commands, etc. They work between the frequencies of 2.4GHz- 60GHz. This connection is now a default setting in all smart phones, and most smart devices. The WLAN standard only requires a transceiver to span the range around it. Wi-fi is simple and low-cost, and this has made wi-fi very popular, in recent years. It is very common to see Wi-fi connection in the public, schools, hospitals, etc. This is an advantage to adding IoT to the public. (Suresh et al, 2014) To use Wi-Fi for an IoT device, you need a microchip, and firmware to manage the device's Wi-Fi credentials. Most devices that use Wi-fi are large hubs, and they need to be close to a Wi-fi access point.

3. Barcode & Quick Response (QR) Code:

A barcode is a symbol that can be attached to every object and is only read by a barcode scanner. They began in the 1970's and can now be seen everywhere in most objects. They can be implemented simply and have no technological difficulties. As they have become more popular, so has the updated 2D matrix, the QR code. A QR code is a machine-readable two-dimensional barcode that gives people information. A camera can identify the details of many things using the QR code. This is like the RFID, but they differ in size. Combining RFID tags with barcodes and QR codes allows consumers to connect to the IoT device with a scan, Having the device marked with a QR or barcode means an improvement to retail environments. This would be simpler for IoT devices. (Suresh et al, 2014) For brands, they can program QR codes to let them know when an item is scanned, something that would tell them if there's an increase or decrease of consumer interest in their offerings.

4. Bluetooth:

To be compatible with Bluetooth, an IoT device must have a microprocessor that handles Bluetooth. There are two different versions of Bluetooth that are used by IoT devices, which are Bluetooth Classic and Bluetooth Low Energy. Bluetooth has become a very popular technology among mobile phones. "They have an open wireless technology for PAN at 2.4 GHz (Suresh et al, 2014) The most popular assets in Bluetooth technology are the inventions of the "Bluetooth low energy" and the "Bluetooth smart" technology. Since its invention in 1998, Bluetooth has many advancements in the technology industry. Mobile phones use Bluetooth technology, which was followed by the Bluetooth mouse, keyboard, printer, etc. The interconnectivity that Bluetooth offers is essential to IoT devices, as Bluetooth is one of the reasons IoT has become so popular. Also, Bluetooth requires physical proximity to initiate signal broadcast so there is no possibility of remote attacks, and Bluetooth requires less energy than other connections, so it is better for low power IoT devices.

The rest of the essay will continue as follows:

Chapter two

We will discuss the reasons why IoT devices are so vulnerable. First, we will discuss all the different areas IoT devices are involved in. Then, we discuss how these areas are affected by the lack of security in IoT devices. We also go into different devices that were directly affected by vulnerabilities.

Chapter three

We will discuss the different vulnerabilities that are most common in IoT devices. First, we define vulnerabilities and unethical hacking. Then we move on to different types of IoT vulnerabilities.

Chapter four

We will discuss solutions to the vulnerabilities discussed in the previous chapter. First, we discuss the different types of solutions that are helpful to the business and the consumer. Then, we discuss awareness of vulnerabilities and how to detect them. I will introduce a scanner that will and can be used to detect vulnerabilities in an IoT device.

Chapter Five: Conclusions and Recommendations

This chapter will conclude our thesis.

Chapter 2: Why Are IoT Devices so Vulnerable?

The vulnerability of IoT devices has been discussed since their beginning. This chapter will cover how many areas Iot devices are involved in and why IoT devices are so vulnerable compared to traditional devices. Besides, examples of some typical IoT devices being hacked are provided.

Different Areas for IOT Devices:

IOT Devices can be used in a multitude of different fields and have many different purposes. They can be separated into three different categories, based on who they serve. These categories include the public, the business, and the personal. IoT Devices can be further categorized by the way that they are used within the public, business, and personal divisions.

<u>Personal Division:</u>

- Smart Health & Wellbeing

These devices allow consumers to wear them in the form of clothes, watches, and telephones, while they are doing other things, such as, exercising, eating, working, sleeping, etc. This form of IoT device monitors the person’s health (physical, mental, emotional), analyzes their healing, notifies the appropriate facilities (doctors, family, 911), makes recommendations, or helps with appropriate actions. For instance, they can help to keep track of fitness goals. This also helps in the business and public sectors, as hospitals can use these systems to monitor medical equipment, drugs, and instruments, using IoT devices. (Economidas, 2017) Hospitals and medical facilities use patient monitors, X-ray devices, trackers and other wearables that connect to a network, and IoT devices cut cost significantly.

- Smart Home

This type of IoT device continuously monitors the home’s safety (motion detection, smoke, gas), environment (heat, air), appliances, equipment, security, and surveillance, makes recommendations or systems to certain states(temperature). Users of these devices could be anyone from infants to the elderly. Also, a user would control and manage home appliances, entertainment devices, and eventually the whole home. -(Economidas, 2017)

- Smart Education

This type of IoT device allows for the continuous monitoring of the learner and encourages them, recommends educational material, and asks appropriate questions depending on the progress of the student. Also, the device can notify the teacher, administrator, and parents about the learner’s progress. (Economidas, 2017)

Public Division:

- Smart Environment

This type of IoT system monitors the environment and tells users about pollution, radiation, extreme weather conditions, natural disasters, etc. Rescuers can use this IoT system to help rescue people in danger. Also, IoT systems can be exploited for territorial monitoring, surveillance, and border protection. (Economidas, 2017)

- Smart Utilities

These IoT systems can be used for smart metering, maintenance, and billing of utilities. (Economidas, 2017)

- Smart City/Community

This refers to automating an entire city or environment and managing it all through the Internet. For example, controlling traffic signals, and monitoring pollution. (Farda)

Business Division:

- Smart Building

This type of IoT device helps monitor and control the building's access, and environments, such as, lighting, temperature, equipment, and resource usage. They can be used for metering to control energy so that it will be able to reduce cost. Furthermore, they can be used for security and surveillance, in case of emergency and take appropriate actions. (Economidas, 2017)

- Smart Industry

This type of IoT system can be used in smart factories, manufacturing, mining, and construction to improve production. (Economidas, 2017) Many companies have interest in chemical sensors and systems, and they want to use IoT for monitoring the operation infrastructure as the need to connect modern machines increases. (Reshetchenko, 2018)

- Smart Services

This type of IoT system can be used in financial, banking, insurance, services to monitor people, data and resources to improve their services. (Economidas, 2017)

- Smart Retailing & Logistics

This form of IoT system can be used to track products, monitor cargo, so they can optimize inventory and stock levels, reduce theft, and maintain quality. Also, they can monitor products in storage and transport, make recommendations, and alert when products are not stored by requirements. (Economidas, 2017)

- Smart Transportation

These IoT systems can be used to monitor passengers, vehicles, luggage, containers, and infrastructure to optimize transportation via land, air, or water. Connected cars and smart vehicles would interact to avoid accidents, enhance infotainment, and reduce traffic congestion, power consumption, pollution, and time waste. Smart fleet management would reduce cost, delivery time, wasted space in tracks, etc. Finally, transportation of hazardous material (e.g. corrosives, flammables, toxic, explosives) would be improved. (Economidas, 2017)

- Smart Agriculture

IoT systems would monitor a farm, crop, vineyard, green house, livestock, animals, farm equipment, and machinery (tractors, fertilizer distribution), make recommendations or take appropriate actions (e.g. irrigation, feeding) to enhance the production quality and quantity (Economidas, 2017).

Risks to IoT Devices:

IoT devices are more at risk than traditional devices for several different reasons as discussed below.

