Optical Wireless Communications High-Speed Bluetooth Secure Pairing Towards Developing a Trust Protocol

by
Mantie N. Reid

Submitted in partial fulfillment
of the requirements for the degree of
Doctor of Professional Studies
in Computing Studies

at the

Seidenberg School of Computer Science and Information Systems

Pace University

October 2022

We hereby certify that this dissertation, submitted by Mantie N. Reid, satisfies the dissertation requirements for the degree of *Doctor of Professional Studies in Computing* and has been approved.

Matthew R Ganis
Matthew R Ganis (Nov 8, 2022 14:41 EST)

Dr. Matthew R. Ganis
Advisor of Dissertation Committee

Date: October 20, 2022

Susan Feather-Gannon
Susan Feather-Gannon (Nov 8, 2022 14:50 EST)

Dr. Susan Feather-Gannon
Dissertation Committee Member

Date: October 20, 2022

Saravanan Jayaraman
Saravanan Jayaraman (Nov 16, 2022 18:04 EST)

Dr. Saravanan Jayaraman
Dissertation Committee Member

Date: October 20, 2022

Seidenberg School of Computer Science and Information Systems
Pace University

Acknowledgements

This dissertation would not have been possible without crediting my cohorts and many others wo helped me throughout my dissertation journey. Special thank you to my dissertation advisor Dr. Matthew R. Ganis for his great support who recognized that I needed help in getting this dissertation completed. His knowledge, advice, coaching, and patience were critical and without it, I would not have completed this dissertation. I am forever grateful for his support.

I would also like to thank my committee members, Dr. Susan Feather-Gannon, and Dr. Jayaraman Saravanan for serving on my dissertation committee. Both provide great encouragement and overall insights and interest in this research. My sincerest gratitude to Dr. Hugh Eng, Dr. Wanda Kellum, Dr. Charles Tappert, Ms. Lauren Clarke, Ms. Alecia Copeland-Barrett, Mr. Paxton J. Louis, and Ms. Arlene A. Martin, all of whom supported and motivated me to continue my dissertation journey until the end. The weekly dissertation update calls, check-ins, encouragement, motivational wisdom, and advice have been greatly appreciated. This dissertation journey is so inspiring that I look forward to continuing learning together.

My sincerest thanks to all my cohorts, my friends, my entire family – Sanina and Mantie II - and most importantly my wonderful wife the late Sandra Lee Meningall-Reid for their love, understanding, patience, and full support as I went through this dissertation journey. By completing this dissertation journey, they are inspired to push through any challenges they may face with conviction and determination and to realized that they can always overcome challenges. Love you all forever!

Abstract

Bluetooth wireless technology is a short-range radio frequency wireless information transfer technology that connects any Bluetooth enabled device to another Bluetooth enabled device. The Bluetooth Service Discovery Protocol, as specified by the official website for the Bluetooth wireless technology, represents a considerable security vulnerability because it only provides a low level of security during identification. Many applications of the technology, such as in automobiles, tend to lag the state-of-the art. Many studies have indicated that Bluetooth's security needs some improvements. This research adds to the existing literature and seal the loopholes providing a systematic review of Bluetooth wireless technology security and systematically analyzing scholarly proposed solutions to the vulnerabilities. A qualitative review of the literature, followed by a design science step to develop a solution. A taxonomy of Bluetooth attacks is quantified with threat level ratings, along with Bluetooth risk mitigation and countermeasures. Finally, A thematic coding analysis, presents a proposed solution to Bluetooth wireless technology vulnerabilities.

Table of Contents

List of Tables vii

List of Figures viii

1. Introduction 1

    1.1 Problem Statement 6

    1.2 Purpose of the Study 7

    1.3 Brief Literature Review 10

    1.4 Dissertation Roadmap 16

2. Literature Review 17

    2.1 Bluetooth Wireless Technology Basics 17

    2.2 Bluetooth Wireless Technology Services 21

    2.3 Bluetooth Wireless Technology Profiles 30

    2.4 Bluetooth Wireless Technology Security 31

    2.5 Secure Simple Pairing (SSP) and its Loopholes 36

    2.6 The Passkey Entry Model 37

    2.7 The Just Works Model 38

    2.8 The Out-of-Band Model 39

    2.9 The Numeric Comparison Model 39

3. Research Methods 61

    3.1 Research Design 61

    3.2 Data Collection 62

    3.3 Data Analysis 63

    3.4 Design 64

    3.5 Ethical Considerations 64

4. Thematic Analysis 66
4.1 Current Bluetooth Security Architecture 69
4.2 Bluetooth 4.2 Security Protocol 73
4.3 Security Vulnerabilities in Bluetooth Technology 74
4.4 Popular Bluetooth Attacks 75
4.5 Present Solutions to Bluetooth's Vulnerabilities 84
4.6 Analysis of the Proposed Solutions 86
5. Conclusion and Future Work 99
Appendix A: Glossary 101
Appendix B: Acronyms and Abbreviations 103
Appendix C: Selected Bluetooth Wireless Networking Functions 105
References 106

List of Tables

Table 1: Bluetooth Wireless Technology Characteristics and Description 2

Table 2: Bluetooth Wireless Technology Security Modes 34

Table 3: Bluetooth Wireless Technology Characteristics..... 36

Table 4: Bluetooth Attacks & Threat Levels (Sandhya & Devi, 2014)..... 56

Table 5: Thematic Categories 68

List of Figures

Figure 1: Bluetooth Wireless Technology RF Power Classes 18

Figure 2: Bluetooth Wireless Technology Piconets 19

Figure 3: Bluetooth Wireless Technology Protocol Stack (Bluetooth 1, 2, & 3) 21

Figure 4: Bluetooth HCI interface Scenario 22

Figure 5: Bluetooth Wireless Technology SDP Protocol Stack 24

Figure 6: Bluetooth Protocol Stack (Bluetooth 4) 29

Figure 7: Bluetooth Profiles 30

Figure 8: Bluetooth Wireless Technology Pass Key Entry Method 37

Figure 9: Bluetooth Wireless Technology Just Works Model 38

Figure 10: Bluetooth Wireless Technology OOB Model 39

Figure 11: Bluetooth Wireless Technology Numeric Comparison 40

Figure 12: Mac Spoofing 53

Figure 13: Link Key Generation 71

Figure 14: SSP with Numeric Comparison 79

Figure 15: Demonstration of The Speed of GiGa-IR 95

Chapter 1

Introduction

Bluetooth wireless technology is a short-range radio frequency (RF) wireless information transfer technology that connects any Bluetooth-enabled device to another Bluetooth-enabled device. Bluetooth technology is available in almost all currently produced smartphones, tablets, laptops, gaming consoles, and many other electronic devices. Bluetooth low energy (BLE) provides a 1 Mbps data transfer rate. It is a low-cost, low-power technology that works on wireless personal area networks (WPAN), commonly observed as ad hoc or peer-to-peer (P2P) networks. Bluetooth employs a frequency hopping technique. Frequency hopping is a transmission technique in which the carrier hops from frequency to frequency according to a certain "hopping" pattern. The advantage of this is that the signal sees a different channel and a different set of interfering signals during each hop. This avoids the problem of failing communication at a particular frequency due to a fade or a particular interferer (Khatod & Manolova, 2020).

Bluetooth contains a total of 79 channels spaced 1 MHz apart. During a connection, radio transceivers hop from one channel to another in a pseudo-random fashion. Based on this method, the data signal is modulated with a narrow band carrier signal that "hops" in random sequence in a regular time from frequency to frequency which is synchronized at both ends. The channel is divided into 625μ slots, and a different hop frequency is used for each slot. This gives a nominal hop rate of 1,600 hops per second. It allows each of the connected devices to use a very particular portion of the available radio wave spectrum and significantly decreases the chance that they will interfere with each other. Additionally, if interference occur, it will only last for

that very short amount of time, making it negligible. One packet can be transmitted per slot. Subsequent slots are alternately used for transmitting and receiving data. Given that the hopping patterns are pseudorandom, the chance that another Bluetooth device would use the same pattern and disrupt a large amount of dataflow is low (Khatod & Manolova, 2020). The key features of Bluetooth are outlined below in Table 1.

Table 1 Bluetooth Wireless Technology Characteristics and Description

Connection Type	Frequency Hopping Spread Spectrum
Frequency Band (Spectrum)	2.4 GHz ISM Band (non-regulated Industrial, Scientific, and Medical)
Hop Frequency Rate	1,600 hops/sec
Time Slot Length	625 μsecs
Channel Capacity	79 Channels (*1 MHz each from 2402MHz to 2480 MHz*)
Operating Range	Approximately 10 meters (30 feet), can be extended to 100 meters (300 feet)
Transmit Power	Nominal = 0dBm. Goes up to 20 dBm with power control.
Maximum Data Rate	721.2 kbps for Basic Rate. 2.1 Mbps with Enhanced Data Rate (BT Spec 2.0+EDR). 24 Mbps with High Speed (BT Spec 3.0+HS).
Data Security: Authentication Key	128 bit key
Data Security - Encryption Key	8-128 bits (configurable).
Piconet	Bluetooth Network topology. Network means in which a Bluetooth link is created; a collection of slave devices operating together with one master. Piconet is the fundamental unit of Bluetooth communications.
Network Type	Ad-hoc; peer-to-peer; point to multipoint
Applications	Wireless Personal Area Network

Applicability	Does not require Line of sight; intended to work anywhere in the world since it uses unlicensed band

Bluetooth wireless technology has become increasingly ubiquitous in the modern world. All smartphones, for example, are Bluetooth-enabled devices (Jeong et al., 2015), and Bluetooth low energy technology is an increasingly common technology used to support the introduction of an impressively wide array of devices to the Internet of Things (Grabovica et al., 2016). Due to its potential to provide security, privacy, and high-quality wireless communication (Cha et al., 2017), this technology will likely only continue to grow in its application as the Internet of Things spreads to encompass an ever-growing list of devices from smartphones to appliances to automobiles (Noor et al., 2018) or even to locks (Jeong et al., 2015). Bluetooth has also seen applications in the medical field, where Bluetooth-enabled wireless sensors may serve to reduce the cognitive load on emergency room doctors (Frisby et al., 2017) or provide essential telemetry data to inform patient treatment (Zegeye, 2015). Bluetooth Low Energy (BLE) has become one of the most popular wireless communication protocols and is used in billions of smart devices. Despite several security features, the hardware and software limitations of these devices makes them vulnerable to Man-in-the-middle (MITM) attacks. Due to the use of these devices in increasingly diverse and safety critical applications, the capability to detect MITM attacks has become more critical. It is estimated that 7.5 billion new devices supporting BLE protocol will be shipped from 2020-2024 (Yurdagul & Sencar, 2021). Given this astoundingly wide array of applications for the technology, many of which include handling very sensitive or private data, one would imagine that security would be perhaps the foremost issue in Bluetooth application and a problem long-since solved; unfortunately, this is not the case.

Bluetooth technology has a checkered security history; in previous versions, something as innocuous as leaving a Bluetooth-enabled device turned on while not in use could allow a malicious attacker to gain complete control of it (Alfaiate & Fonseca, 2012). Recent versions of Bluetooth, up to and including Bluetooth version 4.1, have sought to address many of the security vulnerabilities that have long plagued the technology (Cope et al., 2017). Many challenges remain, however. For example, while Bluetooth can offer security and privacy, it cannot offer both at once, with random address assignment—a privacy feature—contributing significantly to a lack of security because it prevents true device identification and allows for deceptive attacks (Cha et al., 2017). In addition, although national standards suggest that all Bluetooth devices should be run in their highest security mode (Padgette et al., 2012), these high security modes are rarely enabled by default. More troublingly, the users of these devices—whose data are at risk from security vulnerabilities—are often ambivalent or ignorant regarding Bluetooth security practices (Imgraben et al., 2014). Devices that do not support any input or output functions, such as wearable medical devices and trackers, use the default pairing method (Just Works) which does not offer any protection against MITM attack. It is reported that 71.5% of BLE devices are under threat of MITM attacks because of this limitation and insecure configurations (Yurdagul & Sencar, 2021).

Thus, Bluetooth security is an area of increasing importance. The ubiquity of Bluetooth technology and Bluetooth-enabled devices means that these devices have access to an unprecedented amount of data; even a smartwatch can reveal such data about its users. Ching and Singh (2016) studied security issues in wearable devices. Specifically, they were interested in conducting a combined security and privacy analysis for the broad class of wearable devices, such as smart watches (Do et al., 2017). The broader applications of Bluetooth technology, such

as automobiles and medicine, represent a considerably greater risk. In these contexts, an attacker can do more than just gain access to data. Taking control of the computer systems of a car could allow an attacker to create traffic accidents. Intruding on medical devices has the potential to allow an attacker to hold a patient for ransom by preventing medical attention or cause their treatment to be delivered incorrectly, resulting in complications or even death.

In addition, the range of Bluetooth-enabled devices is only growing at present. This means that these new applications may be at risk because they often use aspects of the technology that have not yet been rigorously tested for vulnerabilities (Tay et al., 2016). For example, Bluetooth low energy beacons have traditionally only been used for purposes containing no sensitive data, such as advertising. Recent developments, however, have opened the door for the use of these beacons for other purposes, such as mobile payment processing (Han & Ding, 2017). Thus, this technology may have been already compromised, but because the effects of those compromises on present applications were not significant, the vulnerabilities allowing have yet to be identified or corrected.

In both these emerging applications and others, the Bluetooth service discovery protocol (SDP) as specified by the Bluetooth SIG represents a considerable security vulnerability because it only provides a low level of security during identification (Kaushik et al., 2017). Due to the lack of an effective trust mechanism to identify devices, an attacker need only access the key (ID) generated by the application layer protocol L2CAP in order to breach the network. Although this vulnerability does not allow full access to the system, it does provide the attacker with valuable data about all the other Bluetooth devices and services on the network. These data could be used to follow up with a more dangerous attack, such as a man-in-the-middle (MITM)

attack, which provides the attacker with full access to one or more of these devices (Melamed, 2018).

1.1 Problem Statement

The problem is that although the security of Bluetooth technology has improved with the implementation of Bluetooth 4.1 and 4.2 (Gajbhiye et al., 2018), many applications of the technology, such as in automobiles, tend to lag the state-of-the art (Cheah et al., 2017). Moreover, even up-to-date Bluetooth devices may be significantly vulnerable to MITM attacks and other security exploits, with attackers able to steal data or even take control of the device entirely (Melamed, 2018). This is a serious problem because Bluetooth devices are used in several extremely important contexts, including medical monitoring devices for the elderly (Kumar, 2009) and tactical communications in the military (Thompson et al., 2016). Many common Bluetooth applications, such as mobile watches, can also be compromised to steal a significant amount of personal data, exposing users to identity theft (Do et al., 2017). The Bluetooth SDP represents the source of at least one such continuing vulnerability (Kaushik et al., 2017).

The National Institute for Science and Technology (NIST) standards for Bluetooth technology, NIST Special Publication 800-121 (Padgette et al., 2012), represented the theoretical framework underlying the study. In practice, however, these standards may not be followed by users who do not understand the value of their data (Imgraben et al., 2014) or because of the interaction between Bluetooth devices and third-party applications (Bello, 2017). Future scholars should examine the potential vulnerabilities present in Bluetooth devices to help understand the risks involved, which are overall under researched (Hassan et al., 2017). Such scholars should also consider how parameters such as security, reliability, and throughput may be jointly

optimized (Zou et al., 2016) and explore the potential threats to Bluetooth technologies (e.g., the iBeacon) that have not yet been targeted by malicious attacks (Tay et al., 2016).

1.2 Purpose of the Study

The purpose of this design science research was to analyze the Bluetooth SDP as specified by SIG for vulnerabilities and develop an improved trust protocol to address these vulnerabilities. Many common forms of Bluetooth-enabled devices, such as cars or smart watches, are already vulnerable to malicious attacks that can compromise personal information, and the number of devices using this technology is expanding rapidly. Although the vulnerabilities inherent in the Bluetooth SDP do not explicitly allow attackers to access the system, they do provide access to a significant amount of valuable data, such as information about all Bluetooth devices and services that are available. In turn, this could potentially enable attackers to use other methods to target those services. Moreover, to gain access to these data, the attacker need only obtain access to the key generated by the application layer protocol L2CAP. Through this study, the researcher attempted to fully analyze this problem and develop a solution in the form of a trust protocol to plug this SDP vulnerability.

1.2.1 Research Questions

RQ1: What are the vulnerabilities of the Bluetooth SDP as specified by Bluetooth SIG?

RQ2: How can a better trust protocol be developed to alleviate the vulnerabilities of the Bluetooth SDP as specified by Bluetooth SIG?

1.2.2 Theoretical Framework

The NIST standards for Bluetooth technology, NIST Special Publication 800-121 (Padgette et al., 2012), represented the theoretical framework underlying the current study. In laying out these standards, Padgette et al. wrote on Bluetooth security standards from the

perspective of NIST. The National Institute for Science and Technology has the governmental responsibility to develop standards for good technology use. The standard of interest, therefore, represents the most recent NIST Bluetooth standards for security that are employed by the federal government of the United States, as well as governmental recommendations for Bluetooth security. The most recent version of the NIST guideline noted that Bluetooth 4 is currently the most widely used version of the technology. It is not, however, the most recent version, and the more recent iterations have added significant security features: Bluetooth versions 4.1 added "Basic Rate/Enhanced Data Rate (BR/EDR) technology cryptographic key, device authentication, and encryption by making use of Federal Information Processing Standard (FIPS)-approved algorithm" (p. 4), and Bluetooth 4.2 added "the low energy technology cryptographic key by making use of FIPS-approved algorithms, and provided means to convert BR/EDR technology keys to low energy technology keys and vice versa" (p. 4).

The standards overall recommended that the persons and organizations adopting Bluetooth technologies should use the highest security setting available, develop policies and change Bluetooth devices' default settings, and enhance users' awareness of those policies and their security responsibilities. These guidelines suggest an ideal situation that is significantly different from the reality depicted in the research. Many commercial applications of Bluetooth low energy, for example, utilize none of the technology's available security levels (Bello, 2017). Moreover, most mobile users show little awareness of or concern for device security (Imgraben et al., 2014). Therefore, to practically apply the standards suggested by NIST, a clear understanding of the known vulnerabilities in Bluetooth technologies and any known corresponding solutions is needed. The current study represented an attempt to characterize one such vulnerability and close it to the degree possible.

1.2.3 Significance of the Study

The current study is significant from both a practical standpoint and a theoretical one. Theoretically speaking, the researcher aimed to answer several calls made in the existing literature for further research into the security vulnerabilities of Bluetooth technology. These calls for research were as follows. Hassan et al. (2017) conducted a similar review of the literature, focusing on the existing vulnerabilities present in the technology. Although their review was relatively extensive, they acknowledged that overall, there is not enough research into these vulnerabilities. Therefore, they called for additional research to examine the potential vulnerabilities present in Bluetooth devices so as to help understand the risks involved and characterize the nature of what is known and how that knowledge can be employed to prevent attacks (Hassan et al., 2017). Another aspect of the existing research in need of further development is the consideration of how parameters such as security, reliability, and throughput may be jointly optimized (Zou et al., 2016). Because many existing Bluetooth solutions serve to optimize one parameter at the expense of others, such as affording privacy at the expense of security through the approach of random address assignment, any improvement to the overall security of Bluetooth systems that does not come at significant cost to other parameters would help answer this call to research. Finally, to truly set this review apart from similar literature reviews, the researcher addressed a third call to research from Tay et al. (2016), who recommended that scholars improve the security of emerging Bluetooth applications. The current researcher sought to facilitate a general improvement to Bluetooth security that should help boost all Bluetooth applications, including those that are still emerging. In addition, the nature of the SDP vulnerability, in terms of allowing attackers access to data about other devices on the

network, could he problematic in the large networks created by emerging applications such as iBeacons.

The practical importance of this study stemmed from the theoretical importance of addressing those calls for research, but also from calls for action. Specifically, the NIST has called for users to utilize the strongest security features possible on their Bluetooth-enabled devices (Padgette et al., 2012). In reality, however, most users remain disinterested in the security of their devices and the sensitive data contained therein. Therefore, from a practical standpoint, the researcher attempted to create another layer of Bluetooth security that can be enacted by manufacturers to increase security without needing retailer or customer involvement in so doing. This should serve to improve the overall state of security with respect to the use of Bluetooth technology by denying would-be attackers' important information that might make deeper and more harmful attacks significantly easier to execute.

1.3 Brief Literature Review

To inform this research paper and the study that it supports, a review of the current body of academic literature was carried out through Google Scholar and university libraries. Keywords included *Bluetooth, wireless, Wi-Fi, security, weakness, vulnerability, exploit, hack, hacking, attack, intrusion, data, breach, Internet of Things*, *SDP, SIG,* and appropriate combinations thereof. The results of the literature search were eight broad themes of Bluetooth devices and the Internet of Things, general Bluetooth vulnerability, Bluetooth and smartphones, medical applications and body networks, automotive applications., Bluetooth low energy, and emerging applications. Each of these themes is briefly summarized in this abridged review and will be fully developed in Chapter 2 of the dissertation proposal.

1.3.1 Bluetooth Devices and the Internet of Things

Bluetooth has become a central technology within the Internet of Things. The Internet of Things refers to an ever-growing list of devices from smartphones to appliances to automobiles (Noor et al., 2018) or even to locks (Jeong et al., 2015). Whereas the traditional internet only consisted of computers, the Internet of Things is a wide variety of wireless devices connected to one another. Bluetooth is not the only technology used to connect these wireless devices together, but it is one of the foremost.

1.3.2 Bluetooth Wireless Technology Feature Characteristics

One of the first uses of Bluetooth was to replace cables between devices such as mobile phones, laptops, headphones, printers, fax machines, keyboard, mouse, and a host of other devices. Besides providing data channels, Bluetooth also provides voice channels allowing wireless connections between mobile phones and headsets and car kits. Bluetooth supports ad hoc networks; this means that it does not rely on any preexisting infrastructure, such as routers in wired networks or access points in wireless networks. The devices can dynamically come close to each other, exchange data, and go out of range. Bluetooth supports a maximum distance of 100 meters, although it is typically used for much shorter distances. The specification provides support for different power levels for Bluetooth radios so that the appropriate combination of power consumption and distance can be selected based on the application for which the device is intended (Gupta, 2016).

In July 1999, Bluetooth released specification version 1.0 and 1.0a. These were the very first versions of the Bluetooth specification. The primary objective was to replace the serial cables with a wireless link. Specification version 1.0b was released in Dec 1999. This version added minor updates to fix some of the issues. Specification version 1.1 was released in February

2001, and Bluetooth was ratified as the IEEE 802.15.1-2002 standard. Specification version 1.2 was released in November 2003. This release of the Bluetooth standard added new facilities, including Adaptive Frequency Hopping (AFH), which was introduced to provide better resistance to interference in noisy environments, and Extended Synchronous Connection Oriented (eSCO) links, which were added to provide better voice quality. This was also ratified as IEEE 802.15.1-2005. This was the last version issued by the IEEE, after which Bluetooth technology evolved independently. Specification version 2.0 + EDR was released in November 2004. This release of the Bluetooth standard introduced enhancements to the throughput using Enhanced Data Rates (EDR). The previous versions of the standard supported a throughput up to 721 kbps. Specification version 2.0 + EDR increased the throughput to 2.1 Mbps. This made it more suitable for applications that required fast data transfers like file transfer, browsing, and printing. Specification version 2.1 + EDR was released in July 2007. This version brought in several enhancements and added Secure Simple Pairing (SSP) to both simplify the pairing mechanism and to improve security. Specification version 3.0 + HS was added in April 2009. This version provided a significant increase in throughput by introducing the support for multiple radios. This was referred to as Alternate MAC/PHY (AMP). The supported maximum throughput increased to 24 Mbps. A brief rationale was that several devices like laptops, mobile phones, and tablets have both Bluetooth and 802.11 chips on them. This version of the specification allowed connection using Bluetooth and then moving on to the 802.11 chip to achieve high-speed data transfers.

