Security Drawbacks in Related to Bluetooth Technology in IOT Devices

Offensive Hacking Tactical and Strategic – IE4012
Assignment

Saputhanthri N.D
IT18015140

Bachelor of Science Hons. In Information Technology
(Specialization in Cyber Security)
Sri Lanka Institute of Information Technology
Sri Lanka

Video URL:
https://mysliit-my.sharepoint.com/:f:/g/personal/it18015140_my_sliit_lk/EppqLWWbkXxIiIrVHJ5l2G8BXPpklQTJZ3kkrlYLNw7uSA?e=f9np4B

Security Drawbacks in Related to Bluetooth Technology in IOT Devices

Saputhanthri N.D

Information Systems Engineering (Cyber Security)

Sri Lanka Institute of Information Technology

Malabe, Sri Lanka

IT18015140

Abstract- The main component of wireless communication is Bluetooth technology. It provides a low energy and affordable short-range radio solution. It is available in mobile devices, headphones, speakers, medical equipment, and many other devices. Today Bluetooth technology integrated with IoT. In smart homes and companies, the IoT based Bluetooth technology is also available for monitoring and controlling the lighting, thermostats, door lockers, appliances, safety systems and cameras. But Bluetooth does not provide a centralized security infrastructure for ease and convenience. Therefore, there are significant vulnerabilities to safety and the need to be conscious of security risks as technology increases. With this review paper able to know value of understanding the risks of attacks, Vulnerabilities, mitigation techniques and recommendations involved in our devices using Bluetooth technology.

Keywords— IoT, Gaussian frequency-shift key, Bluetooth attacks, Bluetooth Mitigation, Piconet, Protocol Stack, Bluetooth security, PIN Cracking attack, BlueBorne; Man-in- the-Middle attack, Eavesdropping

I. Introduction

In 1994, Bluetooth was invented by the Ericsson telecommunications company in Sweden. After that in 1998, Ericsson collaborated with Intel, Toshiba, IBM, and Nokia to develop and promote Bluetooth technology's open industry standard. As a consequence, the Bluetooth technology was approved by IEEE for 802.15.1 in 2000, and the headset introduced two years later in March 2002 was the first Bluetooth-enabled device [1].

As a basic rate, Bluetooth 1.1 and Bluetooth 1.2 are subsequently increased by Bluetooth with a transmission speed of up to 1 Mbps. Then Bluetooth Enhanced Data Rate (EDR) 2.0 allows up to 3 Mbps of transmission. Then published version 3.0 of Bluetooth with a speed of up to 24 Mbps [2]. Bluetooth versions of 4.0, 4.1, 4.2 come as Low Energy and more efficiently. Bluetooth 4.1 has 1–3 Mbps speeds, while Bluetooth 4.2, with Gaussian frequency-shift keying (GFSK), offers 1 Mbps. GFSK is a modulation method used in digital communication and one used in Bluetooth technology.

The next version of Bluetooth, Bluetooth 5 is announced as the Low energy mode. Bluetooth Version 5 has become IoT's most popular technology. This is primarily due to its ability to use low power consumption for data exchange. During the exchange, the technology can also maintain its standard communication field. By giving devices the ability to exist and to function successfully in a broad range of applications it can positively affect IoT technology [3,4]**.**

The purposes of this review paper are,

A. Presenting an overview of Bluetooth technology focusing on security, weaknesses, potential risks, and solutions for prevention and reduction of risk.

B. Focus on providing actual examples of Bluetooth's recent exploits.

C. A variety of Bluetooth communication security precautions are advised.

II. Technology of Bluetooth

The Bluetooth technology use for a short distance wireless communication. It enables the communication of the information on mobile phones, computers, medical sector equipment, and other wireless devices. In this review paper about Bluetooth frequency, interference potential and connectivity ranges, the Bluetooth piconet describing and demonstrating the formulation and Bluetooth protocol stack for Bluetooth version of 1.0, 2.0, 3.0 and another for Bluetooth version 4 which described an interface. This paper also discusses the possibility of interference and how Bluetooth prevents interference. Also, potential security attacks and

failures in various layers are described [1].