<u>Hardware-Level Vulnerabilities</u>

IoT devices usually are made to have low computational power and hardware limitations, which does not allow for security built-ins (Craven, 2020). Security features for IoT devices are added only when necessary and, only if the remote attacks are considered as the main threat. Therefore, these devices suffer hardware-level vulnerabilities, because they can be exploited remotely (Wurm et al., 2016). Furthermore, it is not difficult for hackers to use simple techniques to get into the systems. This is why it is important to do all we can, as consumers and producers, to prepare systems for attacks.

Supply & Demand

Companies race to capitalize on the advantages of IoT as they become more popular. The companies attempt to be the first products on the market and keep up with the pace of these devices, so they ignore the security issues that may result. When focusing mainly on the functionality of the IoT device, the device is left open and can be dangerous in not being able to protect sensitive information.

Default Credentials

Many consumers do not reset the passwords on IoT devices, and many companies make the credentials weak, easy to guess, or hardcoded. Hardcoded passwords are unencrypted passwords that they leave in the source code of the device (Craven, 2020).

A Compromised Interface

An interface that an IoT device uses to connect to a larger network, such as 5G networks, can be compromised. When the interface becomes compromised, it usually happens because there is no authentication or authorization in place when accessing the device (Craven, 2020).

No Firmware Validation

If a vulnerability is discovered on the device, some devices cannot be updated because firmware validation is not implemented. The update would be in plain-text, or the user is not made aware of the updates, and there are no “anti-rollback mechanisms.” The anti-rollback mechanisms would stop attackers from downgrading a device to an older version that the attacker can exploit (Craven, 2020).

2.3 Examples of hacked IoT Devices

This section will provide examples of some typical IoT devices being hacked to show the vulnerability of these devices.

Ring Security Camera

Figure 2.1: The Ring Security Camera

Source: The best Ring security cameras and video doorbells, ranked. T3 Smarter Living. (2019).

- Overview

Security Cameras allow you to monitor and record activity in different areas and can see people who approach the front door. There are different security cameras, some are large, and may be used to frighten criminals, while others are small and can be hidden from view (Fuller, 2019).

- Vulnerability

Earlier in the year, a Ring Security Camera was installed in a child’s room, where a hacker managed to get into the system and play “Tiptoe Through the Tulips” into the bedroom. After someone became aware of the unauthorized hack, the hacker began to yell racial slurs and claim they were Santa Claus. This intrusion was part of recent breaches involving the Ring security cameras (Monthly, 2019).

<u>Baby Monitor</u>

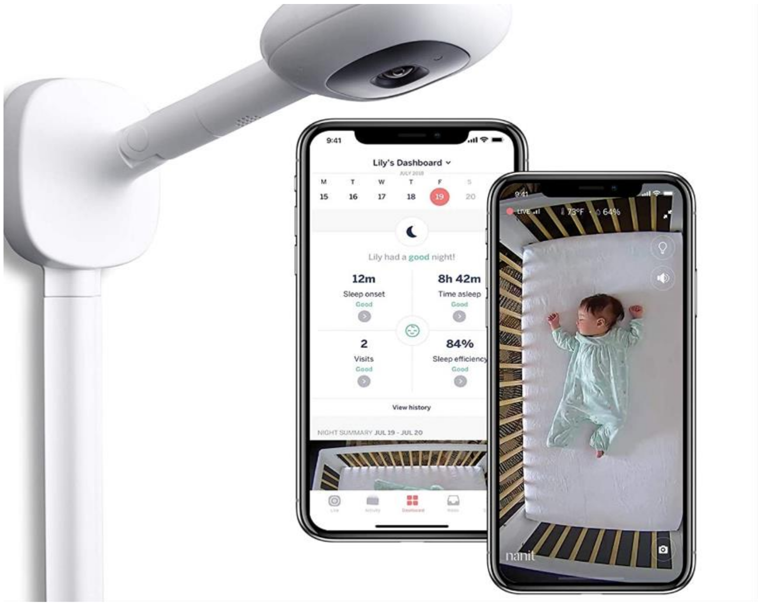


Figure 2.2: The Smart Baby Monitor

Source: Nanit Smart Baby Monitor and Wall Mount Gen 1. Amazon. (2017).

- Overview

This system is one that parents use to monitor the sounds and movements of the baby. These monitors provide a live feed and information about the baby's room. They rest in the infant's room while the parents check in on their mobile devices (Piper, 2016).

- Vulnerabilities

Late last year, a family from the US experienced a real nightmare. A hacker got into the wireless camera system used to keep an eye on the baby and threatened to kidnap him. This case is not an exception. There are several reported incidents of strangers' voices being heard over baby monitors" (Monthly, 2019).

Medical Devices

Figure 2.3: Hackable Pacemaker

Source: Hacking pacemakers, insulin pumps and patients' vital signs in real-time. CSO. (2018).

- Overview

Shiel(2017) describes a pacemaker as a “device that uses electrical impulses to regulate heart rhythm.” They can also detect too long a pause between heartbeats and stimulate the heart.

- Vulnerability

In 2017, the FDA announced the discovery of a vulnerability in the pacemakers by St. Jude Medical. The vulnerability was in the transmitter that the pacemakers used to communicate with external services. The pacemakers had information on the patient’s condition for the physicians, which made monitoring easier. Once an attacker has gained access to the pacemaker, they can alter its functioning, deplete the battery, and produce fatal shocks (Kilpatrick, 2016).

<u>Thermostats</u>

Figure 2.4: Smart Thermostat

Source: CAN SMART THERMOSTATS REALLY SAVE YOU THOUSANDS OF DOLLARS? (2019).

- Overview

A thermostat can be described as something that tries to maintain the temperature.

- Vulnerability

Hackers accessed a casino’s network through the internet-connected thermometer in the aquarium and were able to get sensitive information. Also, in 2016, a thermostat was hacked in Finland by launching a DDoS attack on the environmental control systems via thermostats. (Monthly, 2019)

2.4 Summary

This chapter first introduced the different areas that IoT devices are involved in and explained the reasons why IoT devices are so vulnerable compared to traditional devices. After that, four examples of some typical IOT devices being hacked are provided. From this chapter, we understood why these devices have so many vulnerabilities, and now we will look closer at the actual vulnerabilities and what they do to the devices in the following chapters.

Chapter 3: Vulnerabilities in IoT Devices

This chapter explains the difference between vulnerability, unethical hacking and a threat, and this will give readers a good background. The chapter then moves on to discuss the common threats and vulnerabilities seen within IoT devices.

3.1 What Is Vulnerability?

A vulnerability is defined as, "a flaw within a system, application or service which allows an attacker to circumvent security controls and manipulate systems in ways the developer never intended" (Zhang et. al, 2014). These can be exploited by attackers using unethical hacking, which Shekhar (2020) explains as"an illegal activity of accessing unauthorized information by modifying a system's features and exploiting its loopholes" (Shekhar, 2020). The attackers are considered threats, which are described as "incidents that have the potential to harm a system or device" (Watts, 2020). Some threats are more common in IOT devices, and they will be explained in this section.

3.2 Different Types of Cyber Threats

<u>Keylogger</u>

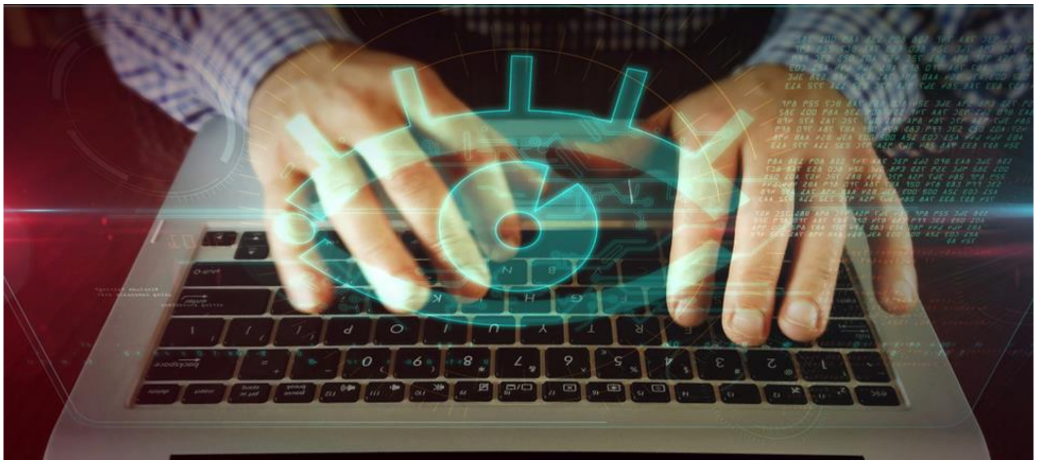


Figure 3.1: An animation of a keylogger.

