International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

Research Article

Eavesdropping in Bluetooth networks

Maruf Farhan* **and Dr. Nasr Abosata**

Department of Engineering and Computers, Northumbria University, London, UK.

Received 05 March 2023, Accepted 25 March 2023, Available online 28 March 2023, **Vol.13, No.2 (March/April 2023)**

Abstract

Bluetooth eavesdropping refers to the unauthorized access and monitoring of Bluetooth communications. This can be done through the use of specialized software and hardware tools that can intercept and analyze Bluetooth traffic. Bluetooth eavesdropping can be used to gain access to sensitive information, such as personal data, login credentials, and financial information, and can also be used to launch attacks on Bluetooth-enabled devices. To prevent Bluetooth eavesdropping, it is important to use strong encryption and authentication methods, as well as to keep Bluetooth-enabled devices in non-discoverable mode when not in use. Additionally, it is important to be aware of the presence of unauthorized devices in the vicinity, and to avoid pairing with unknown devices. This research paper aims to figure out how easy it is to break into Bluetooth networks and listen in on conversations. So, the technical details of this vulnerability will be looked at, as well as how cybercriminals use this type of network intrusion, how it influences network security and the hazards that eavesdropping in Bluetooth networks provides to an organization's networks or other sorts of enterprises.

Keywords: *Bluetooth, Security, Eavesdropping, Vulnerability, wireless*

1. Introduction

Bluetooth is a technical standard that enables electronic devices to communicate wirelessly over a short distance with one another. The Bluetooth SIG (Special Interest Group) issued the Bluetooth 1.0 standards in 1999. Almost two billion Bluetooth-enabled items were delivered in the first ten years of the protocol's existence [1]. That is not to say, however, that Bluetooth is the only technology on the market. ZigBee is a wireless standard introduced in 2005 and governed by the ZigBee Alliance. It enables transmissions to take place over greater distances, up to 100 meters, while simultaneously consuming less power [2]. Bluetooth is utilized in various consumer electronics, and without Bluetooth, it is impossible to imagine the existence of smartphones, tablets, or laptops. Bluetooth devices may be classified into 3 classes: Class I, II, and III. The three main power classes often used to characterize Bluetooth devices are broken down and compared in Table 1. When two devices from different categories are paired together, the maximum communication distance is determined by the one that has the shorter range [3].

Table 1: Classes of Bluetooth devices. Source: SANS Technology institute [3]

Class	Maximum Transmitted Power	Maximum Range	Application
I	100	100	Laptops, Desktop PC
II	2.5	10	Mobile Phones, Headsets
III	1	<10	Bluetooth Adapters

Bluetooth has become popular, and every IoT device and smartphone uses Bluetooth technology. So as a result, it attracts hackers to make attack Bluetooth devices. Those who want to share files, audio, and other things first make a connection to primary devices, and both devices send an address known as BD_ADDR. Hackers were drawn to Bluetooth as its popularity increased because they saw it as an opportunity to break into devices and launch attacks. A BD_ADDR is a unique address transmitted by a Bluetooth device during communication, allowing other devices to find and establish a connection for file /sharing, phonebook access, and other purposes. Even now, anyone can eavesdrop with tools such as a Car whisperer. The proper hardware setup is required to make a breakthrough in the system [4]. Any intermediary device in a network between a sender and a receiver is vulnerable to an eavesdropping attack

*Corresponding author's ORCID ID: 0000-0000-0000-0000
DOI: https://doi.org/10.14741/ijcet/v.13.2.5

[5]. Bluetooth's ability to maximize both active and passive eavesdropping makes it a popular form of network intrusion.

Bluetooth Hacker disguises himseslf when eavesdropping. On passive eavesdropping, the hacker "listens" to Bluetooth data. Network security experts recommend encrypting devices, updating them, and monitoring network malware.

So, in this research paper, I will review previous literature on Bluetooth eavesdropping and other attacks by attackers. After the review, I will propose risk assessment and mitigation to reduce such vulnerabilities.

2. Bluetooth Protocol Stack

A protocol stack is a group of software and hardware that works together to run authentic protocols according to the standard. The standard says how different devices should talk to each other.