A. Bluetooth Connectivity Ranges and Frequency

Bluetooth allows low energy communication between devices in proximity. Bluetooth operates with a 2,4 GHz radio frequency, ranging from 1m to 100 m. Three device categories offer three different connectivity ranges with Bluetooth technology. Devices Category 1 have a 100 m range and a 100mW transmission. The most common Category 2 device has a 10 m range and a transmission range of 2.5mW [1]. The device of Category 3 is about 1 m range and 1mW range. The main benefit of Bluetooth technology is its ability to seamlessly transmit both voice and data. But other wireless technologies have considerably impacted Bluetooth transmissions because wireless systems coexisted. Bluetooth technology consequently utilizes Bluetooth frequency hops at 1600 hops per second and a mechanism called the spectrum to limit collisions. [5].

B. Bluetooth Piconet

By creating a Bluetooth network known as a piconet, devices can be transmitted. A piconet is a temporary spontaneous network that can be used to interact with two or more Bluetooth devices. In the network there is a master device in one device and slaves in all other devices [2]. Only one master device can be used as the piconet control device also, up to 7 active slave devices are available. Under the piconet Bluetooth network devices can request data to the master device and transmit it [6]. (Fig. 1)

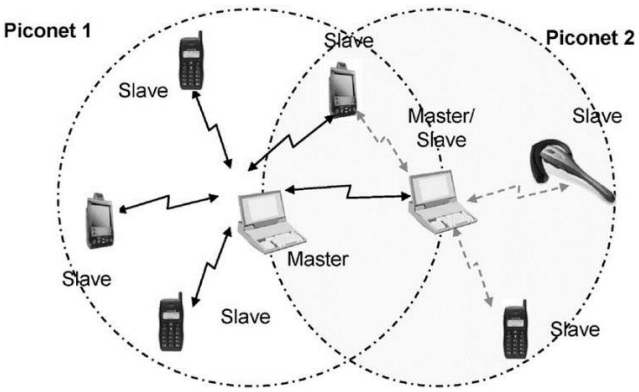

Fig. 1 Example of Bluetooth Piconet Network

C. Bluetooth Protocol Stack

Radio Frequency Communications (RFCOMM) protocol, Link Management Protocol, Logical Link Control Adaptation Protocol (L2CAP) and the Service Discovery Protocol (SDP) are included in Bluetooth versions of 1, 2, and 3 of Bluetooth protocol stack [7]. Also shown in the example is a command interface that has a base band controller and link manager (Fig. 2). The interface offers hardware access, control and register.

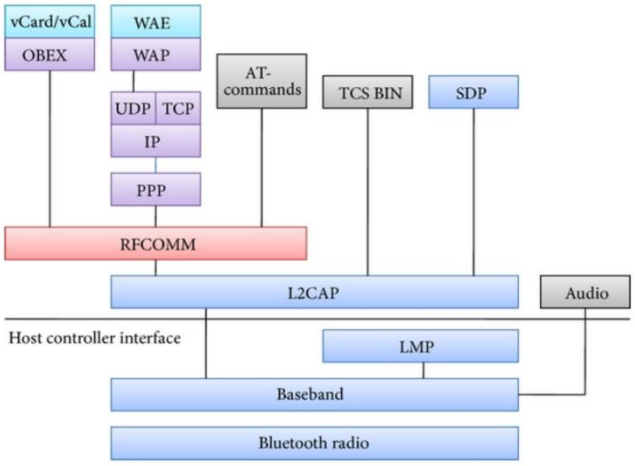

Fig. 2 Bluetooth protocol stack-version 1, ,2, 3

Stack's three levels are Bluetooth version 4, Host Layer, Controller Layer and App Layer. The layer contains direct test mode, physical layer, host control, and link layer interface. Applications in the app layer are included. A logical link control and adaptation Protocol, a protocol for the attributes, a generic access profile, a security manager and a generic attribute profile are included in the Host Layer. [8]. (Fig. 3)

