Intrusion in IoT Devices: Bluetooth attacks and detection system

UGP-I, Supervisor: Dr. Priyanka Bagade

Mohak Singh Rana, Aditya Ajmera
Dept. of Computer Science and Engineering
Indian Institute of Technology Kanpur
Kanpur, India

***Abstract*—Despite the advancements made in WiFi technologies, a lot has to be discovered in Bluetooth technology, an important part of it being security. Especially if these Bluetooth devices have vital responsibilities such as fire alarms or security cameras, security becomes even more important for us. We first studied how the information is encoded, how it is transferred, and how it is finally decoded. We then explored the Bluetooth protocol Stack, payload format, and different types of Bluetooth hacking techniques. We then focused on the security of Bluetooth devices and the potential for attacks, such as denial-of-service (DoS) and man-in-the-middle (MITM) attacks, to compromise the security of Bluetooth-enabled devices. We also explored other attacks like the BlueBorne attack, eavesdropping, etc.**
To demonstrate the vulnerabilities of Bluetooth devices, we conducted DoS and MITM attacks on a BLE device. The DoS attack involved sending a large number of connection requests to the target device, causing it to become unresponsive. The MITM attack, on the other hand, allowed us to intercept and manipulate the data exchanged between the target device and its paired device, giving us access to sensitive information. Most modern devices are secure from this type of attack because of different pairing keys when connecting devices to the host and the proxy. Our findings suggest that despite the prevalence of Bluetooth technology in various applications, it remains highly vulnerable to security breaches. Thus, there is an urgent need for improved security measures and protocols to protect Bluetooth-enabled devices from potential attacks. We aim to build an intrusion detection system to detect the severity and type of attack attempted on the device.

***Index Terms*—Bluetooth attacks, Denial of service attack, Man-in-the-Middle attack, Security, Network attacks, Intrusion detection.**

I. Introduction

In our research, we explored various types of vulnerabilities in Bluetooth communication. Initially, we explored the Bluetooth protocol stack and different types of layers in Bluetooth communication. Then, we focused on the vulnerabilities and how we can create attacks on the devices communicating over Bluetooth. We explored various attacks like DOS(Denial of Service Attack), MITM(Man in the Middle Attack), Blueborne attack, and many more.

Then we conducted DOS attack and captured the PCAP files (both at the attacker device and also at the victim device). We then tried to conduct MITM attack. We are analyzing the captured PCAP files to keep track of various features in the Bluetooth protocol stack when an attack happens. We aim to develop a plugin to detect an intrusion in a device.

An intrusion detection system is a must for Bluetooth communications considering the vulnerabilities. Such a system aims to determine the type of attack and its severity.

II. Related Work

A lot of resources are available over WiFi security, but Bluetooth still remains a vulnerable mode of communication. The amount of resources available over bluetooth communication are too limited. Many attempts are being made to create attacks on Bluetooth devices. Feature extraction from the Bluetooth PCAP files still remains a huge area of concern as all the tools available for feature extraction discard the Bluetooth PCAP files. Currently, they are only meant for web-based PCAP files.

In [10], a potent Man-in-the-middle attack was carried out on a mobile device. The author demonstrated, using Kali Linux and frameworks such as GATTacker and Btlejuice, the process of hacking a BLE mobile app. It was shown that both data interception and data manipulation are fairly easy to perform on a BLE network. In addition, the mobile camera was also hacked using a replay attack.

In [15], smart health systems were targeted using various attacks. As smart health care systems rely on distributed control optimisation, AI and DL offer effective approaches to mitigate cyber-attacks on these devices. The paper presented a decentralised, predictive, DL-based process to autonomously detect and block malicious traffic and provide end-to-end defense against network attacks on these devices. It also introduced the *Bluetack* dataset for BLE-based network attacks on smart Healthcare devices.