•**Bluetooth Radio**: a wireless device network that can communicate by radio waves and hopping frequencies.
•**Baseband:** Piconet-related issues include but are not limited to connection establishment, addressing, packet format, timing, and power management.
• **Link manager protocol (LMP):** This protocol is responsible for link setup and configuration between Bluetooth devices. It can also control and negotiate the size of the baseband packet.

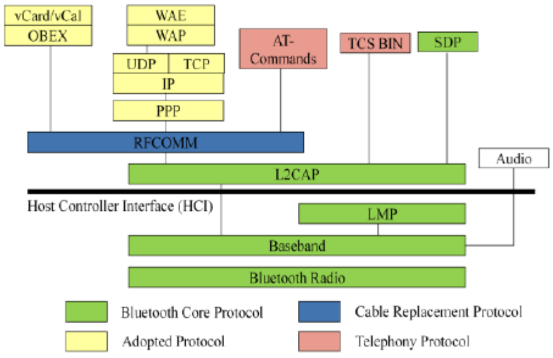

Figure 1. Bluetooth protocol stack [31]

• **Logical link control and adaptation protocol** (L2CAP): customize the top layers' protocols to fit the needs of the baseband layer. Offers services that do not require a connection in addition to those that do require a connection.
• **Service discovery protocol (SDP**): Whenever two or more Bluetooth devices are in the range of one another, this protocol handles exchanges of device data, service requests, and questions about service characteristics.
• **Host Controller Interface (HCI):** offers a means of interaction with the Bluetooth device to access its features. The Baseband controller and link manager are both connected to its command interface.

• **TCS BIN (Telephony Control Service**): binary protocol for controlling B.T. communications (voice and data).
• **OBEX (OBject Exchange):** a method of facilitating the transfer of binary objects from one device to another through a communications protocol.
• **RFCOMM**: Simple transport protocol that emulates RS232 serial ports using L2CAP
• **WAE/WAP:** protects information from being compromised due to eavesdropping by limiting access to only authorized devices.

Bluetooth Protocol

The Bluetooth protocol, also known as IEEE 802.15.1, is a form of wireless communication that is meant to work in the ISM band of 2.4 GHz and has a short range (up to 100 meters) [6, 8 Bluetooth technology operates in a Master/Slave architecture and uses FHSS to transmit over 79 different frequencies as we know that FHSS is very much valuable for counter eavesdropping. A Piconet can be formed by connecting no more than seven slave devices to a single master. As seen in figure 1, a slave device can function as a component of more than one Piconet to form a scatternet. The BD ADDR is the physical address used to identify each Bluetooth device in a Piconet.

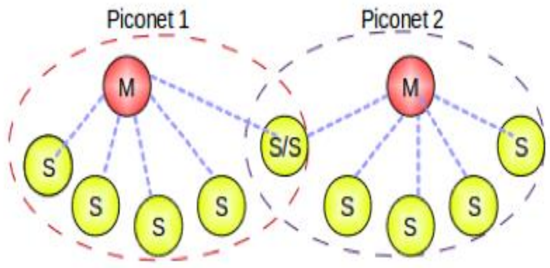

Figure 2: Piconet [32]

When a piece of hardware connects to a Bluetooth network, it immediately initiates several different modes of operation. These modes range from low-power states such as a park, hold, and sniff to active forms such as TxRx and Inquire. As seen in Figure 2, the state transition machine is followed by devices working within a Bluetooth network.

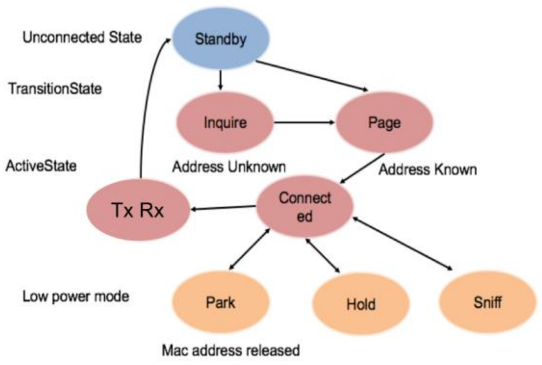

Figure 3: Bluetooth state transition diagram [32]