Source: *Demystifying a Keylogger – How They Monitor What You Type and What You Can Do About It?* Sophos Home. (2019).

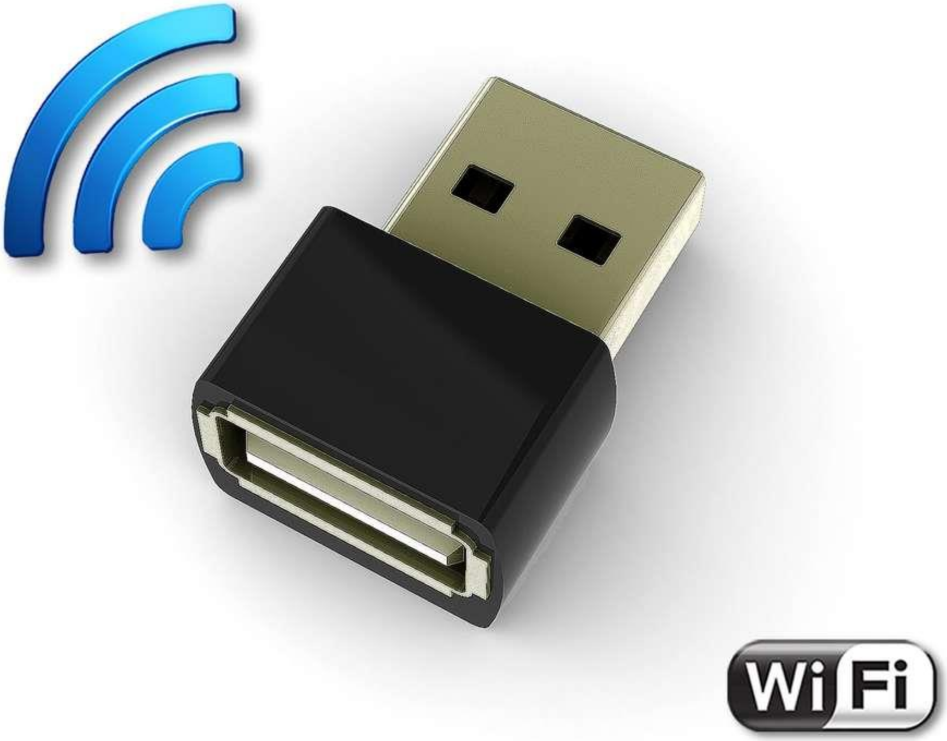


Figure 3.2: A Hardware Keylogger

Source: *USB hardware keyloggers - AirDrive Keylogger & KeyGrabber*. Keelog.com. (n.d.).

Keylogging is a type of monitoring software that records the key sequence and strokes of a keyboard into a website or application and sends it back to a third party. These log files might even contain your personal email IDs and passwords. Also known as keyboard capturing, it can be either software or hardware. While software-based keyloggers target the programs installed on a computer, hardware devices target keyboards, electromagnetic emissions, smartphone sensors, etc. (Shekhar, 2020; Swinhoe, 2018).

Cyber-criminals keep keystroke loggers in their toolkits to capture financial information, such as banking and credit card details, personal information such as emails and passwords, or names and addresses or sensitive business information, including processes and property. They have the ability to sell such information to other organizations as part of a bigger attack (Swinhoe, 2018).

Denial of Service Attack (DDoS)

A Denial of Service attack occurs when users cannot access information systems, or network resources due to an attacker taking down a site or server (by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. DoS attacks can cost an organization both time and money while their resources and services are inaccessible (CISA, 2019).

A distributed denial of service attack(DDoS) happens when multiple devices attack one target. Many attackers use botnets (a group of hijacked internet-connected devices to carry out large-scale attacks). These attacks allow exponentially more requests to be sent to the targets and make the source hard to identify(CISA, 2019).

Phishing

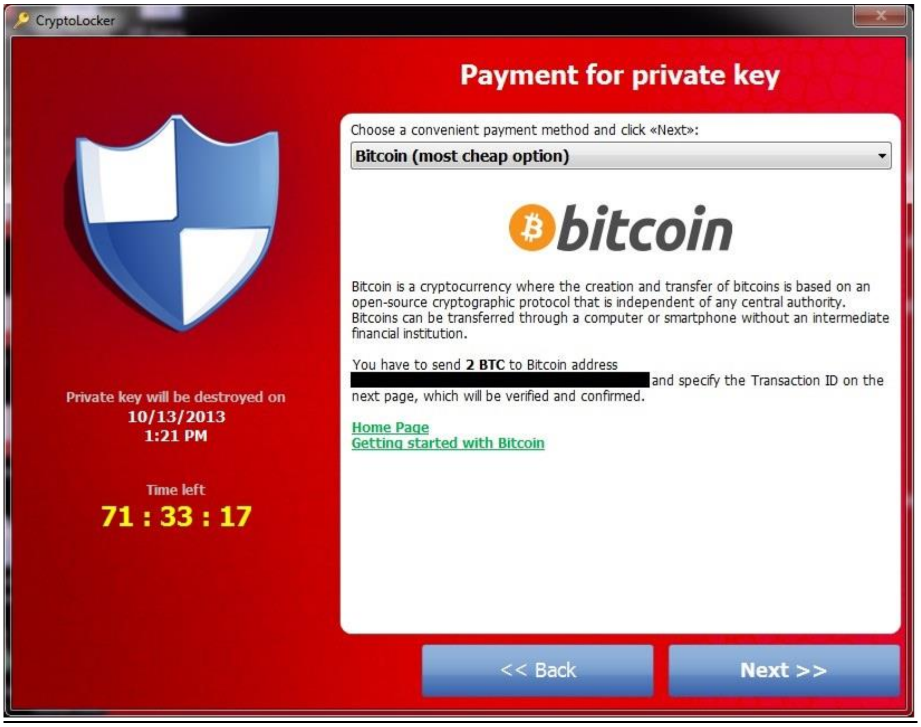
Phishing is a social engineering attack that is used to steal user data, such as, login credentials and passwords. It happens when a hacker replicates the most-accessed sites, emails, or messages and traps the victim by sending that spoofed link. This leads to the installation of malware, which can have devastating effects. It can cause unauthorized purchases, and identity theft (Imperva, 2020).

Eavesdropping

Using passive attacks, hackers can monitor computer systems to get unwanted information. They use software, such as, a packet sniffer, which tracks packets going in and out of a network. They use this method, not to harm the system but to get information without being identified. The hackers target emails, phone calls, web browsing, etc. (Shekar, 2020)

Ransomware

Ransomware prevents a user's endpoint device from properly and fully functioning until a fee is paid. Some pretend they are different entities, such as law enforcement, in order to "warn" businesses of things that would endanger their business. This could include, a license expiring or an issue with an inventory. After the attackers have taken the systems hostage, they demand ransom in exchange for decryption. If the ransom goes unpaid, the attackers may sell the information or expose the company (CISA, 2019).



Payment for private key

Choose a convenient payment method and click «Next»:

Bitcoin (most cheap option)

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send **2 BTC** to Bitcoin address [redacted] and specify the Transaction ID on the next page, which will be verified and confirmed.

