

Spring 2019

Security Analysis of the Internet of Things Using Digital Forensic and Penetration Testing Tools

Olajide Ojagbule

Follow this and additional works at: <https://digitalcommons.georgiasouthern.edu/etd>



Part of the [Information Security Commons](#)

Recommended Citation

Ojagbule, Olajide, "Security Analysis of the Internet of Things Using Digital Forensic and Penetration Testing Tools" (2019). *Electronic Theses and Dissertations*. 1889.
<https://digitalcommons.georgiasouthern.edu/etd/1889>

This thesis (open access) is brought to you for free and open access by the Graduate Studies, Jack N. Averitt College of at Digital Commons@Georgia Southern. It has been accepted for inclusion in Electronic Theses and Dissertations by an authorized administrator of Digital Commons@Georgia Southern. For more information, please contact digitalcommons@georgiasouthern.edu.

SECURITY ANALYSIS OF THE INTERNET OF THINGS USING DIGITAL FORENSIC AND PENETRATION TESTING TOOLS

by

OLAJIDE OJAGBULE

(Under the Direction of Lei Chen)

ABSTRACT

We exist in a universe where everything is related to the internet or each other like smart TVs, smart telephones, smart thermostat, cars and more. Internet of Things has become one of the most talked about technologies across the world and its applications range from the control of home appliances in a smart home to the control of machines on the production floor of an industry that requires less human intervention in performing basic daily tasks. Internet of Things has rapidly developed without adequate attention given to the security and privacy goals involved in its design and implementation. This document contains three research projects all centered on how to improve user's data privacy and security in the Internet of Things. The first research provides a detailed analysis of the Internet of Things architecture, some security vulnerabilities, and countermeasures. We went on to discuss some solutions to these issues and presented some available Internet of Things simulators that could be used to test Internet of Things systems. In the second research, we explored privacy and security challenges faced by consumers of smart devices in this case we used an Amazon Echo Dot as our case study. During this research, we were able to compare two different digital forensic tools to see which performed better at extracting information from the device and if the device observes best practices for user data privacy. In the third research project, we used a tool called GATTacker to exploit security vulnerabilities of a Bluetooth Low Energy device and provide security awareness to users.

INDEX WORDS: Internet of Things, Penetration testing, Digital forensics, IoT simulators, Data privacy, Data security, Smart devices.

SECURITY ANALYSIS OF THE INTERNET OF THINGS USING DIGITAL FORENSIC AND
PENETRATION TESTING TOOLS

by

OLAJIDE OJAGBULE

B.Eng., Covenant University, Nigeria, 2010

M.S., Georgia Southern University, 2019

A Thesis Submitted to the Graduate Faculty of Georgia Southern University in Partial

Fulfillment of the Requirements for the Degree

MASTER OF SCIENCE

STATESBORO, GEORGIA

© 2019

OLAJIDE OJAGBULE

All Rights Reserved.

SECURITY ANALYSIS OF THE INTERNET OF THINGS USING DIGITAL FORENSIC AND
PENETRATION TESTING TOOLS.

by

OLAJIDE OJAGBULE

Major Professor:
Committee:

Lei Chen
Hayden Wimmer
Wietian Tong

Electronic Version Approved:

May 2019

DEDICATION

To our great creator, our Almighty God the author of knowledge and wisdom who made this possible. I would also like to appreciate my parents and siblings for all their financial and moral support.

ACKNOWLEDGMENTS

I have learned a lot while working on this thesis and would like to sincerely thank everyone that provided his or her valuable support during the entire process. I would also like to thank my supervisor, Professor Lei Chen for his guidance, support and contribution all along the way.

TABLE OF CONTENTS

ACKNOWLEDGMENTS	3
TABLE OF CONTENTS.....	4
LIST OF TABLES	5
LIST OF FIGURES	6
1 INTRODUCTION	7
2 LITERATURE REVIEW	9
3 AN OVERVIEW OF SECURITY THREATS TO SMART HOME DEVICES	18
3.1 INTRODUCTION	18
3.2 BACKGROUND STUDY	20
3.2.1 IoT Network Protocols.....	21
3.2.2 IoT Data Protocols	22
3.3 IMPLICATION FOR PRACTICE.....	24
4 INVESTIGATING PRIVACY CHALLENGES ASSOCIATED WITH AMAZON ECHO DOT USING DIGITAL FORENSIC TOOLS	28
4.1 INTRODUCTION	28
4.2 RESEARCH METHODOLOGY	30
4.3 RESULTS	32
4.4 CONCLUSION.....	36
5 HACKING A SMART BLUETOOTH LOW ENERGY DEVICE USING GATTACKER	38
5.1 INTRODUCTION	38
5.2 BACKGROUND STUDY	39
5.2.1 GATT Transactions.....	39
5.2.2 Bluetooth Low Energy Security.....	41
5.3 RESEARCH METHODOLOGY	41
5.4 RESULTS	44
6 CONCLUSION.....	47
7 REFERENCES	49
8 ABBREVIATIONS	52

LIST OF TABLES

Table 3.1 1. Sensors and protocols used by common smart home devices.	20
Table 3.2 1. Security threats and countermeasures.	23
Table 3.3 1. Comparison of Existing IoT simulators.	26
Table 4.3 1. Amazon Echo acquired information and data types.	36

LIST OF FIGURES

Figure 3.1 1. A basic Internet of Things system.	19
Figure 4.2 1. Network set-up for the test environment.	31
Figure 4.2 2. Graphical representation of an Amazon Echo Dot network traffic.	31
Figure 4.3 1. Encrypted packet transmitted using TLS protocol	33
Figure 4.3 2. Metadata of an HTTP packet.....	33
Figure 4.3 3. Mobile device data acquisition using Paraben E3.	35
Figure 4.3 4. Error message while trying cloud import.	35
Figure 5.2 1. Illustration of BLE GATT profile	40
Figure 5.2 2. The Penetration testing framework	42
Figure 5.2 3. Scanning for nearby BLE device advertisement data.....	43
Figure 5.2 4. Advertising the clone device.	44
Figure 5.2 5. BLE device scan on the mobile application	45
Figure 5.2 6. Write commands using a generic BLE scanner.....	45
Figure 5.2 7. Replay-based attack using GATTacker.....	46

1 INTRODUCTION

The three studies in this thesis provide a comprehensive analysis of security and privacy challenges associated with the Internet of Things using digital forensics and penetration testing tools. The first research focuses on the components that make up an Internet of Things system, some potential security vulnerabilities at each layer of the system, and also providing some countermeasures to mitigate them. The second research is based on the comparison of two digital forensic tools in acquiring relevant artifacts from a smart device, in this case, an Amazon Echo Dot. This was done to see how smart home devices handle user data and align with security best practices in their design. In this research, we used two digital forensic tools, one an open source forensic tool called The Sleuth Kit (TSK), which is used to recover artifacts from mobile devices and disk images, while the second is a commercially sold tool called Paraben E3. This research is carried out to aid digital forensic investigation in an Internet of Things environment and shed more light on the kind of security and privacy controls implemented on the smart devices. The third research is on the penetration testing of a commonly used smart device that uses Bluetooth Low Energy protocol. This is a common protocol used in wearable technology and knowing the kind of information they provide to consumers, being aware of its security vulnerabilities would help users stay protected from attacks. This whole research work focuses on the privacy and security concerns associated with the Internet of Things.

Internet of Things is an emerging technology and it keeps growing with the number of devices that are able to connect to the internet. These devices range from home appliances, systems embedded with sensors, actuators, physical devices to smart cities and automobiles that communicate with each other and exchange data over the internet. For every innovation and technology comes its advantages and a fair share of challenges. Privacy and security are the key issues associated with the Internet of Things. In the first research, we broke down the components that make up the Internet of Things system, reviewed some potential security vulnerabilities, and provided some known countermeasures. The study involved the review of various types of network and data protocols used by the Internet of Things, potential security

concerns that could arise due to the framework of an Internet of Things system and simulators that could assist the Internet of Things research community.

The second research centers on privacy concern consumers of IoT devices have in using them. There is a general consensus that most smart device users do not trust companies using data collected to protect their privacy. Currently, the choices regarding privacy are limited to either the customer giving up some level of privacy usually typed up in an agreement extremely complex and difficult to flow or the customer not having access to the service. This has brought about discussions on how best to enlighten consumers about privacy. The aim of this study is to focus on the kind of information Amazon Echo Dot saves locally and comparing two different digital forensic tools in the process to extract data. This project was implemented using an open source tool called The Sleuth Kit and a commercially licensed tool called Paraben E3.

The last research is on using penetration testing to exploit some security vulnerabilities in a smart device that uses Bluetooth Low Energy Protocol for data exchange and communication. The aim is to enlighten developers and users of the Internet of Things to become aware of the various attacks that can be carried out on BLE devices and how to avoid them. This project was implemented using a Linux operating system (Ubuntu) running on two virtual machines, 2 CSR 4.0 adapters and a node.js package for BLE security assessment called GATTacker.

2 LITERATURE REVIEW

The Internet of Things as the name implies is the network connectivity of various devices such as home appliances, systems embedded with sensors, actuators, physical devices and automobiles that allow these objects to communicate with each other and exchange data over the internet.

The concept really gained some attention in the summer of 2010 when information leaked that Google was saving data of peoples' wireless networks and it was in the same year the Chinese government made an announcement to make the Internet of Things a strategic priority in their economic development. A couple of years later was when the concept evolved into a system using multiple technologies like the internet, wireless communications, RFID, etc. The Internet of Things is also supported by traditional automated fields, wireless sensor networks (WSNs), GPS, control systems, etc. When we think of the Internet of Things, we think of various devices that connect over the internet. Imagine getting a weather forecast for the day before stepping out to work, and then simultaneously signaling your coffee maker to start brewing coffee. The aim of IoT is to make our lives better by helping us organize, simplify our daily activities and its many applications provide us with unlimited opportunities. Smart homes, smart city, smart wearables, smart cars are some of the many applications of IoT. In a real-life scenario, a smart city can use the Internet of Things technology for waste management, to help businesses involved increase efficiency and reduce costs (Shahid & Aneja, 2017).

The threat of cyber-attacks to the Internet of Things cannot be overemphasized because of the damages and disruption they could cause to the services they provide. This paper analyzed the security goals of an Internet of Things system, classified different types of attacks that could be targeted at it and provided some countermeasures to mitigate them. Attacks on IoT systems were classified into four categories: Physical Attacks, Network Attacks, Software Attacks, and Encryption Attacks. Furthermore, they discussed future research areas that need to be addressed to improve security in IoT (Andrea, Chrysostomou, & Hadjichristofi, 2015).

Due to the rapid growth in IoT, there is always the possibility of new risks to data security and privacy. This paper offered some experimental evaluation of consumer's IoT devices against cybersecurity threats. Test suites were created to conduct their evaluation in four categories; Confidentiality, Integrity and Authentication, Access Control and Reflection of DDoS attacks. Seventeen consumer IoT devices from four different smart environments (home security, health monitoring, energy management, and entertainment) were used, and each device was given an overall rating based on the threats found in each category. They concluded that the current generation of IoT devices is vulnerable to many security attacks in many different ways. The findings in this paper are aimed at informing consumers, manufacturers and regulators of IoT devices to develop a more secure IoT platform to tackle the problems identified (Sivanathan, Loi, Gharakheili, & Sivaraman, 2017).