Bluetooth Security Features

The Bluetooth standard specifies five critical safety features:

•**Authentication**: Validating the authenticity of interacting devices may be done using their Bluetooth addresses. Bluetooth does not have a built-in authentication system for users [33].
•**Confidentiality**: safeguarding sensitive data from snooping by limiting access to only approved devices [33].
•**Authorization**: enabling the control of resources by checking to see whether a device has been granted permission to utilize a service before granting permission for it to do so [33].
•**Message Integrity**: authentication of a Bluetooth transmission to ensure it has not been tampered with while in transit [33].
Pairing/Bonding: To establish a trusted device pair, generating and storing one or more shared secret keys is necessary [33].

3. Literature review

Although Bluetooth is simple to set up and adapt, the technology has some concerns. When Bluetooth headsets are used, eavesdropping is one of the security risks that could happen. Even though this technology has been changed and improved many times, hackers always find a way to break it [7].

Hackers use an eavesdropping attack to listen in on data as it moves through the network. This gives them access to credit card numbers, passwords, and personal information [8]. Two types of eavesdropping attacks exist that is passive eavesdropping and active eavesdropping. With active eavesdropping, the attacker hides, enabling them to imitate a website where users typically share private information [8]. Passive eavesdropping may readily transform into an active MitM attack, allowing a potential hacker to listen to the transmission and intercept and change the contents [9]. Most mobile users are still unaware of the security risks posed by the technology and do not even view the consequences of such attacks as a top priority [10]. The attacker hacks mobile network services like texting, downloading multimedia, and calling without the victim's consent. Such abilities can be used to cover up a terrorist attack. With service theft, hackers can transform mobile devices into hacking devices to eavesdrop and record conversations [10].

However, Bluetooth devices' software will not be perfect, especially the newer specification Bluetooth 4.0. To overcome this threat, it is suggested that if you are not using Bluetooth, turn it off immediately and stop buying those devices that use Bluetooth 1. x,2.0, or 4.0-LE [11].

Adam Laurie of A.L. Digital Ltd. discovered a security flaw in Bluetooth-enabled mobile devices; he labeled it "Bluebug." Bluebugging is a type of hacking that enables an unauthorized third party to access your device by exploiting any discoverable vulnerabilities in its Bluetooth connection. A hacker can intercept your calls, read and send messages, and steal your contact list through "blue bugging" [12]. However, hackers can eavesdrop and get access to all the devices and messages with the Bluetooth pin crack method. This Bluetooth pin cracking method is not software-based but an algebra-based method where an attacker can locate the P.I.N. during the pairing device process with the help of an algebra solution cryptographic primitive SAFER [13].

4. Technical background of the Vulnerabilities

In table 2. I have shown the classification of Bluetooth attacks with the severity. We all know how much impact these attacks can have on the user. I have also demonstrated the effects of attacks in table 2. Based on their severity, these assaults are categorized as either "high," "middle," or "low.". When the attack level is "High," the attacker has total control over the device they are targeting, allowing them to take data from the memory or external storage or edit or delete it. As a consequence of this, the victim may potentially suffer financial damage as a result of the threats. When the severity is set to "Medium," it is possible for attackers to steal data and obtain required information from a target device while Bluetooth data is being transferred. Attacks that follow, monitor, or bother the target are low severity [14].

Table 2: Severity of Bluetooth attacks

High Severity	Medium Severity	Low Severity
Pin Cracking attack	Mitm Attack	Blue chop
Off-line Pin recovery	Relay attack	DoS attacks
Backdoor attack	Mac address spoofing attack	Blue printing
Blue snarfing	Forced re-pairing attack	Blue stumbling
Blue snarfing	Blue force attack	Blue tracking
Blue bugging	bump	Blue jacking
Free calling		
Car whisperer		

Man in the Middle Attack

Hackers created phony access points to access and manipulate the data. First and foremost, the attacker must ensure that the target endpoints employ the identical hopping sequence. This makes it easy for the attacker to break the security of the transmission [15]. The attacker listens in on the conversation between two devices and changes the data they get, as shown in

Fig. 6. The attacker gets between the two devices in a way that makes the victims honestly believe nothing is wrong. In this attack, the attacker can't get into the devices of the people being attacked. The attacker can only see the information that is sent [15]. Flaws in the pairing process can also lead to a "man in the middle" attack, in which one device attempts to connect with another but ends up doing so with the wrong device [16][17].