In [8] (*SPT-IoT 2021 : The Fifth Workshop on Security*), an Intrusion Detection System (IDS) based on pattern classification recognition of the most classical Denial of Service (DoS) attacks was proposed for BLE Mesh networks. This system operated on a single node and thus did not require much information to function. Another dataset (based on the data collection system of ESP32) was presented, along with various experiments performed on the same. Algorithms that explain the functioning of attacks like the Targeted Grey Hole and Black Hole Attacks in mesh networks were

described.
In [12], a novel method of identifying BLE attacks only based on the power levels of the Bluetooth device was proposed. This method identified reconnaissance, denial of service, and information theft attacks on BLE devices. The attack was inspired from various existing attack methodologies and tools, including CarWhisperer, BlueSnarfer and iPhone MetaSploit. Rules to detect malicious activities in each layer of the BLE Protocol Stack were explained. Various plug-in modules were used to detect attacks that require a stateful inspection of the stream of Bluetooth traffic.
In [9], the author has initially discussed about the Bluetooth technology, Bluetooth piconet and the Bluetooth Scatternet. We also learned about the Bluetooth hardware and got a basic idea on Bluetooth stack. Then the author explained about some the terms which are related to the Bluetooth security vulnerabilities such as Blue snarf, Blue snarf++, Hello Moto, Blue Bug, and Bluetooone. We got an idea in brief over these terms.

In [7], the Blacktooth attack is intorduced. The author has exploited 5 vulnerabilities of Blacktooth that are Identity Forging and Proactive Connection Request, Authentication Spoofing, Encryption Key Negotiation and Brute Force, Profile Change and the Blacktooth MITM attack. We also learnt here about the implementation and the evaluation of the Blacktooth attack. The implementation includes multiple steps as follows, identity forging and proactive connection request, Encryption key negotiation and brute force and then at end checking the attack efficiency.
In [1], we have a GitHub repository, where the authors have shared their attack scripts for performing a DOS attack on a Bluetooth device. The attack script is executed through the terminal of the virtual system that we are operating and during execution we have an option of setting the parameters like threads count, package size etc. We used the repository files and the instructions given in there to perform a successful DOS attack on a wireless Bluetooth earphones
In [3], we have another GitHub repository which contains the files and modules to run a framework called Btlejuice, which we can use to perform a Man-In-The-Middle attack on a bluetooth device. The repository also contains a detailed tutorial on how to setup a host and a proxy, use the web interface to find the target device and finally carry out the MITM attack using the Btlejuice framework.
In [8] the author creates a reliable mechanism of network analysis suited for BLE using a machine learning Intrusion Detection System (IDS) based on pattern classification and recognition of the most classical denial of service attacks affecting this kind of networks, working on a single internal node, thus requiring a small amount of information to operate. Moreover, in order to overcome the gap created by the absence of data, ESP32 based data collection system is used that allowed the collection of the packets from the Network and the Model layers of the BLE Mesh stack, together with a set of experiments conducted to get the necessary data to train the IDS.
In [11], the author show how an external attacker can hook into the personal medical device's communication and eavesdrop the sensitive health data traffic, and implement man in-the-middle, replay, false data injection, and denial-of-service attacks. Furthermore, an Intrusion Detection System (IDS), HEKA, is proposed to monitor personal medical device traffic and detect attacks on them. HEKA passively hooks into the personal medical traffic generated by medical devices to learn the contiguous sequence of packets information from the captured traffic and detects irregular traffic-flow patterns using an n-grambased approach and different machine learning techniques.
In [13], the author demonstrates an inaudible attack on smart speakers using electromagnetic interference (EMI). The EMI induces voltages are converted into baseband signals by exploiting the inherent nonlinearity of microphones. The EMI signal is specially preprocessed to minimize the useless harmonics generation at the microphone output signals, which significantly improves the recognition rate as well as nullify the previous countermeasures based on the harmonics detection. The sensitive carrier frequency found the proposed method can improve the attack distance as well.
In [14], the author represent the denial of service (DoS) attacks applied against devices that are paired with Google Home Mini(GHM). In this study, Bluedoser, L2ping, and Bluetooth DoS script, which are software in the Kali Linux platform, were used to perform DoS attacks, and some devices were used such as GHM, headphones, and two speakers as victim devices. Successful results were observed on Bluetooth headphones.

III. Materials

In our study, Bluetooth earphones, Kali Linux Virtual Machine, Bluetooth Adapter, tools for DoS attack and MitM attack were used. Kali Linux, which includes penetrating test tools, was required for performing DoS attacks and MitM attacks. L2ping [6], and Bluetooth DoS Script [1] are used for performing DoS attacks on victims.Also, Btlejuice [3] is used for performing MitM attacks on victims. In this section, Kali Linux, and tools for attacking are explained.