Private key will be destroyed on
10/13/2013
1:21 PM

Time left
71 : 33 : 17

Figure 3.3: How an attacker may display the ransom request to the victim.

Source: *Petters, J. (2020, March 30). CryptoLocker: Everything you need to know. Retrieved April 08, 2021, from https://www.varonis.com/blog/cryptolocker/*

Crypto Malware

Crypto malware is another form of money extortion. This type of malware imprisons users and encrypts all files on the device so that none of them can be opened. The cost to unlock the crypto-malware increases every hour or day. Some forms of crypto-malware may encrypt all the files on the network. During encryption, the files are ‘scrambled,’ so that they are unreadable. To be restored, a decryption key is needed. Crypto malware or ransomware can be encountered via files or links, through emails, messages, etc. They can be downloaded through other threats, like a trojan horse, or other exploitation devices. (“Crypto-Ransomware”, n.d.).

Virus

There are two types of viruses, a file-based virus and a fileless virus. The file-based virus is malicious code that is attached to a file and can reproduce itself without interaction. These viruses have strong measures to avoid detection, such as split infection and mutation. It unloads a payload (the part of transmitted data that is the actual intended message), to perform the attack, and the virus replicates itself by inserting the code into other files (Ciampa, 2015). There are two types of file viruses, including direct action and resident viruses

A fileless virus is not attached to a file, and it takes advantage of the services and processes in the operating system to avoid detection and carry out attacks. The code is loaded directly into the RAM (random access memory). It can also exploit applications to execute malicious code (Ciampa, 2015; Awake, n.d.).

There are a few advantages (for the attackers) to choose a fileless virus over a file-based virus, which include, easy to infect the device, extensive control, persistence, it is difficult to detect, and difficult to defeat.

Worm

A worm is a malicious program that uses a computer network to replicate. It is designed to enter a computer through the network and exploit a vulnerability in an application or operating system on the device. Some of them leave behind a payload that can infect and cause harm. Worms can perform actions, such as deleting files or allowing the computer to be controlled by an attacker (Ciampa, 2015).

Botnet

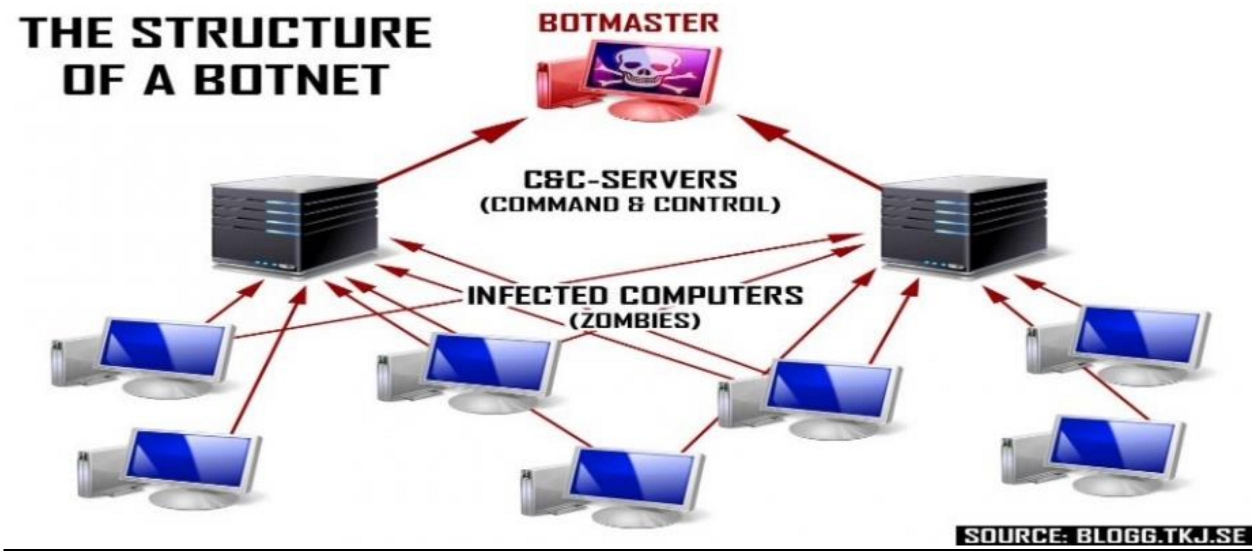


Figure 3.4: An example of how a botnet works.

Source: *Kriegler, A. (Feb. 2021). The Structure of A Botnet. Retrieved from*

https://www.pinterest.com/pin/528961918723783738/

This type of vulnerability allows a network of infected devices to be placed under the control of an attacker to launch attacks. The attacker is known as the bot herder. The bot herder leads the bots to automate mass attacks, including, data theft, server crashing, and malware distribution. This threat allows devices to scam others and cause disruptions without consent. The motive behind most of these attacks is simply because they want to steal something valuable or cause trouble. (Kaspersky, 2021).

Spyware

Spyware is tracking software that is deployed without the consent of the user. The activity leaves users open to data breaches and misuses private data. It also slows down a user’s activities. Spyware can collect things such as, login credentials, account pins, credit card numbers, browsing habits, etc. Different forms of spyware include trojan spyware, adware, tracking cookie files, and monitoring a system to capture sensitive data (Kaspersky, 2021).

Potentially Unwanted Program (PUP)

A Potentially Unwanted Program (PUP) is a software that users do not want on their computer. This may include advertising, toolbars, and pop-ups that download with the software you installed.

Trojan

Figure 3.5: An animation of a trojan horse.

Source: *(n.d.) "WHAT IS THE TROJAN VIRUS AND ITS CHARACTERISTICS". Retrieved from https://enterprise.comodo.com/forensic-analysis/what-is-the-trojan-virus.php*

A computer Trojan is a program that is disguised as a legitimate software that also does something malicious. Users are tricked using a form of social engineering into executing a Trojan on their devices. Once installed, a Trojan can spy on you, steal information and gain backdoor access to your devices (Kaspersky, 2021).

Remote Access Trojan (RAT)

A RAT has identical functions to a Trojan but they differ in that the RAT gives the threat unauthorized remote access to the victim's computer by using configured communication protocols. This allows for an opening to the victim's computer and giving the threat unlimited access. (Ciampa, 2015)

Backdoor

This threat gives access to a computer, program, or service that circumvents any normal security protections and gains a high level of user access. Back doors can be used to steal personal and financial information, install malware and hijack devices ("Backdoor Computing Attacks", 2021).

Logic bomb

Figure 3.6: An illustration of how a logic bomb works.

Source: *Townsend, C. (n.d.). "Logic Bombs: How to Prevent Them" Retrieved from https://www.uscybersecurity.net/logic-bombs/*

A logic bomb is a computer code that is added to a legitimate program but remains dormant and avoids detection until a specific event triggers it. It is activated in the hot network and must meet certain conditions to attack ("Security Encyclopedia: Logic Bomb", n.d.).