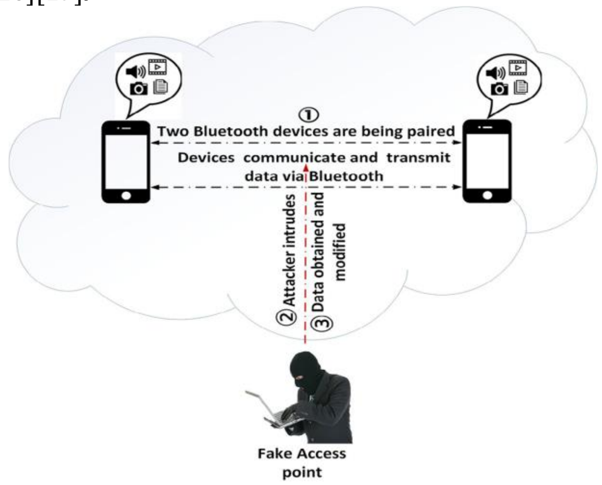
① Two Bluetooth devices are being paired
Devices communicate and transmit data via Bluetooth
② Attacker intrudes
③ Data obtained and modified
Fake Access point

Fig.6: MITM Attack [14]

Replay Attack: A replay attack is a common attack on wireless communications. In this attack, the attacker first intercepts legitimate communication packets and then re-transmits those packets at a later time [18] to cause harm. Before an attacker can carry out a relay attack, they need to begin by connecting two fake devices to both of the victim devices. The victims are oblivious to this fact and continue to believe they are communicating with one another. However, victims send information to the devices used by attackers. As a direct consequence of this, the attack goes undetected. The term "Relay attack" is synonymous with "Reflection attack." The victim devices are constantly provided feedback from the attacking devices, which listen in on the conversation [19].

Headset profile attack: These devices have a pairing PIN. by default (typically 0000). Because the security isn't perfect, it's easy for someone to break in and use the device or listen in on private conversations. Also, some headsets, like the San Francisco Aliph Jawbone, accept requests to pair from unknown devices, even in a non-discoverable mode [24]. When the headset is not being used, To get access to the device, a hacker needs only to know the device's BD ADDR and the preset PIN. and make a sophisticated listening device using a laptop that looks like a phone [27].

Apart from that there are several methods which can be used to perform eavesdropping on the Bluetooth communication such as:

Bluejacking: Hacker send unsolited message or business cards to nearby Bluetooth enabled devices. This may not be harmful, but it can be exploited to get device access for future attacks.

Bluesnarfing: Hacker use Bluetooth sniffer to scan for and connect to nearby Bluetooth devices and them try to exact valuable information from the device.

Bluebugging: hacker gains unauthorized access to a Bluetooth-enabled device and is able to control it remotely. This can include making phone calls, sending text messages, and accessing stored information on the device.

5. Risk Assessment

There are numerous different ways that hackers can access Bluetooth networks and eavesdrop. In the last part of this article, we talked about the Bluetooth shortcomings that lead to vulnerabilities. An attacker can exploit these flaws to take over your smartphone and use it to steal information, send and receive messages, make and receive phone calls, and access the internet [21]. Individuals can implement the correct policies and practices to mitigate Bluetooth network threats by considering a risk assessment and management plan.

From the previous chapter, we have found two types of eavesdropping incidents where a hacker can go for one-to-one or over a network where multiple users are connected or to specific apps. The one-to-one connection may make it possible for hackers to listen in on a chat or record if the user has provided any personal information, such as passwords, bank data, company secrets, etc., during the communication. The user is vulnerable to attack from any prospective hacker who has targeted them specifically for this information. Because of this, the user risks having their money stolen via identity theft. A hacker can impersonate a user if the Hacker duplicates the user's behavior or security measures. There have also been reports of a ransomware assault carried out via Bluetooth eavesdropping.