A. Kali Linux

Kali Linux is a Debian [4] based Linux operating system developed for penetration tests and security audits. Penetration tests are used to find, analyze and report vulnerabilities in systems. With a lot of tools and components for cybersecurity, Kali Linux is widely used for performing penetration tests. In this study, DoS attacks were performed using l2ping, and Bluetooth DoS script tools on the Kali Linux system.
Bluez [2] is a library that provides the Bluetooth layer and protocol requirements necessary for us to use Bluetooth on our Kali Linux operating system. Bluez is developed in a modular structure that can support more than one Bluetooth adapter, and also it contains many useful modules. Bluez, which can run on almost all Linux systems, can be downloaded using the

"sudo apt-get install bluez" command.
Hcitool [5] contains many useful commands such as "dev", "scan", "inq". To reach all commands and detailed descriptions, the "hcitool -h" command can be used on the terminal. Finding the media access control (MAC) addresses of Bluetooth devices during our attacks is the first step to do before starting any operation. "hcitool scan" command finds those MAC addresses with their device names.

B. L2ping

L2ping allows us to send packets to Bluetooth devices. During performing l2ping, we need to determine some parameters such as "-i", "-s", "-f". The computer's Bluetooth adapter should be selected using the "-i" parameter. In this study, our Bluetooth adapter was hci0.

C. Bluetooth Dos Script

Bluetooth DoS script (BDS) is a script that works on only Linux systems and is used to perform Bluetooth DoS attacks. It is required by l2ping in the Kali Linux system to use BDS. The working principle of BDS is similar to Bluedoser, but the only difference is that BDS allows attackers to define thread count as a parameter. This parameter provides performing DoS attacks using a defined number of threads. Figure 2 explains how BDS uses it for attacking.

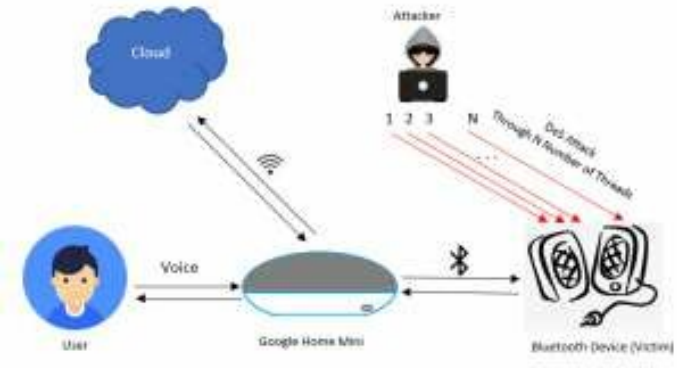
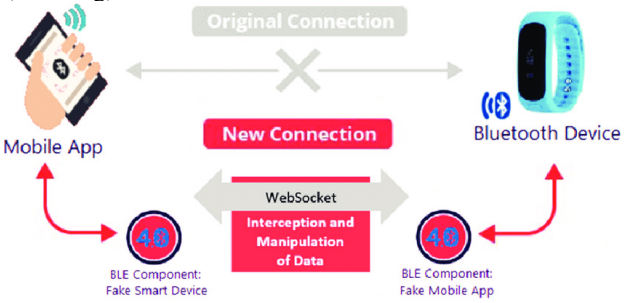


Figure 2. Performing DoS attack using BDS.

As soon as BDS attacks any unpaired Bluetooth device, it prevents other devices from connecting to the attacked victim device. For some devices that are not very secure, it may stop communicating with the corresponding device connected via Bluetooth. The security of the device to be attacked is the most important measure in the disconnection process via a DOS attack.

D. BtleJuice

BtleJuice is a framework to perform MitM attacks on Bluetooth Smart devices, which was developed by Damien Cauquil (Digital Security) and first presented at the DefCon 24 conference in 2016. BtleJuice includes two components, which must be run on independent machines to operate two Bluetooth 4.0+ adapters simultaneously. Also, in this case, the two components communicate with each other over the WebSocket protocol. BtleJuice includes a web interface and – among other useful features – presents Replay GATT operations (Replay attack) and On-the-fly data modification capabilities (Hooking).



