COMPUTERS & SECURITY 74 (2018) 308–322

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Security threats in Bluetooth technology

Shaikh Shahriar Hassan [a], *Soumik Das Bibon* [a], *Md Shohrab Hossain* [b], *Mohammed Atiquzzaman* [c,*]

[a] *Department of Computer Science and Engineering, Ahsanullah University of Science and Technology, Dhaka, Bangladesh*
[b] *Department of Computer Science and Engineering, Bangladesh University of Engineering and Technology, Dhaka, Bangladesh*
[c] *School of Computer Science, University of Oklahoma, Norman, OK, USA*

ARTICLE INFO

Article history:
Available online 18 March 2017

Keywords:
Bluetooth threat
Security attack
DoS attack
Worm
Trojan

ABSTRACT

Bluetooth allows connecting mobile devices in short range in order to transfer files/videos. It is now a popular means of short range wireless communication. Although Bluetooth is acceptably reliable, there are still some weaknesses in this protocol. Bluetooth is vulnerable to several threats. Since these threats are seldom reported, people are not much aware of them. Existing surveys on Bluetooth security outline only a few threats without much illustration and categorization. In this paper, we have performed a comprehensive survey to identify major security threats in Bluetooth communication and presented them with illustrations. Although Bluetooth device manufacturers are doing their part to keep the technology secure, the users should also be aware of these security threats and take a minimum level of precaution. The objective of this paper is to provide a comprehensive survey of existing threats in Bluetooth technology and suggest probable solutions.

© 2017 Elsevier Ltd. All rights reserved.

1. Introduction

From the very inception of the network and communication era, wires have been used to exchange data. Bluetooth is one of the solutions to a wireless communication. First invented in 1994 and ever since then it has been a popular technology, primarily due to being a cost free technology. Since Bluetooth use unlicensed ISM band, it does not require any regulatory authority and consumes very limited power. Moreover, Bluetooth is an automated technology that requires no extra setup to initiate a communication. Devices of different manufacturers and models can easily communicate without any compatibility error through Bluetooth. People can easily share files, photos, music, videos, etc. through Bluetooth. For all these reasons Bluetooth is a well preferred and frequently used technology.

Bluetooth technology is available nearly in every phone, tablet, PDA, laptop, gaming console, smart card reader and many other electronic gadgets. However, Bluetooth is prone to several attacks and malware infections. Attacks may steal, alter or delete sensitive data (such as personal photos, videos, banking information, credit card numbers, text messages, calendar schedule, email messages, contact information, etc.) from the device, cause financial loss, eavesdrop communication, gain full control of the device, track and manipulate the activities of the victim. DoS attacks may paralyze the device and may also drain out the battery very quickly. Malware infection may corrupt the system, infect files, steal personal information, cause financial damages by sending SMS, MMS or forwarding call. Therefore, security of Bluetooth communication is very crucial.

Bluetooth technology has some vulnerabilities. A group of wireless devices may connect to one another via Bluetooth technology in an ad-hoc fashion (Ullah, 2009), thereby forming a piconet. Here, the network topology may change dynamically due to the movement of the devices inside the piconet (Colleen, 2006). In ad-hoc networks, centralized security management

* *Corresponding author.*
E-mail address: atiq@ou.edu (M. Atiquzzaman).
https://doi.org/10.1016/j.cose.2017.03.008
0167-4048/© 2017 Elsevier Ltd. All rights reserved.

system is absent. The frequency hopping sequence of a piconet can be determined through the use of inexpensive tool kit and free open source software (Padgette et al., 2012). Moreover, every Bluetooth device has a unique Bluetooth device address. Using this address a certain Bluetooth device can be identified, tracked and monitored (Colleen, 2006). All these facts together make Bluetooth devices vulnerable to attackers and malware. As a result, the security of Bluetooth is skeptical.

There are a few research works available in the literature on Bluetooth security threats. Some of the works (Babamir et al., 2010; Bose and Shin, 2006; Haataja et al., 2013; Iqbal et al., 2010; Lawton, 2008; Mutchukota et al., 2011; Nilsson et al., 2007; Zanero, 2009) are confined to a particular type of attack, such as Man-In-the-Middle (MITM) attack, DoS attack, pin cracking attack, etc. Few other works (Chen et al., 2013; Colleen, 2006; McFedries, 2005) discussed only a limited number of threats with little explanation. They did not cover all the Bluetooth threats. There are a few works (Dunning, 2010; Kumar, 2011; Minar and Tarique, 2012; Padgette, 2009; Panigrahy et al., 2011; Panse and Panse, 2013; Tan and Masagca, 2011) that describe the security threats of Bluetooth without much illustration and categorization, neither did they rate the severity of the threats. Therefore, there is a lack of survey work that compiles all the security threats on Bluetooth technology in a comprehensive manner with illustrations and categorizations.

The *objective* of this work is to perform a comprehensive survey to identify and categorize major security threats in Bluetooth communication and present them with illustrations. *No such comprehensive survey* on Bluetooth security exists in the literature.

The *contributions* of this work are (i) survey of Bluetooth security loopholes with illustrations, (ii) classifying the threats according to their severity, and (iii) proposing techniques for mitigation of the attacks.