The impact on the network is being felt most strongly in the locations where Bluetooth-enabled Internet of Things devices have been discovered. Since the introduction of the Internet of Things technology, there have been worries about large amounts of data. The whole of the communication that took place between the user and the application has been logged in Order to ensure that it may be used later to make the devices more effective. This allows a gadget to completely comprehend the requirements of its users by following the directions they provide. However, hackers within range of the device can access the data recorded on the computers and use it to fake themselves since the gadget is part of a personal area network and has Bluetooth enabled. When this occurs, the device can identify the attackers as the primary user and will provide attackers permission to view and modify the security settings connected with the device. Consequently, the whole device linked to the same IoT network is now vulnerable. The attackers have complete control over what they do with it and may even prohibit the principal user from logging into the system if they want.

6. Protection measures against this kind of invasion

While it's true that hackers can easily penetrate most systems, there are measures in place to make Bluetooth safer for users. The most efficient approach is secure simple pairing (S.S.P.) and enhanced passkey entry protocol [26,27]. Initially, the two devices were linked by pin-based pairings, with the source device generating a random number and sending it to the destination device via the corresponding pin. The Bluetooth 2.1 standard included a new feature called secure, simple pairing (SSP).

However, the devices have a set pin that the user or the moderator cannot manipulate, nor can they be altered. These PIN's are later transformed into link keys using the LMP pairing key generation technique. This process also has limitations. The generated PIN typically consists of four to eight numbers. Many easily cracked PIN codes may be generated from a random combination of the available options. Locating the 16-bit random digits used as link keys to pair the devices is also simple. The link key can only be used in 2128 different ways. With this simple pairing, public key cryptography takes the place of the PIN [28]. Another study compared the security analysis of SSP with their suggested protocol SSP-APKE-DECE (Secure, simple pairing with authenticated public key exchange and delayed encrypted capability exchange). It concluded that SSP-APKE-DECE offers much higher levels of security [29].

DH key is the new link key made by the new pairing process. It is a random number with 192 bits and private and public keys. During pairing, only the public key is shown. The private key stays hidden. After the first connection, that will only be shared between the two devices. You can't use the public key to figure out the private key. Communication can happen if all the keys on the source device match the keys on the destination device.

However, there are situations when this passkey entry protocol fails. Due to a lack of mutual certification, the two devices are communicating using the same key. The certificate, if available, needs to be checked over the internet, but Bluetooth can't connect to the internet because it is a private network. Therefore, the keys might be compromised during a man-in-the-middle exchange. Because of this, DHKey supports four distinct authentication mechanisms. The "Just Works" design principle applies to these devices, which lack a display and user input. The "Numerical Comparison" model is for devices that both have displays but not much else; the "Out of Band" model is for devices that can talk to each other over other wireless channels, and the "Passkey Entry" model is for devices that don't have displays but can still enter passcodes [9].

Even though Bluetooth is used in everything from smartphones to car stereos, it's not easy for hackers to get into your device without your permission. Even if no one is listening in on your conversation, you might say something important that could risk your digital and personal security. If you don't want to be spied on, ensure your Bluetooth connection is secure and limit who can use your devices. These methods include private connections, updating software, linking devices in disguise, and keeping one's PIN safe [22].

You could still be spied on even if you're not connected to a Bluetooth device. Sometimes, someone could use the victim's tablet or phone microphone to listen to everything happening around them. Turning off Bluetooth and obscuring your devices from search results are two of the easiest and most reliable ways to increase security and prevent eavesdropping. It may take a few more seconds to pair a device each time, but you'll protect your Bluetooth gadget from prying eyes while it's not in use. There are a lot of Bluetooth devices out there, and many of them have default Passcodes and device names that allow anybody to connect to the network. The Better Business Bureau recommends changing your default Passcode, typically "0000." Create a password of eight characters to safeguard your account. For most devices, the P.I.N. must be changed on the device itself. The location of this option varies by model and manufacturer; on Epson printers, for example, it may be found in the "Bluetooth Settings" part of the "Setup" menu under the "Bluetooth" header. In addition, Bluetooth tech device makers have recognized the need for enhanced security and are attempting to create more effective means of protecting their customers' data [22]. Apart from that, avoid using the "Just Works" security model in Secure Simple Pairing (S.S.P.), as it does not offer protection against MITM attacks [23]. The researcher also suggested developing a Bluetooth firewall that can be used to block unauthorized Bluetooth connections and protect against eavesdropping [25,30]. As shown in Figure 7, the RFCOMM protocol, the second protocol layer on the host side of the Bluetooth protocol stack, must be protected by the Bluetooth Firewall. Through the protection of this protocol, it is possible to filter all connections that use OBEX or TCP or are designed to convey AT commands.