IV. Experiments and Results

A. Denial of Service Attack

DoS attack is a type of cyber-attack in which a malicious attacker aims to render a computer or IoT device unavailable by interrupting the device's service. DoS attacks harm by overwhelming a victim machine with requests until normal traffic is unable to be processed, resulting in a denial of service to users.

Using l2ping, an attack was carried out on the Bluetooth earphone paired with the device. The victim device's MAC address was searched using hcitool. After determining the victim device, the related MAC address with the victim was set up as the parameter. Then DoS attack using Bluetooth Dos Script was started on the Bluetooth earphone.

BDS requires Victim MAC address, packet size, and several threads as parameters. After the DoS attack starts, packets of 600 bytes are sent to the victim over 100 different threads. The number of threads and packet length for disconnection of the device vary as per the victim device. The optimal thread count and packet length were found by performing lots of attacks on the victim and observing those trials.

Figure 1 shows the PCAP file when a device tries to connect to the earphones. The highlighted packet is a request made by the device to connect to the earphones. Figure 2 shows the packets when the earphones are connected and music is playing. Figure 3 shows the interface of Bluetooth Dos Script. Figure 4 shows the interface when the attack is being carried out. Figure 5 shows the PCAP files between the device and earphone. We can see the music packets have stopped. This shows the devices have been disconnected. Moreover, we also observed that the earphones were switched off.

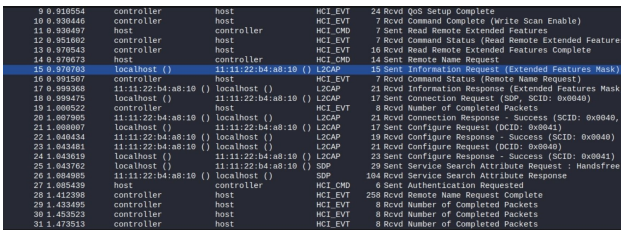


Figure 1. Setting up connection between device

and earphone

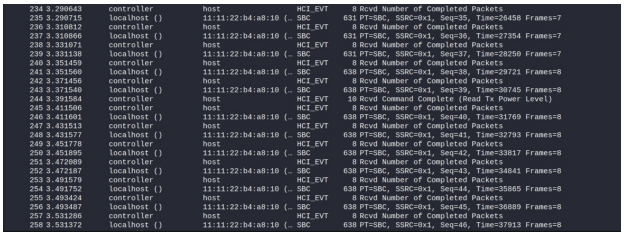


Figure 2. Music playing in the earphones

Figure 3. Interface of Bluetooth Dos Script

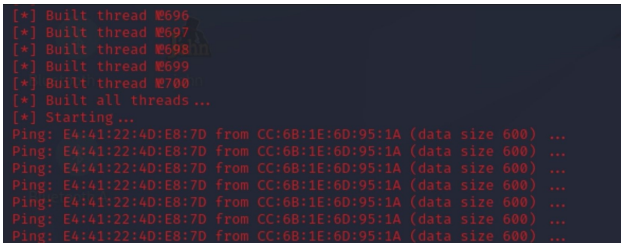


Figure 4. Threads being sent to the earphones (Attack in progress)

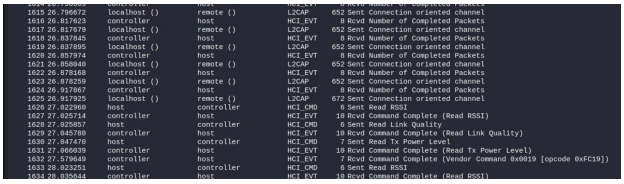


Figure 5. Earphones Disconnected from the device.

B. Man-in-the-Middle Attack

MITM attack is a type of cyber-attack in which an attacker sets an alternate connection between the devices and hence has complete control over the information that is being transferred. MITM attack causes great harm by providing complete control of the information to be sent to the receiver. In this way, the attacker can also inject false data into the receiver.