Rootkits

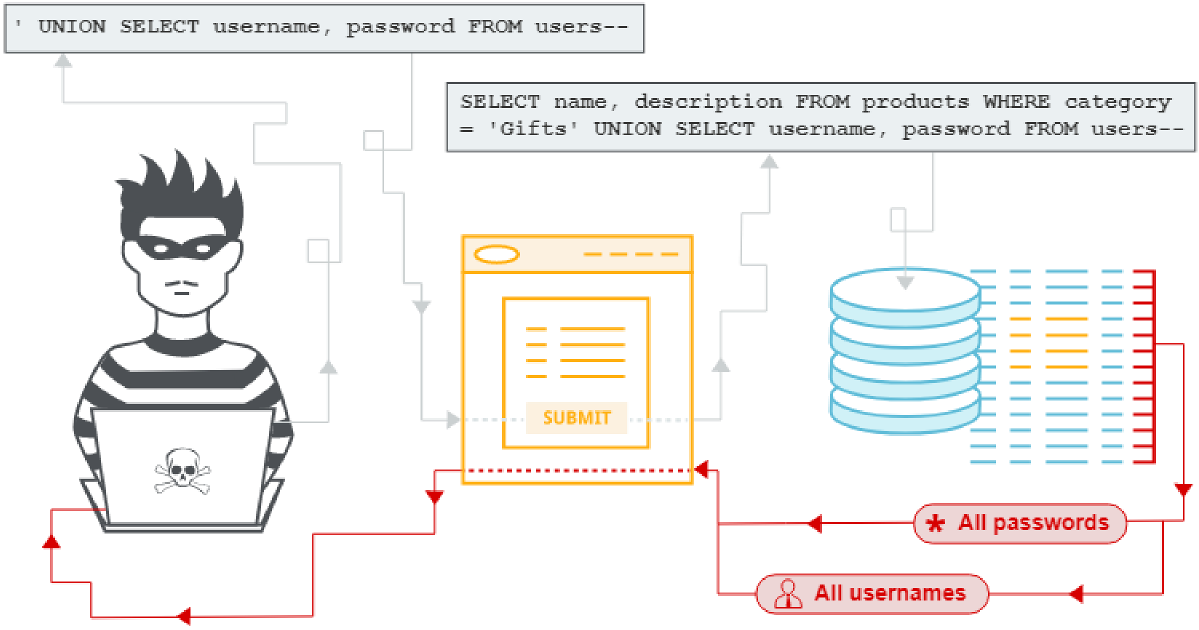
Figure 3.7: An illustration of how hackers work.

Source: *Jareth. (10 January 2018). "What is a Rootkit?" Retrieved from*

https://blog.emsisoft.com/en/29468/rootkits/

A rootkit is an attack that can hide its presence and the presence of other malware on the computer. It accesses the lower layer of the operating system to make changes. It allows someone to get control of a device without the user's knowledge. Once installed, the root kit can execute files and change a device's configuration on the host. It can also log files and spy on the user's usage ("Rootkit: What is a Rootkit?", n.d.).

SQL Injection



```
' UNION SELECT username, password FROM users--
```

```
SELECT name, description FROM products WHERE category
= 'Gifts' UNION SELECT username, password FROM users--
```

Figure 3.8: An animation of how an SQL Injection Attack works.

Source: *(n.d). "SQL Injection". Retrieved from* *https://portswigger.net/web-security/sql-injection*

A SQL (Structured Query Language) injection attack inserts a statement to manipulate a database server.

One of the most common injection attacks (SQL injection) inserts statements to manipulate a database server. A successful attack can read sensitive data from the database and modify information ("SQL Injection," n.d.).

Buffer Overflow Attack

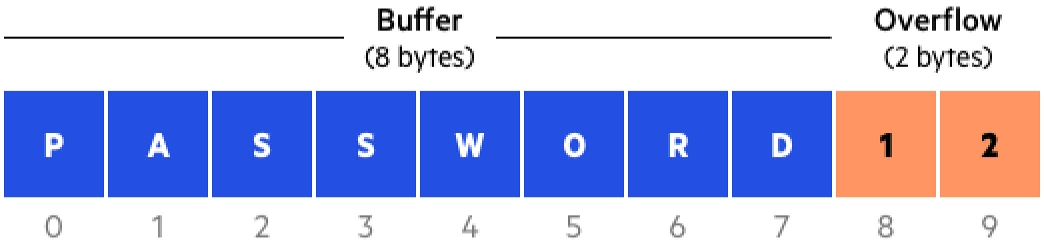


Figure 3.9: Explains how a buffer overflow attack works

Source: *(n.d.). "Buffer Overflow Attack." Retrieved from*

https://www.imperva.com/learn/application-security/buffer-overflow/

A buffer overflow attack occurs when a process attempts to store information in RAM (Random Access Memory) beyond the boundaries of a fixed-length storage buffer. The extra data overflows into the memory locations adjacent to the RAM. An attacker can exploit this threat by overwriting the memory of an application, which changes the execution path of the program and damages files or exposes information ("Buffer Overflow Attack," n.d.).

3.3 Summary

This chapter reviewed the different threats that are commonly found in IoT devices, because of vulnerabilities. It is important to be aware of them, so users understand how vital cybersecurity is. The next section will discuss solutions to flaws and vulnerabilities, how to defend and protect users against threats, and how to scan devices for vulnerabilities.

Chapter 4: Countermeasures for Reducing the IoT Vulnerabilities

Vulnerabilities and threats in IoT devices, can be very dangerous, as we introduced in the previous chapters. They can make it seem as if users of IoT devices are under constant attack. However, there are ways to protect the users and systems with different measures. In this section, we will discuss several different methods, techniques, and tools that will keep user's information safe.

Firewall

They prevent unauthorized access to your business network and alert you of any intrusion attempts.The first thing to do with a new computer (or any computer for that matter) is to make sure the firewall is enabled before you go online (Dove,2019). This should be one of the first things to be checked when doing vulnerability assessments. Furthermore, businesses should purchase an extra firewall to help secure their network.

Antivirus Software

These programs help to fight against unauthorized code or software that threatens the operating system. They play a major role in protecting the system by detecting threats to ensure the safety of data. Some advanced antivirus programs provide automatic updates, further protecting your machine from the new viruses that generate every day (Dove, 2019).

Complex Passwords

Passwords are the first line of defense for the system, so they must be strong. Many IoT users make the mistake of not changing their default passwords or having weak passwords that are easy for hackers to guess. More secure often means longer and more complex: Use a password that has at least eight characters and a combination of numbers, upper- and lowercase letters, and computer symbols. Hackers have an arsenal of tools to break short, easy passwords in minutes (Dove, 2019).

Keep Changing Passwords

It is very important to change passwords often on IoT devices. Being diligent with these passwords and ensuring that these passwords are unique, is an integral part of making sure your information is safe. This can be done by using a password manager to remember these passwords or writing them down (Viswanathan, 2019).

Keeping Operating System, and Apps Up to Date

Make sure to install the new updates to your operating systems. Most updates include security fixes that prevent hackers from accessing and exploiting your data. (Dove, 2019) This allows your system to block the out-of-date information that hackers have learned how to hack. It is a good idea to bookmark the manufacturer’s web page so the user can check for updates in the device’s firmware and software (Kaspersky, 2021).

Use Secondary Network

Consumers should create an extra network, for the Internet of Things devices. This will help stop unauthorized access to data in IoT devices. This will be a buffer that will help to ensure that outside sources are not allowed to access sensitive files and data (Viswanathan, 2019).

Two-Factor Authentication

While passwords are considered the first line of defense against hackers, the second layer of authentication adds protection (Dove,2019). Two-factor authentication includes sending codes to another person to verify the user.

Avoid Public Wireless Networks

It is easy to use Wi-fi networks offered in coffee shops, restaurants, and airports. However, this can be very dangerous. A solution would be to use a Virtual Private Network(VPN), which gives you a private, encrypted gateway to the Internet and stops eavesdroppers from intercepting communications (Kaspersky, 2021).

Guest Networks

Visitors should have a separate network when visiting someone's home. This will not allow them to have access to your main network or email or other accounts.

Individualize IoT Devices

Each IoT device needs a different name and passwords. If an attacker breaks into a network from one device, they will try and expand to other devices. If all devices have separate credentials, then expanding to other devices will be almost impossible (Symanovich, 2019).

Network Scan

A very important proactive tool for a user or business to utilize is the scanning of the network. I came up with a variation of this concept during my Capstone Project. I will use the idea of a vulnerability and threat scanner below.