Specification version 4.0, which was released in June 2010, represented a completely different direction compared to the previous versions. While the main focus in the previous versions was to introduce new features and enhance the throughput, specification version 4

addressed the markets where the need was not of high throughput but of ultra-low power. This was referred to as Bluetooth low energy (LE). Specification version 4.1 was released in December 2013; it enhanced the Bluetooth low energy feature by allowing an LE device to act as both a hub and an end point. This was useful in Internet of Things, where devices could exchange data with each other. It also provided support for coexistence with LTE (4G) because LTE may occupy frequencies that are close to or have harmonics near those of Bluetooth. It also provided support for additional topologies to make the technology applicable for newer use case scenarios. The main notable changes done in this version were to put in the "Reliable BLE Packet Support by introducing the LE L2CAP Connection Oriented channels" to carry the short LE packets and add more reliability. Another notable feature is called Privacy 4.1, wherein the private addresses are scrambled during connection so that any eavesdropper has a lesser chance of capturing the information. Specification version 4.2 was released in December 2014; this version further enhanced the Bluetooth low energy feature by allowing sensors to access the Internet, thereby lowering energy requirements and boosting security and privacy. One of the shortcomings of the previous version was that the packet size was smaller; therefore, the maximum throughput was lower, which made it unsuitable for applications that required high throughput, even if for a short duration of time. This version increased the packet capacity by ten times leading to a data throughput increase of 2.5 times. Comparing the specifications of 4.2 to 4.1, there are also an increased security procedure and power preserving security procedure. This power-preserving security procedure offloads most of the key management to the controller. On 4.2 dual-mode devices, there is also a provision of pairing only once with the remote device, irrespective of the authentication mode used by the device (Gupta, 2016).

1.3.3 General Bluetooth Vulnerability

Bluetooth technology has a long history of security vulnerabilities. Most versions have security features available that can be effective if engaged properly, but which are not active by default and rarely activated by the average user (Padgette et al., 2012). Security features in the past were especially weak, allowing for a wide range of cyber-attacks to seize control of almost any Bluetooth device (Alfaiate & Fonseca, 2012). Recent advances in Bluetooth technology and protocols—such as Bluetooth 4.0, 4.1, and 4.2—have decreased the severity of these vulnerabilities (Cope et al., 2017). Many aspects of the technology, however, such as the nature of the device pairing and random address assignment represent a continuing source of security vulnerability in Bluetooth-enabled devices (Cha et al., 2017). Ultimately, even devices running on the most up-to-date version of Bluetooth 4.2 remain vulnerable to malicious attacks under certain circumstances (Melamed, 2018).

1.3.4 Bluetooth Wireless Technology and Smartphones

Bluetooth's dominance is in part because of its use in smartphones. All modern smartphones are Bluetooth-enabled devices, and the presence of Bluetooth in phones increasingly makes them function as control devices through the Internet of Things (Jeong et al., 2015). Over 60% of the Bluetooth market consists of smartphones (Nair et al., 2015). Given the importance of the smartphone in day-to-day life in the modern world and the kind of data stored on these phones, they represent a prime target for attacks making use of Bluetooth security vulnerabilities (Nair et al., 2015). The nature of smartphone networks also offers a unique attack vector for hackers (Thompson et al., 2016).

1.3.5 Medical Applications and Body Networks

There are increasing applications for Bluetooth technology in medicine. These range from tracking the length of waits until emergency room patients see a doctor (Frisby et al., 2017) to providing real-time telemetric data for treatment (Zegeye, 2015). An important subfield of this is that of body area networks—that is, a network of devices monitoring the same person's body (Hasan et al., 2016). These have much in common with nonmedical devices like smart watches (Ching & Singh, 2016), both of which use Bluetooth and represent a short-range wireless device worn on the body. Medical applications of Bluetooth create danger not only because of sensitive patient data, but the possibility of patient harm from malicious attacks.

1.3.5 Automotive Applications

Cars are another application of Bluetooth technology. Modern automobiles rely on an increasingly complex and interconnected set of technological innovations to offer increased quality-of-life (Noor et al., 2018). These same features, however, represent security vulnerabilities, as a potential attacker no longer needs to physically infiltrate a car to manipulate its systems. Aftermarket accessories are a common source of increased vulnerability (Cheah et al., 2017). The risk to cars is significant due to the potential for an attacker to provoke traffic accidents.

1.3.6 Emerging Applications

Some Bluetooth applications are still emerging, or have not yet become important enough to be targeted by attackers—but are poised to become so (Tay et al., 2016). A key example of such technology is the Bluetooth beacon. This technology has traditionally been used for advertising purposes, for which attackers could make at most minimal gains. These beacons are beginning to find other uses, however, such as forming the basis of indoor navigation systems in

large spaces (Faragher & Harle, 2015) or providing the basis of new payment processing approaches (Han & Ding, 2017). The growth of such additional applications considerably increases the risk that the technology, not yet hardened against attackers, will become the target of malicious attacks. Therefore, such emerging applications must be identified and protected.

1.4 Dissertation Roadmap

This research paper is structured as follows. In Chapter 2, the researcher discusses the literature review and thematic analysis of Bluetooth wireless technology, its key components, the current security architecture and vulnerabilities, and mitigation techniques. In Chapter 3, the researcher outlines the methodology and design that guided this study, including the data collection procedures, data analysis technique, and ethical considerations. Chapter 4 includes a presentation of the initial codes, themes, current security architecture and protocols, popular Bluetooth attacks, solutions to Bluetooth vulnerabilities, and an analysis of these solutions. In Chapter 5, the researcher summarizes the major contributions of this research and provides recommendations for future studies.

Chapter 2

Literature Review

In this chapter, the researcher presents a systematic literature review and thematic analysis of Bluetooth's vulnerability from scholarly sources. Afterward, the researcher employs thematic analysis to decipher the relationships in the collected literature. To decrypt the concept of Bluetooth wireless technology fully, it is prudent to understand how it works. As such, the researcher provides a brief description of Bluetooth's functionality in this chapter. Next, the researcher outlines the plethora of potential Bluetooth attacks. The researcher delves deeper into explaining these security vulnerabilities to develop a better trust protocol as a solution.

2.1 Bluetooth Wireless Technology Basics

To understand the concept of Bluetooth, it is pertinent to learn its basic functionality features. Bluetooth allows electronic devices to send and receive data wirelessly through a 2.4GH link (Feng et al., 2002). Most of the time, it works over a short radius and uses negligible power and costs. Its application has been utilized in a wide variety of consumer products such as livestock trackers, game controllers, and headsets. Owing to its short-range capability over a secure protocol, it is not vulnerable to attacks (Hassan et al., 2018). With the increasing sensitization of web security, however, most of its security breaches have been exposed. These attacks are discussed in the subsequent sections.

2.1.1 How Bluetooth wireless Technology Works

The Bluetooth wireless technology radio layer defines the technical characteristics of the Bluetooth radios. The radio operates in the license-free 2.4 GHz ISM band, and it is compliant with the FCC part 15 regulations for international radiators in this band. It employs a fast (1,600

hops/sec), frequency hopping spread spectrum (FHSS) technique. The radio hops in a pseudo random fashion on 79 one-MHZ channels. The frequencies are located at (2,402 +k) MHz, where k = 0, 1, 2, … The modulation technique is a binary Gaussian frequency shift-keying, and the baud rate is 1 MBS. The Bluetooth wireless technology radio comes in three power classes, depending on their transmit power. Class 1 radios have transmitted power of 20 dBm (100 mW); Class 2 radios have transmitted power of 4 dBm (2.5mW); and Class 3 radios have transmit power of only 0 dBm (1mW). Due to the power and cost constraints of the various personal devices that uses Bluetooth radios, Class 3 and Class 2 radios are expected to be the ones mostly use in these devices (Bisdikian, 2001). The table below list the Bluetooth wireless technology power, distance, and signal strength ratings.

Class	Maximum Power Rated (mW)	Theoretical Radio Range (meters/feet)	Radio Signal Strength Gain (dB)
Class 1	100 mW	100 meters (300 feet)	20
Class 2	2.5 mW	10 meters (30 feet)	4
Class 3	1mW	1 meter (3 feet)	0

Figure 1 Bluetooth Wireless Technology RF Power Classes

The Bluetooth protocol works with 2.4GHz in a similar frequency band with Wi-Fi and ZigBee (Feng et al., 2002). Bluetooth uses synchronous connection oriented (SCO) and Asynchronous connection (AL) links to establish a connection among devices. SCO provides a circuit switched connection between the master and the slave by establishing a point to point and symmetric dedicated link between two services thereby providing guaranteed delay and bandwidth to transmit average quality voice and music through the use of a link management protocol (LMP). On the other hand, ACL provides a packet switched connection between the

master and slave and establishes a point-to-multipoint and asynchronous link between two devices, which is suitable for non-real time data transmission (Gupta, 2016). Despite sharing the property with other radio frequency protocols, it has a set of rules that differentiate it from the group. The features are as follows.

2.1.2 Bluetooth Wireless Technology Masters, Slaves, and Piconets

Bluetooth uses the slave/master model to regulate when and where an electronic device can send data. As such, one master connects with seven different devices, which are the 'slaves,' whereas a slave connects to one master in the piconet- a network of Bluetooth electronic devices where each one can be the former or latter. The master oversees communication around the piconet (Dahiya, 2017). A piconet is a collection of Bluetooth devices that can communicate with each other and is formed in an ad hoc manner without any infrastructure assistance; it last as long as the creator of it needs and is available to communicate with other devices. A piconet contains at least one device identified as the master of the piconet and at most seven other devices identified as slaves with which the master is actively involved in communications (Bisdikian, 2001).

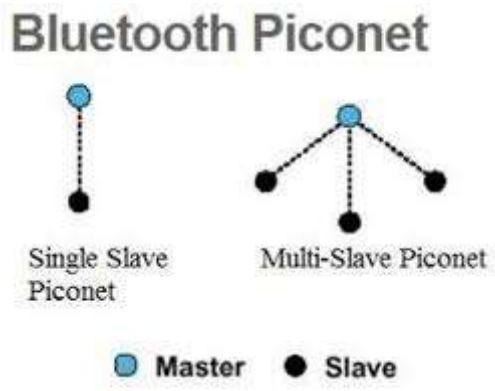


Figure 2 Bluetooth Wireless Technology Piconets

A master can request as well as send data to any of its slaves. These slaves cannot communicate with each other, as they are only allowed to intercommunicate with their masters. Besides, they can be either active or passive (Dahiya, 2017). An active slave is in data transmission mode, while passive slaves enable their RF intermittently to check whether there is an inquiry request by the master.

2.1.3 Bluetooth Wireless Technology Addresses, Names & connection Process

Every electronic device with Bluetooth capability has a distinct 48-bit address. This code is usually given as an abbreviation of BD_ADDR. Each BR/EDR controller has a globally unique 48-bit Bluetooth device address, also referred to as BD_ADDR. This address is used to identify the device. It is similar to an Ethernet MAC address, and is in fact, administered by the same organization, IEEE. BD_ADDR consists of two fields. The first is one 24-bit company ID assigned by IEEE Registration authority, which is called Organizationally Unique Identifier (OUI, with 24 most significant bits). The second is two 24-bit unique number assigned by the company to each controller, with 24 least significant bits. Unlike the BD_ADDR, this can be changed by the user or application and provides an easy mechanism to identify and remember a device. It is possible—though not desirable—for several devices to have the same name. This device name is generally fetched from the remote device to identify it (Gupta, 2016).

2.1.4 Connection Process

The connection procedure for Bluetooth requires three stages. First, it has to make an inquiry request, and if the other device is on, it will determine the address and start to page. The inquiry process is a device discovery process during which the master of a future piconet discovers other devices in its vicinity; the master makes its presence known by transmitting inquiry messages that, among other things, contain the BD_ADDR of the device (Bisdikian,

2001). After finishing the paging stage, it will enter the connection phase (Dahiya, 2017). Here, the devices can remain either in sniff mode, active mode, park model, and hold mode. When there is an established connection between two devices, they can bond with each other automatically if they are close to each other.

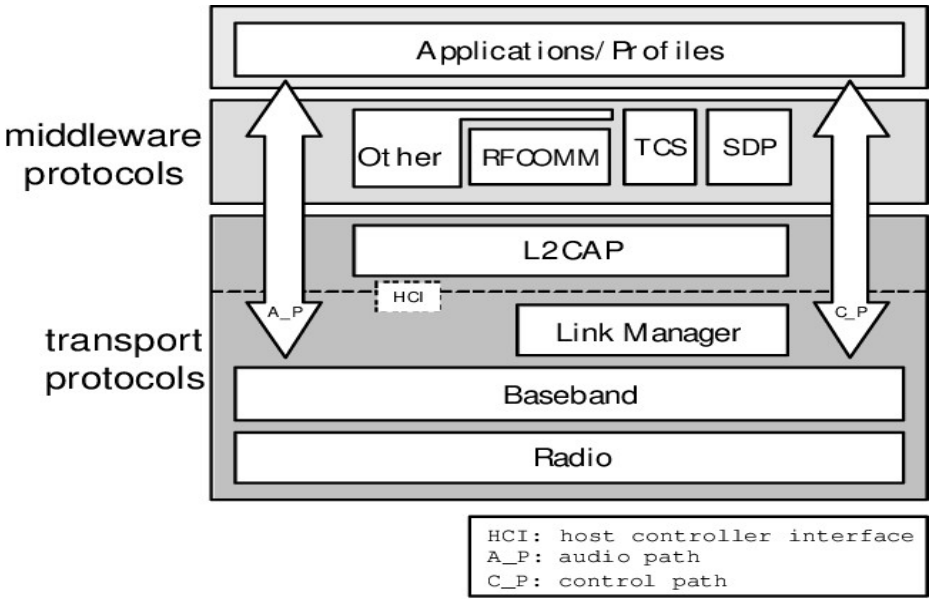


Figure 3 Bluetooth Wireless Technology Protocol Stack (Bluetooth 1, 2, & 3)

2.2 Bluetooth Wireless Technology Services

Typically, the Host software executes on an application processor or microcontroller. The Controller is a logical entity that executes the lower layers of the protocol stack. It includes all layers below the Host Controller Interface—Radio, Link Manager, and Baseband. The Controller functionality is embedded in a Bluetooth chip that is attached to the Host (Gupta, 2016).

The Host Controller Interface (HCI) provides a communication interface between the Host and the Controller. Physically, this may run on top of an interface like UART, RS-232, USB or SD. The set of packets that can be exchanged on this interface is defined by the Bluetooth specification. One of the strong points of the Bluetooth specification as compared to few other standards is a well-defined interface layer between the host and the wireless controller.

It allows independent and parallel development of the host and controller and ensures compatibility of a host from one vendor with a controller from a different vendor. The HCI interface is optional and may be omitted in implementations where the host and the controller are tightly coupled with each other and run on the same processor. If this interface is omitted, then the upper layers interact directly with the lower layers. These scenarios are shown in Figure 4 below (Gupta, 2016).

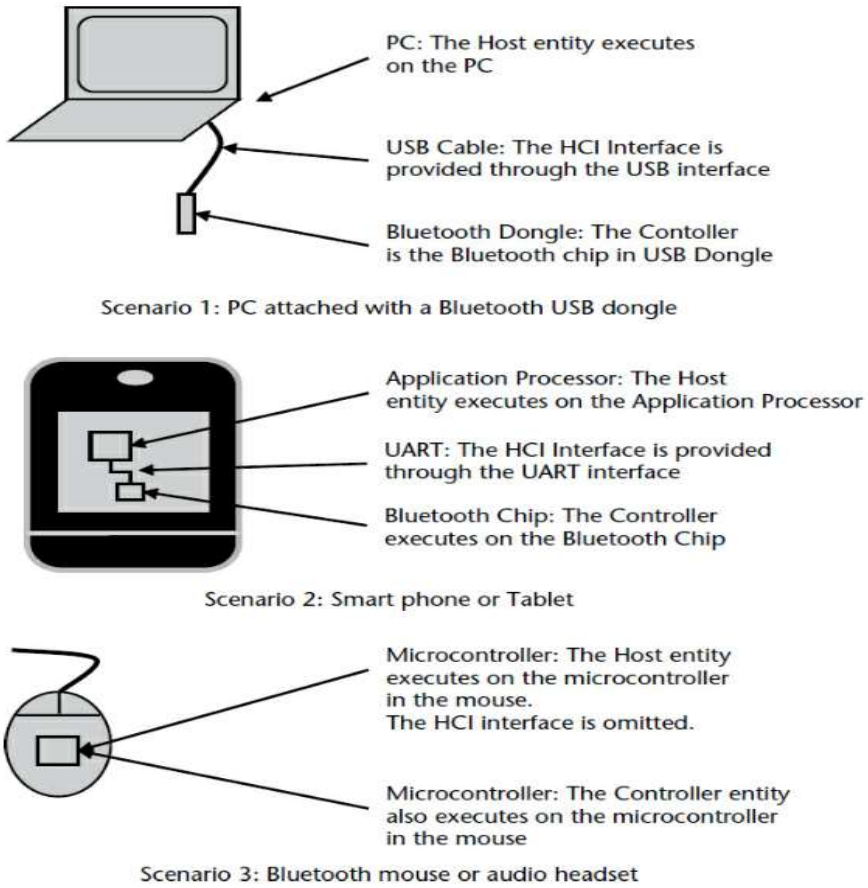


Figure 4 Bluetooth HCI interface Scenario

1. Scenario 1: PC Attached with a Bluetooth USB Dongle. In this scenario, the Host entity executes on the PC (i.e., the Bluetooth software running on the PC Operating System). The Controller entity executes on the Bluetooth chip that resides inside the Bluetooth USB Dongle. The Host Controller interface is provided through the USB interface.
2. Scenario 2: Smartphone or Tablet in this Scenario. The Host entity executes on the Phone's application processor, the Controller entity executes on the Bluetooth chip that is mounted on the Phone's PCB. The Host Controller interface is provided through the UART (or some other) connection on the PCB between the application processor and Bluetooth chip.
3. Scenario 3: Bluetooth Mouse or Audio Headset. In this scenario, both the Host and the Controller entities run on a single microcontroller. The Host Controller interface is omitted, and the upper layers of the stack interact directly with lower layers of the stack. Prior to the Bluetooth 3.0 + HS specification, a Bluetooth system could have only one Host and one Controller. From the Bluetooth 3.0 + HS specification onwards, a system can have one host and multiple controllers. Two types of controllers are defined by Bluetooth 3.0 + HS specification: the primary controller and secondary controller. A system can have only one primary controller, and may have zero or more secondary controllers. The primary controller may support BR/EDR only, LE only or a combination of BR/EDR + LE functionality. The secondary controllers support one or more Alternate MAC/PHY (AMP) controllers. These AMP controllers help in increasing the throughput up to 24 Mbps by using the 802.11 transport layer instead of the classic Bluetooth transport layer for high-speed data transfers (Gupta, 2016).

2.2.1 Service Discovery Protocol (SDP)

In Bluetooth environments, before a connection can be established, a procedure involving procedures of device discovery must be performed before packets start flowing on the wireless links between the master and slave devices and vice-versa. The device discovery includes inquiry and paging procedures (Shorney & Miller, 2000). Bluetooth has a mechanism to detect services provides by other devices that are within the supported range (Becker & Paar, 2007). Through this protocol, Bluetooth understands whether a device is active or switched off. To support the rich application space environment for Bluetooth wireless technology devices, a service discovery protocol was added to the Bluetooth protocols.

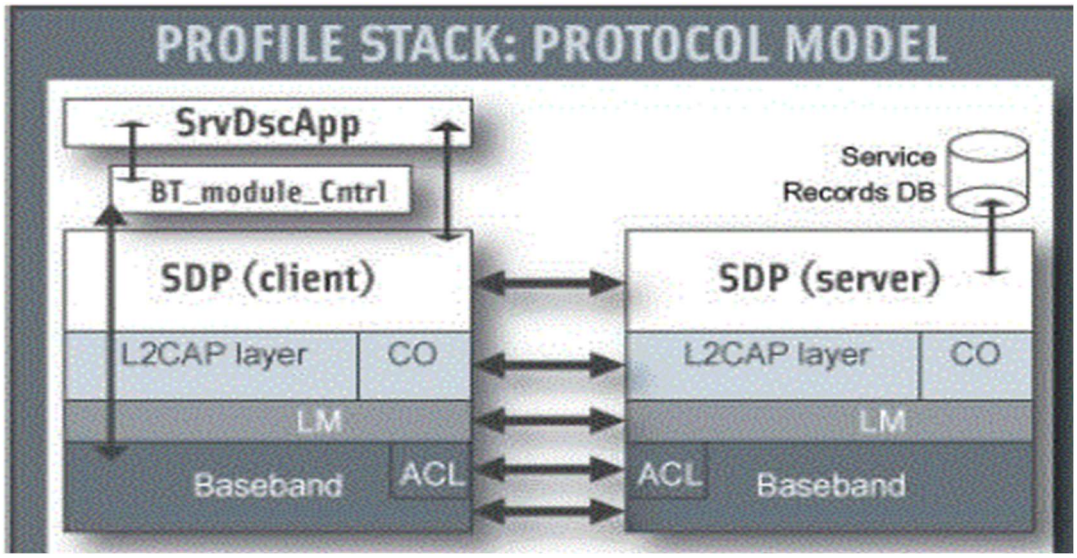


Figure 5 Bluetooth Wireless Technology SDP Protocol Stack

Using the SDP protocol, a Bluetooth wireless technology device can inquire about the services that another device across a Bluetooth link may have, as well as how to have access to it. The SDP only provide information about services; SDP does not provide access to them. A Bluetooth device may access the service via different means using the information learned through service discovery. SDP is optimized for usage by devices of possible limited capabilities

over wireless links; bandwidth is preserved by utilizing binary encoding of information over the air. Universally unique identifiers (UUIDs) are used to described services and attributes of these services in a manner that may not require a central registration authority for registering services. Typically, the UUIDs are 128 bits long; however, for known services, 16-bit and 32-bit UUIDs may also be used (Bisdikian, 2001).

2.2.2 Link Managing Protocol (LMP)

In this protocol, there is the implementation of one security mode. It also has a Link Manager Unit that shows a record of connected devices (Das, 2015). These link managers exchange information through protocol data units (PDU). At the Baseband level, commands are translated into operations by the Link Manager (LM), attaching slaves to Piconets, and allocating their active member addresses; establishing ACL and SCO links; putting connections into Low Power modes: Hold, Sniff and Park. Bluetooth Link Manager communicates with Link Managers on other Bluetooth devices using the Link Management protocol (Kumar et al., 2017). By using the inquiry routine, the devices can detect their addresses and then page afterward.

The link manager protocol is a transactional protocol between two link management entities in communicating Bluetooth devices whose responsibilities is to set up the properties of the Bluetooth link. Through LMP transactions, one device may authenticate another device through a challenge response mechanism. For authenticated devices, the link may be further encrypted. The two link managers may learn each other's features—for example, whether the devices support SCO links, what size of packet transmissions do they support, or whether they support any of the low power consumption modes. SCO connections are established using LMP transactions, polling intervals and agreed upon packet sizes are also set up through LMP

transactions (Bisdikian, 2001). Overall, the LMP is responsible for establishing and maintaining the link between Bluetooth devices .

2.2.3 Logical Link Control and Adaption Protocol (L2CAP)

This protocol assists its users by providing connection-oriented service in the upper layers (Becker & Paar, 2007). It uses asynchronous connectionless (ACL) in the Baseband as packets of communication. The L2CAP layer shields the specifics of the Bluetooth lower layers and provides a packet interface to higher layers. At the L2CAP layer, the concept of master and slave devices do not exist anymore. The L2CAP support the multiplexing of several logical channels over the device's ACL links. Note that a slave only has one ACL link, while a master has one for each slave with which it actively communicates (Bisdikian, 2001).

2.2.4 Radio Frequency Communication (RFCOMM)

The RFCOMM Protocol is an important layer that is used to expose a serial interface to the packet-based Bluetooth transport layers. In particular, the RFCOMM layer emulates the signals on the nine wires of an RS32 interconnected cable. The RFCOMM is based on the ETSI 07.10 standard, which permits the emulation and multiplexing of several ports over a single transport. RFCOMM enables legacy applications that have been written to operate over serial cables to run on top of a Bluetooth link without modification. Several of the applications developed for Bluetooth use the RFCOMM of part of their implementation stack (Bisdikian, 2001). It uses the L2CAP protocol to provide serial ports (Becker & Paar, 2007). With this channel, 60 connections to other Bluetooth devices are possible.

2.2.5 Telephony Control Protocol (TCS)

This protocol delivers its functions to telephony programs. Telephony control can be performed using the AT command set. Since the AT command set have been designed to passed

over serial lines, Bluetooth device use the RFCOMM to send and receive control signal based on the AT command set. For example, using these commands a dialer application in a notebook computer may instruct a cellular phone to dial up an ISP location. The AT command set is well established and can be used for supporting legacy applications such as the dialer application. In addition to this control protocol, referred to as TCS-AT, the Bluetooth technical group developed an additional package-based telephony control signaling protocol called TCS-BIN that supports point-to-multipoint communications as well, allowing, for example, a cordless base station to pass the ringing signal of an incoming call to several cordless headsets associated with the base station (Bisdikian, 2001).