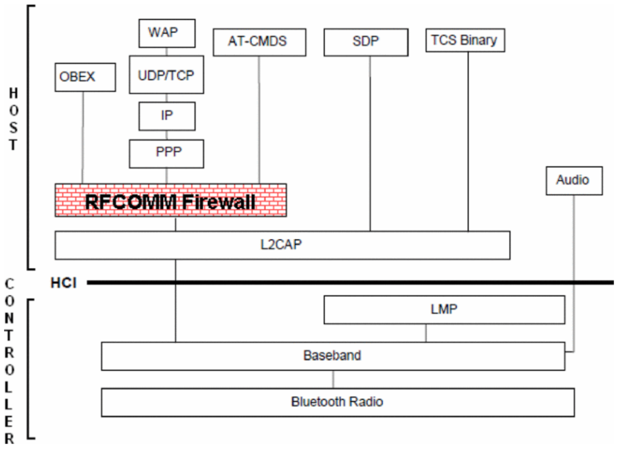

Fig 7: Bluetooth protocol stack with firewall [25]

7. Recommendation

As we discussed earlier, Bluetooth eavesdropping occurred due to technical flaws. This flaw allows attackers to steal data, make calls or send messages from the victim's phone. When mobile companies and other companies learned about these attacks and flows, they tried to resolve them by updating the Bluetooth software. When pin verification was first implemented, encryption made communication more secure. As we all know, the previous device pairing method was highly insecure, and engaging in eavesdropping using various devices is straightforward. The procedure that was described above is level-one security for a Bluetooth device. Afterward, three more pairing processes were implemented. After level one, the second level of protection was added, where a P.I.N. is always needed to pair two devices. This isn't a perfect security measure, but it did help lower some of the risks. The third level of security for devices is based on swapping security codes. This speedy process reduces all the gaps between the pairing process to ensure no security breach. However, poorly and incorrectly designed software can make this procedure insecure. Regardless of the number of safety precautions the manufacturer takes, users should always be proactive in their protection and think one step ahead. Users must alter the default configuration to a personalized one to protect themselves from cyberattacks. Aside from that, I would like to provide a few suggestions that every user should take into consideration, and they are the following:

1. Device-related recommendation	Please turn off the Bluetooth when it's not needed. Try to keep your device in non-discoverable mode. When we need to use Bluetooth, only that time makes it discoverable. To secure your device from attack, try to use anti-virus, firewall, and premium anti-spam software. Always try to update this security software. Never download from unauthenticated sources. Have proper knowledge of social engineering. Users should change the device name as well from the default name. While using Bluetooth, many services are required, and the device user should monitor those services and disable the unnecessary services.
2.Pairing-related recommendation	While pairing with devices, always follow the strong pin; after each scheduled maintenance period, the P.I.N. should be updated, and pairing should only be attempted with nearby devices if possible. Avoid unknown pairing, avoid forming pairs in familiar places such as malls, train stations, movie theatres, food courts, and other areas, and keep an eye on pair listings [14].
3.Device Behavior related recommendation	To stop the eavesdropping attack, we also should observe the device behavior as well such as carefully observe the device activities such as whether the transmission of data between the devices is getting slower or not than the regular or weird pop-up messages or system crashes which may be the indication of phone may be attacked. Apart from that, users should check the battery life regularly, observe anti-virus activities (crashes regularly or disabled automatically), and monitor data usage (application log of the devices) [14].

Conclusion

No doubt that Bluetooth has become the most popular and efficient wireless medium for data exchange. in this paper, I have expressed the security flows of Bluetooth networks, how eavesdropping can happen, and it could be. Most users pay less attention to this type of security threat; hence, most Bluetooth attacks go undetected. More and more industries have started seeing the benefits of Bluetooth devices. According to the Bluetooth special interest group (SIG), more than 400 million devices with Bluetooth-enabled location services will be in use by the end of 2023. As a result, this will be the broadest area within the wireless security market, and there will be a great need for a research effort to secure such devices from cybercriminals.