We cannot underestimate the importance of sensors in a smart home and how the knowledge of that could help in the future design of smart cities. In this paper, they categorized smart home services and analyzed the types of sensors used. The aim was to estimate the importance of sensors used in a smart home by using a Sensor Tree. Sensor Tree was a model created to show the relationships between smart home services and sensors highlighted in the paper. The more connection a sensor had to multiple services, the higher the relative importance ranking. From the results, they considered the motion sensor to be the most important because it was used in seven smart home services more than any other sensor (Kang et al., 2016).

The non-standardization of security and privacy mechanisms implanted in the design of IoT devices makes them susceptible to various types of attacks. This paper puts to test the vulnerability of an IoT device to a Denial of Service attack using Kali Linux. Three different methods were used to launch an attack on the device and the results were compared to analyze the effect of this cyber-attack method. The experimental platform used in this paper consisted of the following components: a personal computer for collecting data from the IoT device, the IoT device based on Arduino, Attacker (Kali Linux) installed on a virtual machine, and a router to connect of the components of the network together. The experiment results

showed that each method of Denial of Service attack used influenced the connection between the IoT device and the PC. Cyber-attacks can be carried out on a large scale IoT environment to disrupt normal services (Liang, Zheng, Sheng, & Huang, 2016).

A survey was carried out on the security and privacy issues in IoT, which detailed some limitations of IoT devices such as battery capacity, computing power and provided some solutions. They also went further to classify attacks on IoT, mechanisms for authentication and access control. Based on this survey, it was concluded that there is a need for standardization in both security and privacy policies for IoT. This would help manufacturers develop reliable and robust IoT platforms to tackle emerging threats (Yang, Wu, Yin, Li, & Zhao, 2017).

Over the past years, we have seen a steady increase in technical researches done in the field of IoT. Most researchers use test beds and simulators to develop IoT prototypes and validate initial proof of concept. There are few or no simulators in the market that covers the entire scope of an IoT system. To assist researchers in their work, this paper provides a comparative analysis of existing simulators that support IoT systems, and large-scale testbeds used to develop and test IoT prototypes. A couple of challenges were highlighted from the use of existing simulators and test beds that needed to be addressed to provide better IoT simulation (Chernyshev, Baig, Bello, & Zeadally, 2018).

The advantages of using IoT devices far outweigh the disadvantages; nevertheless, its limitations still need to be taken seriously because of the kind of damage that could arise from a compromised IoT system. Encryption and authentication are one of the ways to prevent unauthorized access to IoT devices. Many countermeasures based on encryption are gaining steam in the research community, and one topic that stands out is lightweight cryptography. This method features a low computational complexity, which addresses computational constraint of IoT devices. The major limitation of this method is the management and exchange of key operations and functions in real applications (Toshihiko, 2017).

Many users still do not know the level of privacy they surrender when they use IoT devices or the variety of sensitive data they give manufacturers access to when we agree to those long license agreements that most consumers never read. Some smart devices are known to record offline activities and transmit information about these activities to the internet. By analyzing network traffic from smart home devices, a third party observing the network can deduce a user's home activities. Blocking, tunneling and traffic rate shaping are some strategies that can be used to mitigate the privacy risks associated with smart home devices. The experiment carried out in this research paper showed that traffic rate shaping was able to mitigate most privacy concerns with smart home devices effectively without any significant drop in network performance or implying an extra cost (Apthorpe, Reisman, Sundaresan, Narayanan, & Feamster, 2017).

Urban IoT is designed to be the framework that would help achieve the goal of building smart cities. Smart cities comprise of smart things such as smart grid, smart systems, smart industries which are embedded with microcontrollers and sensors for digital communication. The main vision of smart cities is to utilize the most advanced technologies to support value-adding services for the administration of the city and for the people. We are starting to see some applications of IoT in supporting smart cities in areas of waste management, power grids, traffic congestion, and smart parking. It is safe to say the concept of IoT and smart city are closely intertwined (Zanella, Bui, Castellani, Vangelista, & Zorzi, 2014).

Neito et al. (2017) proposed a model called ProFIT for IoT forensics, which takes privacy into cognizance by incorporating the privacy requirements established by ISO/IEC 29100 – 2011 that is observed throughout an investigation period (Nieto, Rios, & Lopez, 2017). The model is made up of six phases which are preparation, context-based collection, data analysis and correlation, information sharing, presentation, and review. Since privacy was considered in this model, it helps facilitate the voluntary collaboration of IoT devices, both personal and non-personal either belonging to an individual or an organization in digital forensic investigations. This model was tested in a staged case scenario and was

successful. Testing this model on a larger scale case with different persons of interest would be an ideal scenario to evaluate its performance and efficiency.

The continual growth of cloud computing and the Internet of Things continues to change the way business processes and daily human activities are carried out. This paper proposes a cloud-centric framework that isolates big data as forensic evidence from IoT infrastructures for proper analysis and examination by digital forensic investigators. The conceptual framework introduced in this paper consists of three high-level layers, which includes cloud/IoT infrastructure, the forensic evidence isolation, and digital forensic investigation layer. As of now, there is no acceptable framework for digital forensic investigation on cloud-based IoT infrastructures. This being a conceptual idea, developing a prototype with a detailed architecture of the framework would allow us the opportunities for testing this framework in a real-life scenario (Kebande, Karie, & Venter, 2017).

IoT environments provide a rich source of data that can be used to aid digital forensic investigation without the help of human witness evidence. This paper talks about the challenges IoT poses to digital forensics identifies areas of concentration researchers should look to improve and provide solutions. A typical digital forensic investigation is broken down into four phases, which are identification, preservation, analysis, and presentation. This paper highlights key challenges IoT poses to each phase of a digital forensic investigation and identifies areas to be targeted by solutions and improvement. To be able to fulfill the approach presented in this paper, a test environment is required for implementation, deployment, analysis, and evaluation (Hegarty, Lamb, & Attwood, 2014).

Harbawi and Varol (2017) presented a revised IoT digital evidence acquisition procedure and an improved conceptual framework for IoT forensic to handle the issues around the acquisition of evidence (Harbawi & Varol, 2017). This model tackles the issue of acquiring evidence by identifying the device or thing that produces the initial traces of evidence. To achieve this a LOS (Last on Scene) algorithm was used which is a procedural process that helps digital forensic investigators to identify things of interests and narrow down workloads and overheads so as to avoid them from searching through irrelevant

evidence. This increases the effectiveness and productivity of digital forensic investigators. An IoT management platform was introduced to help restrict access to materials to only concerned parties such as digital forensic investigators, security personnel, courts, etc. This being a theoretical framework gives room for future work to improve the research. For future work, one thing that should be considered is implementing this framework based on LOS algorithm and creating the needed testing in a real-world scenario to prove its applicability (Harbawi & Varol, 2017).

A Generic Digital Forensic Investigation Framework for the Internet of Things (IoT) was proposed in this paper to assist digital forensic investigators in collecting and analyzing potential evidence from IoT environments with a high degree of certainty that can be accepted in the court of law for criminal cases. Compared to other models previously proposed, this framework provides a more detailed approach for digital forensic investigation in an IoT environment. This helps provide a proper groundwork for the future development of digital forensic tools that would enable better and efficient digital forensic investigation in an IoT environment (Kebande & Ray, 2016).

A general review of existing methods for collecting IoT data from Amazon Echo, Z-wave protocol and home routers was presented to describe the various types of forensic data that has already been collected from them and techniques used in achieving that. Forensic data described in this paper can be used by researchers and investigators as proper groundwork to come up with additional mechanisms that can be used for obtaining forensic data from these devices (Shin, Chandok, Liu, Nielson, & Leschke, 2017).

To help address the challenges faced by digital forensic investigators in knowing the steps and processes to take in identifying relevant, meaningful and court-admissible forensic evidence data when conducting an investigation on an IoT device, some necessary steps need to be taken. This paper presents a model based on a triage model design and 1-2-3 zone model for volatile-based data preservation to help digital forensic professionals and experts to coordinate investigation situations and processes properly. One of the weaknesses of this paper is the fact that the privacy interests of individuals, groups, and

organizations were not put into consideration. For future work on this research, more emphasis should be placed on IoT data privacy (Perumal, Norwawi, & Raman, 2015).

Some of these IoT devices are known to have security vulnerabilities and with the access they have to big data, it opens doors to cybercriminals looking to exfiltrate data. In this paper, they used IOS devices as a case study and highlighted the potential of exploited IOS devices in a paired mode to covertly exfiltrate data. They found out an IOS device could be susceptible to cyber-attacks. They advised in the paper that device manufacturers should provide a mechanism to authorize client software that has access to device resources and for the device users, it was recommended they verify the origin of applications before going ahead to install them on their devices (D'Orazio, Choo, & Yang, 2017).

Most IoT devices do not have local or persistent data storage, which is why all of their data is stored in the cloud. This feature of IoT makes it susceptible to the challenges faced by other cloud platforms. The main issue of cloud forensic is that data stored in the cloud are distributed over multiple nodes, which may also reside in multiple legal jurisdictions making it hard for digital forensic investigators to acquire such data. In relation to my research topic which has to do with extracting data stored from an IoT device (Amazon Echo Dot), I envisage encountering the same issue faced in cloud forensics. The research directions mentioned in this paper, for example, a distributed processor using a graphics processing unit would help reduce the backlog in digital forensics (Lillis, Becker, O'Sullivan, & Scanlon, 2016).

IoT devices are new targets for attacks and may contain many potential security and privacy risks. In this paper, a penetration testing system for IoT was presented called PENTOS with the main aim of improving security around IoT technology. This system puts together penetration tools necessary for IoT devices, providing an easy, systematic guide to users on how to perform penetration testing and build security awareness when building and deploying IoT devices. This prototype was implemented on Kali Linux 2.0 and the target device used was Raspberry Pi 3 model B board running on Raspbian OS. The summarized results of the penetration testing showed the device was unsafe because the tool was able to

successfully carry out some of the attacks launched at it. PENTOS also analyzes all the vulnerabilities found in each category and this can be exported to file to provide more details and information (Visoottiviseth, Akarasiriwong, Chaiyasart, & Chotivatunyu, 2017).

Smart things are changing the way humans interact with the outside world. We have various applications of IoT technology like home automation, smart grid, smart industries, etc. As this technology becomes widespread it becomes easy for anyone to misuse it for malicious purposes and it is very important to secure it. In this paper, an architecture was presented to detect Denial of Service (DOS) on 6LoWPAN communication standard protocol, which integrates an intrusion detection system into the framework developed within project ebbits. Intrusion detection systems are considered to be the first line of defense for any network system and it helps in being proactive rather than reactive in the case of a possible cyber-attack (Kasinathan, Pastrone, Spirito, & Vinkovits, 2013).

A network of interconnected devices that can be accessed via the internet brings about potential security threats. This paper proposes a visualization tool called VisIoT that is capable of detecting and monitoring several types of security attacks on an IP-enabled Wireless Sensor Network. VisIoT is built on a powerful visualization engine that uses a cross-free radial layout to monitor the states of the network and to effectively unravel sensor network attacks. After several simulations, VisIoT was able to help detect and expose concurrent sensor network attacks and identify the root cause of these attacks. This visualization tool in the hands of a network security expert would assist in detecting network anomalies in a large scale IoT enabled system by analyzing large amounts of data (Sarigiannidis, Karapistoli, & Economides, 2015).