2.2.6 Object Exchange Protocol (OBEX)

OBEX is a compact, efficient, binary session layer protocol that enables a wide range of devices to exchange data in a simple and spontaneous manner. OBEX is defined by members of IrDA for the purpose of object exchange between wide ranges of devices that support IrDA protocols. The protocol has also been adopted by other wireless technology transports, including Bluetooth, as the framework for wireless object exchange (Boucouvalas & Huang, 2009). Through this protocol, the exchange of binary data is possible. It facilitates security through OBEX authentication (Becker & Paar, 2007). OBEX is developed for ad hoc wireless links, and can be used to exchange all kind of objects like files, pictures, calendar entries (vCal) and business cards (vCard). It is designed especially for the resource limited wireless devices with different Web usage models. The Push and Pull applications are the two major uses of OBEX to allow the rapid and ubiquitous communications among portable devices in the ad hoc environments. Here are a few typical examples: a laptop “pushes” a file to another laptop, a PDA “pushes” the authenticated credit card information to toll booth to pay the toll, and a mobile

“pulls” the business cards from a laptop. Besides the simple connect-transfer-disconnect scenarios, in order to allow devices to exchange large objects (MP3, movie clips), an OBEX session can maintain the connection even the session is idle over a period of time. After assigning the roles of the client and server, OBEX uses the request and response (i.e., stop and wait) conversation format for the object exchange. The OBEX client/server denotes the originator/receiver of the OBEX connection but not necessary the one who originates the IrLAP connection. Being the one initiating the OBEX connection, the client sends the request packet to the server and waits for the response packet from the server before sending another request. An OBEX operation is carried out in a request/response pair. There are two types of OBEX operations: a PUT and a GET. The PUT operation is to send an object from the client to the server and the GET operation is to return an object from the server to the client. As defined in the standard, the maximum and minimum length for both request and response packets are 512K bits and 2048 bits, respectively. Here, the commands available are GET, ABORT, and PUT. It used within OBEX Object Push Profile (OPP) and Synchronization Profile (SYNCH; Boucouvalas & Huang, 2009).

2.2.7 OBEX Object Push Profile (OPP)

This profile uses vCards in Bluetooth to exchange binary entities. A vCard is a type of file used as an electronic business card. There is no protection against such files, hence the absence of authorization or authentication process (Becker & Paar, 2007). Commands in this profile include 'abort, connect, disconnect, get, and put.'

2.2.8 Synchronization Profile (SYNCH)

It presents the exchange functions of PIM (Personal Information Manager). Private data such as calendar and address book use this profile (Becker & Paar, 2007). Owing to the reason mentioned above, it utilizes authentication processes as a means of protection.

2.2.8 Other Protocols

To support various applications, several industry standards have been adopted. Such protocols include the point-to-point protocol (PPP), which is an IEFT standard for enabling communications, including IP communications, over serial lines, the Object Exchange (OBEX) Protocol, and IrDA standard for transporting objects between devices, and the Infrared Mobile Communications (IrDA) standard for describing and encoding information in business cards, calendar entries, and messages. All these protocols run on top of RFCOMM (Bisdikian, 2001).

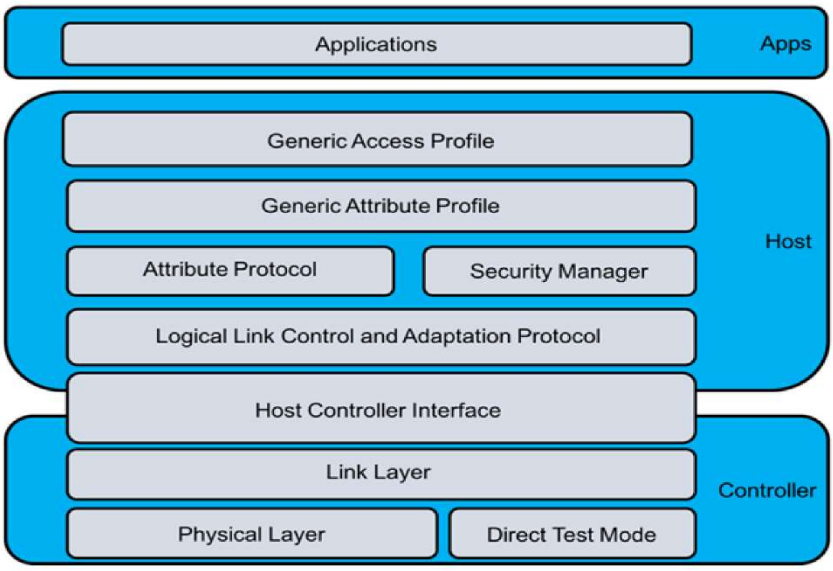


Figure 6 Bluetooth Protocol Stack (Bluetooth 4)

The figure above illustrates the protocol stack for Bluetooth 4. The stack consists of three layers: the Control Layer, the host layer, and the app layer. Each of these layers incorporate different protocols. The control layer incorporates the physical layer, Direct test mode, Link

Layer, and Host Controller Interface. The host layer incorporates the Logical Link Control and Adaptation Protocol, Attribute Protocol, Security Manager, Generic Attribute Profile, and Generic Access Profile. The App layer incorporates Applications.

2.3 Bluetooth Wireless Technology Profiles

The Bluetooth wireless technology specification comprises not only communications protocols but applications as well. This distinguishes Bluetooth wireless technology from many other communications technologies that focus primarily on the physical, data link, and possible networking aspects of communications. Because Bluetooth wireless technology is used primarily by consumers, the technology must require minimal technical expertise from its users. For this to be possible, a set of simple but useful applications had to be developed to allow Bluetooth devices to perform useful tasks with other Bluetooth devices right out of the box. This would provide added value to the users of the technology and aid in establishing this technology as the *de facto* means for short-range communications of personal devices. The specification for building interoperable applications is called profiles (Bisdikian, 2001).

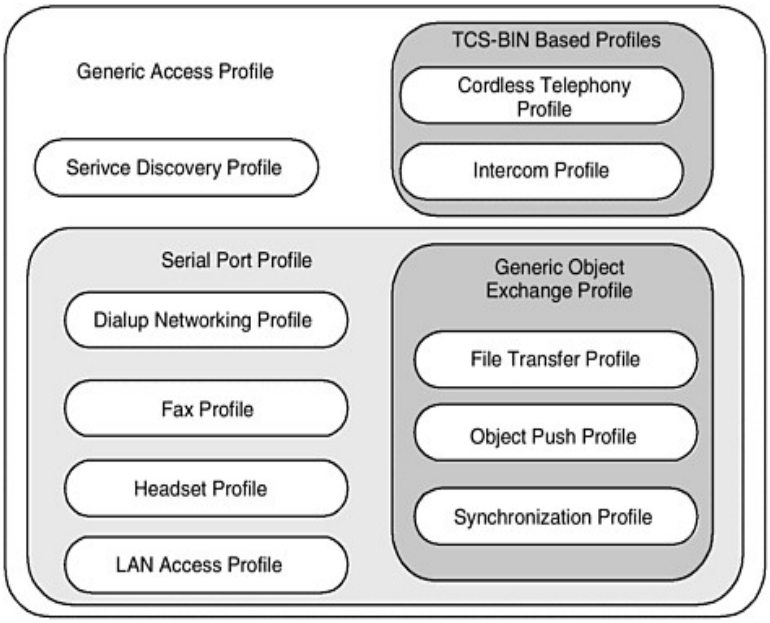


Figure 7 Bluetooth Profiles

All profiles depend on the Generic Access Profile (GAP), which defines the basic rules and conditions for connecting devices with each other and establishing Bluetooth links and L2CAP channels. It also defines security levels according to which devices may allow themselves to be discovered or allow to be connected, be authenticated, or authenticate other devices. It also defines the conditions necessary to establish trust relationships between devices (Bisdikian, 2001).

There are two protocol profiles that depend on each other. The serial port profile defines how RFCOMM runs on top of the Bluetooth transport protocols, while the generic object exchange profile defines how objects can be exchanged using the OBEX protocol running on top of RFCOMM, as defined in the serial port profile *(*Bisdikian, 2001). A Bluetooth profile presents a set of its services depending on the task. For instance, a Bluetooth headset requires a Headset Profile (HSP; Becker & Paar, 2007). Thus, it is pertinent to have prior knowledge of its common profiles while enabling the researcher to understand how attacks such as Bluebugging and Bluesnagging work.

2.4 Bluetooth Wireless Technology Security

Previous researchers have indicated that Bluetooth's security needs some improvements. The current researcher aimed to add to the existing literature and seal the loopholes. Thus, it is critical to evaluate its background before drawing strong thematic relationships.

As with any other wireless network in the world today, accessibility for Bluetooth is open to both intruders and legitimate users. This aspect makes it critical to analyze its security features. Its coverage of up to 10 meters for communication purposes exposes the users to vulnerabilities (Albahar, 2017). These can result in loss of files and other confidential information. As such, there is a need for security measures to be set in the Bluetooth architecture.

Before diving deeper into its vulnerabilities, it is vital to look at its modes and layers of security. The first layer comprises Bluetooth technology users. Here, the user can fall under four modes: silent, public, low energy (LE), and private. In silent mode, the Bluetooth evaluates its traffic but does not accept any requests. A public mode is what makes the Bluetooth "discoverable," and any master can find as well as connect with it (Albahar, 2017). Regarding LE or privacy mode, the electronic device can send data to other devices in wireless mode. Last is the private mode, which is not discoverable unless the address is familiar to their master. The extent to which the device is secure in the modes mentioned above depends on the type of pairing operation (Albahar, 2017). When two electronic devices share a Bluetooth connection, they generate a code which is secured in a range of protocols.

The "secret key" method was the only known technique to secure the connected devices until the introduction of Bluetooth 2.0 Enhanced Data Rate (EDR). One of the primary weaknesses of the secret key is that individuals could crack it using typical computational procedures. Active eavesdropping attacks could easily bypass the security mechanism. Nevertheless, Bluetooth 2.1 +EDR introduced the Secure Simple Pairing (SSP), which revolutionized the safety protocol of the network (Mutchukota et al., 2011). Subsequently, there was a conception of LE Privacy in Bluetooth 4.0 (Jakobsson & Wetzel, 2001). This version was easier and faster to pair, and above all, more secure. It utilizes advertisement as a technique for delivering data between Bluetooth-enabled devices in a wireless mode, and it is still one of the commonly used methods today. In all the distinct Bluetooth versions, four unique security modes can be used in one or more versions. A device operates only one mode at any given time. The list below shows the four-security modes:

2.4.1 Security Mode 1 (Nonsecure)

In this state, the device pairs with any discoverable device that inquires on establishing a connection (Albahar, 2017). A device will not initiate any security procedures, and the link level security features will not be implemented. The device will operate faster and use less power. As such, it has no security measures at all as it does not require any authentication or encryption. This mode is used in applications where security is not necessary such as the exchange of business cards. All Bluetooth wireless technology versions up to Bluetooth 2.0+ EDR supported this mode.

2.4.2 Security Mode 2 (Service-Level Enforced Security)

This mode allows for encryption and authentication only after the devices have paired. This security mode introduced authentication and authorization. A device does not initiate security procedures before channel establishment at the L2CAP level but the device initiates security procedures only after a channel establishment on the L2CAP layer. Most Bluetooth devices support this security function, but version 2.1+EDR only utilizes it for compatibility purposes in a backward process (Albahar, 2017). Verifying the identity of communicating devices based on their Bluetooth device address. Native user authentications are provided by Bluetooth (Kumar et al., 2017). This mode allows different and flexible access policies for applications, especially running applications with different security requirements in parallel (Kui & Xiuying, 2003). This is a service-level enforced level security, where Bluetooth service security can be configured to use authentication and authorization, authentication only, or open to all devices (Alfaiate & Fonseca, 2012). In this mode, applications with different security requirements can run simultaneously.

2.4.3 Security Mode 3 (Link Level Enforced Security)

This security feature has similarities with the above mode. The only difference is that it protects the Link Management Protocol layer. This link employs link level enforced security mechanisms. As such, before connecting any devices, there is security. The versions supported are up to 2.0+EDR (Albahar, 2017). It protects information from intruders by ensuring that the transmitted data can only be accessed by authorized devices (Kumar et al., 2017). A device initiates security procedure before the link set-up at the LMP level is completed (Kui & Xiuying, 2003). A secure physical link between the devices is created, while the channel is established. This mode initiates link-level security before the physical link is fully established (Alfaiate & Fonseca, 2012). This mode is also used in critical applications where security is mandatory.

2.4.4 Security Mode 4 (Simple Secure Pairing)

Bluetooth security at this level has the same properties as in Security Mode 2. It provides SSP, which prevents MITM attacks through encryption. It encrypts the secret authentication keys using the Elliptic Curve Diffie-Hellman (ECDH) method (Albahar, 2017). This mode uses SSP to create service-level security. The mode does not work in versions 2.1 +EDR and below. Table 2 below highlights the Bluetooth wireless technology security modes features and descriptions.

Table 2 Bluetooth Wireless Technology Security Modes

Security Mode	Feature Characteristics	Enforcement Description
1	Non-Secure	No Security feature is implemented; device pair with any discovered device
2	Service Level Security	Security feature is granted to individual services. Security features initiated AFTER the channel is established. Supports authentication, encryption, and authorization
3	Link Level Security	Security features are initiated BEFORE the channel is established; Protects the Link Management Protocol layer; used in critical applications where security is mandatory

4	Simple Secure Pairing	Enforcement description same as mode 2; encrypts secret authentication keys; Implement ECDH which helps protect against MITM

All services that are provided by Bluetooth wireless technology use the default level of security. Some services require authentication, some require authorization, and some require both. Therefore, it depends on the Bluetooth service which security mode to be used (Kumar & Gupta, 2015). Although the Bluetooth protocol by design defines security measures, these measures are typically not followed during the deployment (Satam et al., 2018).

2.4.5 Bluetooth Wireless Technology Trust Modes

The Bluetooth wireless technology security configuration is done with the help of discoverability and connection ability available in the Bluetooth enable devices. For secure communications, the authentication of Bluetooth enable devices is necessary. The basis of authentication security level for the Bluetooth enable devices is divided into trust level and service level (Kumar & Gupta, 2015). There are two types of trust for Bluetooth-enabled devices.

1. Trusted: This level of trust is after the two devices have established a fixed relationship, which allows the other device to have unbarred access to all its services (Becker & Paar, 2007). The device is marked “TRUSTED” in the device database and is authenticated previously, and a link key is also stored in the device database (Kumar & Gupta, 2015).
2. Untrusted: These devices have limited access to a set of services. Even though they have completed the authentication process successfully. These are devices in which a link is stored in their database but not marked as “TRUSTED” by the device (Kumar & Gupta, 2015).

Table 3 Bluetooth Wireless Technology Characteristics

Device Trust Level	Service Level	Characteristics Description
Trusted	Authenticated	Link key stored in device database; Full access to data services; have a paired relationship with device pair
Untrusted	No authorization	Link key stored in device database; fully authenticated; not marked "trusted"; limited access to set of services

Service level includes several aspects. Authorization is the verification of users' identity in order to provide access to something. The protection of secret or private information is called confidentiality (Kumar & Gupta, 2015).

2.5 Secure Simple Pairing (SSP) and its Loopholes

Pairing is a pertinent process in the Bluetooth technology realm. Versions 2.1+EDR and above replaced the conventionally pairing process with SSP protocol. It uses the "public-key cryptography" technique. This procedure uses visual matching with an integer value between the communicating Bluetooth devices (Padgette et al., 2012). The reason why it surpasses the former PIN authentication is because of its visual aspect, which eliminates intrusion while exchanging data. SSP incorporates the use of ECDH protocol to develop its link keys, which allows the devices to involve their physical address and private-public key sets (Padgette et al., 2012). SSP allows the devices to establish a link key based on ECDH key agreement. and supports four methods of authenticating the key agreement.

These four methods target devices with different combinations of user interfaces such as key boards, displays, or special pairing buttons (Barnickel et al., 2012). The computational processes to generate such as key utilizes a lot of resources and time, hence preventing MITM

attacks. The SSP model uses four approaches depending on the Input and Output (I/O) rankings of the communicating devices:

2.6 The Passkey Entry Model

When all the devices have input or display capabilities, they can use this model. Input capabilities are aspects such as the keyboard. In this case, both devices enter a similar 6-digit password to establish a connection (Albahar, 2017).

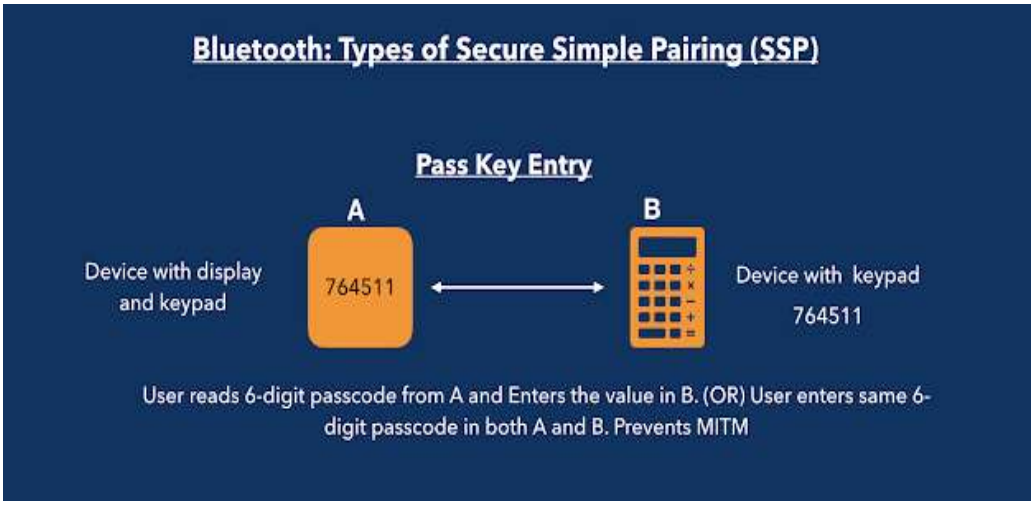


Figure 8 Bluetooth Wireless Technology Pass Key Entry Method

The passkey method also used a PIN (displayed on one and entered on the other device or entered on both devices) to authenticate the Defie-Hellman key agreement. The Passkey Entry method has been shown to be vulnerable against a man-in-the -middle attack. This attack allows an attacker that is able to record the legitimate pairing process and is able to prevent its successful completion (e.g., by jamming) to replace the link key established between the legitimate devices with link keys known to himself. Therefore, the attacker can impersonate one device to the other and eavesdrop on and manipulate the traffic exchanged between devices (Barnickel et al., 2012). The prerequisite to this success of this attack is that the user that pairs

the two legitimate devices reuses the sane PIN on the second try when the first try to pair the two devices has failed.

2.7 The Just Works Model

In this type of connection, one of the communicating devices does not have input or display characteristics (Albahar, 2017). As such, the connection is an automatic procedure and does not provide any means to authenticate the initial ECDH key exchange (Barnickel et al., 2012). Here, there is no security from MITM attacks.

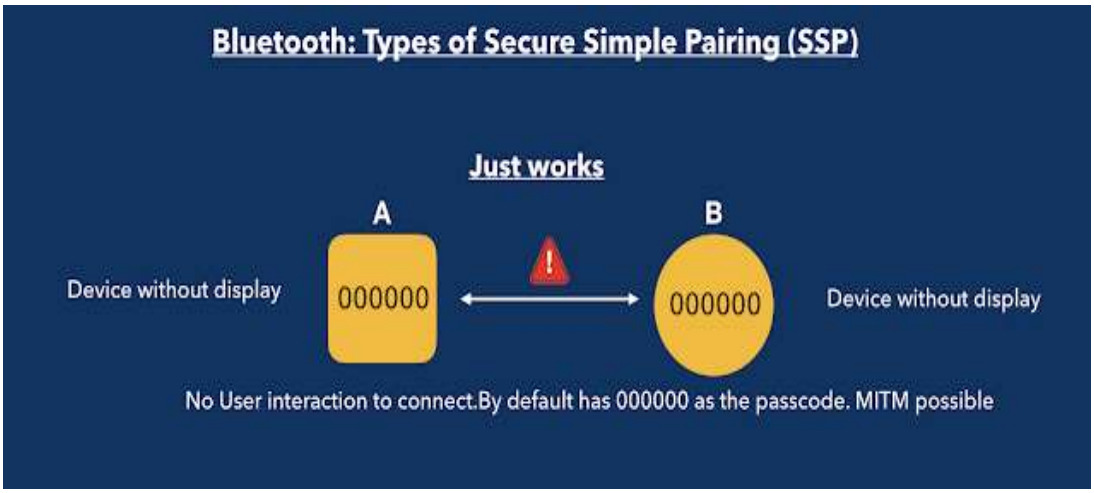


Figure 9 Bluetooth Wireless Technology Just Works Model

The Just Works model does not require a display or keyboard, and it is most common on headsets today. This is a pairing mechanism in which the devices do not ask for anything to authenticate to other devices; as a result, anyone can easily connect to the device. The device temporary key (TK) is 0. Hence, it is the weakest pairing method with no security against the MITM attacks. The devices that do not have display or keypad mechanisms will use this “Just Works” as pairing model (Pallavi & Narayanan, 2019).

2.8 The Out-of-Band Model

This connection model enables devices that have varied wireless technologies such as Near Field Communication (NFC; Albahar, 2017). It identifies Bluetooth appliances and establishes a connection through swapping cryptographic keys. Out of Band (OOB) refers to communications which occur outside of a previously established communication methods or channel.

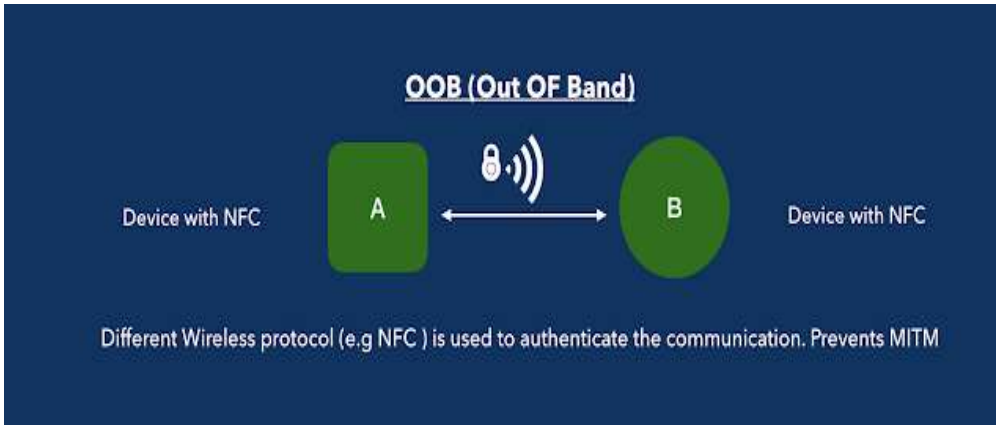


Figure 10 Bluetooth Wireless Technology OOB Model

The cryptographic systems that are secure against MITM attacks require an additional exchange or transmission of information over a secure channel (Kiruba et al., 2009). This is a pairing mechanism in which the temporary key (TK) is shared between the devices by other wireless devices, such as in NFC. The length of the TK can be less than or equal to 128 digits. Hence, the TK provides strong security if the OOB channel is secure by preventing attackers from eavesdropping (Pallavi & Narayanan, 2019).

2.9 The Numeric Comparison Model

This has similarities to the above-mentioned models, but it applies to devices that have both the input and display capabilities (Padgette et al., 2012). Both screens will show a 6-key value, where the users will confirm and establish a connection. This model has an additional step

to the Just Works method. If both the devices have a display, a digit numeric key is shown on both the devices, which the user must verify. This model provides protection against MITM attacks.

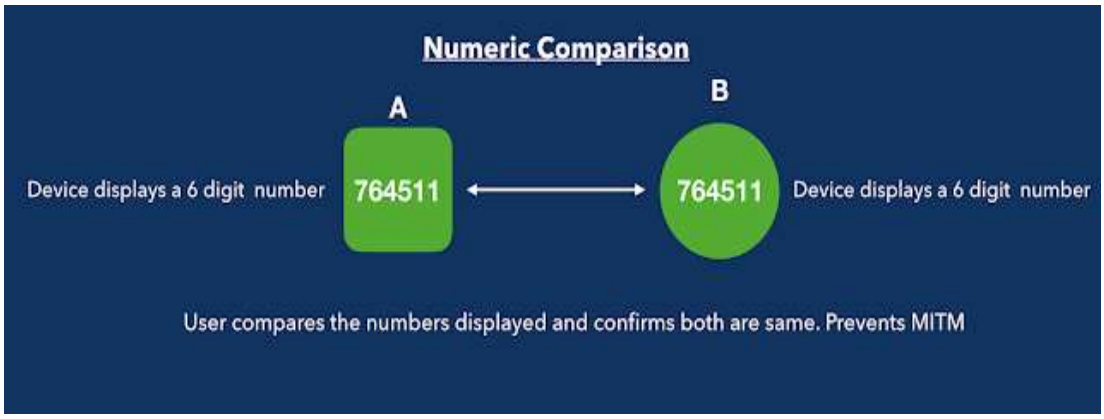


Figure 11 Bluetooth Wireless Technology Numeric Comparison

Secure Simple Pairing (SSP) uses six phases in its operations:

1. Capabilities Exchange: Communicating devices which have never paired hitherto send information to each other regarding their I/O capability. The outcome of the process determines the association model for pairing (Padgette et al., 2012).
2. Public Key Exchange: Bluetooth devices create public/private key sets. Afterward, they bring forth the public keys and generate the Diffie-Hellman key.
3. Authentication Phase 1: This phase relies on the connection models. It eliminates MITM attacks through scouring integrity checksums.
4. Authentication Phase 2: At this stage, the communicating Bluetooth devices share and verify the public key.
5. Calculation of the Link Key: The devices compute a link key from the shared public key, Diffie-Hellman key, and the public key.