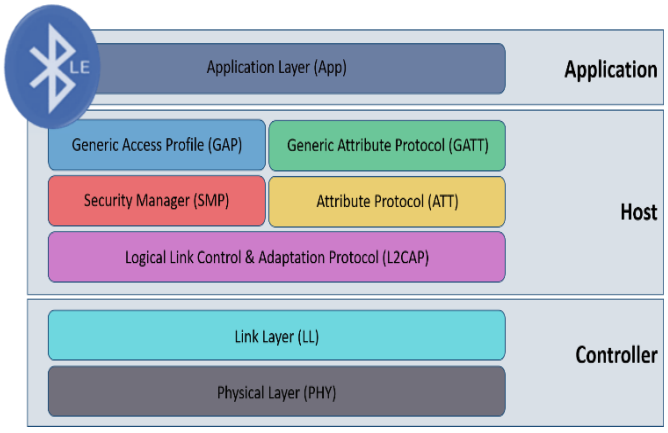

Fig. 3 Bluetooth protocol stack-version 4

III. Security of Bluetooth

For Bluetooth protocols, there are two sets of guidelines and standards. Details of recommended security processes are provided in NIST 800-121-R1. According to that, Sender authentication and verification, information confidentiality and permission for persons controlled by access to the information. The second standard is IEEE 802.15.1, here includes the protocol for Bluetooth technology.

A. Security Modes

Bluetooth devices work with four access security modes. The Security mode determines the level of security available to the service. Non-secure mode, service-level enforced security mode, link-level enforced security mode, and service-level enforced security mode with encrypted key exchange are only some of the security options available. [2].

The non-secure mode and link level enforced security mode does not specify levels of service security. Service level enforced security mode can apply the authentication, confidentiality, and authorization basic security services in any combination. Enforced security mode service level with encrypted key exchange provides few layers of security. AES for encryption and hashing is used for SHA-256. Secure Simple Pairing (SSP) is also used to create key systems. For Bluetooth versions 2.1, newer versions and EDR, this mode is required. [7].

Furthermore, Bluetooth security modes have Trusted and Untrusted modes. A trusted device is paired to another device, giving it full access to all services. Under the untrusted mode, only a limited set of services are available to a distrusted device. Although the device has successfully gone through authentication, its relation to another device is not fixed.

B. Device Discoverability

Bluetooth device discovery modes also affect the security of the device. Devices are more vulnerable, as recognizable in discoverable mode. approximately 10 m, the device type, name, technical information, and services list are all exchanged in Bluetooth devices which are discoverable and are available. Each Bluetooth device has a unique 48-bit ID address called BD ADDR. This address is comparable to the MAC address, a hardware manufacturer's address used as a single ID. The producer assigns the BD ADDR, as a MAC address [1].

C. Security Features

Bluetooth includes some integrated security features such as Adaptive Frequency Hopping, E0 Cipher Suite, Pairing and, Un discoverability. By adopting adaptive frequency hopping in Bluetooth, Hops are able to utilize a 2.4 GHz ISM band with 79 channels at 1600 hops a second. Existing frequencies will be excluded during the hopping process. The ability to hop frequency reduces interference and jamming. Using the E0 Cipher Suite, the main length is 128 bits, and stream chips are used. Also, With the aid of un discoverability, devices prevent reactions to scan attempts. The BD ADDR address of a device 48-bit is also disguised. Pairing allows devices to communicate is another method of security. BD ADDR device must be known for a pairing request. BD ADDR is recognized from a prior pairing or scanning knowledge [1,2].