Security is very difficult to implement in IoT systems because most of the embedded devices are deployed in areas that are uncontrolled and are resource constrained which make them susceptible to various security attacks. IoT networks with real-time constraints are prone to denial of service attacks, which affects the application availability by injecting harmful packets into the network. Chifor et al (2017) proposed a lightweight security system to help mitigate DoS attacks on IoT publish-subscribe applications. To mitigate against some of these attacks most especially IoT Denial of Service attacks, the proposed

architecture allows trusted devices to enforce security policies to the broker by using the CoP channel, this way the broker authenticates and collects data from trusted devices and drops messages from untrusted ones (Chifor, Bica, & Patriciu, 2017).

A number of IoT devices communicate with BLE, which requires low power to operate and can be deployed in uncontrolled environments to communicate with other devices. The framework aims to connect anyone with anything anywhere in the world. This paper presents a real-life hacking of a device that uses BLE protocol (smart bulb). The hacking was successful using soft hardware hacking method, which shows that other devices that use this protocol can be susceptible to cyber-attacks. This highlights the importance of implementing a secure BLE connection between IoT devices (Chandan & Khairnar, 2018).

In the design of home automation, one of the most used smart devices is the intelligent, digital personal assistant. Users interact with these devices using voice commands to perform a variety of useful tasks that include but are not limited to streaming music and media, controlling other smart devices, retrieving real-time news and so on. A security analysis of the Amazon Echo Dot was presented in this paper and a couple of attacks were carried out on this device to identify possible security vulnerabilities. From the results, Amazon Echo Dot was found to provide a suitable level of security, it was resistant to both network and API based attacks (Bispham, Agrafiotis, & Goldsmith, 2018).

Wearable technology is a current trend in the field of IoT that can be incorporated into clothing, accessories, implants, etc. The most common smart wearables used by consumers are fitness and activity trackers, which help track and monitor key health vitals. This paper provides a detailed security analysis of the Fitbit Flex ecosystem. Fitbit is one of the leading companies that produce wireless-enabled wearable technology. The main goal of this research was to determine how Fitbit manages data collected from users. To achieve this goal, experiments were carried out that revealed some flaws in the system. Overall, it was concluded that Fitbit provides a decent level of privacy for user data, but still has room for improvement (Cyr, Horn, Miao, & Specter, 2014).

3 AN OVERVIEW OF SECURITY THREATS TO SMART HOME DEVICES

3.1 INTRODUCTION

The Internet of Things provides an endless supply of opportunities to interconnect devices, which gives room for innovation and creativity. The rapid growth in the Internet of Things has made home and industrial automation a reality. For every innovation and technology comes its fair share of challenges. Some fundamental problems that have been identified by industry experts are data security, data privacy, data management and scalability of the Internet of Things systems. The challenges of security and privacy have to do with making sure data being transmitted are encrypted to prevent unauthorized access and data being collected do not infringe on user privacy and confidentiality.

Many factors need to be considered when implementing an IoT system. Due to the sheer number of devices that could be connected to the internet, IoT systems have to be very robust to allow various devices to connect and establish an internet enabled connection amongst themselves for communication and transmission of data. For every IoT system, we have three major components which are sensing, processing and communicating (Gubbi, Buyya, Marusic, & Palaniswami, 2013).

The heterogeneous nature of IoT devices would require some of these devices to play both the role of data producers as well as consumers. It would be necessary that not all data produced by IoT devices are transmitted to the cloud for processing. Some data should be processed at the edge of the network to provide faster feedback to users and help reduce the load on network bandwidth.

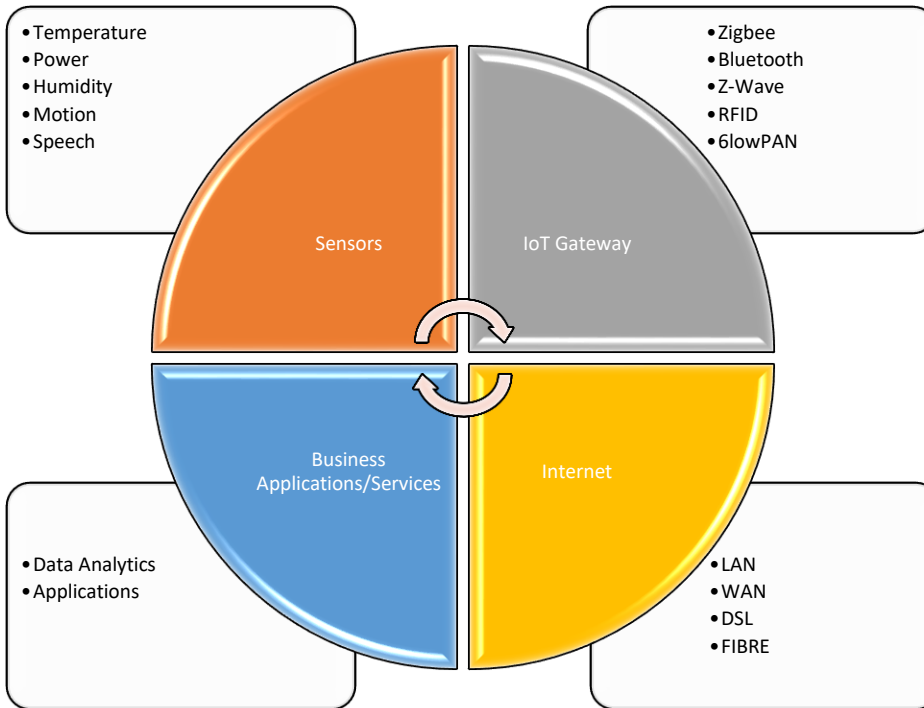


Figure 3.1 1. A basic Internet of Things system.

It is at this point we might discuss edge computing as a solution because more data is produced at the edge of the network by mobile devices, routers. Due to this fact, it would be more efficient to process data at the edge of a network to achieve faster results. One of the reasons for edge computing is that the speed of data transportation has become a thorn for cloud-based computing, which is the framework IoT operates on. Over the past couple of years, we have experienced fast development in data processing speed while no significant upgrade has been done in the area of network bandwidth. Therefore, data has to be processed at the edge for quicker feedbacks and also to help reduce the load on bandwidth.

According to an article posted by Forbes Technology Council, they provided a list of the most commonly used smart home devices currently in the market and how these devices have changed the way we live. A few of the devices are as follows: Amazon Echo, Nest Thermostat, Phillip Hue Lightbulb, Rachio Smart Sprinklers, Amazon Cloud Camera, and Google Home (Council, 2017). In the table below, we took a look at each device, analyzed all its components for sensing, processing and communicating.

DEVICES	SENSORS	NETWORK PROTOCOLS
Amazon Echo	Automated Speech Recognition, Sound	Wi-Fi, Bluetooth, Zigbee
Nest Thermostat	Temperature, Humidity, Proximity	Wi-Fi, Bluetooth
Phillip Hue Smart bulb	Light, Motion	Zigbee
Rachio Smart Sprinkler	Flowmeter, soil, rain	Wi-Fi
Amazon Cloud Cam	Image, Motion, Light, Sound	Wi-Fi
Google Home	Automatic Speech Recognition, Sound	Wi-Fi, Bluetooth

Table 3.1 1. Sensors and protocols used by common smart home devices.

This research aims to provide consumers with an idea of common security threats smart home devices could be susceptible to and the best ways to guard against them. The rest of the paper is coordinated as follows; section 3.2 provides a background study on the Internet of Things, communication protocols it uses and possible security threats with some countermeasures. Section 3.3 presents implications for practice that should be considered during the implementation of the Internet of Things and a review of existing simulators that support the testing and development of IoT.

3.2 BACKGROUND STUDY

A sensor is a device with the primary purpose of detecting occurrences or changes in its environment, records and sends this information to other electronics, which are often devices with a processor. Sensors are used with other electronics, whether as simple as a light or as complex as a computer and used in everyday objects such as touch-sensitive buttons in ATMs and so on. The most commonly used sensors for smart home automation are temperature, motion, humidity, speech, sound, pressure, magnetic fields, gas, touch sensors, and others.

The whole idea behind a smart home is to have everything talking to each other, so you stay informed about situations and anomalies in your home. IoT protocols mostly used by smart home devices are ZigBee, Z-wave, Bluetooth LE and Wi-Fi. ZigBee and Z-wave are wireless standards which are alternatives for smart home devices to communicate with one another rather than using Wi-Fi. Devices like smart door locks and windows, which consume less power and bandwidth use standards like ZigBee, Z-wave or Bluetooth because of their low data and power rate feature. They are simpler and cheaper to implement in smart devices compared to Wi-Fi, which makes them suitable for home automation.

There is a perplexing choice of connectivity options for developers working on systems and devices designed for the Internet of Things. The choice of connectivity usually used depends on the function the device is meant to perform. A small device that only collects the temperature of a particular room might require a lower power communication protocol to exchange data compared to a device that uses voice commands to perform activities and tasks. IoT protocols can be divided into two major types: IoT network protocols, and IoT data protocols that handle different layers in an IoT system.

3.2.1 IoT Network Protocols

We have compiled a list of the most commonly used IoT network protocols available to developers below. Deciding on which protocol to use depends on factors such as data requirements, security, power demands, and battery life would determine the choice of protocol to use (Postscapes, 2019).

1. *Bluetooth*: It is commonly used for short-range wireless communication. The new Bluetooth Low Energy (BLE) or Bluetooth Smart is significant for the Internet of Things. Wearable Technology uses this protocol because it makes use of fewer data and conserves more energy. Examples of devices that use BLE are Smartwatch fitness trackers.
2. *ZigBee*: It operates at a 2.4GHz frequency just the same as Bluetooth. It is a mesh network protocol originally designed for building automation and controls. Smart home devices like wireless thermostats, lighting systems often use ZigBee.

3. *Z-Wave*: This is a mesh network protocol primarily designed for home automation. It is optimized for reliable, low latency communication of small data packets within IoT network devices like security systems and lighting controls.
4. *6LowPan*: It is a network protocol that uses lightweight IP based communication, which allows data the freedom to travel over lower data rate networks, and is used across multiple communication platforms. It is primarily used for home and building automation.
5. *Wi-Fi*: This protocol is considered the favored choice among smart device designers for IoT integration. It has an existing infrastructure that offers fast data transfer rates and the capacity to handle a large quantity of data. The major drawback of using Wi-Fi in IoT development is the excessive power it consumes.

3.2.2 IoT Data Protocols

1. *Message Queuing Telemetry Transport (MQTT)*: It is one of the most commonly used protocols in IoT development and projects. It makes use of a publish and subscribe messaging model to exchange data between clients and servers in an extremely lightweight way. Its lower power usage, minimized data packets and the simplicity in implementation make it an ideal protocol for the IoT world.
2. *Constrained Application Protocol*: It is a specialized web transfer protocol designed for use between devices in a constrained network, devices and general nodes on the Internet, and between devices on different constrained networks both joined by an internet. The protocol is designed for M2M applications such as smart grid and building automation where resource constrained internet devices are used.
3. *Advanced Message Queuing Protocol*: It is a message-oriented application layer protocol designed for middleware environments. It consists of 3 main components; Exchange, Message queue and Binding. The process flow involves the exchange component getting the message and queuing them up which are then stored in the message queue and remain there until the messages are safely

developed by the client application. The final component, which is the binding, states the connection between the exchange component and the message queue component.