6. Link Manager Protocol (LMP) Encryption and Authentication: Both devices generate an encryption security code (Padgette et al., 2012).

Mobile technology has significantly improved in recent years. Presently, many devices support the use of Bluetooth. Its short-range capabilities with no costs make sharing files to be convenient (Albahar, 2017). Despite its uses, it faces challenges regarding data security owing to malicious attacks such as MITM. For instance, during the MITM attack, the layer that entails the physical network faces intrusions into its piconet. As such, it corrupts the exchange of data.

2.9.1 A Systematic Review of Bluetooth Security

After looking at the basic functionality of Bluetooth and its security features, it is now appropriate to evaluate the existing literature regarding the same. Several types of research have been conducted on its pairing mechanism. The investigators of such studies have discovered that Bluetooth connectivity is vulnerable to intrusions. Scholars have proposed solutions, and these will be evaluated systematically in this chapter. The researcher then selected the most dominant ones in the quest to develop a strong recommendation in the current Bluetooth architecture. The following sections highlight relevant studies on this topic.

Theoretically, Hermelin and Nyberg (1999) confirmed that the Bluetooth stream cipher of a 128-bit could be segmented in O(264) steps. This separation utilizes the provided output keystream segment of length O(264). Jakobsson and Wetzel (2001) utilized this aspect to devise the first MITM security breach on Bluetooth. This attack worked on version 2.0+ EDR and below. To achieve this, two devices and the attacker are in a circle. In this case, the attacker knows the link key which the two connecting devices are using. After formulating this first attack protocol, the duo discovered other weaknesses. For instance, they depicted the procedure of getting a link key by utilizing an offline PIN crunching attack. This process uses passive

eavesdropping when the key is establishing its initialization protocol (Jakobsson & Wetzel, 2001). Other attacks focused on the cipher, while the rest centered on the device's location.

Owing to the identified vulnerabilities, Gehrmann and Nyberg (2001) introduced an anonymous mode that eliminated location tracing. These researchers added that extending the link key could assist in securing Bluetooth Baseband connection, as well as utilizing the private-public key combination for the same. Kügler (2003) modified the attack by depicting that the attacker can manipulate the connecting devices to use different clocks, but the same channel-hopping sequence. This action is through changing the clock setting. As such, the communicating devices can only see the data sent to them by the attacker. Additionally, Kügler also explained how a MITM attack is possible in the paging phase. During the stage, an intruder can provide feedback to the master's request faster than the slave and can reboot the paging process with the slave by utilizing a different clock (Singelée & Preneel, 2004). The researchers also hinted that using the unit keys is a vulnerability as the non-variable memory stores their data. This action implies that they are rarely changed. In the study, these mentioned inferences were due to the discovery that attackers can access the instantaneous number generated, which gives them access to the key and PINs during the initialization process.

After the attacks have been exposed by Jakobsson and Wetzel (2001) and Aissi et al. (2004) presented a proposal on using a bolstered Diffie-Hellman key exchange protocol. This suggestion could restrict intruders by introducing a one-way cryptographic function. These scholars proposed a more advanced but user-friendly PIN with a value between 5 and 12. Apart from the longer PIN, they introduced the Elliptic Curve Diffie-Hellman key in the subsequent versions. They intended to control offline attacks and wiretapping. On the same theme, Bluetooth

SIG realized that Secure Remote Control could be a dictionary attack in both the passive and active ways. Thus, they suggested the use of a longer PIN.

In the quest to minimize dictionary attacks, Sayegh and El-Hadidi (2005) also proposed the utilization of BT-EC-SRP protocol. This system develops a strong initialization code. Giousouf and Lemke (n.d.) also evaluated various Bluetooth vulnerabilities, particularly eavesdropping attacks and short PINs. Eavesdropping attack facilitated by unit key sharing. Another imminent weakness was that Bluetooth lacked a procedure for validating the connecting device addresses. This disadvantage made intruders interfere with addresses easily. Other vulnerabilities included lack of end-to-end encryption, absence of mutual authentication, a poor EO stream cipher protocol, a limited security service, and a poorly drafted encryption key length. Although Shaked and Wool (2005) observed that a short PIN is advantageous, they dismissed this notion by implementing an attack that decrypted easily the PIN used during the connection phase. Haataja (2005) presented possible solutions to the problem:

1. The technology should use 16-digit PINs.
2. Encryption should be a default feature from the manufacturer.
3. The BD_ADDR (Bluetooth device address) should be on every manual and the level of private security to be present.
4. The level of Bluetooth security should always be private, rather than public.

As more researchers became interested in the Bluetooth security dynamics, Kim et al. (2005) developed a bypassing security architecture that entailed link key creation, authentication, and negotiation on devices with limited power. This model proved to be useful in securing peer communication devices. The research asserted that their formula was cost-effective and faster

than the ECDH technique. Additionally, Lu et al. (2005) pointed out a flaw in the resynchronization of E0 through using a plaintext attack on the technology's encryption.

In a study conducted by Lindell (2008), a loophole appeared in Bluetooth 2.1+ EDR by utilizing the Passkey Entry Mode. Barnickel et al. (2012) proved the results of the research by implementing a similar attack. In this process, the intruders utilize the design weaknesses of the Passkey Entry, especially during the first stage of authentication. In order for this attack to be a success, it is prudent for the devices to use the Passkey twice for connection purposes. This type of attack depends on two stages. First, it needs the intruder to eavesdrop on two connecting devices during the Simple Securing Pairing process. Afterward, the attacker records the data exchanged at the initial authentication and DH exchange. With this information, the intruders can jam the SSP mechanism. In the second stage, attackers assume the identity of either of connecting devices by initializing a fresh pairing process and uses a similar passkey to link the two devices at the first step. This way, the intrusion assumes the role of a MITM and utilizes the Passkey to authenticate and negotiate the link keys. As such, the attacker can manipulate the data exchanged between the original connecting devices. In addition, with the reusability of the link key in the future, the intruders can impersonate either of the two connected in forthcoming authentication processes, even though one device is missing. This vulnerability gave rise to another form of attack on versions 2.1+EDR. Here, the attackers utilize the JW pairing model or fabricate the I/O information during the initial stage of SSP.

Haataja and Toivanen (2008) developed two different MITM attacks from their predecessors concerning the Bluetooth SSP. In the first attack, one can fabricate the I/O data at the initial phase. The second requires attackers to have a visualization of the victim device to misdirect the user in selecting a model with less security, such as the Just Works association

protocol, rather than the OOB (Out-Of-Band) model. These weaknesses in the OOB model proved that recent improvements in security were not adequate to seal all the loopholes in Bluetooth wireless technology. For instance, some new electronic devices can easily change their Bluetooth address, while others can point out devices in non-discoverable mode. As such, MITM attacks pose a threat to all the SSP connection models, and the danger continues to increase with advancements in modern technology.

According to a study conducted by Chang and Shmatikov (2007) to analyze the first instance of human authentication protocols through automation, if the same Bluetooth device is encompassed in two SSP sessions, authentication can fail. The researchers then modified the authentication architecture by involving SSP process identifiers and confirmed that their model bolsters authentication capabilities of the Simple Pairing operation.

Concerning the invention of Bluetooth low energy (BLE) devices, Das et al. (2016) discovered they were vulnerable to privacy leakage. An example of a BLE device is the fitness tracker used by health experts (Ching & Singh, 2016). The results reported by Ryan (2013) and Zegeye (2015) proved the danger of these attacks in medical telemetry applications. Shaked and Wool (2005) suggested that the loopholes in the cryptography process used in passkey connection allow the intrudes to initiate an active attack on the BLE equipment. Nevertheless, as the intrusions to BLE use passive sniffing of packets when connecting, the researchers needed to exploit the weaknesses of BLE pairing. Afterward, they linked the pairing process to another technology, the Fitbit Flex, which utilizes a distinct exchange protocol coined as ANT for additional security. Besides, the studies depicted how simple it was to crack BTE pairing using tools from the open-source pool. Drawing from the NIST statistics, version 4.2 suffered immensely from the mentioned security vulnerability and others (Padgette et al., 2012). One

article demonstrated an attack referred to as a BlueBorne attack, which moves from one device to another within the supported radius.

As observed above, there are many Bluetooth vulnerabilities that put users at risk (Frisby et al., 2017). To counter this issue, individuals need to learn how to make their devices non-discoverable at any given time unless they want to pair with a known device. This way, they can minimize the chances of BlueBugging, BlueJacking, and BlueSnarfing. The research presented in this review should serve as a starting point for individuals to find solutions rather than exposing the degree of the present threat. The attacks highlighted include eavesdropping and MITM. Others have focused on weak encryption keys as well as short PINs.

The BLE protocol emerged as a variation of the Classic Bluetooth protocol with a consideration for low-power, low cost devices. The protocol runs on the license-free 2.4 GHz ISM band and operates over 40 link-layer channels, each with a 2 MHz bandwidth. Three of these channels are designated as advertising channels that are used for device discovery and connection establishment. Server devices broadcast their existence to client devices through advertising packets sent over these channels. The remainder of the channels are data channels and used for communication between devices after a connection is established. The process and the format for exchanging device specific attributes over a BLE connection is specified by the Generic Attribute Profile (GATT) which organizes the information in the form of services, characteristics, and characteristic descriptors. Services and their characteristics are identified by a universally unique identifier (UUID) value. Characteristics are the main data transfer units communicated between BLE devices, and they consist of properties, values and optional descriptor fields. GATT uses Attribute Protocol (ATT) as the data transfer protocol for discovering services and carrying out operations on characteristics. Permitted operations on a

characteristic, such as read, write, notify, and indicate are set as part of its properties. In this context, indicate and notify operations are both used to notify the client when the value of a characteristic changes with the difference that the indicate operation requires a confirmation from the client. Similarly, a read operation obtains a characteristic's value, and a write operation changes it. When reading from or writing to a target characteristic value, the client sends a request to the server with the handle of the characteristic that is of interest, as well as the corresponding value if it is a write request. The server then responds to each request with a message including the read value or the status of the write request unless otherwise specified (Yurdagul & Sencar, 2021)

2.9.2 A Review of the Solutions to Bluetooth Vulnerability

In response to these attacks, various computer science scholars have drafted solutions as a countermeasure. From the study conducted by Gehrmann and Nyberg (2001), Bluetooth could increase its length of link keys and use the private-public key pairing to their advantage. Another research performed by 28 suggested and proved that the Diffie-Hellman key exchange process could eliminate some of the technology's weaknesses. Consequently, Kim et al. (2005) recommended that bypassing the security architecture of power-limited devices could be a faster substitute for the latter technique. Additionally, to curb MITM attacks, the scholars proposed the use of elliptic curve cryptography and integrating interlock procedures during pairing could eliminate the threat (Hellman key exchange process could eliminate some of the technology's weaknesses (Kim et al., 2005). As studies progressed, BLE devices came into the market. Despite their advantages, Mikhaylov et al. (2013) discovered that they had several vulnerabilities, such as increased communication time, exposing them to attackers. Thus, Kumar (2009) suggested the use of "au ID" for connecting purposes. Soriente et al. (2009) developed a

pairing mechanism that utilized the human body as a medium for communication. Mutchukota et al. (2011) also developed an anti-jamming mechanism that prevented attacks on the physical layer regarding MITM.

Other developments involved the use of cryptography on ECDH public key and the 16-alphanumeric-digit PIN. These discoveries apply to versions 4.0 and BLE mode. As such, they hinder attacks due to passive eavesdropping. Additionally, at the passkey entry, a user-supported numeric method has been used to suppress MITM attacks, as observed by Sandhya and Devi (2012). They also paralleled two algorithms, Triple DES-Tiger and AES-Blake, to find out which is better than the other (Sandhya & Devi, 2013). From their study, the latter was more reliable as a mode of Bluetooth security. In their 2014 research, the scholars investigated the use of the PRESENT-Blake algorithm in an environment dominated by NetBeans (Sandhya & Devi, 2014). Here, they concluded that it yielded a more perfect throughout than the AES-Blake algorithm due to its lightweight trait. To improve Bluetooth security, Yeh et al. (2012) improvised the protocol used in authentication procedures by requiring the same PIN to be entered on the connecting devices rather than displaying the number on the screens. Gajbhiye et al. (2018) proposed a Simple Securing Pairing-Delayed-Encryption-Input-Output (SSP-DEIO) protocol to counter MITM security vulnerability by rescheduling the I/O capabilities during the first stage of SSP. This protection architecture increases both the level of security and time needed for pairing. As version 5.0 also indicated susceptibility to MITM attacks, Sun et al. (2018) proposed a bolstered passkey entry procedure that fixed the reuse of passkey.

2.9.3 Dissecting Bluetooth Wireless Technology Security

Understanding the constituents of Bluetooth security is prudent in decrypting its architecture. Through specifying the literature involved in the technology, the focus of the

research emerges. In this section, the researcher breaks down the different elements of Bluetooth security as well as their relevant existing literature. The results of this discussion inform the thematic analysis of the literature review.

2.9.4 Overview of the Attacker's Tools

2.9.4.1 Generic Tools

Attackers can use services offered by the Bluetooth system itself. Information found in units such as the Service Discovery Protocol (SDP) can assist the intruders to formulate their hacks. For instance, they can state which "port" is open, like Object Exchange Protocol (OBEX) requests. As such, tools such as hcitool and BTScanner are applied to Bluetooth stack via Linux platforms to phish basic data on the devices within the supported range (Becker & Paar, 2007). This information consists of device names, device classes, and addresses. Regarding Microsoft Windows operating systems, the BlueScanner can collect information concerning the type of devices and its services. These tools depend on a laptop; hence a victim can easily spot the potential attacker.

2.9.4.2 Blooover

This tool is a Java program, and it is present on mobile phones. It conducts security auditing in mobile phones to detect vulnerabilities. Afterward, the application can execute a Bluesnarf or BlueBug attack (Becker & Paar, 2007). In the following sections, the research will delve deeper into how these attacks occur. For instance, Bluesnarf enables one to siphon private data from the victim's phone, while Bluebugging enables the attacker to assume remote control of the device.

2.9.4.3 BackTrack

This is a Linux distribution that is Slax-based and offers complex automatic attacks on Bluetooth devices. The pack has analysis tools such as Wireshark and ettercap (Becker & Paar, 2007). Besides, it is capable of Buebugging and Bluesnaffing.

2.9.4.4 BTCrack

This program serves a graphical interface in the eavesdropping process when two devices are pairing. It presents a passive attack that decrypts the generated link key and Bluetooth PIN. As such, the attacker can enter the Bluetooth addresses of the two victim's device to pair them forcefully (Becker & Paar, 2007). Consequently, it results in eavesdropping, where the application scours for the PIN used in the pairing process.

2.9.5 Taxonomy of Bluetooth Attacks

2.9.5.1 Bluesnarf

This attack utilizes the vulnerability of mobile phones concerning OBEX implementation of the Bluetooth profile. As a result, there is no need for authentication; only vCards are sent through the OBEX PUSH profile (OPP). This weakness is in specific mobile phones which have OPP and SYNCH profiles (Becker & Paar, 2007). The former and the latter have access to the same OBEX stack, which inquires through the protected SYNCH profile and OBEX through the same file system. To execute the attack through Bluesnarfing, the intruder connects to an OPP initially. The attacker should have detected the OPP using an SDP scan. Afterward, in insecure implementations, the attacker can initiate a successful OBEX GET inquiry for familiar filenames such as telecom/pb.vcf. This action enables intruders to download confidential data from the victim's phone. In this type of attack, there is no pairing process with users; as such, users cannot know that their phone is being spied upon through Bluetooth. The attackers do not have to be

within the range of sight with the victim, and the increased range in recent devices makes this attack more effective.

2.9.5.2 Bluesnarf++

This attack is an improvement of Bluesnarf discussed above. In the previous version, intruders had to encounter the OPP daemon with the intention of phishing confidential information. When using Bluesnarf++, attackers establish a connection with an OBEX FTP server (Becker & Paar, 2007). This action enables them to transfer files easily. To counter this attack, mobile phones usually offer firmware updates with updated security features. Blusnarfing targets legacy devices by giving the attacker control of the device's phonebook, text messages, calendar data, business cards, and images (Satam et al., 2018).

2.9.5.3 BlueBug

This attack uses the RFCOMM protocol in its execution process. Here, attackers must know the BB-ADDR of the victim's device. First, they connect to RFCOMM channel 17. This port provides an open backdoor in vulnerable phones through AT-parser, which does not have an authentication process (Becker & Paar, 2007). This tool allows attackers to control the victim's device remotely, enabling them to initiate phone calls or write and read SMS. The solution to this type of attack is usually updating a mobile phone to the latest firmware.

2.9.5.4 BlueJacking

This type of attack is different from the others in this list, as it focuses on the Bluetooth capability to send vCards (Becker & Paar, 2007). These are electronic business cards containing personal information, and they do not cost anything to send. To counter this attack, users should always turn Bluetooth off and utilize it only when needed. Bluejacking is used to send anonymous business cards with offensive messages to Bluetooth devices (Satam et al., 2018).

2.9.5.5 HeloMoto

HeloMoto is a blend of BlueBug and Bluesnarf attacks that uses the vulnerability in the implementation of "trusted devices" feature in mobile phones. First, the intruders establish a connection with OPP, similar to Bluesnarf. If there is a presence of vulnerable execution of OBEX, a Bluesnarf attack will occur. As explained by Bluetooth, it utilizes the "trusted device" characteristic. Next, the attacker can transmit the vCard to the target device through BlueJacking and promptly terminates the request. As such, the 'target device' appears in the "trusted devices" record (Becker & Paar, 2007). Subsequently, intruders utilize the "trusted device" state to implement AT commands, similar to Bluebugging. The solution to this attack depends on firmware updates such as Motorola or Bluetooth deactivation.

2.9.5.6 BlueSmack

BlueSmack uses the Denial of Service (DoS) concept if a device uses Bluetooth. It is an attack targeted towards IP-based electronic gadgets (Becker & Paar, 2007). The intruders transmit L2CAP echo inquiry of a large proportion. This inquiry is always between 500–700 bytes, and it is sent to a Bluetooth device that has limited hardware capabilities. When the victims receive the ping request, their input buffer overflows. As such, the attackers immediately disable the target gadget.

2.9.5.7 MAC Spoofing Attack

This type of attack occurs prior to encryption, particularly during the development of the piconet. The intruders usually imitate another device. They also have the authority to cancel the connection and alter data by using a range of special tools.

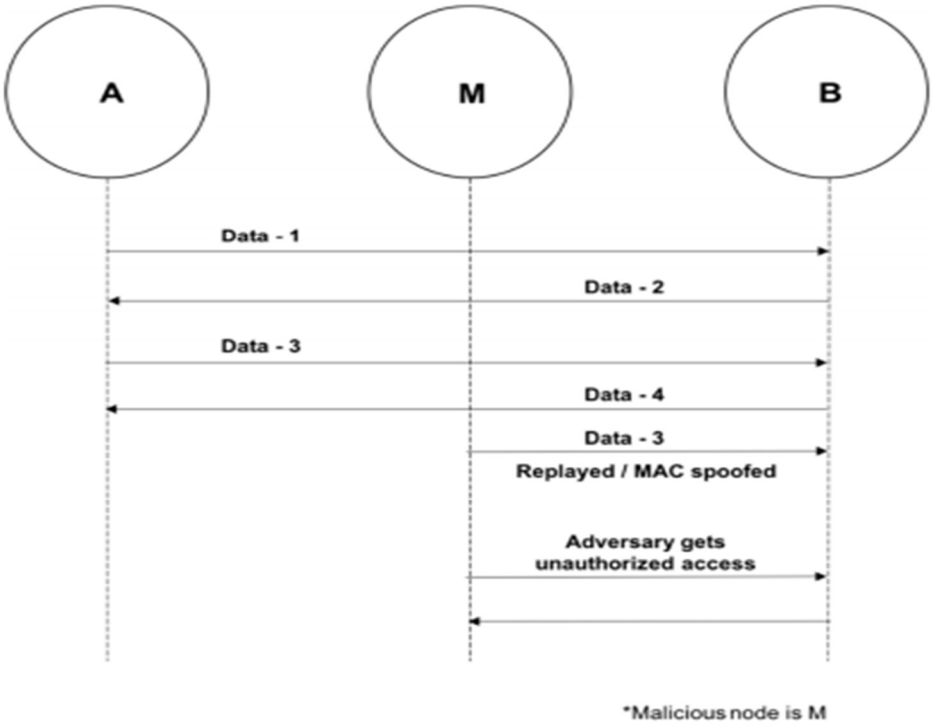


Figure 12 Mac Spoofing (Lonzetta et al., 2018)

2.9.5.7 Man-in-the-Middle (MITM) Attack

MITM attacks occur when two devices are in the pairing process. As intrusion progresses, there is the exchange of messages unknowingly between the devices. This action allows one to authenticate without the secret keys (Lonzetta et al., 2018). In a complete attack, users can think they have paired successfully, but in this case, they have been connected to the attackers.

Launching an MITM attack requires an attacker to simultaneously operate as a BLE client server. The attacker intercepts that data received in one BLE connection interface, modifies it when necessary and relays it to the other interface for transmission. There are several BLE MITM attack frameworks to perform these tasks. Most notably, these includes Btlejuice, Gattacker, and Mirage (Yurdagul & Sencar, 2021)

2.9.5.8 Scanning for Bluetooth Addresses and Surveillance

Bluetooth address scanning (i.e., scanning for BD_ADDR) gives the attacker information on the Bluetooth device manufacturer. This enables them to target the device specific vulnerabilities. BD_ADDR is transmitted unencrypted, and hence can be sniffed easily. Tools like Blueprinting and Bt_audit can be used to easily fingerprint and target Bluetooth devices (Satam et al., 2018).

2.9.5.9 Pairing Attack

A pairing attack can be executed only during the pairing process. The pairing process, which is used to exchange the link key and the initialization key, is dependent on a PIN code; in the case of many Bluetooth devices, this code is set to the default (e.g., in Bluetooth speakers) or has a length of 4 digits, which can be brute forced (e.g., in cars). Tools like BTCrack and btpincrack can be used to brute force the PIN (Satam et al., 2018).

2.9.5.10 BlueDump Attack

Here, attackers spoof the Bluetooth device address of one gadget to connect another. During the connection process, the victim device sends an inquiry for authentication purposes. The intruders reply with “HCI_Link_Key_Request_Negative_Reply.” This response is due to the attackers not possessing the link key (Trifinite, n.d.). In other scenarios, the targeted device deletes its link key and enters a pairing state.

2.9.5.11 Backdoor Attack

A backdoor attack is executed by establishing a trusted relationship with—and pairing with—the target devices. One the pairing is done, attackers can perform attacks like stack smashing on target devices (Satam et al., 2018).

2.9.5.12 BluePrinting Attack

This intrusion requires the attacker to obtain data regarding the type of devices such as the firmware version, model, and manufacturer. In addition, the attacker needs to know the BD-ADDR of the victim's device for it to be successful.

2.9.5.13 BlueBorne Attack

In a BlueBorne attack, the stack buffer overflow trait is used to control a victim's device. As such, attackers utilize the open L2CAP process to intercept Bluetooth connection (Nateq Be-Nazir & Tarique, 2012). This action enables one to manipulate the targeted device. Nevertheless, it requires the attacker to know the Bluetooth and MAC address in order to be possible.

2.9.5.14 Fuzzing Attack

In this case, the attackers determine whether are vulnerabilities to the protocol stack in a victim's device. They then send flawed data packets to the Bluetooth radio. The intruder then observes their behavior to determine the device's weaknesses.

2.9.5.15 Positioning and Tracking Attack

The sniffed BD_ADDR, combined with the use of the Received Signal Strength Indicator (RSSI), can be used to track and locate the position of a Bluetooth device (Satam et al., 2018).