D. Security Services in Bluetooth

When two devices first try to connect, authentication must establish a trustworthy relationship. The BD ADDR is used to carry out authentication and link key challenge response. Once established, the connection keys will be maintained by both devices for future pairing. By used common secret PIN codes passkeys needed for the first try to connect Bluetooth connections in Bluetooth version 2.0 and earlier. Both devices use PINs and consist of four to sixteen characters. These codes are used to generate a link key [9]. (Fig.4)

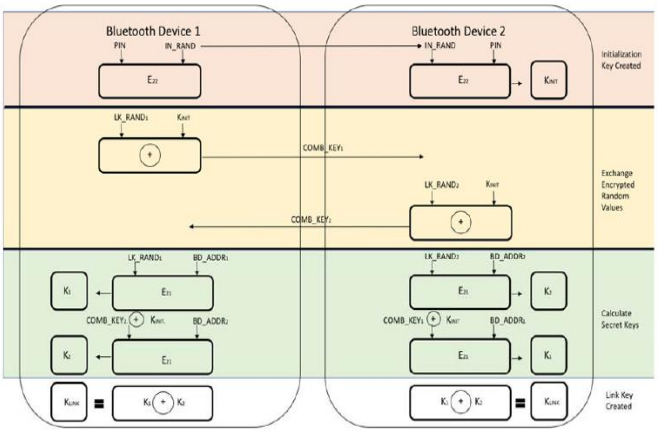

Fig. 4 Generate Link-key using PIN

The disadvantage of this PIN code method cannot change once the PIN is set. So then, newer Bluetooth versions are using the SSP for the connecting, using public-key cryptography. (Fig.5) In this SSP method, Authorization initiates by determining first whether the device was authorized as a trustworthy device previously. Encryption, specifically the E0 stream cypher, is used to guarantee confidentiality. To construct a keystream that accomplishes an encrypted text in collaboration with plaintext, the link key and BD ADDR device are utilized. E0 cryptanalysis attacks and efforts have shown that the Stream Cipher is susceptible to assaults. [10].

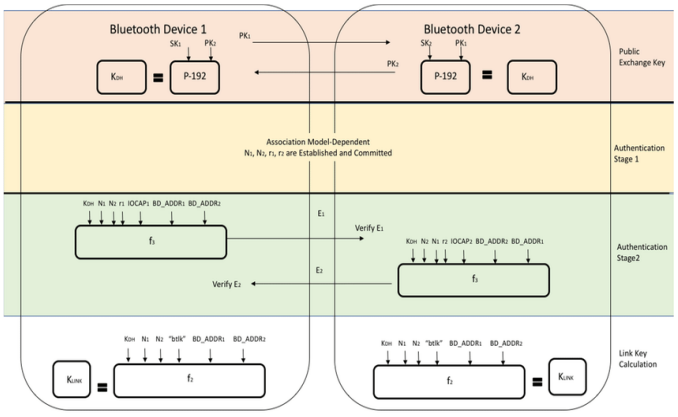

Fig. 5 Link-Key Establishment for Secure Simple Pairing.

IV. Vulnerabilities of Bluetooth Versions

The Bluetooth version and the security of communication between the devices utilized. Since many outdated devices are being used today, vulnerabilities still exist in previous Bluetooth versions.

In versions before Bluetooth 1.2, For pairing and reusability, link keys based on static unit keys are used. If the key is recovered, malicious devices may spoof the original device and/or connected devices in the original devices.

In versions before Bluetooth 2.1 and EDR, allowed to use codes consisting of short PINs. Because of their short length these PINs are easy for attackers to imagine. These versions lack PIN management, which at an enterprise level represents a desirable security capability. Moreover, after 23.3 hours of connection, In these early versions, keystreams become insecure. This is the time the keystream repeats and enhances the ability of the opponent to decrypt messages [1,2].