4. *Hypertext Transfer Protocol (HTTP)*: It is the protocol used by the worldwide web for communication between web servers and web browsers over the internet. It can also be used by IoT devices that need to publish large amounts of data.

Most of the challenges faced by the Internet of Things are passed onto it by default because of the numerous technologies and network infrastructures it integrates such as the internet, cloud computing, wireless sensor networks, etc. More security threats tend to arise from its collaboration with other new technologies due to the open standards and protocols it uses. A broader attempt to capture security vulnerabilities and possible attacks on IoT is presented in the table below. This categorization of attacks makes it easier to mitigate existing security threats, empowers consumers and manufacturers to develop countermeasures to secure IoT devices (Al-Fuqaha et al., 2015)

IoT layers	Possible Attacks	Countermeasures
Sensors	Node Tampering Node Jamming Social Engineering RF Interference	Regulated transmitted power. Secure Booting for all IoT devices. Two-factor Authentication. Device Identification and access control.
IoT Gateway/ Network	Denial of Service Traffic Analysis attacks Man-in-the-Middle (MITM) Replay Attacks Spoofing	Implementation of Routing Security. Sending of dummy packet, and regular monitoring of the network. Point-to-Point Encryption for data confidentiality. Timestamps, one-time passwords.
Business Applications / Services	SQL Injection Cross-site scripting(XSS) Password attack	Strong password enforcement. Ensure account lockout after a few attempts. Application layer encryption.

Table 3.2 1. Security threats and countermeasures.

According to the functionalities and features of each layer, an attacker can choose a specific attack to carry out. The table above provides an overview of existing countermeasures that would improve the security level of an Internet of Things system.

3.3 IMPLICATION FOR PRACTICE

There is a lot of research opportunity in the area of IoT and the first that comes to mind is finding effective ways for analyzing big data produced by IoT devices. We recommend Internet of Things gateway as a solution to help tackle the challenges faced in the processing of IoT data.

IoT gateway is a device that bridges the communication between IoT devices and cloud/data center infrastructures that enable them. The application of IoT is more evident today with the immense growth of internet enabled devices. This can be seen everywhere in our lives from smart speakers that require voice commands to serve its purpose to smart thermostats that improve customer's comfort by collecting and analyzing temperature data to create dynamic home conditions that fit the user's preferences.

Many devices used in various applications require a different set of processing while they collect, analyze and take actions on data inputs to function. Internet of Things gateway is very important because it supports the requirements of different devices, so they can all perform optimally together. Configuring an IoT gateway to perform the preprocessing of data collected from sensors before being transmitted is one of its many functions. Examples of IoT gateway devices are Wink Hub, Samsung Smart Hub and more.

Described below are some of the main functions performed by an IoT gateway device;

1. Provides an advanced level of security for IoT devices. They make sure data is encrypted in transit, that no unauthorized user can gain access to the device and protects it from been compromised by cyber attackers.
2. It plays a crucial role in the analytics and processing capacity they provide to an IoT environment. Many devices generate a vast amount of data that has to be transmitted over the internet for

processing in the cloud. IoT gateway helps share the processing load and takes some burden of cloud operating systems in both computing power and network bandwidth.

3. IoT devices often need to collaborate to serve the needs of consumers. An example would be the aggregation of a security camera and an alarm to help detect home intrusion. Alone a security camera monitors the environment without being able to perform any action with the information collected. The way an IoT gateway device works in this example is by sorting through images captured by security cameras to make meaning of it and then trigger an action like sounding an alarm when an intrusion or motion anomaly is detected.
4. Devices like window sensors or battery powered door locks use standards like ZigBee, Z-wave or Bluetooth wireless communication protocol because of their low power consumption feature while AC powered smart devices like Smart TVs use protocols like Wi-Fi to communicate. IoT gateway translates different communication protocols, allows interoperability of all connected devices and sensors, thus creating a central control unit for all devices where communications or control commands to devices can be coordinated.
5. IoT gateway can be deployed for the management of IoT devices in a smart home or smart industry environment. It helps in configuring, monitoring and maintaining devices' firmware that provides functional capabilities. Better device management could help prolong the longevity, maintain connectivity and security of IoT devices.

Most researchers use simulators to develop IoT prototypes and validate proof of concepts. In academia, building prototypes using physical boards can be time-consuming and prone to errors which cannot be easily rectified, this is why simulators are preferred for research purposes. IoT simulators allow us to create, design and test front-end applications and devices for functionality without the use of real IoT boards. Since the Internet of Things is a relatively new and evolving concept, there are no simulators in the market that cover the end-to-end simulation of an IoT system. We provide the three layers of a conventional IoT system and review some simulators that are currently being used for IoT development

and research. To better understand functions the simulators perform, we explained the layers that make up an IoT system.

1. *Perception Layer*: This layer is responsible for collecting useful information from devices or the environment via sensors and transforms them into a digital form that can be transmitted.
2. *Network Layer*: This layer ensures secure data transmission between the perception layer and the application layer of IoT architecture.
3. *Application Layer*: This layer bridges the gap between users and application; it provides users with personalized services based on their needs.

The table below presents a review of existing simulators that support IoT simulation and the scope of their functions.

Simulators	IoT architecture Layer	Scope	Source
IoTify	Network Layer and Application layer	<ul style="list-style-type: none"> Offers simulation as a Service Generates traffic in real time via MQTT, HTTP or CoAP Simulates underlying network conditions 	Commercial
Tetcos NetSim	Network layer	Test and demonstrate network designs in realistic scenarios <ul style="list-style-type: none"> Optimize protocol and application performance 	Commercial
BevyWise IoT simulator	Application Layer	<ul style="list-style-type: none"> Offers simulation as a Service Generates traffic in real time via MQTT, HTTP or CoAP 	Freeware
Tetcos NetSim	Network layer	Test and demonstrate network designs in realistic scenarios <ul style="list-style-type: none"> Optimize protocol and application performance 	Commercial
Qualnet	Network Layer	<ul style="list-style-type: none"> Provides an environment for designing protocols, creating and animating network scenarios, and analyzing their performance. 	Commercial
CupCarbon	Network Layer	<ul style="list-style-type: none"> Simulates a Smart City and Internet of Things Wireless Sensor Network. 	Freeware

Table 3.3 1. Comparison of Existing IoT simulators

Most of these existing simulators only focus on a particular layer of an IoT system such as Network or Application Layer without being able to adequately represent an end-to-end simulation of an IoT service with high accuracy. A viable solution would be combining multiple simulators to represent the different layers in the architecture to achieve the goal of an end to end IoT simulation.

From this review research, we see that different security attacks can be carried out at different levels of an IoT architecture, thus the need for manufacturers to develop strong and robust security standards to tackle existing and emerging threats.

4 INVESTIGATING PRIVACY CHALLENGES ASSOCIATED WITH AMAZON ECHO DOT USING DIGITAL FORENSIC TOOLS

4.1 INTRODUCTION

The need to have our mobile devices, home appliances, devices embedded with sensors interconnected to each other has become a trending topic over recent years. Internet of Things is an emerging technology that encompasses these ideas and it is currently implemented in our daily lives, such as smart homes, smart cars and even in some smart industries. Every emerging technology raises new challenges, some challenges that come to mind when we talk about IoT are data privacy and data security. Following the review presented in the first study that shows the susceptibility of IoT to security attacks, this next study delves into the concerns consumers have with IoT data privacy and security.

The development and recent explosion of IoT present digital forensic investigators with new challenges. There are currently no established frameworks that describe the process to be taken during the digital forensic investigation of a dynamic environment such as cloud computing and IoT environments. Due to the sheer number of IoT devices currently and their heterogeneous nature, a large amount of data will be generated which would bring about challenges in areas of data management and privacy.

Not knowing exactly what is being stored by IoT devices or how secure their communication channels are for transmitting sensitive information attracts hackers to eavesdrop on peoples' networks to see what information can be captured with malicious intent in mind. Most companies that provide services for IoT devices claim to observe best practice guidelines for user privacy and network security during development. This has led us to investigate some security and privacy challenges that could be associated with IoT devices.

Amazon Echo Dot a hands free, voice-controlled smart speaker that uses Amazon's cloud-based voice service called "Alexa" to control smart home devices, play music, send and receive messages, etc. Amazon cloud-based voice service 'Alexa' requires that developers implement all reasonable security

measures to prevent unauthorized access to the Alexa service. For developers and manufacturers that want to integrate their products with the Alexa service, they are required to follow some guidelines to ensure that their products meet security best practices. Some of these guidelines are:

- They must use secure software update distribution, incorporate cryptographic signing so that only authentic and authorized updates are applied to the device.
- They should have a strategy that defines how software updates will be created and distributed when vulnerabilities are identified within a reasonable period of discovery.
- Include information on their website on how security researchers can notify them when a security vulnerability has been identified.
- They must use a secure, authenticated channel for transmitting sensitive information and data (Alexa, 2017).

As for privacy best practices, the Amazon Echo Dot transmits and stores all voice commands in cloud storage owned by Amazon. History of voice commands can be deleted at any time by an authorized user on the Alexa mobile application. Amazon says no data is saved locally on the device and without the wake-up word "Alexa" spoken; the device does not record or transmit any surrounding noise.

An Amazon spokesperson has been quoted saying "Amazon will not release customer information without a valid and binding legal demand properly served on us. Amazon objects to overbroad or otherwise inappropriate demands as a matter of course (Forbes, 2017)."

This paper is organized as follows, section 4.2 details the steps that were taken in setting up the test environment and acquiring our results using two different digital forensic tools and section 4.3 is where we discussed the results and provided some suggestions on how to achieve better results.

4.2 RESEARCH METHODOLOGY

This research seeks to address the concerns around data privacy associated with IoT devices, in this case we would be focusing our research on the Amazon Echo Dot a voice-controlled device and speaker that uses Amazon's cloud-based voice service called "Alexa" to control smart home devices, play music, send and receive messages and so on. To explore the question of privacy surrounding IoT devices and be sure no sensitive data is being saved on the device we used two different digital forensic tools to see what information can be extracted from the Amazon Echo Dot and compared the results from the tests to see which performed better. The first digital forensic tool used is an open source forensic tool called The Sleuth Kit, which is used to extract information from mobile devices and raw image files while the second one is a commercial digital forensic tool called Paraben E3:DS (Raji, Wimmer, & Haddad, 2018). Wireshark was used to capture the network traffic from our test environment and visualize the trend in the data being transmitted to get more insights.

To set up our test environment, we configured the Amazon Echo Dot with an Amazon account using the Amazon Alexa mobile application, then went on to configure a laptop as a wireless access point. Having the laptop act as a router would give us full control of the environment's network traffic. The device was then connected to the internet via the laptop. To capture the network traffic flowing out of the Amazon Echo Dot through the configured laptop to the internet, remote servers and vice versa, we installed Wireshark network analyzer to see exactly what is happening on the network at a microscopic level.