2.9.5.16 Battery Draining Attacks

In battery draining attacks, the attacker sends random packets like pairing request packets or device information request packet to the target device at a high rate. This results in the target device draining its battery at a higher rate (Satam et al., 2018).

2.9.5.17 Bluetooth Viruses

In the modern world, viruses have become a significant part of technology. Attackers have formulated various ways in which they can attack the Bluetooth architecture. The most

popular one was the Cabir worm in 2004, which utilized the Symbian Operating System and spread from one mobile phone to another automatically. In this case, users needed to accept a file transfer request emanating from the infected phone. Next, they ran the file, which automatically found the discoverable devices and repeated the process.

In a survey of Bluetooth threats, Sandhya and Devi (2014) documented and analyzed nine different classes of threats. They also explained each of these classes and provided a list of attack classifications in the form of a table (see Table 4).

Table 4 Bluetooth Attacks & Threat Levels (Sandhya & Devi, 2014)

Vulnerability Attack Classification	Threats	Threat Levels	Threat Levels Ranking
Surveillance	Blueprinting, bt_audit,redfang, War-nibbing, Bluefish, sdptool,Bluescanner,BTScanner	Main purpose is to observe and gather information about the device and its location	Low
Range Extension	Bluesnipping,bluetoone,Vera-NG	Main purpose is to extend the device range so that attacks could be extended from far away distance	Low
Obfuscation	Bdaddr,hciconfig,Spooftooph	Main Purpose is to hide the attacker's identity	Low
Fuzzer	BluePass, Bluetooth Stack, Smasher, BlueSmack, Tanya, BlueStab	Main purpose is to submit nonstandard input to get different results	Medium
Sniffing	FTS4BT, Merlin, BlueSniff, HCIDunp, Wireshark, kismet	Main purpose is to capture the Bluetooth Wireless Technology traffic in transit	Medium
Denial of Service	Battery exhaustion, signal jamming,BlueSYN, Blueper, BlueJacking, vCardBlaster	Main purpose is to deny resources to a target by saturating the communication channel	Medium

Malware	BlueBag, Caribe, CommWarrior	Main purpose is to carry out attacks typically using self-replicating forms of software	Medium
Unauthorized Direct Data Access	Bloover, BlueBug, BlueSnarf, BlueSnarf++, BTCrack, CarWhisper, HeloMoto, btpincrack	Main purpose is to gather private information in an unauthorized manner. This is a very serious as very important information can be stolen	High
Man-in-the-Middle Attack	BT-SSP-Printer-MITM, BlueSpoof, bthidproxy	Main purpose is to place a device between connected devices. All the information sent through the channel are available to the device in between	High

2.10 Cracking the Bluetooth's Personal Information Number (PIN)

A majority of Bluetooth attacks focus on vulnerable implementation. Thus, firmware updates eliminate these weaknesses. This attack deviates from the trend by utilizing the Bluetooth security protocol itself. As Shaked and Wool (2005) present, the adversary eavesdrops communication during the connection process of two devices (2005). Here, the intruders can get the initialization key abbreviated as $K_{init.}$ In order to thoroughly understand the concept, it is important to have the basic knowledge of Bluetooth's security architecture. When two devices are connecting, an inquiry routine detects their BD_ADDR (Becker & Paar, 2007). Next, both parties must key in the same Bluetooth PIN. Before establishing a connection, one device has a distinct PIN, which is set to complement the other device's fixed PIN. Below is the airing process:

1. Development of the $K_{init.}$,which allows both parties to exchange random values in a confidential manner;

2. Link key K_{ab} creation, which discards K_{init} and acts as a function of A or B; and
3. A simple challenge-response system for authentication.

The attacking process starts by eavesdropping communication between devices A and B. Afterward, attackers conduct an extensive search of the plausible Bluetooth PIN. Next, they feed the algorithm E_{22} with the possible values to receive guesses for K_{init}. At this point, the initial two requests during the mutual authentication process are decrypted; thus, a hypothesis for the link key random values develops. An algorithm, E_{21}, calculates the hypothesis of $K_{ab.}$ After the process, the adversary utilizes the last few messages between the device to confirm the hypothesis of K_{ab} (Becker & Paar, 2007). The procedure is conducted repeatedly until the right Bluetooth PIN is phished. Contrary to the other method, solutions to this process are not through firmware updates. Nevertheless, users should be wary when they are prompted to reenter the PIN for the established connection.

2.11 A Brief Review on Bluetooth Risk Mitigation and Countermeasures

Many recent researchers have focused on exposing Bluetooth vulnerabilities. Very few, however, have provided a stepwise solution in mitigating the risks. As this technology has advanced and changed, new challenges have emerged. In this section, the researcher presents plausible solutions to hitherto mentioned attacks. Through this research, these contribution are utilized as a building block for a more robust solution.

2.11.1 Mitigation Methods

The concept of mitigating Bluetooth vulnerabilities is distinct when compared to a computer system. Bluetooth relies on firmware upgrades, while computers depend on application software. The development of these upgrades is at the manufacturing level, which is not possible with the general public (Lonzetta et al., 2018). As such, Bluetooth devices are exposed to these

vulnerabilities continually, even if solutions are present. The section includes a discussion of the current scope regarding mitigation techniques.

2.11.2 Bluetooth User Awareness on Basic Security Measures

The Bluetooth user community should be aware of the basic security measures of this technology. For instance, they should ensure their devices are in a secure range by setting them to the lowest power level. They should also modify their PIN regularly; a change of PINs once a month is advisable. Additionally, the default setting for Bluetooth's discoverability should be "undiscoverable mode" except when needed; this prevents connection to other devices automatically in public (Lonzetta et al., 2018). Users should avoid entering PINs and Passkeys when prompted randomly to do so. They should ensure that they use SSP instead of the legacy PIN authentication process, and they should unpair with devices after exchanging files. Lastly, they should accept data from only trusted devices.

2.11.3 Prevention of Man-in-the-Middle Attacks

MITM intrusion is preventable by basing link keys on combination keys rather than the usual unit keys. The security issues inherent in Bluetooth are largely due to the process of pairing one device to another. Various attacks can be performed before the pairing process has completed. Even after the devices are paired, an adversary can still gain enough information to be able to perform Man in the Middle attacks or to impersonate another device (Cope, Campbell, Hayajneh, T. 2017).

2.11.4 Link Encryption

The encryption of data transmitted prevents attacks that utilize eavesdropping. A HID boot protocol assists in encryption. It is pertinent to avoid a human interface that is connectionless, as it creates traffic in plain text.

2.11.5 Multi-Hop Communication

Bluetooth users should ensure that link keys during this process have been encrypted. The absence of encryption compromises communication due to imminent attacks.

2.11.6 Mutual Authentication

Device users should ensure that they authorize their connection. This enables them to verify the authenticity of the connecting devices.

2.11.7 Broadcast Interceptions

When using broadcast interception, users can lower this risk through encryption.

2.11.8 Security Mode 3

This level is one of the best among three modes since its implementation is at the link level. It implements link-level security before the physical link is fully stablished (Alfaiate & Fonseca, 2012).

2.11.9 Key Size

A maximum key size and a minimum one of 128 bits should be applicable in preventing brute-force attacks.

2.11.10 Applications for Bluetooth Security

Applications such as Bluetooth firewall secure devices from attacks. Users receive an alert in case of any Bluetooth activity. Another application, Bluetooth file transfer, allows only authorized devices to connect; this serves as an additional method of security.

Chapter 3

Research Methods

The methodology of the current study was that of design science research. Design science research is a third pillar of research methodology, neither qualitative nor quantitative (Vaishnavi & Kuechler, 2015). Instead, design science research is an intrinsically applied type of research with the explicit purpose of developing a practical solution to a real-world technical problem (Vaishnavi & Kuechler, 2015). The results of successful design science research take the form of a technological artifact, the nature of which is dependent upon the problem being studied. Some examples of the artifacts created include algorithms, fabrication techniques, or protocols (Vaishnavi & Kuechler, 2015). In this case, the results of the study take the form of a trust protocol designed to effectively patch the gap in Bluetooth security that is manifest in the Bluetooth SDP, allowing attackers to access valuable data. The clearly applied and technical nature of this problem makes it a good fit for design science research. Rather than trying to understand a relationship between variables, as in quantitative research, or to describe/explore a phenomenon, as in qualitative research, the current researcher's aim was to develop a solution to a specific technical problem. Therefore, design science was the strongest and most appropriate choice of research methodology.

3.1 Research Design

The specific research design consisted of two phases: a qualitative review of the technical and academic literature, followed by a design science step in which the researcher attempted to develop a solution. Qualitative literature reviews are used when a researcher wishes to examine the ideas and overall trains of thought present in the research regarding a topic rather than

studying it directly (Thomas & Harden, 2008). A qualitative literature review is a synthesis of what is known; by nature, it is broader than a quantitative meta-analysis or systematic review; rather than bringing together the results of multiple quantitative studies of a single quantitative question to achieve a stronger result, a qualitative review brings together the results from a wide array of qualitative and quantitative studies to explore the overall trends and ideas present in the literature (Thomas & Harden, 2008). In that sense, a qualitative review—like qualitative research as a whole—is exploratory. In this case, such exploration is needed due to the relatively limited research into the problem in the first place (Hassan et al., 2017), and the existing research is scattered across different contexts and from different perspectives. The creation of a coherent, unified single picture of what is known about Bluetooth security vulnerabilities requires casting a wide net and adopting an exploratory approach. Once this exploratory review has been carried out, the researcher applied a design science approach (Vaishnavi & Kuechler, 2015) to develop a solution. This involved drawing upon various aspects of the literature—namely, tools that have been used in other contexts, such as solutions to other Bluetooth vulnerabilities or solutions to SDP vulnerabilities for other technologies. These tools represent the basis from which the researcher sought a solution to the problem of SDP vulnerability in Bluetooth technology. The researcher predicted that the results of the design stage of the research design would be either a working protocol to patch the security vulnerability or a detailed explanation of how each attempted approach failed to solve the problem.

3.2 Data Collection

Data collection was carried out through a comprehensive review of the literature. This review was comprised of two phases, the first of which was background information on Bluetooth and Bluetooth security issues. Therefore, the first stage of the literature search did not

have a set date range, but extended back as far as necessary to characterize the history of Bluetooth technology, its development, and issues with security along the way. The second stage of the literature review targeted more recent research regarding Bluetooth security vulnerabilities and emerging applications of Bluetooth technology. This phase of the literature search was limited to the last 5–8 years to ensure relevance to the present. The literature search was carried out through all the major academic databases available through university libraries and Google Scholar. The keywords used in the literature search included *Bluetooth, security, virus, DoS, DDoS, man-in-the-middle, application, vulnerability, exploit, weakness*, and other similar terms plus combinations thereof. The initial search involved examining the titles of articles. For those with seemingly relevant titles, the researcher read the abstract and determined from that whether the article should be included in the review. For those included in the review, the researcher obtained a PDF full text and read it carefully, then compiled the full set of relevant full articles for use in data analysis.

3.3 Data Analysis

The notion of data analysis primarily applies to the first stage of the research design: the literature review. The data analysis process consisted of a combination of content analysis and qualitative thematic analysis. The content analysis stage was carried out on each individual article. Using a template designed in advance and approved by a panel of experts, the researcher summarized each article's content in terms of key points. The points included the type of the study, the research questions or research purpose, the location of the study, the sample size, the version of Bluetooth included, the length of the study, and any threats to the validity of the study. Once each study had been textually analyzed, the researcher moved on to thematic analysis. In

the thematic analysis stage, the results were reviewed carefully to ensure familiarity, then coded for important ideas (Clarke & Braun, 2013).

After the results were coded, the researcher identified themes in terms of where the results draw connections between two or more codes and defined these larger ideas as themes. Once the themes were identified, they were cross-checked against the data to ensure that they were actually present and also against each other to ensure the uniqueness and completeness of each theme (Clarke & Braun, 2013). The final stage was synthetizing the results of the analysis; this stage involved recontextualizing the themes in their original studies in terms of strength of results, type of results, and threats to validity. The final result of this analysis should be a comprehensive understanding of the problem.

3.4 Design

Following the data analysis stage, the researcher used the results of the analysis to move on to the design phase. This constituted trial and error, development, and testing of a new trust protocol. This new protocol was tested against the methods that have been shown to violate the security of the traditional Bluetooth SDP. The design phase was considered finished when either the researcher had successfully developed a method that can be demonstrated to frustrate these attack techniques or when the researcher had exhausted the available tools for developing such a solution without success. The results of this design and testing process were then documented.

3.5 Ethical Considerations

Because the current researcher drew data primarily from prior research and direct study of Bluetooth documentation, few ethical issues are anticipated. There is one potential issue in that drawing attention to the common vulnerabilities of Bluetooth technology could allow malicious actors to more easily target this technology. All the research findings presented in this

study were drawn from existing research; therefore, no new information about the vulnerabilities was created. Given that, no data were such that a malicious actor could not have arrived as a similar conclusion without reference to the study. Moreover, the benefits of bringing these security issues to the attention of users and manufacturers so as to encourage better protection against them is considered to outweigh any risk of malicious parties becoming more aware of those vulnerabilities. The identification and highlighting of vulnerabilities with the intention of seeing them corrected is a traditional aspect of computer science as a whole.

Chapter 4

Thematic Analysis

The current researcher adhered to the thematic analysis proposed by Braun and Clarke (2006). These authors presented a six-step process, which served as the foundation of this evaluation. In the first stage, researchers familiarize themselves with the data. As such, it was prudent to understand the literature review section to decrypt patterns in the text. During this process, the researcher took notes and commented on the various information using the Microsoft OneNote Digital Note Taking App. It was important to take notes at first to a space for the work the researcher was going to do and find approaches and concepts that would be integral to build on during the study. This process enabled themes, patterns, and significant language to be discovered. In the second stage, and as suggested by Clarke & Braun (2013) the researcher generated the codes for the various themes identified during the literature review(see Table 5).

In the third phase, the researcher used coding blocks identified to develop plausible thematic categories (see Table 5); in this stage, the codes were sorted with the goal of finding primary themes. This process was the initial stage for code placement and theme development. In the fourth stage, the researcher reviewed the themes if they were relating to the coded extracts. Here, refining themes was crucial using the initial two phases. In the first stage, the researcher conducted a superficial examination, and if a clear pattern became apparent, the researcher could move to the second stage of analysis. In the second state, the themes were analyzed to find establish relations with the topic of study. At this point, the researcher also checked to determine whether any significant information was missing in the codes.

As the researcher progressed to the fifth phase, the themes were renamed to be more concise. This enabled the reader to understand what the themes represented. The research question and data related to the theme were crafted as the analysis moved to the sixth phase (Braun & Clarke, 2006). In the last step, the researcher focused on producing a report which related the analysis to the research questions and literature review. To illustrate this process, the researcher used a table indicating the different thematic categories.

Table 5 Thematic Categories and Codes

Initial Coding	Number of Journals	Thematic Categories
Vulnerability	36	Security Vulnerabilities in Bluetooth Technology
Bluetooth Attacks	6	
BlueSmack	30	
BlueJacking	16	
BlueBugging	10	
Man-in-the-Middle	32	
Cracking Bluetooth PIN	12	
Secure Simple Sharing (SSP)	8	Current Bluetooth Security Architecture
Bluetooth Layers	11	
Security Modes	5	
Link Keys	34	
Mitigation Measures	5	Present Solutions to Bluetooth's Vulnerabilities
Combination Keys	10	
Bluetooth Security	32	

After categorizing the literature review into unit themes, as shown above, it was prudent to analyze the constituent elements making up the themes.

4.1 Current Bluetooth Security Architecture

4.1.1. Security Levels in the Bluetooth Security Architecture

As discussed in the literature review, there are four levels of security in the Bluetooth design. In Level 1, the devices have no security, while in Level 2, encryption is present but no authentication. At Level 3, authentication occurs during pairing as well as encryption. The utmost level has an authentication process as well as encryption (Lonzetta et al., 2018). Furthermore, it utilizes a stronger encryption key. This type of security is discussed below. Previous scholars have highlighted that the security for Bluetooth is offered through radio paths. This stance implies that encryption and link authentication are applicable, but the end-to-end security feature cannot be possible without improving the protection solution of Bluetooth's higher layers. In a nutshell, Bluetooth provides security on the following services;

1. Confidentiality: Here, the objective of the Bluetooth SDP is privacy. As such, it is difficult for an eavesdropper to retrieve information (Panse & Panse, 2013). Only an authorized user can access the data.
2. Authorization: The goal of Bluetooth SDP in this section is to verify the connecting devices (Hassan et al., 2018).
3. Authentication: As observed in the literature review, Bluetooth security controls individuals when having access to resources. Here, it must authorize whether a user has the authority to view the resources.

4.1.2 Keys Used in Bluetooth Security

4.1.2.1 Unit Keys

Encryption and authentication procedures based on combination keys are similar to the unit keys. Nevertheless, a unit key uses a single key in all protected connections. Thus, it must share the same key with devices it trusts (Hassan et al., 2018). As a result, all trusted devices can eavesdrop traffic by utilizing the key. This impersonation makes it vulnerable to intrusion from the "trusted devices."

4.1.2.2 Combination Keys

The generation of this key occurs during the initialization process. Here, the two connecting devices create the key at the same time (Panse & Panse, 2013). At the first stage, both devices develop a random number. An algorithm, E21, develops a unique number by combining the prompt number and their BD-ADDR. Afterward, the units transmit their random numbers securely between each other and compute the combination key K_{ab}.

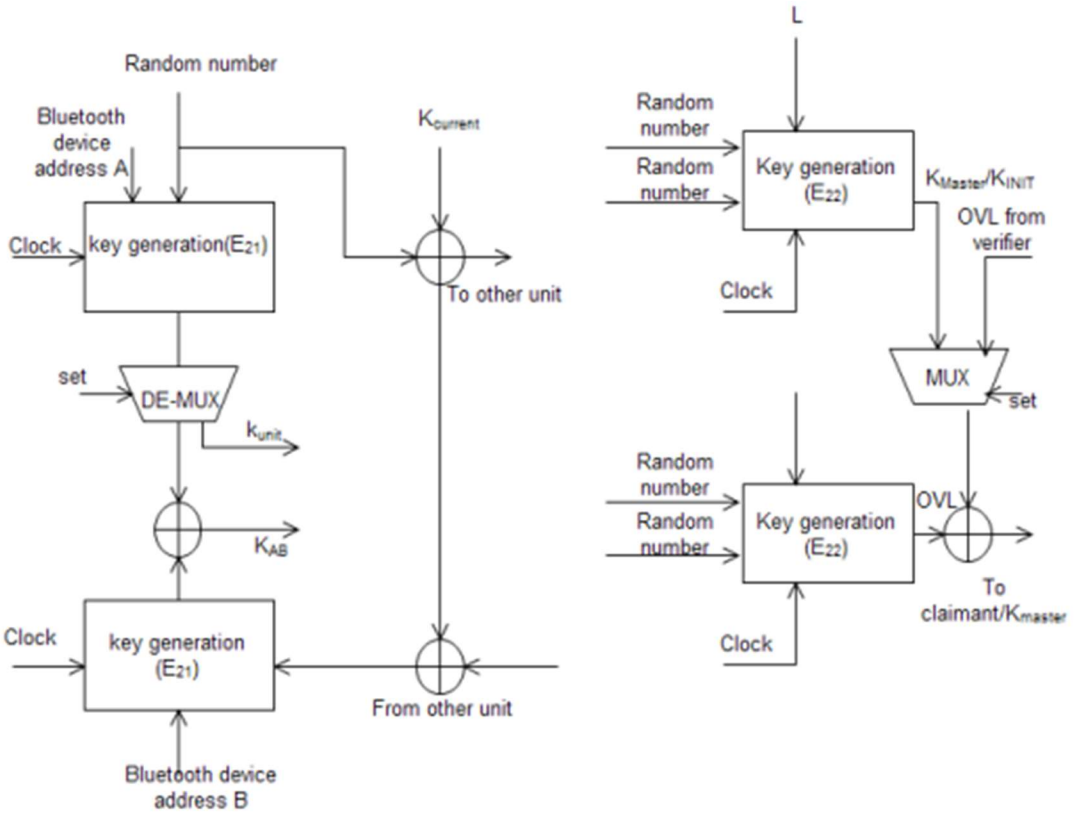


Figure 13 Link Key Generation (Panse & Panse, 2013)

4.1.2.3 Encryption Keys

The development of this key is from a 128-bit random value, a 96-bit COF (Ciphering Offset Number), and the link key (Giousouf & Lemke, n.d.). This COF is as a result of Authenticated Ciphering Offset (ACO) created during the authentication stage. The link manager (LM) initiates the encryption, which has an output as the "encryption" key. This value changes when the device goes into encryption mode.

4.2.2 Built-In Security in Bluetooth Wireless Technology

In the quest to provide security, Bluetooth SIG has embedded features to counter malicious attacks. First, Bluetooth has an undiscoverable mode. In this state, the device cannot respond to scanning requests. It also hides the BD_ADDR, which is vital data for attackers as it allows them to to masquerade as trusted paired devices (Lonzetta et al., 2018). Additionally,

Bluetooth has an Adaptive Frequency Hopping technique. This process enables a device to hop 1600 times per second (Lonzetta et al., 2018). It utilizes 79 channels under the 2.4GHz ISM band. During this procedure, there is an exclusion of the current frequency. Overall, the suitability of this operation eliminates interference and jamming. Another built-in security feature is the E0 Cipher Suite. Its length of 128 bits and streaming prevents attackers from exploiting the technology's vulnerability. Regarding pairing, devices can communicate their BD-ADDR. The address must be known to both the devices for a pairing request to be possible from previous connections.

4.2.2.1 Pairing

This process ensures that the connecting devices have established trust. It is through this process that the security keys are generated and exchanged at the same. The model used in this step is the SSP, which depends on the I/O capabilities of the devices as well as the security requirements. For instance, in “Just Works,” the devices will pair without authentication, but the encryption process will occur (Lonzetta et al., 2018). The primary reason for this model of pairing is that there is no method of confirming the details of the connecting devices. In the passkey entry mode, users must input a passkey that displays on both screens. This protection eliminates the possibility of Man in the middle (MITM) attacks. Additionally, numeric pairing provides a numeric comparison for the users to compare the passkeys on the devices' display. This security feature also offers protection against MITM attacks.

4.2.2.2 Bonding

This security feature enables the devices to keep security to reuse in forthcoming connection (Haataja et al., 2010). Thus, it will assist the devices to verify their identities. On iOS and Android smartphones, bonding is stored in the operating system (Panse & Panse, 2013). As a

result, other mobile applications will be able to utilize the same bonding information to identify and connect to the peripheral device. Bonding does not protect device communications at the application level (Hassan et al., 2017). It is possible to provide privacy measures equivalent to the built-in Bluetooth privacy features without pairing or bonding when application-level protection is necessary.

4.2.2.4 Attribute Permissions

This type of security feature has permissions that regulate what can be read or write. It can also decide whether to send data over an encrypted link or not (Lonzetta et al., 2018). Attribute permissions differ depending on the descriptors' characteristics.

4.3 Bluetooth 4.2 Security Protocol

Version 4.2 is one of the recent Bluetooth SIG (Special Interest Group) developments. The technology uses low energy security connections while utilizing the ECDH (Elliptic Curve Diffie-Hellman) feature and numerical comparison using the public-private key pairs (Faragher & Harle, 2015). Elliptic-curve two parties can establish a shared secret across an unsecured channel using the Diffie–Hellman (ECDH) key agreement protocol, which uses elliptic-curve public–private key pairs (Iqbal et al., 2010). Using this shared secret as a key or deriving another key is possible. A symmetric-key cipher can be used to encrypt subsequent communications with the original key or a derived key. Using elliptic-curve cryptography (ECC), it's a Diffie–Hellman protocol variant (Cheah et al., 2017). With ECC, we can use public-key cryptography to make use of elliptic curves over finite fields, which has an algebraic structure we can work with. When compared to non-EC encryption, ECC allows smaller keys to be used to achieve the same level of security. Key agreement, digital signatures, pseudo-random generators, and other activities can benefit from elliptic curves. This new comparison technique utilizes a 6-digit key, which

both users must confirm by pressing a button. The identity confirmation has been shifted from the host to the controller for lower power and faster operations.

4.4 Security Vulnerabilities in Bluetooth Technology

Another theme emanating from the literature review revolves around the security vulnerabilities of the current Bluetooth wireless technology architecture. In the modern world, there has been a surge of malicious attacks targeting electronic devices. Bluetooth technology is prone to interceptions and jamming (Panse & Panse, 2013). Attackers can modify the information being passed between devices. These attacks can be categorized into three primary classes:

1. Denial of Service threat: In a DoS attack, users cannot access services as the intruders make them unavailable or limited.
2. Disclosure threat: In this type of threat, private data can leak from the victim's device to an eavesdropper who is the legitimate owner of the information.
3. Integrity threat: Here, the attackers alter the information in order to mislead the target.