IoT Vulnerability Scanner

In this section, we will discuss the development of a vulnerability scanner, specifically made for IoT devices. It will detect the vulnerabilities on the network and the device because:

1. Network-level security can be implemented across many different IoT devices.
2. This security can be implemented in the cloud and can be enhanced.
3. This network-level security can be offered by a third-party, who has expertise.
4. Network-level security adds an extra layer of protection. (Sivaraman et al, 2015)

This system will monitor what data that the IoT device receives and sends out daily, then the scanner will search this information for vulnerabilities in the system. Currently there is an extreme lack of security in IoT devices, and many users are not aware of the potential danger that their information is in and they do not know how to properly protect themselves. This scanner will help ease their worries, by allowing them to monitor activity and be made aware of vulnerabilities. This system could be used at home or at work, depending on the system, because IoT devices are everywhere! The main benefit of this system is monitoring the activity of the IoT device and being able to scan for vulnerabilities. This system should work on a frequently used wifi network, that has all the IoT devices connected. This will be used to monitor and scan the information that an IoT device sends and receives. A packet sniffer software will be included on the backend of the scanner, so that their information can be searched for insecurities. This device should be used when an individual or group of individuals want to test how secure their wifi and their devices are. This device should be placed on a wifi network that has all the IoT devices on it, so that it can scan for the devices and monitor their activity, individually. After the information is scanned, the device will have a list of tips and suggestions to fix vulnerabilities, which will help protect the user's information. This system was created for people, with little technology experience, and attempting to monitor the device under their care, or for users involved with a business, who want to test their offices and their products for vulnerabilities before giving them out to the public.

The features of this device include:

- *Monitor Activity*
  - *Scan devices*
    - *Input manually*
  - *Scanner links to wifi*
    - *Input manually*
  - *Scanner receives basic information*
  - *Time set and filtering*
  - *Begins Monitoring the IoT devices network actives*
- *Scanner*
  - *Display scanner information*
  - *Display filtering information*
  - *Begins scanning IoT device*
  - *Packet sniffing or other hacking*
  - *Present Results*
- *The product should display the results*
  - *User can save the information after that scan/run of the program*
  - *User can simplify the results or have "pro results" easier to understand*
  - *Activity Log*
- *Monitor the activity of the device*
  - *Set a time limit for how long the program will run*
  - *Able to start the program at any time*
  - *Able to stop the program at any time*
- *Display suggestions on how to protect their device*
  - *Display Solutions*
  - *See more info about solutions*
  - *Permissions*

This device is implemented using the following hardware and software.

Hardware

- Raspberry Pi

Figure 4.1: A photo of a raspberry pi

Source: Raspberry Pi. (2021, April 12). Retrieved April 16, 2021, from https://en.wikipedia.org/wiki/Raspberry_Pi

This device is a low-cost computer that can plug into a computer monitor or tv and it uses a mouse and keyboard. It can be used as a variation of different things, in this project, it is used as a sensor to help monitor traffic coming in and out of the IoT devices.

- *Router*

Figure 4.2: A picture of a router

Source: As a Contributing Editor for PC Magazine. (2021, March 25). The best wi-fi 6 routers for 2021. Retrieved April 16, 2021, from https://in.pcmag.com/switches/137088/the-best-wi-fi-6-routers-for-2020

A router is a networking device that forwards packets between computer networks. In this project, the router is used to test the validity of the scanner. We scan the network unauthorized users, threats, and monitor it's traffic.

- Testing IoT Device (Amazon Alexa, Smart TV, Smart Fridge, etc.)

These devices are used to test the validity of the scanner and monitoring features of the software. We check these devices to monitor their traffic and check for vulnerabilities and threats.

Software

- *HTML, CSS, Javascript*

These are front-end languages that were used to create the GUI (Graphical User Interface), so that the user does not need to see what is happening in the back end.

- *PHP, MySQL*

  MySQL is a database language that was used to create and encrypt the databases for user information, IoT devices on the network, the previous monitoring and scanning logs and the explanation of the vulnerabilities that may be on a system.

- *Kali Linux, NMAP, Port Scanner*

  Kali Linux is an operating system that houses a multitude of security tools. I was able to use this with a Windows operating system because of software called VirtualBox. VirtualBox allows you to use a different operating system on your device, without it affecting your original operating system or its configurations. One of the important features is the NMAP Scanner, which scans the network for different vulnerabilities and threats. Also, a port scanner scans for any open ports, which can be considered a vulnerability if any of them are open.

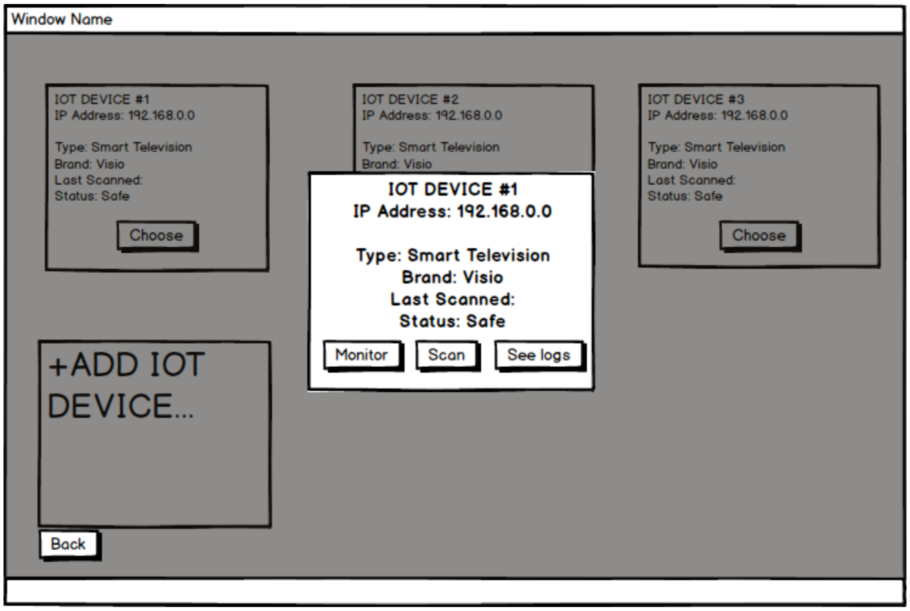
- *Python Scripts*

  Python Scripts are used to connect the tools in Kali Linux to the database, interface, and raspberry pi, so they can execute the appropriate scans on the devices.

- *Wireshark*

This platform is used to monitor network traffic. Criminals may use it for social engineering, but it can also be used for good. In this project, we use it to monitor incoming and outgoing traffic on the network to check for vulnerabilities and threats.

All of these features were brought forth to help the user have more control and awareness of their devices. Below are mockups of the GUI (Graphical User Interface), and how the software would look to the user.