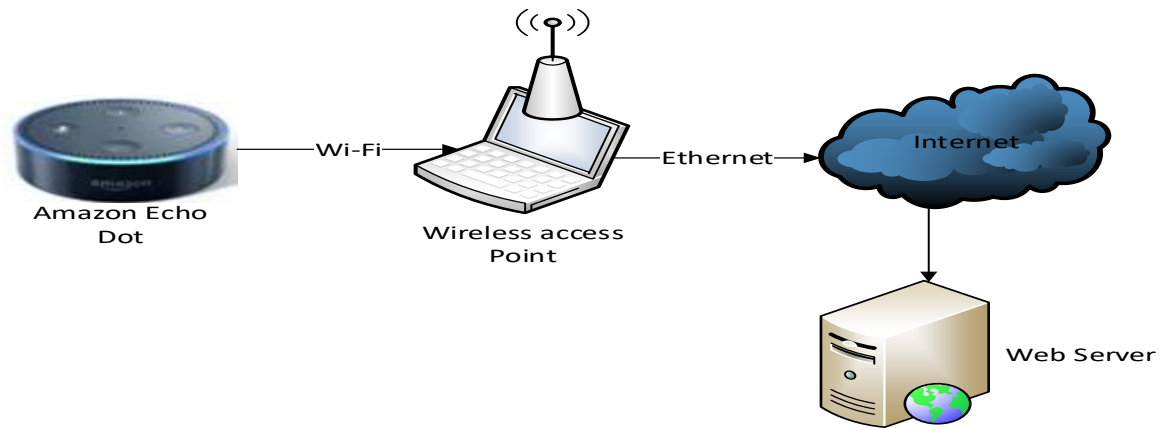


Figure 4.2 1. Network set-up for the test environment.

The diagram above illustrates the network set-up for our test environment. Now that the device has been configured and connected to the internet we moved to the next phase of the experiment. In the next phase, we documented a number of interactions with the device, captured the traffic using Wireshark network analyzer to provide a graphical illustration to see how data is transmitted over the internet to Amazon web servers.

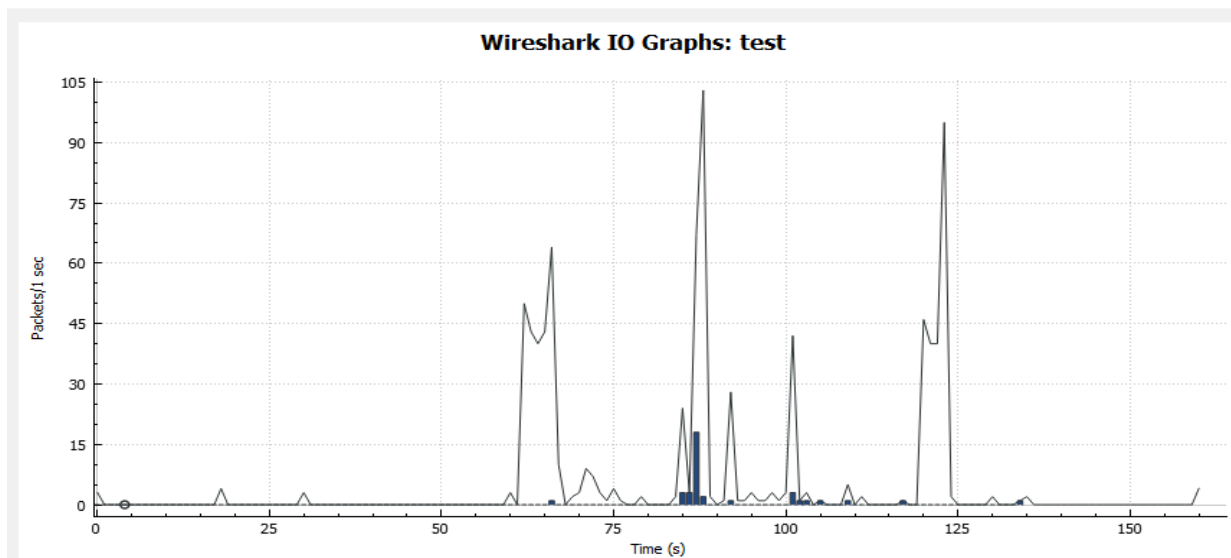


Figure 4.2 2. Graphical representation of an Amazon Echo Dot network traffic.

The above graph represents the network transmission that occurred during our interaction with the device. We documented the interactions that occurred to better understand the graph pictured above. Listed below are the commands the device was given to execute;

- Alexa, what is today's date?
- Alexa responds, then silence for 10 seconds
- Alexa, tell me a joke.
- Alexa responds, silence for another 20 seconds
- Alexa, what is the weather forecast for Tomorrow?
- Alexa responds, silence for 15 seconds and we ended the capture.

From the graph, we deduced that when the wake word Alexa was said followed by a command, a large number of packets were transmitted while during the silent period very few packets were transmitted which appeared to be packets that ensured connectivity between the device and the web servers was still alive. To begin the experiment, we installed both The Sleuth Kit and Paraben E3:DS on the laptop and connected the device to it. A Samsung Galaxy 8 phone with an Android operating system, a quad-core CPU and an internal memory of 32GB was paired with the device for the initial configuration.

4.3 RESULTS

To verify that security and privacy best practice guidelines were implemented in the design of an Amazon Echo Dot, we used Wireshark network analyzer to capture the network traffic and analyze the various types of packets transmitted by the device over the internet. The screenshots below show us some packets transmitted over the internet by the Amazon Echo Dot.

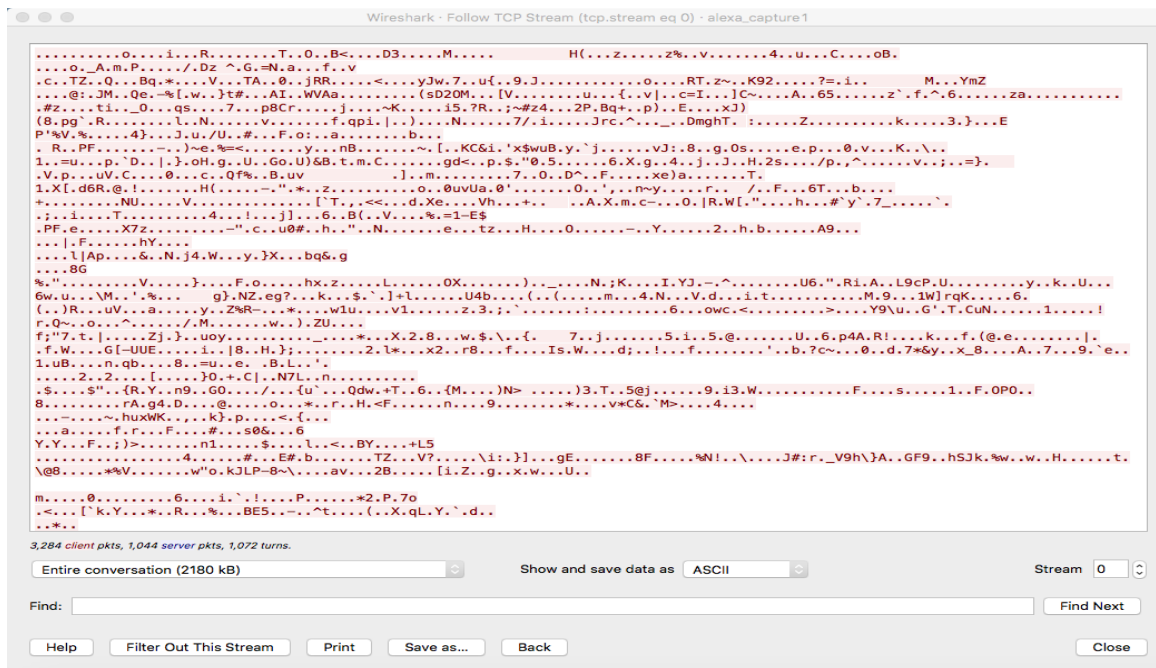


Figure 4.3 1. An encrypted packet transmitted using TLS protocol

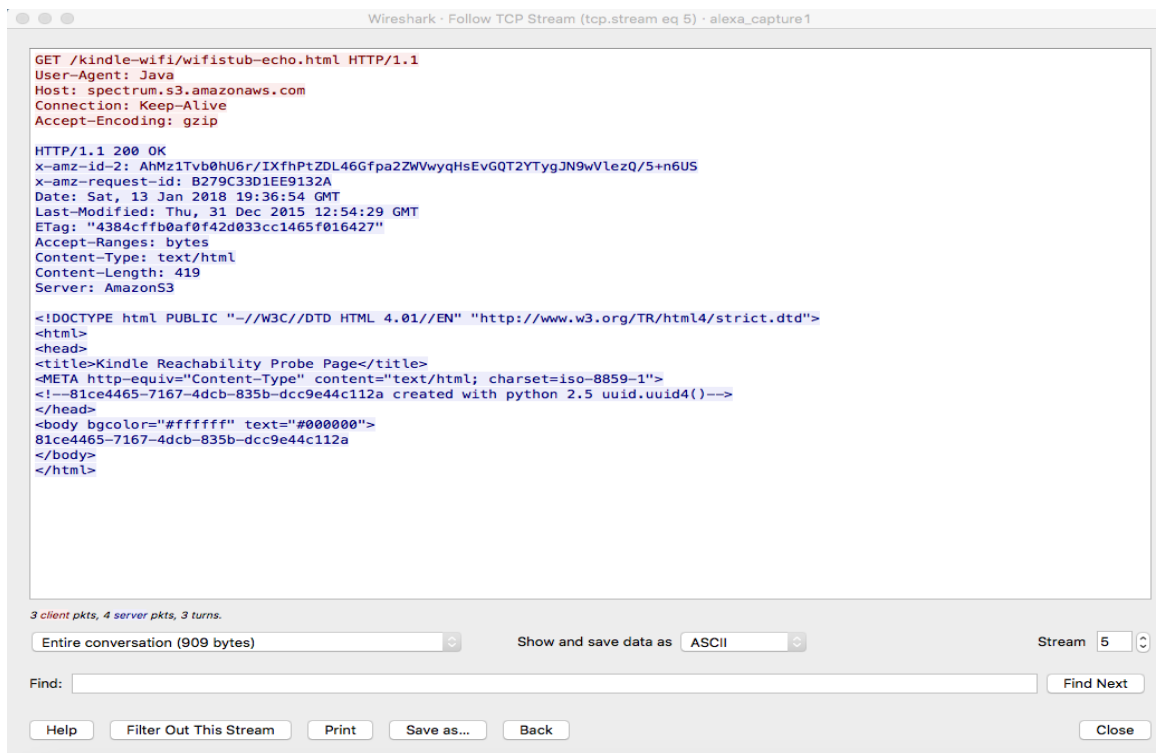


Figure 4.3 2. Metadata of an HTTP packet

The Figure 4.3.1 shows the encrypted data transmitted to Amazon web servers using the TLS protocol, while Figure 4.3.2 shows an HTTP request sent from the device to Amazon web servers in plain text just to confirm its connection to the service. Packets using other network protocols were also captured and they are ICMP (Internet Control Message Protocol), MDNS (Multicast DNS), ARP (Address Resolution Protocol) and TCP (Transmission Control Protocol). From the diagrams above and after carefully analyzing the packets it is safe to say that the device does not transmit personal data, voice commands or user credentials over unsecured channels. Although the Amazon Echo Dot has a USB connector, no wired communication is possible, making it impossible to copy data from it via USB which aligns with what Amazon says about user data privacy regarding the device.