In the current scope of Bluetooth application, it is plausible to change a dongle into Bluetooth Sniffer (Panse & Panse, 2013). Individuals use reverse engineering to understand the firmware capabilities of Bluetooth dongles. It is possible to draft a custom firmware for Bluetooth dongle, which can assist them in accessing Bluetooth sniffing architecture. Additionally, individuals have crafted ways to expose nondiscoverable devices. As much as it will pave the way for more studies in the Bluetooth security niche, attackers will also gain from the same through the sniffing algorithm. Some threats presented in the literature review fell outside the threats as mentioned above; these are discussed in the following sections.

4.5 Popular Bluetooth Attacks

4.5.1 BlueJacking

This type of attack has spamming characteristics. Users can send their electronic business cards to individuals within 30 feet (Panse & Panse, 2013). If intruders download the e-card, they can add their contact to the victim's address book and begin to transmit messages to the user's device. Some attackers have modified this technique by using an amplifier and antenna to infect the victim's phone from a 300 feet radius.

4.5.2 Bluebugging

Bluebugging enables the intruders to have access to the victim's device remotely. As such, they can forward calls, listen to calls, send messages, and place calls. The user cannot be aware of the attack. These can lead to the high cost of bills that are used to make premium or international calls.

4.5.3 Eavesdropping

In this type of attack, the attackers can bypass the encryption process. This action enables them to access data on the victim's phone as well as listen to calls.

4.5.4 Denial of Service Attacks

In this process, intruders crash the victim's device and deter them from receiving calls. This attack can also drain the victim's battery. This is a type of assault known as a denial of service (DoS) attack, in which the attacker aims to prevent the intended users from accessing the system or network resource by temporarily or forever disrupting its functions (Lonzetta et al., 2018). The most common method of denial of service is to flood a target computer or resource with unnecessary requests to prevent queries from being performed. There are numerous distinct sources of traffic flooding a victim during a distributed denial-of-service attack (DDoS). To protect

against this form of assault, more sophisticated tactics are needed, as merely trying to block a single source is inadequate.

4.5.5 MAC Spoofing Attack

These attackers perform this intrusion during piconet formation and link key generation. The attackers intercepts data and manipulates it to the target devices. The Bluetooth SIG has not provided a robust solution to this kind of attack (Lonzetta et al., 2018). Individuals are advised to execute the connection while using privacy settings. Additionally, longer and random PIN values are recommended.

4.5.6 PIN Cracking Attack

Through having a protocol analyzer or frequency sniffer and an FHS packet, intruders acquire the initialization key, LK_RAND, and IN_RAND during the authentication and pairing processes (Hassan et al., 2017). Here, the attackers provide all the likely permutation of the PIN. After they have obtained BD_ADDR and IN_RAND, they attempt permutation in an algorithm known as E_{22}. The process might need several attempts for the intruders to acquire the right initialization keys. This process is difficult if Bluetooth uses a combination of private and public keys.

4.5.7 Impersonation Attack

MITM or impersonation attacks entail data modification between connecting devices in a piconet. Here, the intruders can send the authentication to two users without them knowing the shared secret keys. The attacker can trick the users into believing that they have paired; in reality, however, they have paired with the intruders. Nested mutual authentication can solve this problem by identifying the validity of a device before responding to the request.

4.5.8 BluePrinting Attack

In this type of attack, attackers obtain the device model, firmware, and the name of the manufacturer (Cope et al., 2017). An intruder uses Blueprinting to formulate information regarding the device and evaluating if there is vulnerability. This intrusion is successful if the attackers know the Bluetooth device address.

4.5.9 Brute-Force Attack

This type of attack utilizes the last three values of the BD_ADDR. The primary reason for leaving the other part is because it is a fixed value, and it is public (Lonzetta et al., 2018). Its execution is through BD_ADDR scanning to find vulnerable devices.

4.5.10 Backdoor Attack

Backdoor intrusion uses the trust established during the pairing process. It does not present itself in the victim's record of paired devices unless the user observes the moment when the connection starts. The attacker can access the resources granted by the “trusted relationship” with the victim's phone (Lonzetta et al., 2018). Through this connection, intruders can obtain personal data, GPRS, and WAP gateways without the victim knowing that there is a breach. This attack is possible only when the attackers know the device's BD_ADDR.

4.5.11 *Man-in-The middle attack*

The use of wireless communication systems and their interconnections via networks have grown rapidly in recent years. Because radio frequency waves (RF) waves can penetrate obstacles, wireless devices can communicate with no direct line of sight between them. This makes RF communication easier to use than wired or infrared communication, but it also makes eavesdropping easier. . Moreover, it is easier to disrupt and jam wireless RF communication than wired communication. Because wireless RF communication can suffer from these threats,

additional counter measures are needed to protect against them (Haataja et al., 2010).The basic Bluetooth security configuration is done by the user who decides how a Bluetooth device will implement its connectability and discoverability options. The different combinations of connectability and discoverability capabilities can be divided into three categories or security levels:

1) Silent: The device will never accept any connections . It simple monitors Bluetooth traffic.

2) Private: The device cannot be discovered , i.e. it is a so called non-discoverable device. Connections will be accepted only if the Bluetooth device address (BD_ADDR) is known to the prospective master, A 48-bit BD_ADDR is normally unique and refers globally to only one individual Bluetooth device

3) Public: The device can be both discovered and connected to. It is therefore called a discoverable device.

Because Bluetooth is a wireless communication system, there is always a possibility that the transmission could be deliberately jammed or intercepted, or the false or modified information could be passed to the piconet device (Haataja et al., 2010). Powerful directional antennas can be used to increase the scanning, eavesdropping, and attacking range of almost any kind of Bluetooth attack considerably. One very good example of a long distance attacking too is the BlueSniper Rifle. It is a rifle stock with a powerful directional antenna attached to a small Bluetooth compatible computer. Scanning, eavesdropping, and attacking can be done over a mile away from the target device (Haataja et al., 2010). Moreover, anyone with some basic skills and a few hundred dollars can build her own BlueSniper Rifle. Therefore, the possibility that an attacker is using range enhancement for improving the performance of the attacks should be taken seriously (Haataja et al., 2010). Bluetooth security is based on building a chain of events,

none of which should provide meaningful information to an eavesdropper. All events must occur in a specific sequence for security to be set up successfully. For two Bluetooth devices to start communicating, procedure called pairing must be performed. As a result of pairing, two devices form a trusted pair and establish a link key which is used for creating a data encryption key for each session. In Bluetooth versions up to 2.0+EDR, pairing is based exclusively on the fact that both devices share the same Personal Identification Number (PIN) or passkey. When the user enters the same passkey in both devices, the devices generate the same shared secret which is used for authentication and encryption of traffic exchanged by them. The PIN is the only source of entropy for the shared secret. As the PINs often contain only four decimal digits, the strength of the resulting keys is not enough for protection against passive eavesdropping on communication. Even with longer 16-character alphanumeric PINs, full protection against active eavesdropping cannot be achieved: it has been shown that MITM attacks on Bluetooth communications (versions up to 2.0+EDR) can be performed (Haataja et al., 2010).Bluetooth versions 2.1+EDR and 3.0+HS (High Speed) add a specification for the pairing procedure, namely SSP . Its main goal is to improve the security of pairing by providing protection against passive eavesdropping and MITM attacks. Instead of using (often short) passkeys as the only source of entropy for building the link keys, SSP employs Elliptic Curve Diffie-Hellman public-key cryptography. To construct the link key, devices use public-private key pairs, a number of nonces, and Bluetooth addresses of the devices. Passive eavesdropping is effectively thwarted by SSP, as running an exhaustive search on a private key with approximately 95 bits of entropy is currently considered to be infeasible in short time. To provide protection against MITM attacks, SSP either uses an Out-Of-Band (OOB) channel (e.g.,Near Field Communication, NFC), or asks for the user’s help: for example

, when both devices have displays and keyboards, the user is asked to compare two six-digit numbers. Such a comparison can be also thought as an OOB channel which is not controlled by the MITM. If the values used in the pairing process have been tampered with by the MITM, the six-digit integrity checksums will differ with the probability of 0.999999.

SSP uses four association models. In addition to the two association models mentioned previously, OOB and Numeric Comparison (NC), models named Passkey Entry (PE) and Just Works (JW) are defined. The PE association model is used in the cases when one device has input capability, but no screen that can display six digits. A six-digit checksum is shown to the user on the device that has output capability, and the user is asked to enter it on the device with input capability. The PE association model is also used if both devices have input, but no output capabilities. In this case the user chooses a 6-digit checksum and enters it in both devices. Finally, if at least one of the devices has neither input nor output capability, and an OOB cannot be used, the JW association model is used. In this model the user is not asked to perform any operations on numbers; instead, the device may simply ask the user to accept the connection. SSP is comprised of six phases:

1) Capabilities exchange: The devices that have never met before or want to perform re-pairing for some reason, first exchange their Input/Output (IO) capabilities to determine the proper association model to be used.

2) Public key exchange: The devices generate their public private key pairs and send the public keys to each other. They also compute the Diffie-Hellman key.

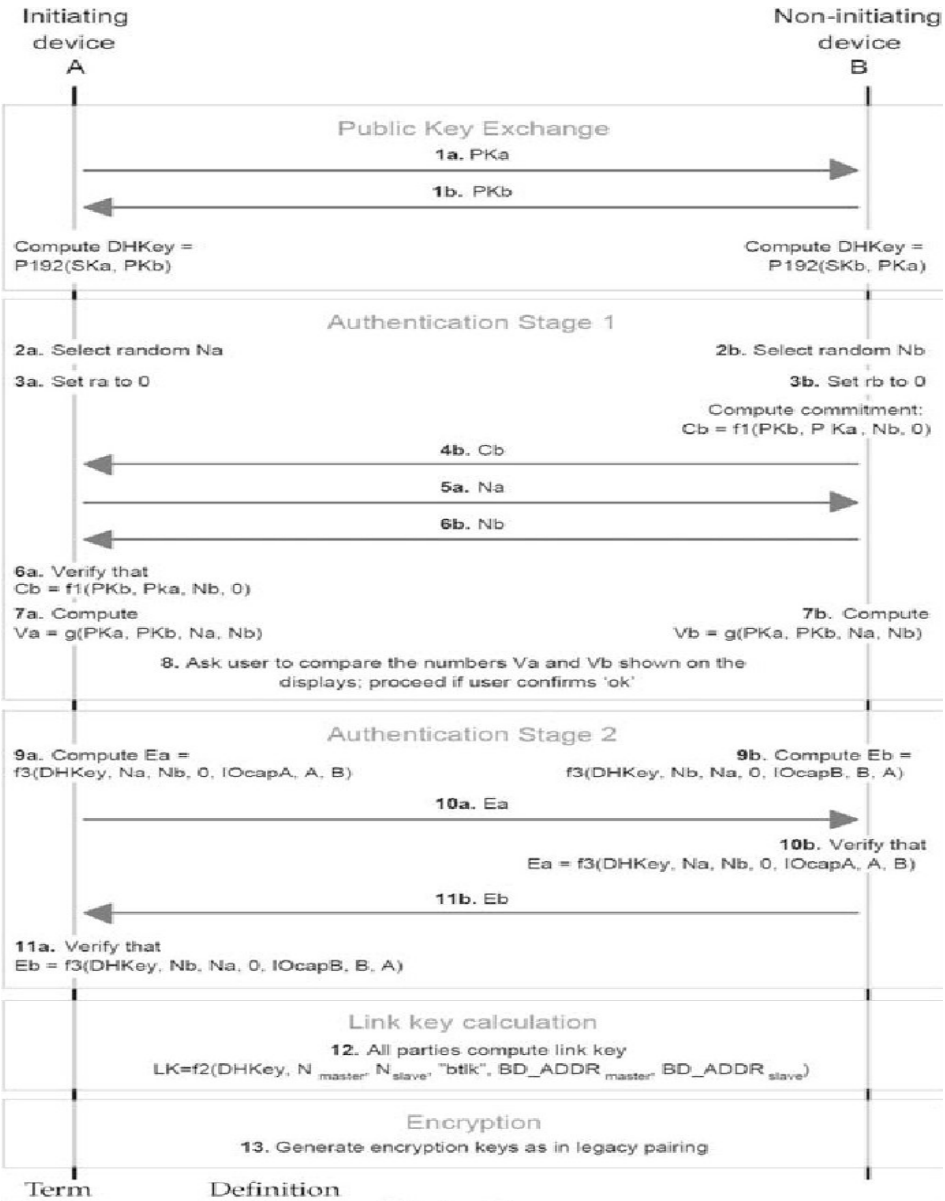
3) Authentication stage 1: The protocol that is run at this stage depends on the association model. One of the goals of this stage is to ensure that there is no MITM in the communication between the devices. This is achieved by using a series of nonces, commitments

to the nonces, and a final check of integrity checksums performed either through the OOB channel or with the help of user.

4) Authentication stage 2: The devices complete the exchange of values (public keys and nonces) and verify the integrity of them.

5) Link key calculation: The parties compute the link key using their Bluetooth addresses, the previously exchanged values and the Diffie-Hellman key constructed in phase 2.

6) LMP authentication and encryption: Encryption keys are generated in this phase, which is the same as the final steps of pairing in Bluetooth versions up to 2.0+EDR. The contents of messages sent during the SSP phase are outlined in Fig. 14. The used notations are also explained in figure 14.



Term	Definition
PKx	Public key of device X
SKx	Private key of device X
DHKey	Diffie-Hellman key generated after key exchange
Nx	Nonce generated by device X
rx	Random number generated by device X; equals 0 in the NC association model
Cx	Commitment value from device X
f1	One-way function used to compute commitment values
f2	One-way function used to compute the link key
f3	One-way function used to compute check values
g	One-way function used to compute numeric check values
IOcapX	Input/Output capabilities of device X
BD_ADDR	48-bit Bluetooth device address

Fig. 14. SSP with Numeric comparison (Haataja et al., 2010).

Even though SSP improves the security of Bluetooth pairing, it has been shown that MITM attacks against Bluetooth 2.1+EDR and 3.0+HS devices are also possible by forcing victim devices to use the JW association model (Haataja et al., 2010).The main idea of this attack is that the MITM uses two separate Bluetooth devices . The MITM first disrupts (jams) the physical layer (PHY) by hopping along with the victim devices and sending random data in every timeslot. Another possibility was to jam the entire 2.4 GHz band altogether by using a wideband signal. In this way, the MITM shuts down all piconets within the range of susceptibility and there is no need to use a Bluetooth chipset to generate hopping patterns. Finally, a frustrated user thinks that something is wrong with her Bluetooth devices and deletes previously stored link keys. After that the user initiates a new pairing process by using SSP, and the MITM can forge messages exchanged during the IO capabilities exchange phase. When the JW association model has been forced into use, the attack continues as illustrated in Figure 15 (Haataja et al., 2010).

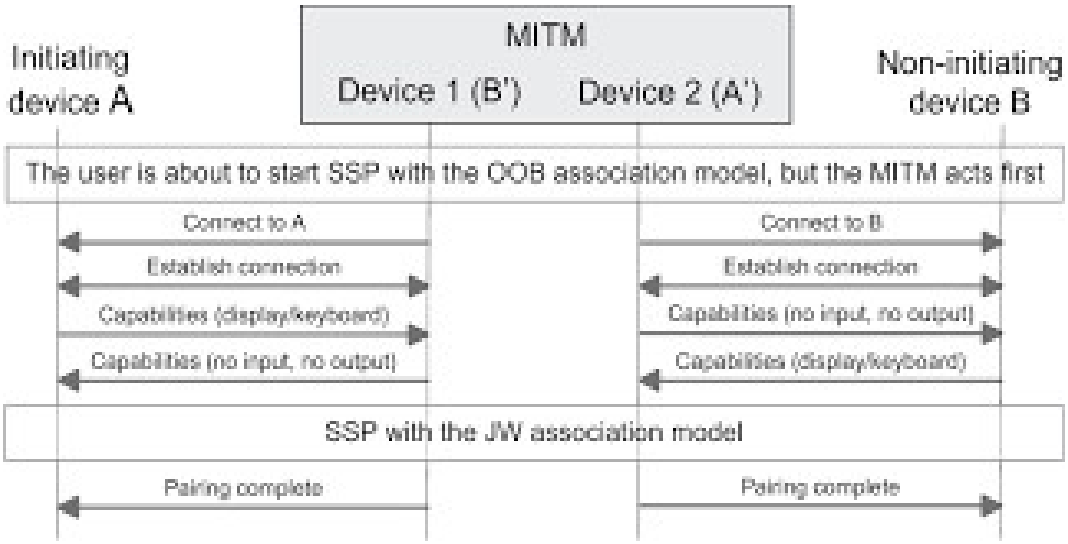


Fig.15 – Bluetooth no-input-no-output MITM attack

The victim device (A or B) initiates SSP. The MITM waits until A or B initiates SSP . After that, the attacks proceeds as illustrated in figure 15 above.

After an MITM attack, the MITM can intercept and modify all data exchanged between the victim's devices and even use certain services that victim devices offer. (Haataja et al., 2010).

4.6 Present Solutions to Bluetooth's Vulnerabilities

As the public becomes more enlightened on issues regarding security, several scholars have developed authoritative solutions to the challenge. Iqbal et al. (2010) proposed a refined security architecture. They provided a new authentication and link generation protocol with the potential to counter attacks such as MITM. In the suggested scheme, connected devices through the unit key must input the PIN into a keyed hash algorithm. This method uses the unit key because it is one of the primary areas that exploited MITM attacks. Afterward, the link key's keyed hash and the PIN are taken through another algorithm known as E3. This way, a unique encryption key will be generated. As only the two devices know the PIN, an untrusted device will not generate the encryption key of the connected devices.

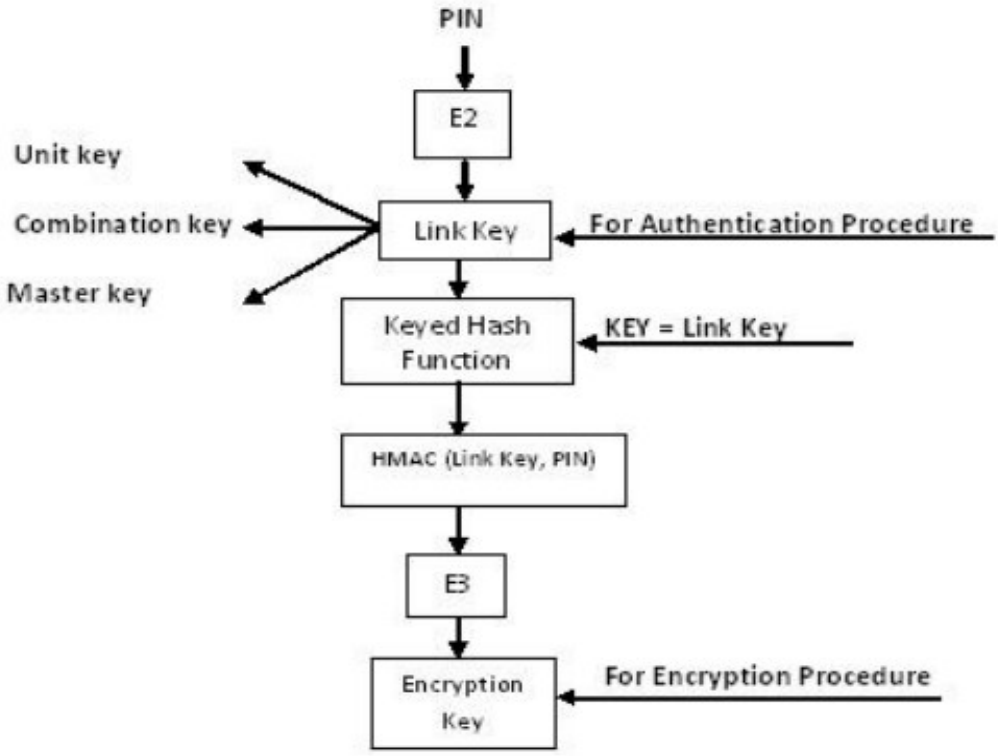


Figure 14 Enhanced Link Generation (Iqbal et al., 2010)

Iqbal et al. (2010) created a new authentication scheme that focused on managing DoS attacks. This concept includes the mechanism of anti-clogging cookies. In the first message, the master develops and transmits a Nonce-C. This Nounce-C is secure and distinct to the receiver. It is the result of a unique combination of information on both devices. The verifier creates a validation request and communicates it to the claimant. Regarding Nounce-V, only the verifier can generate its value, and it maps one to one with Nounce-C. The mentioned properties terminate the need for the verifier to remember Nounce-V or Nounce-C in the first and second processes. During the third message, the claimant transmits Nounce-V=AU_RAND and Nounce-C, as well as BD_ADDR as confirmation (Iqbal et al., 2010). The verifier calculates the new Nounce-V from the recipient and assesses whether it is similar to the third message. If they match, the verifier comprehends that the claimant is not the attacker; if they do not match, the opportunity to terminate the message remains.

In providing the security solution in the piconet, Iqbal et al. (2010) recommended the use of certain piconet information in SRES computation. There is no limit to information regarding the piconet. The authors suggested that the function output be AU_RAND. This function (F) will appear in the following schemes: Part of MAC Address Value (PAV), Channel Access Code (CAC), Nounce-C, and MAC Address of claimant. The resultant value of the AU_RAND is utilized in computing SRES. Basically, the AU_RAND value links with PAV, Nounce-C, and CAC. In two legitimate devices, the PAV and CAC would be different. If the intruder attempts to have access to the "trusted" piconet, there would be a mix-up (Iqbal et al., 2010). The Bluetooth architecture involves the use of four messages between the verifier and claimant, while this proposed protocol entails five messages. The added one reduces the effect of the DoS attack and

prevents an intrusion to the piconet. In this case, the master device alerts the slaves in case of intrusion in the piconet. If the MAC address received by the master is the same, it is labeled as an attacker.

Apart from the authentication mechanisms, users have a role to play in Bluetooth security. One of the primary security measures is increasing the length of PIN. Besides, as Iqbal et al. (2010) advices, a user should not utilize the default PIN of the device. It is recommended that they should regularly change PINs (e.g., each month). Additionally, the Bluetooth connection between two legitimate devices should be done in private. Public places are prone to attacks such as MITM. In an unknown area, users should switch their devices to the non-discoverable state after usage. Bluetooth security is an all-inclusive effort; hence, the Bluetooth SIG should outline the security measures provided by the device.

4.7 Analysis of the Proposed Solutions

In this section, the proposed solution will enable the victims to avoid MITM and DoS attacks. MITM uses the unit key and a fake address when the devices connect. In the scheme proposed by the researcher, one needs to enter a PIN to authenticate the process through a keyed hash algorithm. This key will only be available between the two communicating devices, and it will go through the E3 algorithm to generate the encryption key (Iqbal et al., 2010). The fake devices cannot be able to develop the encryption key of the connecting device. As such, attackers in the middle would not be possible.

With the generation of the device link key, near field communication technologies (such as NFC) should be used to allocate link keys between devices; the peer-to-peer mode of NFC results in the use of separate channels to bond the keys between devices which will occur in Out

of Band signaling (OOB), separately from the Bluetooth radio band. OOB signaling (wireless or wired) will also add its security features and provide maximum protection against MITM attacks.

Additionally, the use of anti-clogging cookies enables the users to minimize the impact of a DoS attack. One goal of these types of attacks is that they occupy computing resources. The cookies ensure the verifier does delegate many resources until the legitimacy of the recipient is confirmed. In authenticated devices, the researchers introduced the one-bit flag. The master device refines this flag to "1" after authenticating a slave device against its MAC address (Iqbal et al., 2010). When the authenticated device attempts to transmit a request to the master device, the connection will halt due to the assumption that it is an attacker.

Another viable solution to MITM & eavesdropping solution for Bluetooth is the application of Giga-IR in the transfer of information. As illustrated by the Infrared Data Association (n.d) in Figure 14 below, and in comparison to the other forms of wave transmission platforms, the technology has low transmission powers. According to Infrared Data Association (n.d), this technology does not create radio frequency (RF) interference and can operate side by side with the RF systems in personal communication networks. All these capabilities make it possible to create a trust protocol as it can increase security and is immune to interferences (IRDA, 2022). The demand for more data transmission capacity has increased as the storage capacity of mobile devices has increased.