IOT DEVICE #1
IP Address: 192.168.0.0

Type: Smart Television
Brand: Visio
Last Scanned:
Status: Safe

IOT DEVICE #2
IP Address: 192.168.0.0

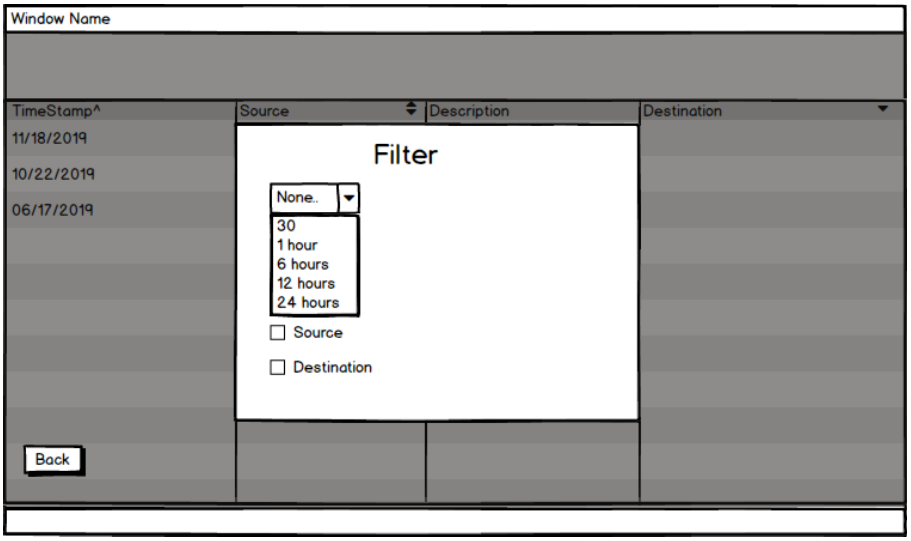
Type: Smart Television
Brand: Visio

IOT DEVICE #3
IP Address: 192.168.0.0

Type: Smart Television
Brand: Visio
Last Scanned:
Status: Safe

IOT DEVICE #1
IP Address: 192.168.0.0

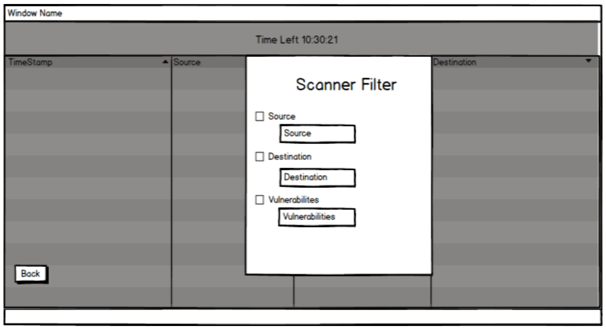
Type: Smart Television
Brand: Visio
Last Scanned:
Status: Safe

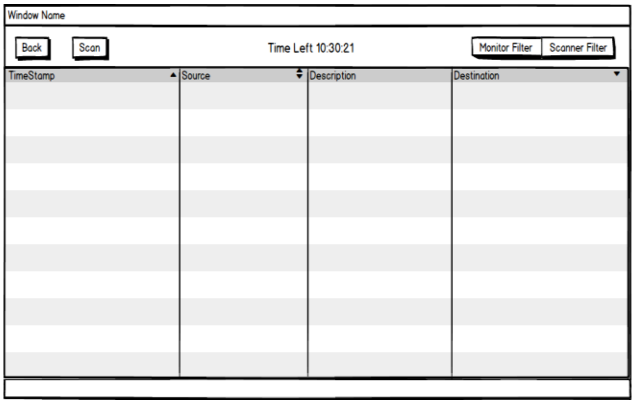


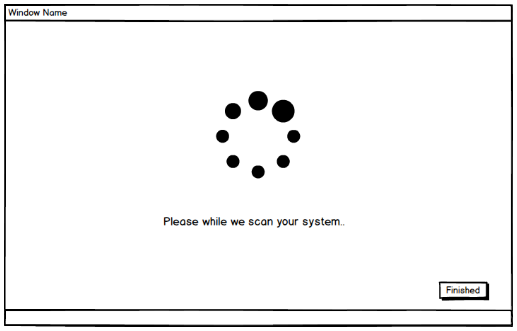
TimeStamp^	Source	Description	Destination
11/18/2019			
10/22/2019			
06/17/2019			

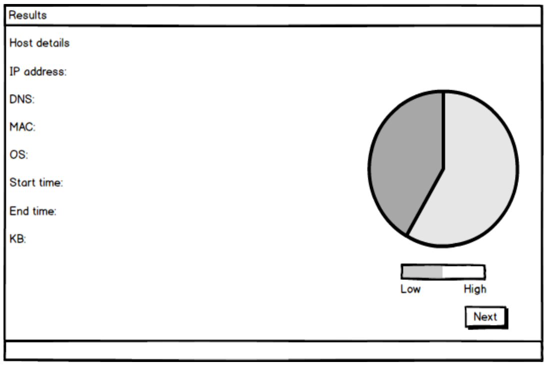
□ Source

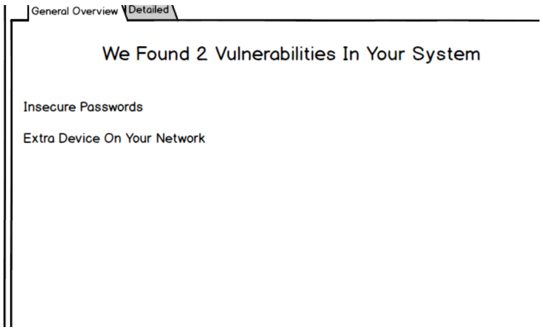
□ Destination






Please while we scan your system..

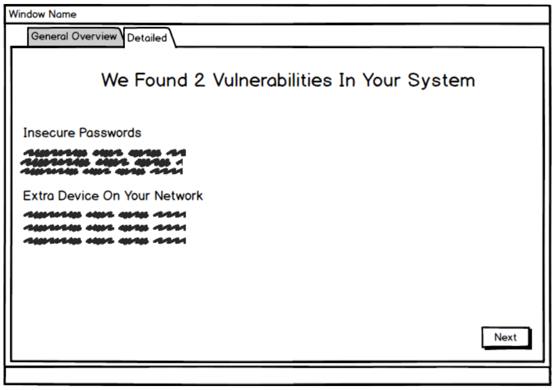



We Found 2 Vulnerabilities In Your System

Insecure Passwords

Extra Device On Your Network

Figure 4.3: Mockups of GUI (Graphical User Interface)


We Found 2 Vulnerabilities In Your System

Insecure Passwords

Extra Device On Your Network

The next chapter will conclude this thesis.

Chapter 5: Conclusion

The purpose of this thesis is analyze why IoT devices are more vulnerable than traditional devices, make readers aware of the threats that are common in IoT devices, and find solutions to these threats. These solutions included a scanner, which could be a proactive tool in finding problems before they arise.

Chapter 1 introduces Internet of Things (IoT) devices, and the benefits that they provide to people. This chapter helps readers understand the difference between IoT devices and traditional devices, and highlights their statistics and how popular these devices have become. Also, this chapter covers how they connect to other devices and how to connect to different networks.

Chapter 2 explains to readers why IoT devices can be so vulnerable. First, the chapter highlights the different areas that IoT devices can be involved in. Then, it moves on to explain the different reasons why these devices are so vulnerable. IoT devices are created and released quickly as companies compete to meet the demand. When they are released so quickly, companies tend to forget the cybersecurity measures. Also, many users do not have adequate security awareness, so many habits, such as, weak passwords, leave their devices vulnerable to many threats.

Chapter 3 shows what threats and vulnerabilities that IoT devices can be exposed to and how they affect the systems. These threats include hardware, memory, network, and application vulnerabilities. Readers were given overviews of the devices and how they affect their devices.

Chapter 4 shows readers that there is hope in solving computer vulnerabilities. This thesis has given solutions to those threats and vulnerabilities, including, a proactive tool that could stop issues before they arise.

IOT devices are ever changing and quickly growing in popularity throughout the world, as people try harder and harder to make their lives more convenient and productive. However, when they are not properly protected, they pose a risk to users and their sensitive information. It is especially important to find solutions to combat such threats and vulnerabilities, as they could cause more harm than good. IoT devices are fantastic tools that can better the lives of all people, as long as they are properly made and taken care of.