Using The Sleuth Kit, we were unable to view the device as one with any form of storage in it due to the limited options provided by the tool and also the fact the device was not visible when connected to a computer. Data collected by the Amazon Echo Dot is stored in the cloud, and this tool does not provide us with the feature for acquiring data from cloud accounts. Using Paraben E3:DS we were still unable to see the device when connected to a computer for us to extract data from it, but this tool provided us with more options like cloud data acquisition, etc. This device is designed to save all human interactions with it in the cloud and knowing this we could get some vital information associated with the user. This tool works by acquiring all the data on the mobile device paired with the device to obtain a file called "Authentication data" which authenticates cloud accounts. This file is used to authenticate cloud import from Facebook, Twitter and Amazon Alexa, etc. The screenshots below show some steps that were taken during the cloud import for the Amazon Echo Dot.

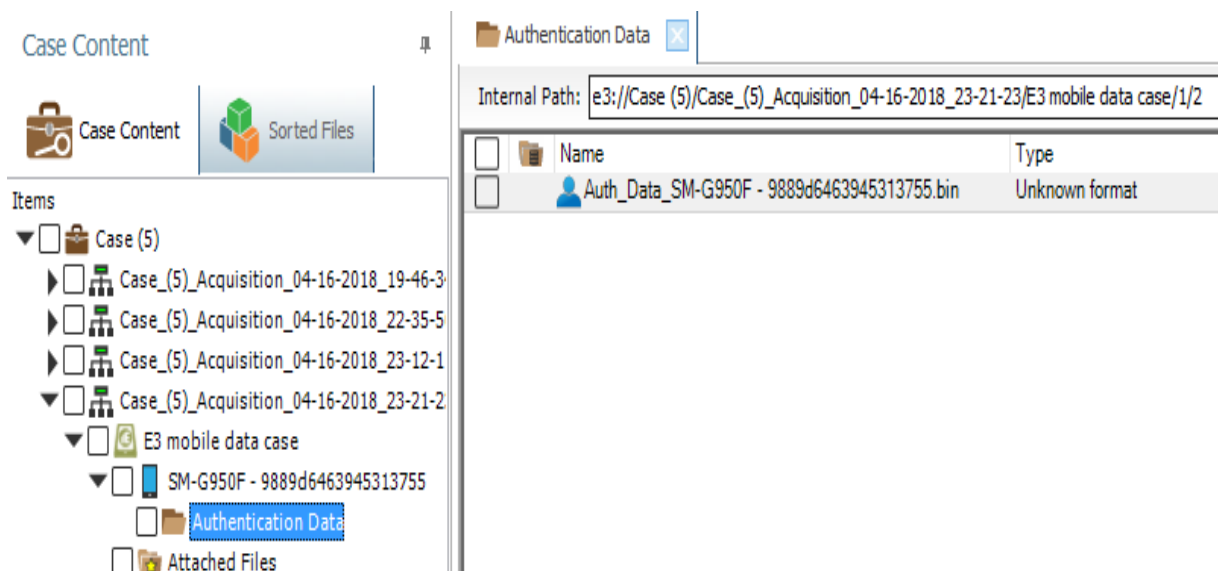


Figure 4.3 3. Mobile device data acquisition using Paraben E3.

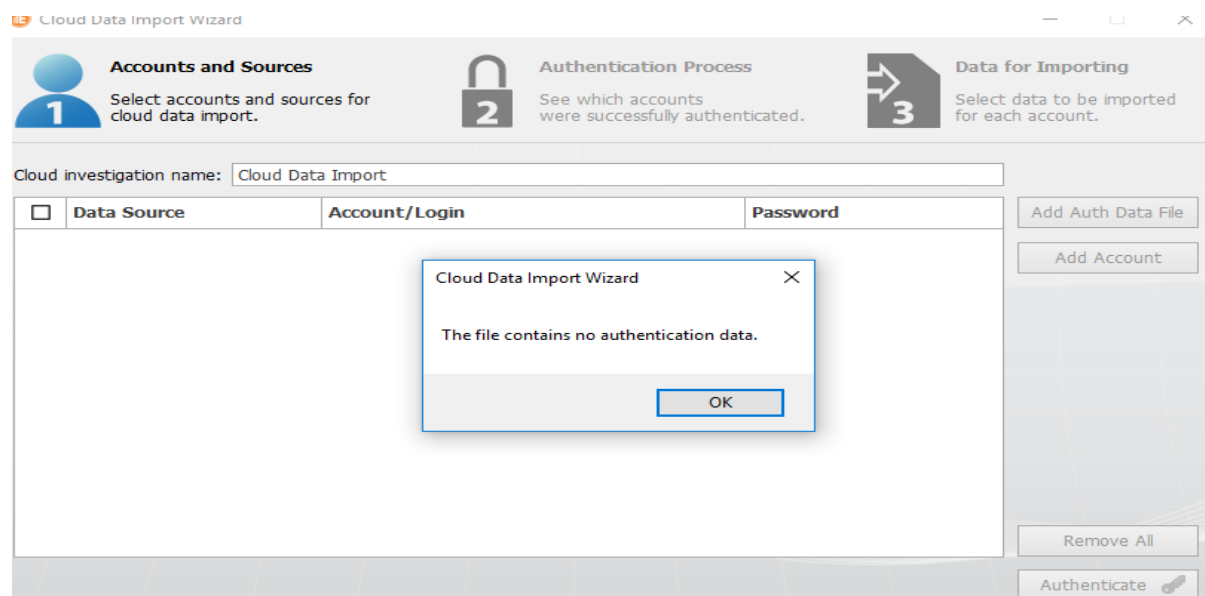


Figure 4.3 4. Error message while trying cloud import.

While performing the mobile acquisition for the mobile device, the authentication file required for cloud import was not successfully acquired. Trying to use the authentication file found in the authentication data folder to authorize cloud import, we got the error message “This file contains no authentication data.”

However, according to the information provided on Paraben Corporation website, it has been documented that the tool can be used to obtain IoT cloud data from Amazon Alexa account associated with an Amazon Echo device. The chart below shows data and information that can be gotten from the device (Corporation, 2018).

Basic User Information	Types of data Acquired
Username	Recording Time
User ID	Summary of activity
User Email	Audio (link to the recording)
Access to Prime music or not	Device Type

Table 4.3 1. Amazon Echo acquired information and data types.

4.4 CONCLUSION

Users of IoT devices still do not know what level of privacy they surrender in using them if their data are being sold to other people for consumer marketing or have sensitive information saved without consent. From the experiment carried out in this research, we were able to discover that no sensitive data was sent in plaintext over the internet, all data sent back and forth were encrypted. The commercial tool Paraben E3:DS would also be more helpful in recovering data from IoT devices during a digital forensic investigation than The Sleuth Kit due to the option it provides for cloud data acquisition. The device when connected via USB to a computer was not visible and no local storage was found which made it impossible for us to extract data from it. According to an online article that documented the teardown of the device, it showed that the device has a type of NAND flash memory storage (IFIXIT, 2018). This research was

carried out for educational purposes in a controlled environment and should not be done in a real-life scenario without legal authorization to do so. For future work, open source digital forensic tools should include the option for cloud data acquisition on their platforms, and ways of extracting data from a NAND flash memory should be explored.

5 HACKING A SMART BLUETOOTH LOW ENERGY DEVICE USING GATTACKER

5.1 INTRODUCTION

By the year 2025, predictions have it that the number of connected devices would reach 100 billion and this would come with many challenges in the areas of security and privacy. While there has been tremendous growth in the use of smartphones and smart devices, the advancement of wearable technology has also been on the rise with more appearances of wearable devices in our daily lives.

While adequate measures are being taken to secure IoT environments, it comes as no surprise that security is still one of the main concerns with the continuous growth of the Internet of Things. The way billions of devices are interconnected introduces new security vulnerabilities, where it is possible for a cybercriminal or a hacker to hack your refrigerator and gain access to your entire network. With billions of devices interconnected over the internet, companies are faced with challenges on how to securely store data produced by these devices, while still being able to access, track and analyze them (Dataversity, 2016).

Penetration testing is a method used by security experts to test computer systems, web applications and networks to identify security vulnerabilities that could be exploited by hackers for malicious intent. Penetration testing helps provide many benefits to IoT by providing manufacturers with proactive actions to help improve device security, protect against unauthorized access and set strong and reliable end to end encryption to avoid various cyber-attacks (Bishop & Privacy, 2007).

Smart devices are electronics that connect to each other or to other networks via different wireless protocols like Bluetooth, Wi-Fi, 3G, etc. Smart devices make up the Internet of Things and can operate autonomously. Examples of smart devices are smartphones, smartwatches, smart car, and others. In this paper, we used a smart fitness watch, which tracks user activities like the steps taken per day, heart rate and other vitals as the target device. This device communicates with a mobile application using Bluetooth Low Energy protocol, which we would attempt to exploit, using GATTacker to initiate a MiTM attack or replay

based attacks on the device and see to what extent data transmitted, could be modified and used to disrupt its functionality.

5.2 BACKGROUND STUDY

The implementation of Bluetooth should include device pairing, bonding and link layer encryption in its transmission, but a number of devices that use this protocol do not implement these features and research communities have identified several security vulnerabilities. Devices that use Bluetooth are susceptible to different kinds of attacks from a denial of service, by spoofing, active transmission interception and others. Protocol standards like Bluetooth Low Energy and ANT have been designed for low data rate, short range and low power communication (Ting & Lin, 2017). According to a research by Artem et al. (Dementyev, Hodges, Taylor, & Smith, 2013) BLE was found to have achieved the lowest power consumption when compared to other standards like ZigBee and ANT which makes it very popular among developers of small IoT devices.

Connected Bluetooth devices transfer data back and forth using concepts called services and characteristics, which is defined by the Generic Attribute Profile (GATT). GATT makes use of a generic data protocol called Attributes (ATT), which stores services and related data in a simple lookup table using 16-bit IDs for each entry in the table. Establishing a connection is the only way two devices can make a two-way communication and these connections are exclusive, which means BLE devices can only be connected to one central device at a time. As soon as a connection is established, the BLE device stops advertising itself and other devices will no longer be able to see it or connect to it.

5.2.1 GATT Transactions

GATT adopts the concept of a server/client relationship model, so before any transaction takes place between the peripheral device and central device, GATT defines the roles each interacting device adopts. A peripheral device is known to be the GATT server; it holds the ATT lookup data, services &

characteristics while the GATT client is the central device, which sends requests to the server. Every BLE device should at least include a basic GATT server that responds to requests from the client.