In versions 2.1 and 3.0, If devices that do not support service level enforced security mode with encrypted key exchange are connected to devices, earlier security modes will be used. In security modes, this rollback vulnerabilities are increased to versions 2.1 and 3.0. Furthermore, Secure Simple Pairing static keys in 2.1 and 3.0 versions are used to increase the vulnerability of the device to MITM attacks [1,2].

In versions before Bluetooth 4.0 an enormous amount of authentication requests is available so that opponents may learn about a variety of obstacles. This offers them insight into hidden link keys. In addition, the early versions of the E0 stream cypher are deemed weak. Overview of all Bluetooth versions, if opponents store wrongly, they may examine and change link keys. In order to make them vulnerable to attackers, small encryption key lengths may also be required. Crypt key can be as small as 1 byte. It is possible [1,2].

V. Threats of Bluetooth

Bluetooth pairing is a key security component. Attacks may be performed at many phases during pairing, including before and after pairing. For example, an attacker might launch Middle-in-the-Middle attacks (MITM) utilizing information collected after pairing. In view of the Bluetooth assaults,

A. PIN Cracking Attack

During device pairing and authentication, the attack happens. An attacker uses the RAND and BD ADDR Frequency sniffer tool for the target device. A brute-force algorithm (E22) is then used to test the PIN with data previously obtained for all possible permutations up to the correct PIN [13]. (Fig. 6)

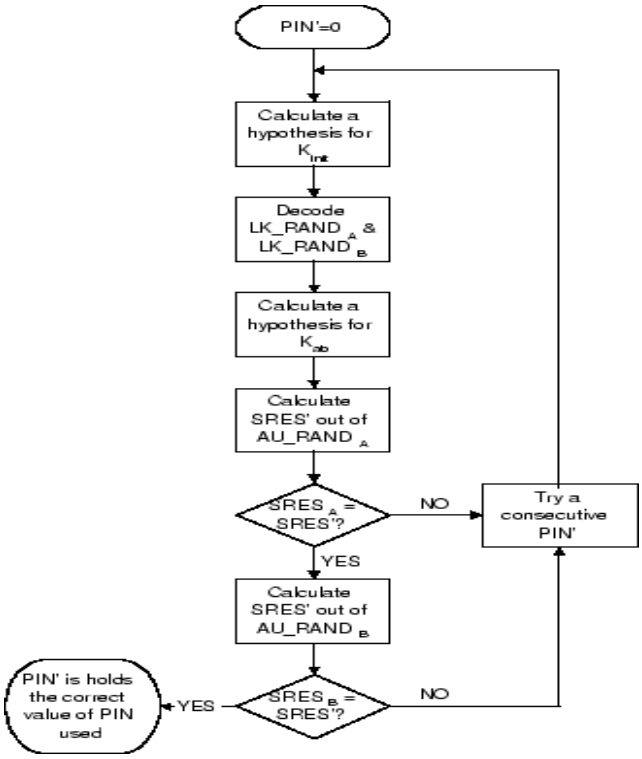

Fig. 6 Cracking Bluetooth PIN

B. Man-in-the-Middle Attack (MITM)

This MITM attack may strike if devices attempt to pair. Messages are transferred inadvertently between devices during the assault. This enables authentication without sharing the secret keys. The user feels that a successful assault resulted in the pairing. (Fig.7)