Before carrying out the planned MitM attack, we downloaded a Kali Linux virtual image (available at https://kali.org) and installed all the required libraries and tools (see Materials Section). Then we installed btlejuice. Environment check is important while downloading btlejuice as module hci socket should be accessible when setting up btlejuice proxy. Then we set up btlejuice proxy in one terminal and btlejuice host in another. (Host and proxy need to be set up in 2 terminals in the same virtual machine as the connection between them is set up over localhost. Hence, we need them to be setup in the same virtual machine). Then we open the btlejuice web interface and connect the phone using the web interface to the btlejuice host.

At this stage, btlejuice proxy will be available to the environment as a copy of the phone (it will have the same MAC address as that of the phone). Now connect the earphones to the phone (Actually to the btlejuice proxy visible as the phone). This will set an alternate path between the earphones and the mobile phone through the btlejuice host and btlejuice proxy. Now we change the information coming from the mobile phone to completely different information to be sent to the earphones, indirectly having control over the mobile phone.

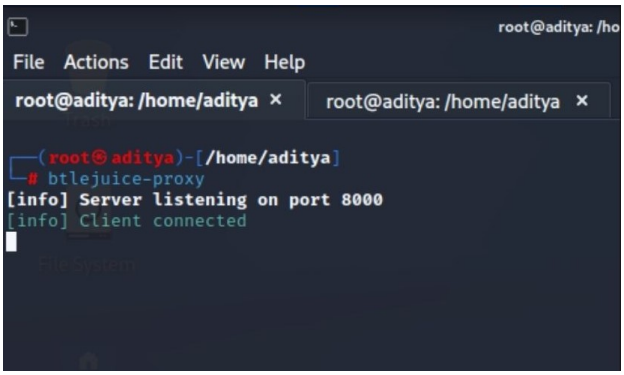


Figure 6. Btlejuice proxy interface

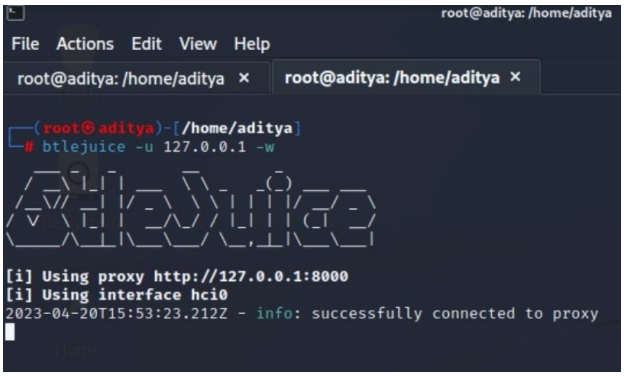


Figure 7. Btlejuice host connected to proxy

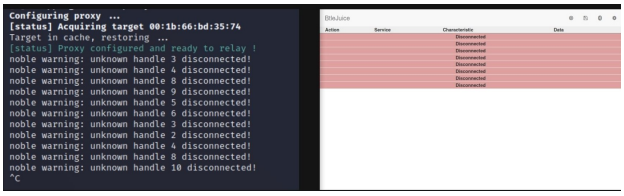


Figure 8. Device got disconnected due to pairing key incompatibility.

This method works for simple earphones. Sometimes, there might be some error in connection due to pairing key. While connecting the btlejuice host and mobile phone, a unique pairing key is set automatically. This same pairing key is needed when connecting the earphones to the btlejuice proxy. But this is not necessary. Hence, you sometimes might not connect the earphones with the btlejuice proxy. Hence, devices

are somewhat secure to MITM attack but this is still a huge loophole in Bluetooth connections.

To overcome pairing key compatibility, researchers have come up with a concept called KNOB (Key Negotiation of Bluetooth). It exploits a vulnerability in the bluetooth specification that affects the encryption process. KNOB forces the devices to use a weaker encryption. It lowers the entropy of the link to 1-byte. The level of entropy indicates how much encryption changes over time, and is the most significant determinant of Bluetooth security. Once the link is decrypted using KNOB, it can be passed onto a controlled hijacking Bluetooth session. The MITM framework can be setup with all the previously discussed tools.

V. Future Work

In addition to analyzing the features during a DoS attack, it would be beneficial to analyze other attack scenarios to comprehensively understand Bluetooth security issues. This could include analyzing packet captures of other attack types, such as eavesdropping and man-in-the-middle attacks.