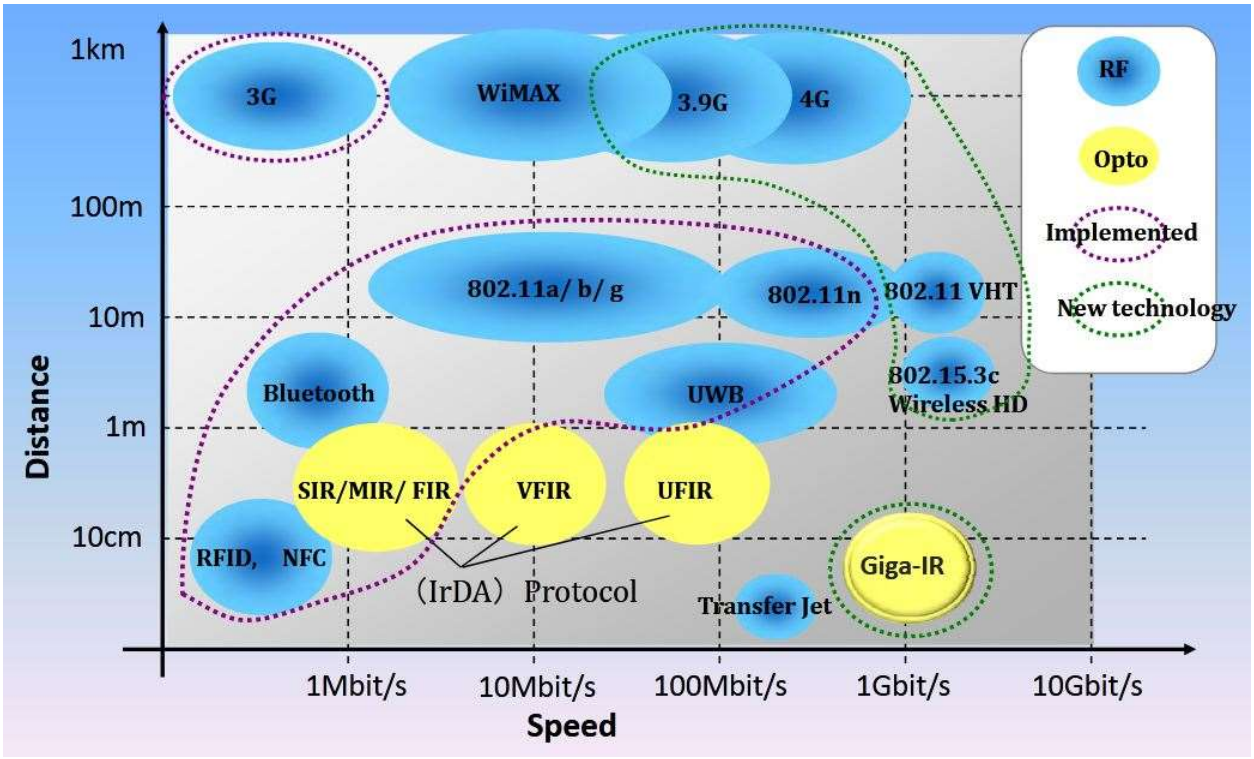


Figure 5: Demonstration of the Speeds of Giga-IR (Infrared Data Association, n.d).

Multi-purpose mobile devices may now snap photos, download movies, music, and videos, and send big data packets across users. To fulfill current demand, the IrDA Giga-IR Special Interest Group (SIG) produced requirements for 1Gbps (125Mbyte/sec) infrared communication (Infrared Data Association, n.d; IRDA, 2022). Giga-IR has been a game-changer in the development of optical communications, and this explains why the Giga-IR SIG is working to achieve even faster optical wireless communication speeds to tackle future difficulties (Destradi et al., 2018; IRDA, 2022). Recent advancements in protocol layers and transceiver designs have made IrDA technology more efficient, allowing it to reach distances of up to 3 meters and allowing for significantly wider angles (Zizyte, 2016). A multinational consortium of technology businesses is leading the current effort to make rates of 5 and 10 Gigabits per second possible using infrared technology.

By enhancing the performance of the current infrared IrDA protocol inherent in many mobile devices such as phones, Giga-IR provides greater data transfer speeds (at least 4 to 10 times quicker than currently) (Aruna & Vetrivelan, 2015; Zizyte, 2016). The inclusion of IrSimple in digital consumer electronics products and home appliances is predicted to result in a major increase in IrSimple applications. High-resolution images shot with a smartphone or digital camera, for example, can be instantaneously transmitted to a flat-panel TV or printer using a simple action comparable to that of remote control (Aruna & Vetrivelan, 2015). Giga-IR improves protocol efficiency by lowering the time it takes for a receiver/transmitter pair to be ready to communicate. Adding and/or modifying software for current IrDA protocols can be used to implement Giga-IR (Zizyte, 2016). Comparison with Existing System The technology is backward consistent with current Giga-IR-enabled telecommunications implemented into devices and sensors (IrDA Protocols).

Gigabit Infrared (Giga-IR): Giga-IR supports 512 Mb/s and 1.024 Gb/s. Line coding in Giga-IR is based on the 8010B DC-balanced encoding scheme, in which a data byte is encoded on a 10-bit character, to facilitate clock recovery at the receiver and to meet the stringer timing requirements of Giga-IR links. The Giga-IR optical transmitter can be either a LED or LD: if a LED is used as the transmitter, then the encoded characters are sent over the infrared link using a four-level ASK modulation format, otherwise if an LD is used as the transmitter, then the modulation format is a two-level (Bora et al., 2012).

4.8 Optical Wireless Solution for Bluetooth Pairing

The underlying concept of optical wireless (OW) is very simple: utilize optical beams to carry data through the atmosphere or vacuum. As a result, OW link architectures are very similar to optical fiber communication point-to-point links, with the exception that no optical fibers are

deployed as a transmission medium. OW is also very similar to RF wireless, but radio waves are replaced with light and antennas with free-space optical transceivers. Despite this superficial resemblance between OW and RF links, OW exhibits several appealing attributes when compared to RF. OW links are inherently broadband and optical frequencies in the infrared and visible spectrum are neither regulated nor licensed. Optical components are also cheaper and consume less electrical power than high-speed RF components. Finally, OW links do not suffer from multipath fading and have much less potential for interference with RF-sensitive electronic systems. These advantages do not, however, imply that OW is a universal replacement for RF communications. The application of OW systems is limited when considering area coverage and user mobility, where RF technologies prove invaluable. In addition, OW systems operate under strict eye safety regulations, while at the same time incoherent OW receivers present lower sensitivity than their RF counterparts because of their photo-electric conversion mechanisms and the impact of ambient light noise sources. To better understand the place of OW systems in the wireless world, technologies are presented with respect to their area of coverage, ranging from a few centimeters in personal communications to over 1 km in outdoor communications, and the data rates they attain, including low-rate legacy links under 1 Mb/s (Bluetooth and older IrDA systems).

Contemporary OW links provide channel rates up to 10 Gb/s, which directly compare to the ones of optical fibers. At the same time, commercial OW links operate at link distances that are challenging to attain in RF (3G/4G) and millimeter-wave (60 GHz) broadband communications. OW is a unique technology that provides an attractive alternative in niche application areas, complementing fiber-optic and RF wireless solutions when they are too costly to deploy. Two mainstream application areas of OW are last-mile broadband access and office

interconnection; both are the business objectives of several components and system manufacturers. In such applications, state-of-the-art OW systems support 10 Gb/s Ethernet, which equals the bandwidth provided by metro fiber optic systems and is significantly higher than the 1.25 Gb/s Ethernet provided by competing RF wireless systems that operate in the 60 GHz frequency range (Bora et al., 2012).

Short-range OW has attracted considerable attention for personal communication systems over the past decade because OW systems offer a viable, low cost and complex, high bandwidth solution to user terminal connectivity. OW provides considerable unlicensed (free) bandwidth in the infrared spectrum, the use of which results in significant cost savings to equipment manufacturers since they do not have to pay an extra fee for using this spectrum and their transceiver designs do not have to strictly conform to spectral masks. Additionally, OW is preferable when health, safety, and aesthetic issues are raised to challenge personal communication systems, since its low transmission powers, short link distances, low profile transceivers, and limited spatial coverage make OW one of the least obtrusive personal network technologies. OW neither suffers from nor directly creates RF interference and OW systems can operate side-by-side with RF systems in personal communication networks. The highspeed electronics that drive OW transmissions must be designed not to be an indirect source of RF interference. Apart from the generic requirements mentioned above, OW has been quite successful in personal communication systems since it exhibits attributes that closely match key requirements in these systems and their applications. From an application perspective, applications like contact information exchange or file transfer between mobile devices are required to have a very short interaction time. In addition, several applications, for instance, secure payment, require increased security and immunity to interference. The short distances

involved and the limited spatial coverage of OW, which results from the narrow beams that are utilized, provide inherent security, and interference rejection, while at the same time allowing for faster completion of the device discovery process that affects the application interaction time. Moreover, the abundant bandwidth of OW transceivers, more than 1 Gb/s at the time of writing of this article, facilitates speedy file transmissions and as a net result, the total interaction time is minimized. The suitability of OW for personal communication systems has drawn the attention of two key players in personal communication systems: IEEE and the Infrared Data Association (IrDA). IEEE had included an OW option in its original 802.11 MAC and PHY standards. The standards defined a wireless communication scheme using diffuse optical channels at 1 and 2 Mb/s. However, they were never updated and are now rendered obsolete. Recently, IEEE launched a separate Task-Group within the framework of 802.15 (IEEE 802.15.7), which is responsible for producing MAC and PHY standards for OW communications based on visible light (Bora et al., 2012).

A possible solution to allow for an optical wireless solution for Bluetooth pairing for security purposes would be to integrate Optical wireless (OW) that uses infrared (IR) waves with Bluetooth devices. With this connection, data that leaves one Bluetooth device leaves as and IR and then is received by another Bluetooth device and converted back to BLE for decoding purpose. Since IR cannot be converted straight into BLE however, it would first be converted to RF so that the flow from one BLE device to the other becomes as illustrated in Figure 18. This could solve the MITM and eavesdropping issue with Bluetooth as Giga-IR that does the in-between transmission and is not easily intercepted as with BLE waves. To achieve IR-RF transmission, Saddam (2016) recommended the use of RF and TSOP Transmitter & Receiver pair. To achieve this pairing, the following components are needed:

- RF Pair (433.92 MHz ASK TX and RX)
- TSOP1738
- Power supply
- IR Remote
- BC557 Transistor
- 100-ohm Resistor
- 1k Resistor
- Breadboard
- Connecting Wires
- 10uf Capacitor

According to Saadam (2016), the operation of this converter is not complicated and starts with the activation of the IR energy transmission. When one presses any button on the IR remote, the TSOP will sense it and transmit it to the RF Transmitter (See Figure 16 below for an illustration of the circuit). The RF transmitter will then convert and send the signal to RF Receiver. The TX-ASK RF transmitter used in this circuit has an Output Power of 4 ~ 12 Dbm, which is based on a 3v ~ 12v power supply (see illustration in Figure 18 below). The transformed RF signal is then received by the RF ASK Receiver, which decodes it and sends it to the LED through the PNP transistor BC557. The LED will now illuminate in response to the incoming signal. The LED is for testing purposes, and you may use any TV/DVD control to check the circuit. The LED should glow when any button on the IR remote is pressed while pointed towards the TSOP1738.

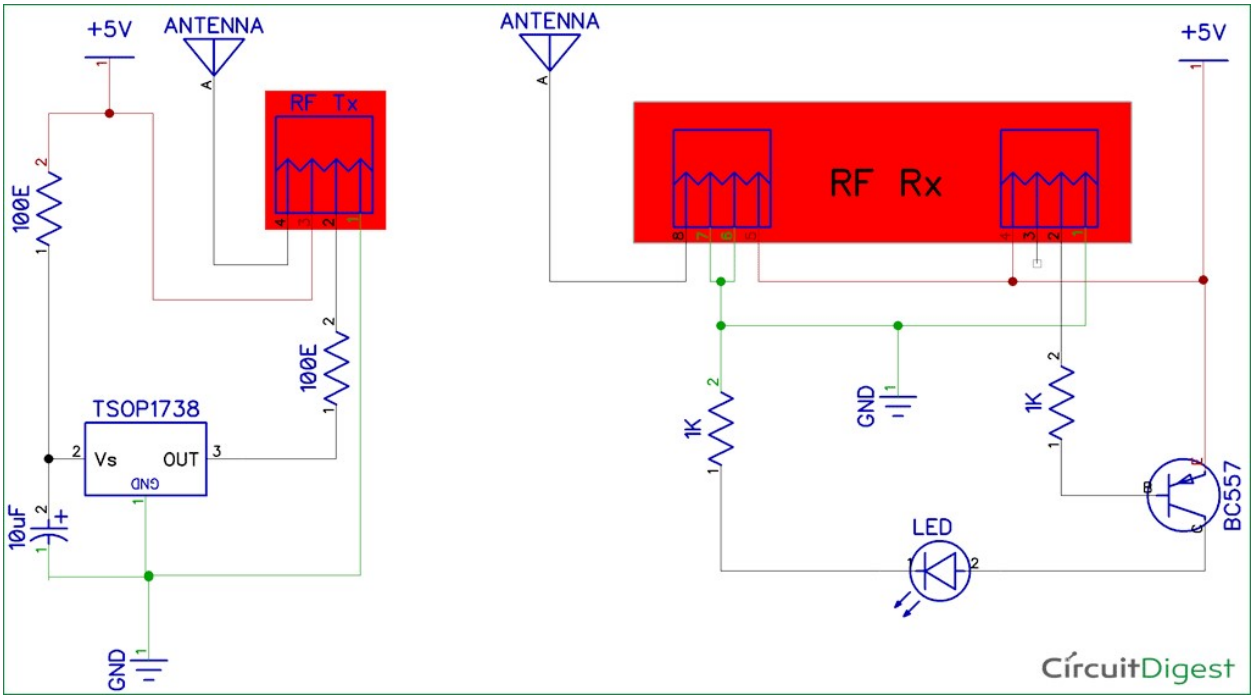


Figure 16: Circuit Diagram Explaining IR-RF conversion using TSOP (Saadam, 2016).

A 100 OHM resistor connects the TSOP output pin to the data pin of the RF module, and a 1K resistor connects the data pin of the RF receiver to the base of the BC557 PNP transistor. The LED is attached to the transistor's collector. The TSOP1738 is used as an infrared detector or receiver in this application (Saddam, 2016). When the TSOP1738 receives IR light encoded at 38 kHz, it reacts, and most TV/DVD remotes work at this frequency. The output of TSOP is active low, which means it remains HIGH when there is no IR and drops low when IR radiation is detected. For wireless RF communication, an RF pair is employed. Other RF modules, such as the 3- Pin RF Module, are also available; consult the datasheet for suitable connections. The ASK Hybrid receiver module used is the one that operates at 433 MHz and an ASK hybrid transmission module.

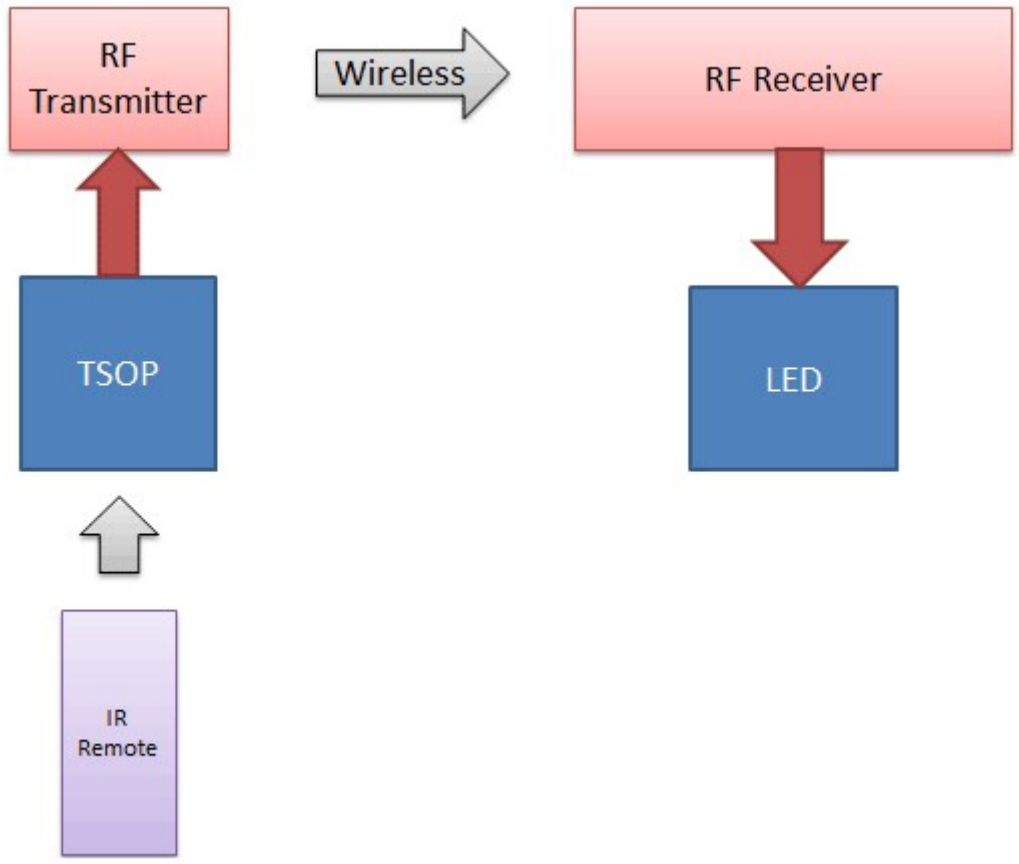


Figure 17: Demonstration of the IR-RF conversion (Saddam, 2016)

The IR Transmitter and IR Receiver are often used to control electronic items wirelessly, primarily via remote control. The best examples of IR transmitters are TV and AC remote controls. The IR receiver in most TVs is the TSOP1738, which detects modulating IR pulses and converts them to an electrical signal (Saddam, 2016). The transmitter is an IR LED, and the receiver is a TSOP1738. IR LEDs emit infrared light, which implies they emit light with a frequency in the infrared spectrum. Infrared light has a wavelength of 700nm – 1mm, which is just beyond visible light. Infrared is emitted by anything that produces heat, including our bodies. Infrared light has the same characteristics as visible light in that it can be focused, reflected, and polarized. Aside from releasing invisible infrared light, the IR LED looks and functions like a regular LED, consuming 20mA current and 3volts of electricity. The light-

emitting angle of IR LEDs is approximately 20-60 degrees, and the range is approximately a few centimeters to several feet, depending on the type of IR transmitter and the vendor. The range of some transmitters is measured in kilometers.

When the HT12D's data pin receives no signal, it enters inactive mode and consumes very little current (less than 1A) at 5V. The signal is transmitted to the HT12D's DIN pin when it is detected by the receiver (pin14). When a signal is received, the HT12D oscillator is activated. The address bits are checked three times by the IC HT12D once the serial data is decoded. The data bits are transmitted to the data pins (pins 10-13) and the VT pin is set to high if these bits match the HT12D's local address pins (pins 1-8). The VT pin (pin17) of the decoder is connected to an LED. This LED indicates that the transfer was successful. The equivalent output is generated by the decoder IC's data pins. A signal is sent by lowering any or all of the pins 10-13 of HT12E, and a similar signal is received at the receiver's end (at HT12D).Both decoder and codec ICs use the first eight pins to configure address bits. To send a specific signal, the address bits at the transmitter and receiver ICs must be the same. By configuring the address bits correctly, a single RF transmitter can control several RF receivers on the same frequency (RF Based Wireless Remote, n.d). In summary, each transmission has 12 bits of data, including 8 address bits and 4 data bits. The signal is obtained at the receiver's end and delivered to the decoder IC. If the address bits are the same, the decoder converts it to parallel data and lowers the corresponding data bits, allowing the LEDs to be powered. The outputs of this system can be used in negative logic, or NOT gates (like the 74LS04) can be used as data pins.

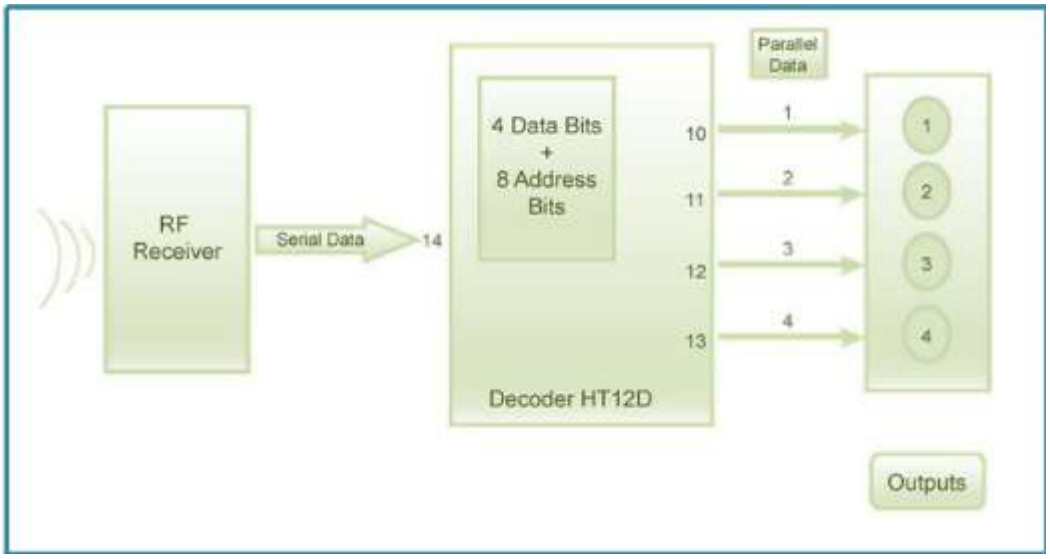


Figure 18: Conversion from RF to Output (RF Based Wireless Remote, n.d).

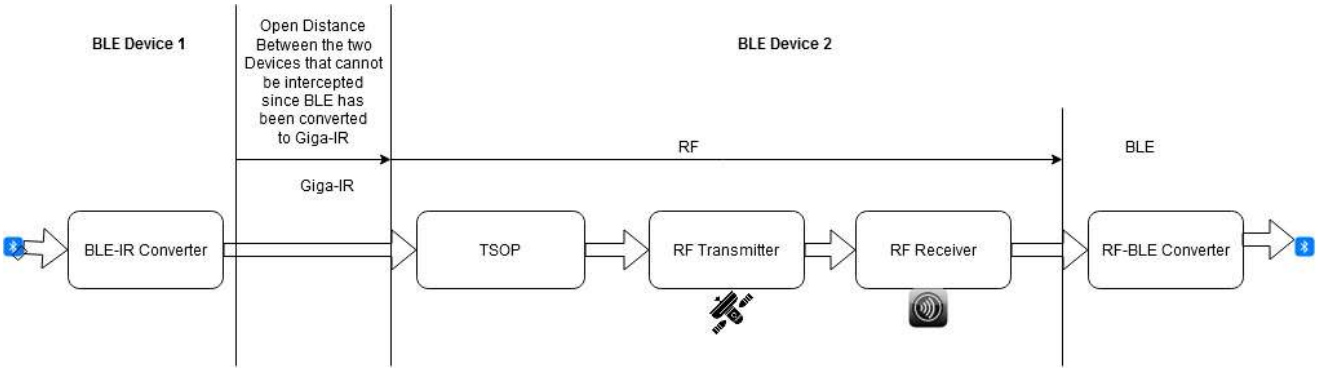


Figure 19: Complete Transmission from Giga-IR to Bluetooth (Created for the purposes of this study)

As presented above in figure 19, the process starts with Bluetooth device one (BLE Device 1) that has a BLE to IR converted. Since IR (Giga-IR) cannot be converted straight to BLE, it if first converted to RF when it gets to the second BLE device. The IR-RF converter (TSOP-RF Transmitter-RF receiver) consists of a pair of 433.92 MHz ASK TX and RX, BC557 Transistor, 100-ohm Resistor, 1k Resistor, Breadboard, Connecting Wires, and 10uf Capacitor. All these are encased into TSOP1738 which transmits its output to the RF transmitter. The RF

transmitter relays the RF to the RF receiver. At the RF receiver, each transmission has 12 bits of data, including 8 address bits and 4 data bits. The decoder IC in the RF receiver records signal received and decodes it. The decoder lowers the data bits corresponding to the address bits if they are the identical, allowing the LEDs to be powered. There are two ways to use this system's outputs: in negative logic or as data pins for NOT gates (like the 74LS04). The RF energy from the RF receiver then moves to the RF-BLE converter, that emits BLE wavelengths.