Universally Unique IDs (UUIDs) are used in many protocols and applications but are used a lot more in Bluetooth Low Energy devices. In BLE, UUIDs are used to identify services and characteristics known as attributes. These IDs are transmitted by a peripheral to inform the central devices of what services it provides. There are two types of UUIDs used in BLE; a short 16-bit UUID which is energy and memory efficient and can only transmit the predefined UUID directly over the air and the 128-bit UUID often referred to as a vendor-specific UUID which allows developers to make custom services and characteristics. Attributes are the smallest data chunk defined by GATT. They are pieces of information that review relevant data about the user structure and grouping of different attributes contained in the server (Prtvar, Mihajlović, Lazić, & Miljković, 2015).



Figure 5.2 1. Illustration of BLE GATT profile

5.2.2 Bluetooth Low Energy Security

In Bluetooth Low Energy when two devices are connected, they establish a connection link in two ways. The first is called “Pairing” where connected devices exchange features and information required to establish a secure connection to exchange data while the second one is “Bonding” when the information for pairing is stored on the devices so that the pairing process does not need to be repeated every time these devices try to reconnect. There are three security models used in pairing devices in BLE implementation. Devices choose which model to use based on the input and output capability of the devices (Heydon, 2013).

1. *Just Works*: This method is not authenticated and uses a temporary key with no value, meaning devices are not verified during connection, making them susceptible to Man in the Middle attack, passive eavesdropping, etc.
2. *Out of Band Pairing*: This is the most secure model for pairing devices in BLE, instead of sharing the temporary key over Bluetooth frequency of 2.4GHz, it makes use of other mediums such as NFC to exchange the key. Once the exchange is done, it encrypts the communication link to ensure a very high level of security.
3. *Passkey Entry*: This method requires a 6-digit temporary key passed between the devices by the user. In this model, a device auto-generates a random 6-digit pin, which is entered on the other device to establish a link for communication. The con to this model is that devices require a keypad to enter the temporary key that makes it not feasible for use in most smart wearable devices.

5.3 RESEARCH METHODOLOGY

This section explains the steps taken in carrying out a penetration test on a Bluetooth Low energy device, in this case, a smart fitness watch. For this experiment, we used two CSR 4.0 Bluetooth adapters and two virtual machines both running on Ubuntu 18.0 (master and slave) for our test environment. The

penetration testing tool we used is called GATTacker, which is a Node.js package for BLE security assessment using Man-in-the-Middle, replay based attacks, and other attacks. The goal is to eavesdrop on transmitted packets between the smart device and the mobile application to allow us to perform some type of data modification or MiTM attack.

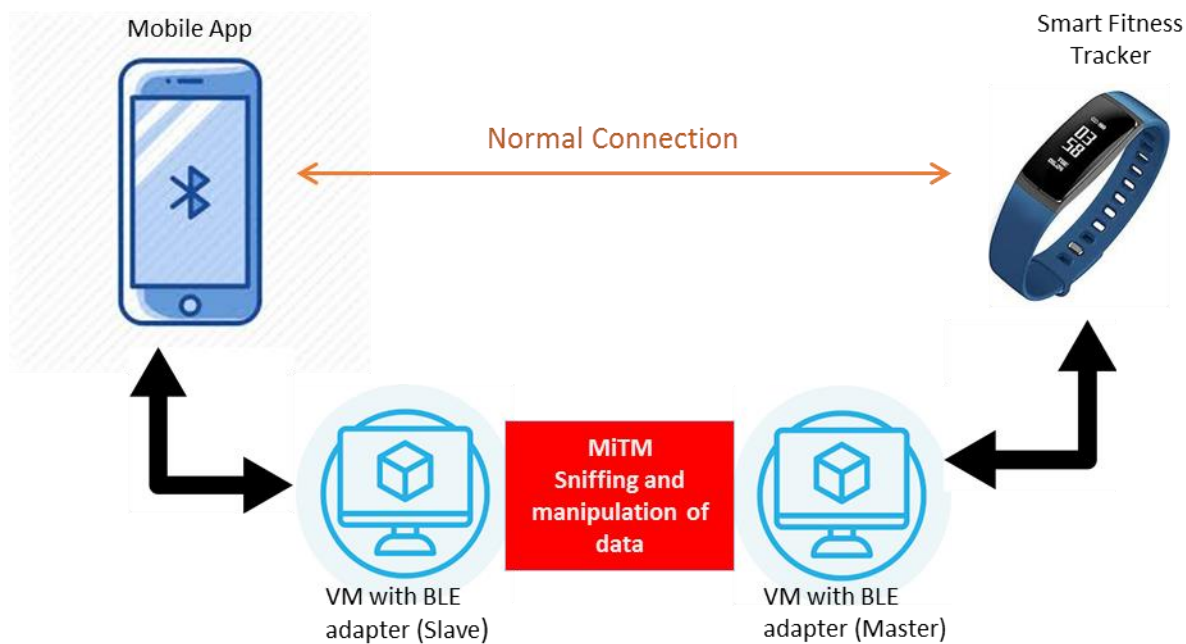


Figure 5.2 2. The Penetration testing framework

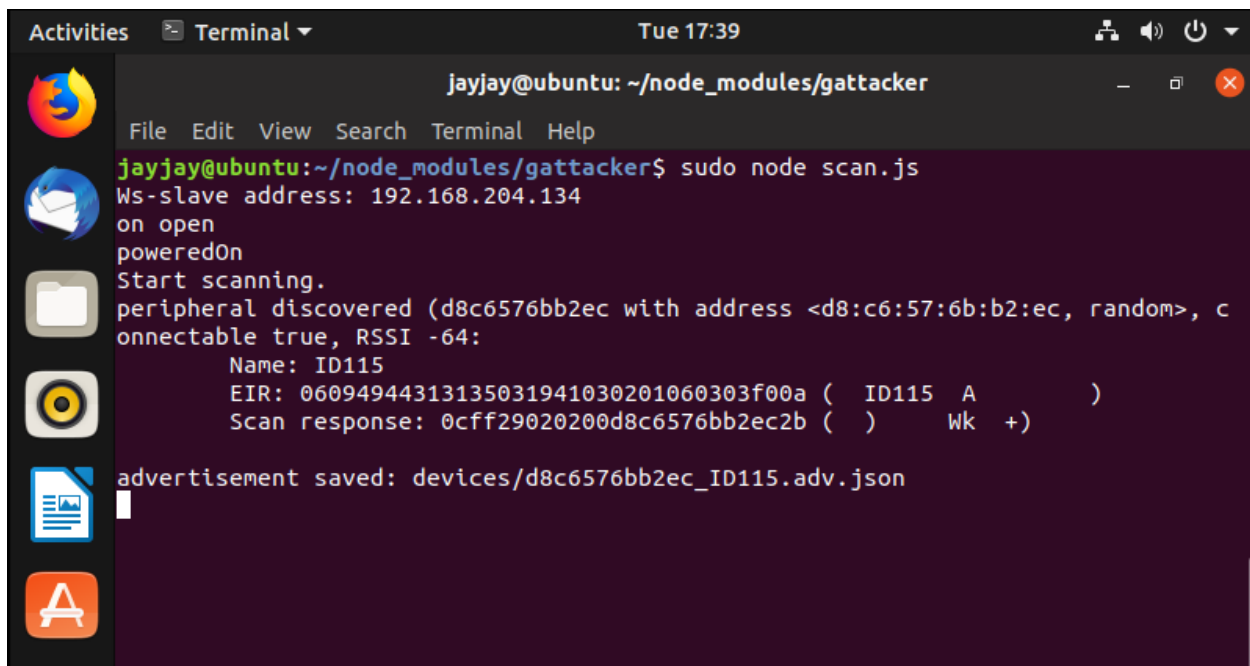
To setup up the test environment, we installed Ubuntu 18.0 on both virtual machines, once completed we launch Ubuntu terminal to update all archives and pre-installed applications on the VMs. To install GATTacker, the latest version of node package manager has to be installed. After the above steps, to implement both BLE central module and peripheral module, we installed bleno and noble using the commands below;

`npm install bleno` - A Node.js module for implementing BLE peripherals.

`npm install noble` - A Node.js for implementing BLE central module.

Next step, we installed GATTacker and repeated all the steps on the second virtual machine as well, one to act as the master machine and the other the slave machine. Once all the requirements were

installed successfully, we proceeded to configure the slave machine. Each Bluetooth adapter is connected to a virtual machine which clones the functions of the mobile application and the BLE device respectively. They communicate with each other via WebSocket, which has been configured on the master machine using the slave machine's IP address. The master stores all the GATT profiles and characteristics of the original device. To make sure the Bluetooth adapters were plugged in correctly, we used the command `sudo hciconfig`, which displays name and basic information of all Bluetooth devices installed on the system. Following the successful configuration of both the slave and master machines, we launched the slave machine to activate the WebSocket channel for communication. While on the master machine we ran a simple scan command which discovers all nearby BLE device advertisement data.



```

jayjay@ubuntu: ~/node_modules/gattacker
File Edit View Search Terminal Help
jayjay@ubuntu:~/node_modules/gattacker$ sudo node scan.js
Ws-slave address: 192.168.204.134
on open
poweredOn
Start scanning.
peripheral discovered (d8c6576bb2ec with address <d8:c6:57:6b:b2:ec, random>, c
onnectable true, RSSI -64:
    Name: ID115
    EIR: 06094944313135031941030201060303f00a ( ID115 A )
    Scan response: 0cff29020200d8c6576bb2ec2b ( ) wk +)
advertisement saved: devices/d8c6576bb2ec_ID115.adv.json
  
```

Figure 5.2 3. Scanning for nearby BLE device advertisement data

The intervals at which BLE devices advertise their presence are short, so they constantly broadcast advertisement packets. The tool was able to discover our smart fitness watch, along with its physical address and device name. After successfully scanning and saving the advertisement data for the target device with the name ID115, we then scanned the device to save its GATT profiles and services. We used



Figure 5.2 5. BLE device scan on the mobile application

The cloned device was advertised with the mac address 00:1A:7D: DA: 71:13 with all the profiles and characteristics of the original device. Connection to the clone device did not last long enough for the mobile application to pair and bind with it. The device probably has some form of security implemented which prevents the mobile application from pairing with the clone device.

We then proceeded to use a generic BLE scanner application to scan for the clone device and we were able to discover its services and attributes. From the application, we wrote some values to the clone device and the figure below shows the interaction that took place.

```
>> Write: 1800 (Generic Access) -> 2a00 (Device Name ) : 447261676f6e (Dragon)
Client disconnected: 5d:e1:4b:e9:bf:82
Client connected: 5d:e1:4b:e9:bf:82
>> Write: af0 -> af6 : 3636363636363636 (66666666)
Client disconnected: 5d:e1:4b:e9:bf:82
Client connected: 59:81:1a:e5:88:e5
>> Write: af0 -> af1 : 03050617 ( )
Client disconnected: 59:81:1a:e5:88:e5
```

Figure 5.2 6. Write commands using a generic BLE scanner.

```

jayjay@ubuntu:~/node_modules/gattacker$ sudo node replay.js -i dump/d8c6576bb2e
c.log -p d8c6576bb2ec -s devices/d8c6576bb2ec.srv.json
[sudo] password for jayjay:
Ws-slave address: 192.168.204.139
on open
poweredOn
Noble MAC address : 00:1a:7d:da:71:13
initialized !
WRITE CMD: 447261676f6e
WRITE CMD: 3636363636363636
WRITE CMD: 03050617

```

Figure 5.2 7. Replay-based attack using GATTacker

After initiating a replay based attack with the file saved when we used the BLE generic scanner to write some values, the tool connected to the original device disguising to be an original connection from the mobile application. The tool was able to cause a temporary Denial of Service to the original device. During this time, we were unable to discover and connect to the original device from the original mobile application.