It would be useful to prioritize which features of Bluetooth-enabled devices are most affected by DoS attacks. This would help in developing countermeasures that focus on protecting those features first. Once the analysis of the pcap files is complete, the findings should be used to develop more effective countermeasures against DoS attacks. This could include implementing protocols or software patches that mitigate the impact of DoS attacks on Bluetooth-enabled devices.

An intrusion detection system can be developed using the information extracted from Pcap files to detect and prevent attacks on Bluetooth-enabled devices. This includes writing plugins that identify abnormalities or deviations from the standard Bluetooth protocol. These plugins will then be used to develop an intrusion detection system that can detect and prevent attacks on Bluetooth-enabled devices. Therefore, the next priority will be to develop plugins that can extract and analyze specific features from captured pcap files, identifying abnormalities or deviations from the standard Bluetooth protocol.

Acknowledgment

We want to extend our sincere thanks to Dr. Priyanka Bagade for everything that she has done to help with this endeavour. Her advice and insights were crucial in helping us get through the many obstacles we encountered while conducting our study. We were motivated to go above and beyond our comfort zones and give it our all by Dr. Bagade's consistent support and encouragement. We are really grateful to have had the chance to work with her and cannot express our gratitude to her enough for all she has done to help us succeed.

We also extend our sincere thanks to Ms. Ayushi Mishra for her immense support throught our work. Exploring this new area of research with a limited number of resources available would not have been possible without her support. We are grateful to work with her.

References

[1] Bluetooth DOS Script. https://github.com/crypt0b0y/BLUETOOTH-DOS-ATTACK-SCRIPT.

[2] Bluez. http://www.bluez.org/.

[3] Btlejuice. https://github.com/DigitalSecurity/btlejuice.

[4] Debian. https://en.wikipedia.org/wiki/Debian.

[5] Hcitool. https://linux.die.net/man/1/hcitool.

[6] L2ping. https://linux.die.net/man/1/l2ping.

[7] Mingrui Ai, Kaiping Xue, Bo Luo, Lutong Chen, Nenghai Yu, Qibin Sun, and Feng Wu. Blacktooth: Breaking through the defense of bluetooth in silence. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, pages 55–68, 2022.

[8] Andrea Lacava, Emanuele Giacomini, Francesco D'Alterio, and Francesca Cuomo. Intrusion detection system for bluetooth mesh networks: Data gathering and experimental evaluations. In *2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*, pages 661–666. IEEE, 2021.

[9] Adam Laurie and Marcel Holtmann Martin Herfurt. Hacking bluetooth enabled mobile phones and beyond–full disclosure. In *Proceedings of the 21st Chaos Communication Congress, Berliner Congress Center, Berlin, Germany*, pages 27–29, 2004.

[10] Tal Melamed. An active man-in-the-middle attack on bluetooth smart devices. *Safety and Security Studies*, 15:2018, 2018.

[11] AKM Iqtidar Newaz, Amit Kumar Sikder, Leonardo Babun, and A Selcuk Uluagac. Heka: A novel intrusion detection system for attacks to personal medical devices. In *2020 IEEE Conference on Communications and Network Security (CNS)*, pages 1–9. IEEE, 2020.

[12] Terrence OConnor and Douglas Reeves. Bluetooth network-based misuse detection. In *2008 Annual Computer Security Applications Conference (ACSAC)*, pages 377–391. IEEE, 2008.

[13] Zhifei Xu, Runbing Hua, Jack Juang, Shengxuan Xia, Jun Fan, and Chulsoon Hwang. Inaudible attack on smart speakers with intentional electromagnetic interference. *IEEE Transactions on Microwave Theory and Techniques*, 69(5):2642–2650, 2021.

[14] Tuğrul Yüksel, Ömer AYDIN, and Gökhan DALKILIÇ. Performing dos attacks on bluetooth devices paired with google home mini. *Celal Bayar University Journal of Science*, 18(1):53–58, 2022.

[15] Mohammed Zubair, Ali Ghubaish, Devrim Unal, Abdulla Al-Ali, Thomas Reimann, Guillaume Alinier, Mohammad Hammoudeh, and Junaid Qadir. Secure bluetooth communication in smart healthcare systems: A novel community dataset and intrusion detection system. *Sensors*, 22(21):8280, 2022.