Chapter 5

Conclusion and Future Work

Bluetooth wireless technology and associated devices are susceptible to many threats, such as denial of service (DoS) attacks, eavesdropping, and man-in-the-middle (MITM) attacks. They are also vulnerable to more specific attacks related to Bluetooth wireless technology that target known vulnerabilities in Bluetooth implementations and specifications. Attacks against improperly secured Bluetooth implementations can provide attackers with unauthorized access to sensitive information and unauthorized use of Bluetooth devices and other systems or networks to which the devices are connected. In the previous chapter, the researcher presented the meta-analysis of Bluetooth architecture systematically, using scholarly sources to critical decrypt its history and application. The problem that inspired the current study was that although the security of Bluetooth technology has improved with the implementation of Bluetooth 4.1 and 4.2 (Gajbhiye et al., 2018), many applications of the technology, such as in automobiles, tend to lag the state-of-the art (Cheah et al., 2017). Moreover, even up-to-date Bluetooth devices may be significantly vulnerable to MITM attacks and other security exploits, with attackers able to steal data or even take control of the device entirely (Melamed, 2018). The range of Bluetooth-enabled devices is only growing at present. This means that these new applications may be at risk because they often use aspects of the technology that have not yet been tested rigorously for vulnerabilities (Tay et al., 2016).

The researcher has explained concepts in the Bluetooth security scheme as well as its vulnerabilities. The researcher also provided recommendations regarding the possible solutions for Bluetooth's weaknesses within the realms of existing literature. It was prudent for the

researcher to understand these concepts through thematic analysis, as they will pilot the drafting of a refined trust protocol. Few scholarly works provided solid solutions to Bluetooth's vulnerability; hence, this study bridged an identified gap and can serve as a foundation for future research. As storage capacity or constraints of device resources is limited in many aspects of Bluetooth wireless technology devices, future scholars could focus on applying technologies such as blockchain or pBFT as Bluetooth wireless technology platform. Such research could address many of the device design capacity challenges and security issues.

Appendix A: Glossary

Selected terms used in this research paper are defined below:

Access Point (AP): A device that logically connects wireless client devices operating in infrastructure to one another and provides access to a distribution system, if connected, which is typically an organization's enterprise wired network.

Ad Hoc Network: A wireless network that allows easy connection establishment between wireless client devices in the same physical area without the use of an infrastructure device, such as an access point or a base station. A wireless ad hoc network is a decentralized type of wireless network. The network is termed as **ad hoc** because it does not rely on a preexisting infrastructure, such as routers in wired networks or access points in wireless networks like WiFi.

Claimant: The Bluetooth device attempting to prove its identity to the verifier during the Bluetooth connection process.

ISM: Industrial, Scientific and Medical radio band. Some of these bands include frequencies in the range of 2.4 GHz, 13.560 MHz, 27.120 MHz, 5.8 GHz, 24.125 GHz and several more. These bands are reserved internationally and do not require any special license to operate. ISM bands are shared by several devices including Remote control toys, cordless phones, near field communication, wireless LAN, etc. Some microwave ovens also generate interference in these bands. Since these bands may be shared by many devices, different wireless technologies employ different mechanisms to combat interference.

Media Access Control (MAC): A unique 48-bit value that is assigned to a particular wireless network interface by the manufacturer.

Piconet: A small Bluetooth network created on an ad hoc basis that includes two or more devices.

Range: The maximum possible distance for communicating with a wireless network infrastructure or wireless client.

Scatternet: A chain of piconets created by allowing one or more Bluetooth devices to each be a slave in one piconet and act as the master for another piconet simultaneously.

A scatternet: allows several devices to be networked over an extended distance.

Verifier: The Bluetooth device that validates the identity of the claimant during the Bluetooth connection process.

Wireless Local Area Network (WLAN): A group of wireless access points and associated infrastructure within a limited geographic area, such as an office building or building campus, that is capable of radio communications. WLANs are usually implemented as extensions of existing wired LANs to provide enhanced user mobility.

Wireless Personal Area Network (WPAN): A small-scale wireless network that requires little or no infrastructure and operates within a short range. A WPAN is typically used by a few devices in a single room instead of connecting the devices with cables.

Appendix B: Acronyms and Abbreviations

Selected acronyms and abbreviations used in this research paper are defined below.

ACL	Asynchronous Connection-Less
ACO	Authenticated Ciphering Offset
AES	Advanced Encryption Standard
AES-CCM	Advanced Encryption Standard–Counter with CBC-MAC
AES-CMAC	Advanced Encryption Standard-Cipher-based Message Authentication Code
AMP	Alternate MAC/PHY
AP	Access Point
ATT	Attribute Protocol
BR	Basic Rate
COF	Ciphering Offset Number
CSA	Core Specification Addendum
CSRK	Connection Signature Resolving Key
DBm	Decibels referenced to one milliwatt
BD-ADDR	Bluetooth Device Address
DHkey	Diffie-Hellman Key
DoS	Denial of Service
ECDH	Elliptic Curve Diffie-Hellman
EDR	Enhanced Data Rate
FHSS	Frequency Hopping Spread Spectrum
FIPS	Federal Information Processing Standard
GFSK	Gaussian Frequency-Shift Keying
GHz	Gigahertz
HCI	Host Controller Interface
HMAC	Hash Message Authentication Code
HS	High-Speed
IEEE	Institute of Electrical and Electronics Engineers
ILK	Intermediate Link Key
ILTK	Intermediate Long-Term Key
IRK	Identity Resolving Key
ISM	Industrial, Scientific, and Medical
kbps	Kilobits per second
KG	Key Generator
KSG	Key Stream Generator
L2CAP	Logical Link Control and Adaptation Protocol
LAN	Local Area Network
LMP	Link Management Protocol

LLP	Link Layer Protocol
LTK	Long-Term Key
MAC	Media Access Control
Mbps	Megabits per second
M	Meter
MHz	Megahertz
MIC	Message Integrity Check
MITM	Man-in-the-Middle
mW	Milliwatt
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
OBEX	Object Exchange
OOB	Out of Band
PC	Personal Computer
PHY	Physical Layer
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PPP	Point-to-Point
PRNG	Pseudo-Random Number Generator
Rand	Random Number
RF	Radio Frequency
RFCOMM	Radio Frequency Communication Protocol
RNG	Random Number Generator
RPA	Resolvable Private Address
RSSI	Received Signal Strength Indication
SAFER	Secure and Fast Encryption Routine
SDP	Service Discovery Protocol
SHA	Secure Hash Algorithm
SIG	Special Interest Group
SRES	Signed Response
SSP	Secure Simple Pairing
STK	Short Term Key
TCP	Telephony Control Protocol
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TK	Temporary Key
UUID	Universally Unique Identifier
WAP	Wireless Access Point
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network

Appendix C: Selected Bluetooth Wireless Networking Functions

d1	Diversifying function based on AES-128 encryption, used in Legacy Low Energy key generation.
E0	Stream cipher used to encrypt Bluetooth packet payloads.
E1	Bluetooth legacy authentication function based.
E3	Bluetooth key generation function.
E21	Link key generator function, used when generating a key from the 48-bit address
E22	Link key generator function, used when generating a key from the user PIN
f2	BR/EDR and AMP Link key generator function
f3	Simple Pairing check function, used to compute confirmation values
f5	Low Energy Secure Connections key generation function
f6	Low Energy Secure Connections DHKey check generation function
h4	Secure Connections Device Authentication Key generation function
h5	Secure Connections Device Confirmation function
h6	Second Link Key Conversion function, used to create the Low Energy key derivation from a Bluetooth BR/EDR key
h7	First Link Key Conversion function, used to create the Low Energy long term key derivation from a Bluetooth BR/EDR key

References

Aissi, S., Gehrmann, C., & Nyberg, K. (2004, April 19–23). *Proposal for enhancing Bluetooth security using an improved pairing mechanism.* Bluetooth Architecture Review Board at the Bluetooth All–Hands Meeting.

Albahar, M. (2017). *Bluetooth pairing security threats and countermeasures* [Doctoral dissertation, University of Eastern Finland].

Alfaiate, J., & Fonseca, J. (2012, June). Bluetooth security analysis for mobile phones. In *Proceedings of the 2012 7th Iberian Conference on Information Systems and Technologies* (pp. 1–6). IEEE.

Aruna, P., & Vetrivelan, N. (2015). Survey and Comparative Study of Wireless Technologies for Enhanced MANET. International Journal of Applied Engineering Research, 10 (10), pp. 25617-25627

Barnickel, J., Wang, J., & Meyer, U. (2012, June). Implementing an attack on Bluetooth 2.1+ secure, simple pairing in passkey entry mode. In *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications* (pp. 17–24). IEEE.

Becker, A., & Paar, I. C. (2007). *Bluetooth security & hacks.* Ruhr-Universität Bochum.

Bello, G. (2017). *Bluetooth low energy: Secure or unsecure?* [Master's thesis, Columbus State University].

Bisdikian, C. (2001). An overview of the Bluetooth wireless technology. In *Proceedings of IEEE Communications Magazine* (pp. 86–94). IEEE.

Borah, D., Boucouvalas, A., Davis, C., Hranilovic, S., & Yiannopoulos, K., (2012). A Review of Communication – Oriented Optical Wireless Systems. Journal on Wireless Communications and Networking 2012

Boucouvalas, C., & Huang, P. (2009). OBEX over IrDA: Performance analysis and optimization by considering multiple applications. *IEEE/ACM Transactions on Networking, 14*(6).

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Cha, S. C., Yeh, K. H., & Chen, J. F. (2017). Toward a robust security paradigm for Bluetooth low energy-based smart objects in the Internet-of-things. *Sensors*, *17*(10), 2348. https://doi.org/10.3390/s17102348

Chang, R., & Shmatikov, V. (2007). Formal analysis of authentication in Bluetooth device pairing. In *Proceedings of LICS/ICALP Workshop on Foundations of Computer Security and Automated Reasoning for Security Protocol Analysis* (FCSARSPA '07).

Cheah, M., Bryans, J., Fowler, D. S., & Shaikh, S. A. (2017, June). Threat intelligence for Bluetooth-enabled systems with automotive applications: An empirical study. In *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop* (pp. 36–43). IEEE. https://doi.org/10.1109/DSN-W.2017.22

Ching, K. W., & Singh, M. M. (2016). Wearable technology devices security and privacy vulnerability analysis. *International Journal of Network Security and its Applications*, *8*(3), 19–30. https://doi.org/10.5121/ijnsa.2016.8302

Clarke, V., & Braun, V. (2013). Teaching thematic analysis: Overcoming challenges and developing strategies for effective learning. *Psychologist*, *26*(2), 120–123. https://thepsychologist.bps.org.uk/

Cope, P., Campbell, J., & Hayajneh, T. (2017, January). An investigation of Bluetooth security vulnerabilities. In *Computing and Communication Workshop and Conference (CCWC), 2017 IEEE 7th Annual* (pp. 1–7). IEEE. https://doi.org/10.1109/CCWC.2017.7868416

Dahiya, M. (2017). A short range wireless network: Bluetooth. *International Journal of Advanced Research in Computer Science*, *8*(3). http://www.ijarcs.info/index.php/Ijarcs

Das, A. K., Pathak, P. H., Chuah, C.-N., & Mohapatra, P. (2016). Uncovering privacy leakage in BLE network traffic of wearable fitness trackers. In *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications* (pp. 99–104). ACM.

Das, S. (2015). *Link management security in Bluetooth* [Doctoral dissertation, National Institute of Technology Rourkela].

Do, Q., Martini, B., & Choo, K. K. R. (2017). Is the data on your wearable device secure? An Android Wear smartwatch case study. *Software: Practice and Experience*, *47*(3), 391–403. https://doi.org/10.1002/spe.2414

Faragher, R., & Harle, R. (2015). Location fingerprinting with Bluetooth low energy beacons. *IEEE Journal on Selected Areas in Communications*, *33*(11), 2418–2428. https://doi.org/10.1109/JSAC.2015.2430281

Feng, W., Arumugam, N., & Krishna, G. H. (2002, November). Impact of interference on a Bluetooth network in the 2.4 GHz ISM band. In *8th International Conference on Communication Systems* (Vol. 2, pp. 820–823). IEEE.

Frisby, J., Smith, V., Traub, S., & Patel, V. L. (2017). Contextual computing: A Bluetooth based approach for tracking healthcare providers in the emergency room. *Journal of Biomedical Informatics*, *65*, 97–104. https://doi.org/10.1016/j.jbi.2016.11.008

Gajbhiye, S., Karmakar, S., Sharma, M., & Sharma, S. (2018). Two-party secure connection in Bluetooth-enabled devices. *Information Security Journal: A Global Perspective*, *27*(1), 42–56. https://doi.org/10.1080/19393555.2018.1423714

Gehrmann, C., & Nyberg, K. (2001, November). Enhancements to Bluetooth baseband security. In *Proceedings of Nordsec* (Vol. 2001, pp. 191–230). Nordsec.

Giousouf, A., & Lemke, K. (n.d.). *Bluetooth security*. Communication Security Department, Ruhr University, Bochum.

Grabovica, M., Popić, S., Pezer, D., & Knežević, V. (2016, June). Provided security measures of enabling technologies in the Internet of Things (IoT): A survey. In *Zooming Innovation in Consumer Electronics International Conference* (pp. 28–31). IEEE. https://doi.org/10.1109/ZINC.2016.7513647

Gupta, N. (2016). *Inside Bluetooth low* energy (2nd ed.). Artech House.

Haataja, K. (2005). Bluetooth network vulnerability to disclosure, integrity, and denial of service attacks. *Proceedings of the Annual Finnish Data Processing Week at the University of Petrozavodsk: Advances in Methods of Modern Technology, 7,* 63–103.

Haataja, K., & Toivanen, P. (2008, October). Practical man-in-the-middle attacks against Bluetooth secure, simple pairing. In *4th International Conference on Wireless Communications, Networking and Mobile Computing* (pp. 1–5). IEEE.

Haataja, K., & Toivanen, P. (2010, January). Two Practical man-in-the-middle attacks on Bluetooth secure simple pairing and counter measures. IEEE transactions on Wireless Communications (Vol, 9, No, 1, January 2010). IEEE.

Han, T., & Ding, L. (2017, August). Design and implementation of Bluetooth beacon in the mobile payment system. In *AIP Conference Proceedings* (Vol. 1864, No. 1, p. 020019). AIP Publishing. https://doi.org/10.1063/1.4992836

Hasan, R., Zawoad, S., Noor, S., Haque, M. M., & Burke, D. (2016, June). How secure is the healthcare network from insider attacks? An audit guideline for vulnerability analysis. In *Computer Software and Applications Conference (COMPSAC), 2016 IEEE 40th Annual* (Vol. 1, pp. 417–422). IEEE.

Hassan, S. S., Bibon, S. D., Hossain, M. S., & Atiquzzaman, M. (2017). Security threats in Bluetooth technology. *Computers & Security*, *74*, 308–322. https://doi.org/10.1016/j.cose.2017.03.008

Hassan, S. S., Bibon, S. D., Hossain, M. S., & Atiquzzaman, M. (2018). Security threats in Bluetooth technology. *Computers & Security*, *74*, 308–322. https://www.journals.elsevier.com/computers-and-security

Hermelin, M., & Nyberg, K. (1999, December). Correlation properties of the Bluetooth combiner. In *International Conference on Information Security and Cryptology* (pp. 17–29). Springer, Berlin, Heidelberg.

Infrared Data Association (n.d). Giga-IR High Speed Optical Communication. Retrieved from: https://www.soumu.go.jp/soutsu/kinki/studygroup/2009/THz/3_1.pdf

Imgraben, J., Engelbrecht, A., & Choo, K. K. R. (2014). Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. *Behaviour & Information Technology*, *33*(12), 1347–1360. https://doi.org/10.1080/0144929X.2014.934286

Iqbal, M. M. W., Kausar, F., & Wahla, M. A. (2010, June). Attacks on Bluetooth security architecture and its countermeasures. In *International Conference on Information Security and Assurance* (pp. 190–197). Springer.

IRDA (2022). IrSimple Specifications. Retrieved from: http://www.irdajp.org/irsimple/

Jakobsson, M., & Wetzel, S. (2001, April). Security weaknesses in Bluetooth. In *Cryptographers' Track at the RSA Conference* (pp. 176–191). Springer.

Jeong, H. D. J., Lee, W., Lim, J., & Hyun, W. (2015). Utilizing a Bluetooth remote lock system for a smartphone. *Pervasive and Mobile Computing*, *24*, 150–165. https://doi.org/10.1016/j.pmcj.2015.07.010

Kaushik, S., Poonia, R. C., & Khatri, S. K. (2017). Comparative study of various protocols of DDS. *Journal of Statistics and Management Systems*, *20*(4), 647–658. https://doi.org/10.1080/09720510.2017.1395184

Kim, H., Dabbous, W., & Afifi, H. (2005, June). A bypassing security model for anonymous Bluetooth peers. In *2005 International Conference on Wireless Networks, Communications and Mobile Computing* (Vol. 1, pp. 310–315). IEEE.

Kiruba, K., Neelaveni, R., & Shaimila, R. (2009, June 4–6). Bluetooth man-in-the-middle attack based on secure simple pairing using out of band association model. In *International Conference on Control, Automation, Communication and Energy Conversation.* IEEE.

Khatod, V., & Manolova, A. (2020). Effects of man in the middle (MITM) attack on bit error rate of Bluetooth system. In *2020 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering* (pp. 153–157). ECTI DAMT & NCON.

Kügler, D. (2003). “Man in the middle” attacks on Bluetooth. In *Financial cryptography, lecture notes in computer science* (Vol. 2742, pp. 149–161). Springer.

Kui, M., & Xiuying, C. (2003). Research of Bluetooth security manager. In *Proceedings of the International Conference on Neural Networks and Signal Processing*. IEEE.

Kumar, M. (2014, December). Security issues and privacy concerns in the implementation of wireless body area networks. In *2014 International Conference on Information Technology* (pp. 58–62). IEEE. https://doi.org/10.1109/ICIT.2014.73

Kumar, M., & Gupta, B. K. (2015). Security for Bluetooth enabled devices using BlipTrack Bluetooth detector. In *Proceedings of the International Conference on Advances in Computer Engineering and Applications.* IEEE.

Kumar, N. V., Bhuvana, C., & Anushy, A. S. (2017). Comparison of Zigbee and Bluetooth wireless technologies. In *International Conference on Information, Communication, & Embedded Systems.* World Academy of Science, Engineering and Technology.

Kumar, T. (2009). Improving the pairing mechanism in Bluetooth security. *International Journal on Recent Trends in Engineering*, *2*(2). http://journalseek.net/cgi-bin/journalseek/journalsearch.cgi?field=issn&query=2158-5555

Lindell, A. Y. (2008). *Attacks on the pairing protocol of Bluetooth v2.1.* Black Hat.

Lonzetta, A. M., Cope, P., Campbell, J., Mohd, B. J., & Hayajneh, T. (2018). Security vulnerabilities in Bluetooth technology as used in IoT. *Journal of Sensor and Actuator Networks*, *7*(3), 28.

Lu, Y., Meier, W., & Vaudenay, S. (2005, August). The conditional correlation attack: A practical attack on Bluetooth encryption. In *Annual International Cryptology Conference* (pp. 97–117). Springer.

Melamed, T. (2018). An active man-in-the-middle attack on Bluetooth smart devices. *International Journal of Safety and Security Engineering*, *8*(2), 200–211. https://doi.org/10.2495/SAFE-V8-N2-200-211

Mikhaylov, K., Plevritakis, N., & Tervonen, J. (2013). Performance analysis and comparison of Bluetooth Low Energy with IEEE 802.15. 4 and SimpliciTI. *Journal of Sensor and Actuator Networks*, *2*(3), 589–613.

Mutchukota, T. R., Panigrahy, S. K., & Jena, S. K. (2011, August). Man-in-the-middle attack and its countermeasure in Bluetooth secure, simple pairing. In *International Conference on Information Processing* (pp. 367–376). Springer.

Nair, K. K., Helberg, A., & Van Der Merwe, J. (2015). *Intrusion detection in Bluetooth enabled mobile phones* (pp. 1–8). IEEE. https://doi.org/10.1109/ISSA.2015.7335048

Nateq Be-Nazir, I. M., & Tarique, M. (2012). Bluetooth security threats and solutions: A survey. *International Journal of Distributed and Parallel Systems, 3*, 127. https://airccse.org/journal/ijdps/ijdps.html

Noor, N. M., Kamardin, K., Daud, S. M., Sjarif, N. A., Ahmad, N. A., Azmi, A., & Sam, S. M. (2018). External attacks on automotive system through wireless communication channels. *Journal of Fundamental and Applied Sciences*, *10*(2S), 11–23. https://doi.org/10.4314/jfas.v10i2s.2

Padgette, J., Scarfone, K., & Chen, L. (2012). Guide to Bluetooth security. *NIST Special Publication*, *800*(121), 25. https://www.nist.gov/nist-pub-series/special-publication-nist

Pallavi, S., & Narayanan, A. (2019). An overview of practical attacks on BLE based IoT Devices and their security. In *5th International Conference on Advanced Computing & Communication Systems.* IEEE.

Panse, T., & Panse, P. (2013). A survey on security threats and vulnerability attacks on Bluetooth communication. *International Journal of Computer Science and Information Technologies*, *4*(5), 741–746. http://ijcsit.com/

RF Based Wireless Remote (n.d). Retrieved from: https://www.elementzonline.com/downloads/RF_Based_Wireless_Remote.pdf

Ryan, M. (2013). How Smart is Bluetooth Smart. *SchmooCon 9*.

Saddam (2016). IR to RF Converter Circuit. Retrieved from: https://circuitdigest.com/electronic-circuits/ir-to-rf-converter-circuit-diagram

Sandhya, S., & Devi, K. A. S. (2012). Analysis of Bluetooth threats and v4.0 security features. In *International Conference on Computing, Communication, and Applications* (pp. 1–4).

Sandhya, S., & Devi, K. A. S. (2013). Performance evaluation of crypt analytical approaches in Bluetooth networks. *International Journal of Application or Innovation in Engineering & Management, 2*(7), 403–408. https://www.ijaiem.org/

Sandhya, S., & Devi, K. A. S. (2014). A lightweight paradigm for security in Bluetooth. *International Journal of Advanced Research in Computer Engineering & Technology, 3*(4), 1536–1540. http://ijarcet.org/

Satam, P., Satam, S., & Hariri, S. (2018). *Bluetooth intrusion detection system (BIDS).* IEEE.

Sayegh, A. A., & El-Hadidi, M. T. (2005, September). A modified secure remote password (SRP) protocol for key initialization and exchange in Bluetooth systems. In *First International Conference on Security and Privacy for Emerging Areas in Communications Networks* (pp. 261–269). IEEE.

Shaked, Y., & Wool, A. (2005, June). Cracking the Bluetooth pin. In *Proceedings of the 3rd International Conference on Mobile Systems, Applications, and Services* (pp. 39–50).

Singelée, D., & Preneel, B. (2004). *Security overview of Bluetooth* [Technical Report]. COSIC.

Soriente, C., Tsudik, G., & Uzun, E. (2009). Secure pairing of interface constrained devices. *International Journal of Security and Networks*, *4*(1–2), 17–26. https://www.inderscience.com/jhome.php?jcode=ijsn

Sun, D. Z., Mu, Y., & Susilo, W. (2018). Man-in-the-middle attacks on Secure Simple Pairing in Bluetooth standard V5. 0 and its countermeasure. *Personal and Ubiquitous Computing*, *22*(1), 55–67. https://www.springer.com/journal/779

Tay, H. J., Tan, J., & Narasimhan, P. (2016). *A survey of security vulnerabilities in Bluetooth low energy beacons.* Carnegie University Parallel Data Laboratory.

Thomas, J., & Harden, A. (2008). Methods for the thematic synthesis of qualitative research in systematic reviews. *BMC Medical Research Methodology*, *8*(1), 45. https://bmcmedresmethodol.biomedcentral.com/

Thompson, B., Morris-King, J., & Harang, R. (2016, November). Slowing the spread of Bluetooth-based malware in mobile tactical networks. In *Proceedings of the 2016 Military Communications Conference* (pp. 485–490). IEEE. https://doi.org/10.1109/MILCOM.2016.7795374

Trifinite. (n.d.). *BlueBump.* https://trifinite.org/trifinite_stuff_bluebump.html

Vaishnavi, V. K., & Kuechler, W. (2015). *Design science research methods and patterns: innovating information and communication technology*. CRC Press.

Yeh, T. C., Peng, J. R., Wang, S. S., & Hsu, J. P. (2012). Securing Bluetooth communications. *International Journal of Network Security, 14*(4), 229–235.

Yurdagul & Sencar, (2021), BLEKeeper: Response Time Behavior Based Man-In-The-Middle Attack Detection, *IEEE Symposium in Security and Privacy workshops*

Zegeye, W. K. (2015). *Exploiting Bluetooth low energy pairing vulnerability in telemedicine.* International Foundation for Telemetering.

Zizyte, M. (2016). Bluetooth & CAN. Retrieved from: https://users.ece.cmu.edu/~koopman/ece348/lectures/24_embedded_networks.pdf

Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE*, *104*(9), 1727–1765. https://doi.org/10.1109/JPROC.2016.2558521