References

[1]. Britannica, The Editors of Encyclopaedia. "Bluetooth". Encyclopedia Britannica, 22 Aug.2022,https:// www.britannica.com/technology/Bluetooth.Accessed 11 November 2022.

[2]. Nguyen, Tuan C. "Who Invented Bluetooth?" ThoughtCo, Feb. 13, 2021, thoughtco.com/who-invented-bluetooth-4038864.

[3]. Bluetooth Insight (2008) Bluetooth Power Classes.http://bluetoothinsight.blogspot.com/2008/01/ bluetooth-power-classes.html

[4]. McMillan, R. (2005) *'car whisperer' puts hackers in the driver's seat*, *Computerworld*. I.D.G. News Service.

Available at: https://www.computerworld.com/ article/2557329/-car-whisperer--puts-hackers-in-the-driver-s-seat.html (Accessed: November 12, 2022).

[5]. Lonzetta, A., Cope, P., Campbell, J., Mohd, B. & Hayajneh, T. (2018). Security Vulnerabilities in Bluetooth Technology as Used in IoT. *Journal of Sensor and Actuator Networks*. [Online]. 7 (3). p.p. 28. Available from:http://dx.doi.org/10.3390/jsan7030028.

[6]. Peterson, A. (2021) *Yes, terrorists could have hacked Dick Cheney's heart*, *The Washington Post*. W.P. Company. Available at: https://www.washingtonpost.com/ news/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/ (Accessed: November 12, 2022).

[7]. STEINBERG, J.O.S.E.P.H. (2015) *Why your bluetooth devices aren't as secure as you think | inc.com*, *Why Your Bluetooth Devices Arenot as Secure as You Think*. Available at: https://www.inc.com/joseph-steinberg/ are-your-bluetooth-devices-secure-maybe-not.html (Accessed: November 12, 2022).

[8]. Espinosa, C. 2018. The 8 Most Common Cyber Attacks and How to Stop Them. Available at: https://www.alpinesecurity.com/blog/the-8-most-common-cyber-attacks-and-how-to-stop-them/ [Accessed: 12 November 2022].

[9]. T. Melamed, "An active man-in-the-middle attack on bluetooth smart devices," *International Journal of Safety and Security Engineering*, vol. 8, no. 2, pp. 200–211, Feb. 2018, doi: 10.2495/SAFE-V8-N2-200-211.

[10]. Alfred Loo. 2009. Technical opinion Security threats of smart phones and Bluetooth. Commun. A.C.M. 52, 3 (March 2009), 150–152. https://doi.org/ 10.1145/1467247.1467282

[11]. *Bluetooth attacks and how to secure your Mobile Device* (no date) *Webroot*. Available at: https://www.webroot.com/gb/en/resources/tips-articles/a-review-of-bluetooth-attacks-and-how-to-secure-mobile-workforce-devices (Accessed: November 12, 2022).

[12]. Bahar, Z. (2021) *How dangerous are bluebugging attacks?*, *NordVPN*. Available at: https://nordvpn.com/blog/bluebugging/ (Accessed: November 12, 2022).

[13]. Shaked, Yaniv & Wool, Avishai. (2005). Cracking the Bluetooth P.I.N. Proceedings of the 3rd International Conference on Mobile Systems, Applications, and Services, MobiSys 2005. 39-50. 10.1145/1067170.1067176.

[14]. Hassan, S.S. *et al.* (2018) "Security threats in bluetooth technology," *Computers & Security*, 74, pp. 308–322. Available at: https://doi.org/10.1016/ j.cose.2017.03.008.

[15]. Herfurt M, Mulliner C. Bluetooth security vulnerabilities and bluetooth projects,Web page; 2005. Available from: http://trifinite.org/trifinite_stuff.html. [Accessed November 13,2022.

[16]. Phan, R.C.W. and Mingard, P., 2012. Analyzing the camp secure simple pairing in Bluetooth v4. 0. *Wireless Personal Communications*, *64*(4), pp.719-737.