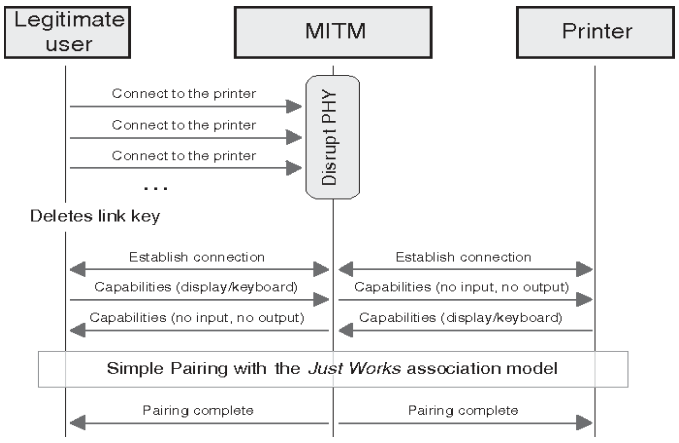

Fig. 7 Man-in-the-Middle Attack on Bluetooth

C. MAC Spoofing Attack

The attack is carried out before encryption is accepted and when link keys are triggered during piconet formation. Devices can authenticate by generating link keys for each other. Another user can be imitated by attackers during the attack.

They can also connect or change data using specialized equipment [12].

D. Fuzzing Attack

When an opponent attempts to make a device unusually compliant by providing faulty data packets and non-standard data to the device's Bluetooth radio, this is referred to as an assault. The attacker then observes the device's response to the data packets that have been sent. If the device's actions get slower or cease during these assaults, the attacker may conclude that the protocol stack includes a vulnerability. [2,12].

E. Back Door Attack

When a trustworthy partnership is formed, the assault occurs. During the attack, the adversary does not appear in the paired device register on the target device; but, after a relationship has been formed, the attacker has access to device services and resources. But the device owner does not know this access. For a successful backdoor attack, the BD ADDR of the target device must be known. The device targeting the attacker is also vulnerable to the attack [10,11].

F. Blue Borne Attack

An overflow issue in the stack buffer is exploited to carry out the attack. By focusing on the processing of pending client L2CAP configuration replies, the attacker may take control of Bluetooth connections. This enables you to manage the content and functionality of a certain device. Only MAC and Bluetooth addresses are necessary to carry out the attack successfully. [14].

G. Blue Bump Attack

When the link keys are handled improperly, the attack occurs. During the attack, a business card is exchanged between the attacker and the user. The user must accept the card and establish a secure and authenticated connection. After pairing, the user may then discard the link key. However, the attacker connection is still live for the user. The attacker may then connect to the device without being authorized by asking the link-key to be regenerated. If the key is not deleted, the attacker can keep on pairing with the target device [15].

H. Bluejacking Attack

The attacker sent unwanted messages on a device in this event to trick the user into the use of a code of access. This allows the opponent to access files on the device. The devices engaged in the assault, as well as the precise source of the received message, must be within 10 meters of each other in order for the assault to be effective. Although this usually does not entail data modification, it may render devices open to other types of assaults. [10].

I. Blue Snarfing Attack

Any data stored in the memory of your phone may be stolen if an attacker gains access to your phone. During the attack, the attacker connects to the OBEX File Transfer Protocol, which is utilized with Bluetooth. This enables the attacker to connect to the user's device. [10,12].

F. Skulls and Cabir Worm Attacks

Skulls Worm, a malicious Trojan program using the Symbian installation system, is targeting Symbian phones running on the Series 60 platform. The worm is like a flash player of Macromedia. To activate the worm, the user must open and install the Symbian system installation file also, then searches for other infecting devices and repeats the process [10,11].

Cabir Warm attack is a malicious software for Bluetooth. The attacks are vulnerable to mobile phones using the interfaces of 60 series Symbian. For the assaults to be successful, the user must accept the worm. Usually, the worms are covered up with applications, so the users accept them unwittingly. The program may then look for and deliver it to other accessible devices using the infected device after it has been installed. This worm spreads itself via the Multimedia Messaging Service and Bluetooth.

VI. Real-world IoT Exploitations and Risk Mitigation Strategies

A. Smart Home Camera Hack

The two initial weaknesses are to transfer parameters through Bluetooth to the camera. Wi-Fi SSID parameters and Wi-Fi password parameters, also known as service set parameters, are examples. SSID is a 32-figure network wireless ID. If these vulnerabilities are exploited, they cause a buffer overflow, crash and restart the camera. The third vulnerability identified allows a camera to be fully unplugged. Bluetooth is used to deliver newer, non-existent Wi-Fi SSID settings to this vulnerability. Attackers targeting Bluetooth cameras took use of these L2CAP flaws. To address the vulnerabilities, users should make sure their devices are updated and the latest patches are implemented.