From our results, we were unsuccessful in carrying out our intended form of attack, but we found out that with the tool we could also perform a denial of service attack to disrupt the services of the device and jeopardize its connection to the mobile application. The severity of this attack might have been low, but imagine a more vital medical device that administers medication to a patient, a disruption in service or connection at any point in time could be very severe. Other BLE devices like sensors, light bulbs, medical devices, and many other products are mostly insecure and could be susceptible to these kinds of attacks.

Consumers of BLE devices need to be aware of these security vulnerabilities and fully understand the limitations of smart devices rather than blindly relying on them because most BLE devices do not implement adequate security for data exchange. We recommend that users keep their devices in sleep mode when not in use because attacks are only possible when these devices are discoverable. Using more secure pairing methods like OOB and passkey entry, data encryption and strong authentication would provide more security protection that needs to be implemented in BLE devices and its mobile applications.

6 CONCLUSION

This study has shown that there is a need for consumers of the Internet of Things to be aware of security and privacy challenges IoT devices present to them. The comprehensive analysis of an Internet of Things system gives users a perspective into the design and implementation of smart devices used in IoT, the different kind of security attacks they could be vulnerable to and measures they can implement to stay protected from malicious attacks.

Penetration testing has been very effective in network security and can translate into IoT security by helping to determine whether a system is vulnerable to attack and if its defenses are sufficient. Extensive research needs to be continuously carried out in securing IoT and the best way to do this would be with the help of simulators because building IoT testbeds can be costly and time-consuming. That is why we provided some of the best simulators in the market that could assist researchers in their work.

The aim of this study is also to help understand to what extent IoT developers observe security and customer privacy best practices in the design of Internet of Things devices. The use of digital forensic tools and penetration testing tools were helpful in analyzing data transmitted back and forth these devices and to exploit security vulnerabilities that could be found. The two devices used in this research were Amazon Echo Dot and a smart fitness watch, which are very popular among consumer of smart devices. From our results, both devices provided a satiable level of privacy and security, no sensitive data was sent in plaintext over their communication channels, all communications were encrypted for the Amazon Echo Dot, which protected it from a Man in The Middle attack and other forms of data manipulation. For the smart fitness tracker, we were able to clone the device, advertise its profile and services, but we were unsuccessful in intercepting or manipulating data, making it resistant to Man in The Middle attacks or passive eavesdropping. The smart fitness watch was found to be vulnerable to DoS attack using a replay-based mode of attack.

Attack methods will continue to evolve and more attacks attempted on smart devices will occur as the number of interconnected devices continue to increase around the world. The general safety of IoT devices depends on the protocols, technologies and security mechanisms implemented by different manufacturers. To help with these challenges there needs to be a standard governing Internet of Things design and implementation. Building an IoT governance model on an already established Internet governance model would provide some principles and rules that would help shape the use of the Internet of things. For a model like this to work, security and privacy policies have to be continually reviewed by all stakeholders involved in the Internet of Things ecosystem because the number devices connected will continue to rise exponentially and this will introduce new security and privacy challenges.

7 REFERENCES

- Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M. J. I. c. s., & tutorials. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *17*(4), 2347-2376.
- Alexa, A. (2017). Security Best Practices.
- Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015). *Internet of Things: Security vulnerabilities and challenges*. Paper presented at the Computers and Communication (ISCC), 2015 IEEE Symposium on.
- Apthorpe, N., Reisman, D., Sundaresan, S., Narayanan, A., & Feamster, N. J. a. p. a. (2017). Spying on the smart home: Privacy attacks and defenses on encrypted iot traffic.
- Bishop, M. J. I. S., & Privacy. (2007). About penetration testing. *5*(6), 84-87.
- Bispham, M. K., Agrafiotis, I., & Goldsmith, M. (2018). A taxonomy of attacks via the speech interface.
- Chandan, A. R., & Khairnar, V. D. (2018). *Bluetooth Low Energy (BLE) Crackdown Using IoT*. Paper presented at the 2018 International Conference on Inventive Research in Computing Applications (ICIRCA).
- Chernyshev, M., Baig, Z., Bello, O., & Zeadally, S. J. I. I. o. T. J. (2018). Internet of Things (IoT): research, simulators, and testbeds. *5*(3), 1637-1647.
- Chifor, B.-C., Bica, I., & Patriciu, V.-V. (2017). *Mitigating DoS attacks in publish-subscribe IoT networks*. Paper presented at the 2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI).
- Corporation, P. (2018). Amazon Echo BFF or Worst nightmare. Retrieved from <https://training.parabens.com/component/content/article?id=103:alexa-your-bff-or-worst-nightmare>
- Council, F. T. (2017). Retrieved from <https://www.forbes.com/sites/forbestechcouncil/2017/06/06/best-smart-home-devices-and-how-iot-is-changing-the-way-we-live/#1d5ba1fb43bd>
- Cyr, B., Horn, W., Miao, D., & Specter, M. J. M. I. o. T. (2014). Security analysis of wearable fitness devices (fitbit). *1*.
- D'Orazio, C. J., Choo, K.-K. R., & Yang, L. T. J. I. I. o. T. J. (2017). Data exfiltration from Internet of Things devices: iOS devices as case studies. *4*(2), 524-535.
- Dataversity. (2016). Brief History of IoT. <http://www.dataversity.net/brief-history-internet-things/>
- Dementyev, A., Hodges, S., Taylor, S., & Smith, J. (2013). *Power consumption analysis of Bluetooth Low Energy, ZigBee and ANT sensor nodes in a cyclic sleep scenario*. Paper presented at the 2013 IEEE International Wireless Symposium (IWS).
- Forbes. (2017). How Amazon Echo Users Can Control Privacy. Retrieved from <https://www.forbes.com/sites/tonybradley/2017/01/05/alexa-is-listening-but-amazon-values-privacy-and-gives-you-control/#335e56ed7ee6>
- Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. J. F. g. c. s. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *29*(7), 1645-1660.
- Harbawi, M., & Varol, A. (2017). *An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework*. Paper presented at the 2017 5th International Symposium on Digital Forensic and Security (ISDFS).
- Hegarty, R., Lamb, D. J., & Attwood, A. (2014). *Digital Evidence Challenges in the Internet of Things*. Paper presented at the INC.
- Heydon, R. (2013). *Bluetooth low energy: the developer's handbook* (Vol. 1): Prentice Hall Upper Saddle River, NJ.
- IFIXIT. (2018). Amazon Echo Dot Teardown. Retrieved from <https://www.ifixit.com/Teardown/Amazon+Echo+Dot+Teardown/61304>

- Kang, B., Kim, S., Choi, M.-I., Cho, K., Jang, S., & Park, S. (2016). *Analysis of Types and Importance of Sensors in Smart Home Services*. Paper presented at the High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2016 IEEE 18th International Conference on.
- Kasinathan, P., Pastrone, C., Spirito, M. A., & Vinkovits, M. (2013). *Denial-of-Service detection in 6LoWPAN based Internet of Things*. Paper presented at the 2013 IEEE 9th international conference on wireless and mobile computing, networking and communications (WiMob).
- Kebande, V. R., Karie, N. M., & Venter, H. (2017). *Cloud-Centric Framework for isolating Big data as forensic evidence from IoT infrastructures*. Paper presented at the 2017 1st International Conference on Next Generation Computing Applications (NextComp).
- Kebande, V. R., & Ray, I. (2016). *A generic digital forensic investigation framework for internet of things (iot)*. Paper presented at the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud).
- Liang, L., Zheng, K., Sheng, Q., & Huang, X. (2016). *A Denial of Service Attack Method for an IoT System*. Paper presented at the Information Technology in Medicine and Education (ITME), 2016 8th International Conference on.
- Lillis, D., Becker, B., O'Sullivan, T., & Scanlon, M. J. a. p. a. (2016). Current challenges and future research areas for digital forensic investigation.
- Nieto, A., Rios, R., & Lopez, J. (2017). *A methodology for privacy-aware IoT-forensics*. Paper presented at the 2017 IEEE Trustcom/BigDataSE/ICeSS.
- Perumal, S., Norwawi, N. M., & Raman, V. (2015). *Internet of Things (IoT) digital forensic investigation model: Top-down forensic approach methodology*. Paper presented at the 2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC).
- Postscapes. (2019). IoT Standards and Protocols. Retrieved from <https://www.postscapes.com/internet-of-things-protocols/>
- Prtvar, B., Mihajlović, D., Lazić, K., & Miljković, G. (2015). *Voice over BLE case study: Using bluetooth LE remote controller inside Google's Voice search framework*. Paper presented at the 2015 IEEE 5th International Conference on Consumer Electronics-Berlin (ICCE-Berlin).
- Raji, M., Wimmer, H., & Haddad, R. J. (2018). *Analyzing Data from an Android Smartphone while Comparing between Two Forensic Tools*. Paper presented at the SoutheastCon 2018.
- Sarigiannidis, P., Karapistoli, E., & Economides, A. A. (2015). *Visiot: A threat visualization tool for iot systems security*. Paper presented at the 2015 IEEE International Conference on Communication Workshop (ICCW).
- Shahid, N., & Aneja, S. (2017). *Internet of Things: Vision, application areas and research challenges*. Paper presented at the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC).
- Shin, C., Chandok, P., Liu, R., Nielson, S. J., & Leschke, T. R. (2017). *Potential forensic analysis of iot data: An overview of the state-of-the-art and future possibilities*. Paper presented at the 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData).
- Sivanathan, A., Loi, F., Gharakheili, H. H., & Sivaraman, V. (2017). *Experimental evaluation of cybersecurity threats to the smart-home*. Paper presented at the 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS).
- Ting, Y.-Y., & Lin, F. J. (2017). *A comparison and evaluation of different BLE connection methods for wearable devices*. Paper presented at the 2017 IEEE Conference on Standards for Communications and Networking (CSCN).
- Toshihiko, O. (2017). Lightweight Cryptography Applicable to Various IoT Devices. *NEC Technical Journal, Vol.12 No.1*.

- Visoottiviseth, V., Akarasiriwong, P., Chaiyasart, S., & Chotivatunyu, S. (2017). *PENTOS: Penetration testing tool for Internet of Thing devices*. Paper presented at the TENCON 2017-2017 IEEE Region 10 Conference.
- Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. J. I. I. o. T. J. (2017). A survey on security and privacy issues in internet-of-things. 4(5), 1250-1258.
- Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. J. I. I. o. T. j. (2014). Internet of things for smart cities. 1(1), 22-32.

8 ABBREVIATIONS

IoT – Internet of Things

WSNs – Wireless Sensor Networks

BLE - Bluetooth Low Energy

MiTM - Man in the Middle

RFID – Radio Frequency Identification

GATT – Generic Attribute Profile

UUID – Universal Unique Identifier

NPM - Node Package Manager

OOB – Out of Band