References

TC Global Insights. (2020)*All You Need to Know About The IoT (Internet of Things*.
Article: What is... crypto-ransomware: F-secure. (n.d.). Retrieved April 08, 2021, from https://www.f-secure.com/v-descs/articles/crypto-ransomware.shtml#:~:text=Crypto%2Dransomware%20is%20a%20type,so%20that%20it%20is%20unreadable

As a Contributing Editor for PC Magazine. (2021, March 25). The best wi-fi 6 routers for 2021. Retrieved April 16, 2021, from https://in.pcmag.com/switches/137088/the-best-wi-fi-6-routers-for-2020

Backdoor computing attacks – Definition & examples. (2021). Retrieved April 16, 2021, from https://www.malwarebytes.com/backdoor/#:~:text=A%20backdoor%20refers%20to%20any,system%2C%20network%20or%20software%20application.

(n.d.). "Buffer Overflow Attack." Retrieved from https://www.imperva.com/learn/application-security/buffer-overflow/

CAN SMART THERMOSTATS REALLY SAVE YOU THOUSANDS OF DOLLARS? Reviewed. (2019).

Ciampa, M. D., & Computing Technology Industry Association, (2015). *CompTIA security+ guide to network security fundamentals*.

Craven, C. (2020, June 2). How Is the Internet of Things (IoT) Vulnerable? Retrieved from https://www.sdxcentral.com/5g/iot/definitions/how-is-internet-of-things-iot-vulnerable/#:~:text=IoT%20devices%20are%20vulnerable%20because,are%20reputable%20and%20security%2Dminded.

Demystifying a Keylogger – How They Monitor What You Type and What You Can Do About It? Sophos Home. (2019).

Opher E (2015). Differences between the IoT and Traditional Internet.

Kriegler, A. (Feb. 2021). The Structure of A Botnet. Retrieved from *https://www.pinterest.com/pin/528961918723783738/*

Economidas, A. (2017). User Perceptions of Internet of Things (IoT) Systems. Retrieved from https://link.springer.com/chapter/10.1007/978-3-319-67876-4_1

Fuller, J. (2009). How Security Cameras Work. Retrieved from https://electronics.howstuffworks.com/gadgets/home/security-cameras.htm

Gupta, A., Do, D., Khanna, G., Rahman, M., Khandelwal, A., Sekhar, N., Roy, S. (2021). Internet of Things (IoT) Testing: Challenges, tools and testing approach. Retrieved April 16, 2021, from https://www.softwaretestinghelp.com/internet-of-things-iot-testing/

Hacking pacemakers, insulin pumps and patients' vital signs in real-time. CSO. (2018).

How do thermostats work? (2019). Retrieved from https://www.explainthatstuff.com/thermostats.html

Internet of Things Forecast: Mobility Report. (2020, February 13). Retrieved from https://www.ericsson.com/en/mobility-report/internet-of-things-forecast

Kilpatrick, H. (2019). 5 Infamous IoT hacks and vulnerabilities: IOT Solutions World Congress: DIGITALIZING INDUSTRIES. Retrieved from https://www.iotsworldcongress.com/5-infamous-iot-hacks-and-vulnerabilities/

M, B. (2017, November 19). Why are iot devices so insecure right now? Retrieved April 16, 2021, from https://www.dogtownmedia.com/iot-devices-insecure-right-now/

Monthly, F. (2019). The Worst and Weirdest IoT Hacks of All Times. Retrieved February 16, 2020, from https://www.finance-monthly.com/2019/09/the-worst-and-weirdest-iot-hacks-of-all-times/

Nanit Smart Baby Monitor and Wall Mount Gen 1. Amazon. (2017).

P. Suresh, P., Vijay Daniel, J., Parthasarathy, V. (n.d.). “A state of the art review on the Internet of Things (IoT).” https://fardapaper.ir/mohavaha/uploads/2018/02/Fardapaper-A-state-of-the-art-review-on-the-Internet-of-Things-IoT-history-technology-and-fields-of-deployment.pdf

Petters, J. (2020). CryptoLocker: Everything you need to know. Retrieved April 08, 2021, from https://www.varonis.com/blog/cryptolocker/

Ransomware guidance and resources. (2019). Retrieved April 08, 2021, from https://www.cisa.gov/ransomware

Raspberry Pi. (2021, April 12). Retrieved April 16, 2021, from https://en.wikipedia.org/wiki/Raspberry_Pi

Reed, T. (2019). 7 real benefits that Iot brings. Retrieved April 16, 2021, from https://www.hellersearch.com/blog/7-real-benefits-iot-brings

Reshetchenko, D. (2018). “Top Five Sectors of IoT: Use Cases and Security.” https://dzone.com/articles/5-sectors-which-use-the-iot-efficiently-but-what-a

Rootkit: What is a rootkit and how to detect it. (n.d.). Retrieved April 16, 2021, from https://www.veracode.com/security/rootkit

Sagar, J., Jones, R., *The best Ring security cameras and video doorbells, ranked.* T3 Smarter Living. (2019).

Shekhar, A. (2020, January 15). Top 10 Common Hacking Techniques You Should Know About. Retrieved from https://fossbytes.com/hacking-techniques/

Smith, M (2018). Hacking pacemakers, insulin pumps and patients' vital signs in real time. CSO.

Stanislav, M., & Beardsley, T. (2015). Hacking IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities. Rapid7, 1–17

Statista Research Department. (2016). Internet of Things - number of connected devices worldwide 2015-2025.

Swinhoe, D. (2018, December 11). What is a keylogger? How attackers can monitor everything you type. Retrieved April 08, 2021, from https://www.csoonline.com/article/3326304/what-is-a-keylogger-how-attackers-can-monitor-everything-you-type.html

Symanovich, S. (2019). 12 tips to secure your smart home and IoT devices. Retrieved April 16, 2021, from https://us.norton.com/internetsecurity-iot-smart-home-security-core.html

The best Ring security cameras and video doorbells, ranked. T3 Smarter Living. (2019).

Townsend, C. (n.d.). “Logic Bombs: How to Prevent Them” Retrieved from https://www.uscybersecurity.net/logic-bombs/

USB hardware keyloggers - AirDrive Keylogger & KeyGrabber. Keelog.com. (n.d.).

Vailshery, L. (2021, January 22). IoT spending DRIVERS worldwide 2019. Retrieved April 16, 2021, from https://www.statista.com/statistics/1079622/iot-spending-drivers-worldwide/#:~:text=According%20to%20a%202019%20IoT,drivers%20behind%20increasing%20IoT%20spending.

Viswanathan, V. (2019, October 14). Eight ways to secure your data on IoT devices. Retrieved from https://www.itproportal.com/features/eight-ways-to-secure-your-data-on-iot-devices/

Watts, S. (2020, May 13). It security vulnerability vs threat vs risk: What are the differences? Retrieved April 08, 2021, from https://www.bmc.com/blogs/security-vulnerability-vs-threat-vs-risk-whats-difference/

What is a logic bomb?: Security encyclopedia. (2021, February 22). Retrieved April 16, 2021, from https://www.hypr.com/logic-bomb/

What is phishing: Attack techniques & scam examples: Imperva. (2020, June 17). Retrieved April 08, 2021, from https://www.imperva.com/learn/application-security/phishing-attack-scam/

(n.d.) "What is Trojan virus and its characteristics". Retrieved from https://enterprise.comodo.com/forensic-analysis/what-is-the-trojan-virus.php

What is SQL Injection? Tutorial & Examples: Web SECURITY ACADEMY. (n.d.). Retrieved April 16, 2021, from https://portswigger.net/web-security/sql-injection

Williams, R., McMahon, E., Samtani, S., Patton, M., and Chen, H., 2017."Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach," 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), Beijing, 2017, pp. 179-181.

Wurm, J., Hoang, K., Arias, O., Sadeghi, A. and Jin,Y., "Security analysis on consumer and industrial IoT devices," 2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC), Macau, 2016, pp. 519-524.

Z. Zhang, M. C. Y. Cho, C. Wang, C. Hsu, C. Chen and S. Shieh, "IoT Security: Ongoing Challenges and Research Opportunities," 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, Matsue, 2014, pp. 230-234