C. Smart Home Personal Assistant Application Hack

To this assault, Blue Borne attacks that exploit L2CAP vulnerabilities are carried out. The Amazon Echo contains a remote code execution vulnerability in the Linux kernel, as well as a data disclosure issue in the SDP server. The vulnerability depended on the operating system of the version. The vulnerability found in Google Home was in the Bluetooth stack

of Android and was characterized as a vulnerability to exposure of information. If exposed, the vulnerability of Google Home may cause DoS. It's important to remember that Bluetooth on these devices can't be turned off, which means they were vulnerable to these assaults prior to the updates and automatic updates. The kind of assaults illustrated above might be carried out by an intruder who is in the range of personal helpers. Manufacturers should correct and distribute patches; thus, on these devices, users should constantly verify that they are up to date.

D. Smart Home Smart Lock Hacks

The vulnerability comes in the way manufacturers constructed the lock's Bluetooth data exchange with the required smartphone app. These vulnerabilities have been identified in the Link Layer Protocol and Link Manager Protocol. In certain circumstances passwords were delivered in unencrypted, allowing anyone with the capacity to grab passwords via Bluetooth sniffing. Passwords were sent twice in other cases, allowing attackers to change the intercepted credentials and lock the user. The Bluetooth communication passwords are encrypted by certain lock manufacturers. However, the locks may be unlocked using passwords that are still encrypted. Attackers did not have to decipher lock open passwords. Attackers might potentially conduct MITM attacks between the lock and the linked app or place an error condition on the lock by modifying a byte in a proprietary encryption.

VII. Bluetooth Risk Countermeasures and Mitigation

To protect against Bluetooth vulnerabilities, Bluetooth devices need software updates. The general public and the user community cannot develop these upgrades. As a result, Bluetooth devices remain susceptible to assaults even when mitigation options are available. Whilst it is impossible to prevent all attacks and the security of Bluetooth communications, counter measures can be utilized [1].

As mitigation techniques, must provide users with an insight into proper Bluetooth security practices. As the best security practices, Standard settings to achieve optimal standards should be updated, should ensure that devices are in a safe range, need to change the default device PIN and update this PIN frequently, PIN numbers should be lengthy and unpredictable, making them less vulnerable to brute force attacks. Devices are placed into undiscoverable mode by default, with the exception of pairing needs. The majority of active discovery techniques need the identification of devices that are discoverable. Undiscoverable devices are not displayed on other Bluetooth devices. Pre-configured devices are better known as trusted devices and in this hidden mode can connect and communicate. Also, Users should use Secure Simple Pairing for the pairing exchange procedures, where possible, rather than the legacy PIN authentication because of reduce the PIN cracking. Always accept only trusted devices. Users never should accept unknown or suspect device transmissions [1].

To eliminate eavesdropping and passive eavesdropping, another mitigating option is to encrypt all data flows using link encryption. Furthermore, peer authentication for network-connected devices is required to ensure the network connection is real. When using multi-hop communication, users should make certain that all connections are secured. If this isn't done, the communication chain as a whole might be jeopardized [1].

Should reduce the risk of broadcast interceptions through broadcast encryption and to protect devices from brute-force attacks users should use the maximum size of the encryption key. Furthermore, with Service level enforced security mode and encrypted key exchange, the minimum suggested key size is 128 bits. [1].

As the mitigation techniques can implement applications like Bluetooth firewall and Bluetooth file transfer applications. In particular Android devices the Bluetooth Firewall helpful for secure the devices from all Bluetooth-related attacks. It can notify activities to users. In moreover, Bluetooth file transfer programs may only connect approved devices.