[17]. Sandhya, S. and Devi, K.S., 2012, November. Contention for man-in-the-middle attacks in Bluetooth networks. In *2012 Fourth International Conference on Computational Intelligence and Communication Networks* (pp. 700-703). IEEE.

[18]. Syverson, P., 1994, June. A taxonomy of replay attacks [cryptographic protocols]. In *Proceedings The Computer Security Foundations Workshop VII* (pp. 187-191). IEEE.

[19]. Nilsson, D.K., Porras, P.A. and Jonsson, E., 2007, September. How to secure bluetooth-based pico networks. In *International Conference on Computer Safety, Reliability, and Security* (pp. 209-223). Springer, Berlin, Heidelberg.

[20]. Carettoni, L., Merloni, C. and Zanero, S., 2007. Studying bluetooth malware propagation: The bluebag project. *IEEE Security & Privacy*, *5*(2), pp.17-25.

[21]. P. Cope, J. Campbell and T. Hayajneh, "An investigation of Bluetooth security vulnerabilities," 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (C.C.W.C.), 2017, pp. 1-7, doi: 10.1109/CCWC.2017.7868416.

[22]. Labib, M., Ghalwash, A., Abdulkader, S. and Elgazzar, M., 2019. Networking solutions for connecting bluetooth low energy devices-a comparison. In *M.A.T.E.C. web of conferences* (Vol. 292, p. 02003). EDP Sciences.

[23]. Kaur, S., 2013. How to secure our Bluetooth insecure world! Pushing frontiers with the first lady of emerging technologies. *I.E.T.E. Technical Review*, *30*(2), pp.95-101.

[24]. Wright, Joshua. "I can hear you now" -eavesdropping on Bluetooth headsets. Joshua. *Will Hack For SUSHI.* [Online] 10 8, 2007. [Cited: 7 4,2011.] http://www.willhackforsushi.com/presentations/icanhearyounow-sansns2007.pdf

[25]. J. Alfaiate and J. Fonseca, "Bluetooth security analysis for mobile phones," 7th Iberian Conference on Information Systems and Technologies (C.I.S.T.I. 2012), 2012, pp. 1-6.

[26]. S. S. Madugula, and R. Wei, "An Enhanced Passkey Entry Protocol for Secure Simple Pairing in Bluetooth," ArXiv, 2021. [Online]. Available: https://arxiv.org/pdf/ 2101.09381.pdf

[27]. D. Z. Sun, and L. Sun, "On Secure Simple Pairing in Bluetooth Standard v5.0-Part I: Authenticated Link Key Security and Its Home Automation and Entertainment Applications," *Sensors,* vol. 19, no. 5, pp. 1150, Dec.2019.

[28]. K.. Sairam, N. Gunasekaran and S. Rama Reddy, (2002, June)."Bluetooth in wireless communication", IEEE Communications Magazine, vol. 40, no. 6, pp. 90-96.

[29]. S. Gajbhiye, S. Karmakar, M. Sharma, and S. Sharma, "Bluetooth Secure Simple Pairing with enhanced security level," *Journal of Information Security and Applications*, vol. 44, pp. 170–183, Feb. 2019, doi: 10.1016/j.jisa.2018.11.009.

[30]. Pandey, T.; Khara, P. Bluetooth Hacking and its Prevention. L & T Technology Services. Available online**:** http://www.larsentoubro.com/media/27618/bluetooth-hacking-and-its-prevention-2014.pdf (accessed on 19 December 2022).

[31]. Trishna Panse and Prashant Panse, "A Survey on Security Threats and Vulnerability attacks on Bluetooth Communication" ISSN: 0975-9646.

[32]. S. Satam, P. Satam and S. Hariri, "Multi-level Bluetooth Intrusion Detection System," 2020 IEEE/ACS 17th International Conference on Computer Systems and Applications (AICCSA), 2020, pp. 1-8, doi: 10.1109/AICCSA50499.2020.9316514.

[33]. Padgette, J. , Bahr, J. , Batra, M. , Smithbey, R. , Chen, L. and Scarfone, K. (2022), Guide to Bluetooth Security, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800-121r2-upd1, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=934038 (Accessed December 14, 2022)