As stated above, Bluetooth technology and appropriate security practices should be trained by users. Users should take due care of the security features and capabilities of the device before purchasing IoT equipment. Device owners should frequently do the firmware updates or patches issued.

The manufacturers of Bluetooth IoT products should identify and apply security principles during the entire process. The development of threat models and the use of know-how derived from prior assaults might assist avoid future intrusions and forecast future threats.

VIII. Conclusion

In wireless devices globally, Bluetooth has become a widespread feature. Bluetooth technology is the ideal solution for the connection of telephones, televisions, speakers, computer accessories, earbuds, IoT-based vehicles, medical equipment with IoT. This has also been aided by the ability to take use of the technology's capabilities for short-distance voice and data transfer.

This study explores Bluetooth security, including security services and features. In various Bluetooth versions, we discussed vulnerabilities, and numerous Bluetooth threats, Bluetooth risk, and countermeasures have also been examined. Finally, mentioned Bluetooth's risk mitigation and given

suggestions on how to keep Bluetooth interactions trustworthy. At the moment, both Technology and Bluetooth devices are vulnerable to a variety of security flaws. As a result, clients must understand how to use Bluetooth on their devices, as well as mitigation measures for protecting their devices and data from attackers. The precautions listed above will assist to reduce any hazards linked with Bluetooth.

REFERENCES

[1] J.Hayajneh, "An Investigation of Bluetooth Security Vulnerabilities", 7th IEEE Annual Computing and Communication Workshop and Conference, Las Vegas, NV, USA, 9–11 January 2017.

[2] "Guide to Bluetooth Security": Recommendations of the National Institute of Standards and Technology, Maryland, MD, USA, 2008.

[3] Guide to Bluetooth Security. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf (accessed on 6 June 2018).

[4] Khanna, V.Tuncay, G.Want, Kravets, "Bluetooth low energy in dense IoT environments", 2016.

[5] Hayajneh, Almashaqbeh, Vasilakos, "A survey of wireless technologies coexistence in WBAN," 2014.

[6] Sairam, Gunasekaran, "Bluetooth in wireless communication", 2002.

[7] Jordan, R.; Abdallah, "Wireless communications and networking",2002

[8] "Bluetooth Versions and Bluetooth 4.0 Low Energy Development Resources". Available online: https://www.cnx-software.com/2013/06/05/bluetooth-versions-walkthrough-and-bluetooth-4-0-low-e (accessed on 6 June 2018).

[9] "Eavesdrop on and Take Part in Nearby Bluetooth Conversations". 2005. Available online: https://www.theinternetpatrol.com/the-car-whisperer-eavesdrop-on-and-take-part-innearby-bluetooth-conversations/ (accessed on 1 May 2016).

[10] Be-Nazir Ibn, "Bluetooth security threats and solutions" 2012.

[11] "Bluetooth Threat Taxonomy". Available online: https://vtechworks.lib.vt.edu/bitstream/ handle/10919/76883/etd-10242010-163002_Dunning_JP_T_2010.pdf?sequence=1&isAllowed=y) (accessed on 13 April 2018).

[12] "Bluetooth Security", Available online: https://cs.stanford.edu/people/eroberts/courses/soco/projects/ 2003-04/wireless-computing/sec_bluetooth.shtml (accessed on 6 June 2018).

[13] Shaked, "Cracking Bluetooth PIN". Available online: http://www.eng.tau.ac.il/~yash/shakedwool-mobisys05/ (accessed on 6 June 2018).

[14] "The Attack Vector BlueBorne Exposes Almost Every Connected Device." Available online: https://www. armis.com/blueborne/ (accessed on 6 June 2018).

[15] IT-Wachdienst.,*"BlueBump" Available online: https://trifinite.org/trifinite_stuff_bluebump.html (accessed on 6 June 2018).*