This paper will help general users of Bluetooth technology to know the possible vulnerabilities of this technology and the countermeasures to mitigate those threats.

The rest of the paper is organized as follows. In Section 2, we discuss the existing works on Bluetooth security. In Section 3, we explain Bluetooth technology and its architecrue briefly. Vulnerabilities in the architecture are pointed out. Section 4, we define and categorize Bluetooth threats. We also describe a brief history of threats on Bluetooth devices. In Section 5, attacks on Bluetooth are categorized and described elaborately with illustration. In Section 6, malwares on Bluetooth are categorized and described elaborately with illustration. Section 7 gives few probable solutions to mitigate the attacks. Finally, Section 8 has the concluding remarks and few guidelines for future research.

2. Existing works

Some of the existing works on Bluetooth security only focus on a specific type of attack on Bluetooth. Haataja et al. (2013) discussed Bluetooth security mechanism including secure simple pairing. Mutchukota et al. (2011) made a comparative study on Bluetooth MITM attacks and proposed how the existing simple secure pairing can be improved to prevent MITM attacks. Iqbal et al. (2010) described weaknesses in existing security architecture and proposed a secure architecture to prevent MITM attack and DoS attack. Nilsson et al. (2007) discussed secured piconet for Bluetooth based on pin cracking attack. Babamir et al. (2010) described attacks with mining and analyzing curve by using the Petri-Net tools. But this work (Babamir et al., 2010) is limited to only Blue-Snarfing, Blue-Jacking and Blue-Bugging. However, each of these works (Babamir et al., 2010; Haataja et al., 2013; Iqbal et al., 2010; Mutchukota et al., 2011; Nilsson et al., 2007) is confined to a particular type of attack. For example Haataja et al. (2013) and Mutchukota et al. (2011) are only limited to the MITM attack and Iqbal et al. (2010) is confined to MITM attack and DoS attack. Nilsson et al. (2007) is qualified to pin cracking attack and they did not mention about any other type of attacks.

Zanero (2009) and Bose and Shin (2006) described some Bluetooth worms but they failed to classify the worms. Lawton (2008) made a generic discussion on mobile malware only, did not focus on Bluetooth. Chen et al. (2013) discussed security modes of Bluetooth and authentication process. They also mentioned few Bluetooth threats. Colleen (2006) and McFedries (2005) discussed some vulnerabilities. However, these (Bose and Shin, 2006; Chen et al., 2013; Colleen, 2006; McFedries, 2005; Zanero, 2009) are simple surveys on Bluetooth threats without much explanation.

Kumar (2011), Panigrahy et al. (2011), and Minar and Tarique (2012) described the threats elaborately. Tan and Masagca (2011) discussed Bluetooth security threats along with perception and awareness of the threats. Panse and Panse (2013) discussed Bluetooth vulnerabilities and counter measures. Dunning (2010) classified only a few Bluetooth threats and proposed few risk mitigation approaches. Padgette et al. (2012) and Padgette (2009) described the Bluetooth security modes as well as security risk and mitigation in general. They discussed Bluetooth security issues and vulnerabilities based on the version of the Bluetooth technology along with with risk mitigation and countermeasures. However, these works (Dunning, 2010; Kumar, 2011; Minar and Tarique, 2012; Padgette et al., 2012; Padgette, 2009; Panigrahy et al., 2011; Panse and Panse, 2013; Tan and Masagca, 2011) did not categorize the attacks and did not rate the severity of the threats.

As discussed in this section, there is a lack of survey work on Bluetooth security that compiles all the security threats on Bluetooth technology with illustrations. The objective of this paper is to provide a comprehensive survey of existing threats to Bluetooth technology, thereby letting users know about these vulnerabilities. We have performed a *comprehensive survey* to identify major security threats for Bluetooth technology and presented them with illustrations.

3. Background

3.1. *Bluetooth*

Bluetooth is a wireless technology widely used for exchanging data by connecting devices. The name Bluetooth came from a 10th century Danish King, Harald Blatand (in English Harold Bluetooth). He united warring nations of DenmarkNorway. Bluetooth does exactly the same thing; it unites wireless devices (Bluetooth). Bluetooth was invented by a Swedish

Telecommunication Company, Ericsson in 1994 as a replacement of RS-232 data cables. In 1999, Bluetooth Special Interest Group (SIG) was formed by Ericsson, Intel, IBM, Nokia, and Toshiba. It is a non-profit association that serves as the governing body for Bluetooth and holds the name and logo trademark of Bluetooth. Today, Bluetooth SIG has over 30,420 member companies (Mark, 2014).

Bluetooth uses Ultra High Frequency (UHF) radio waves. The effective range of operation between two Bluetooth devices is from 10 to 100 meters. However, this range can be extended up to a mile by using a directional antenna and an amplifier. It operates between the frequency range of 2402 MHz to 2480 MHz and uses guard bands of 2 MHz at the bottom and 3.5 MHz on the top. Bluetooth uses the unlicensed (2.4000 to 2.4835) GHz ISM (Industrial, Scientific, and Medical) band. Therefore to use Bluetooth local communication authority is not required, thereby making Bluetooth a cost free technology. Bluetooth technology is a combination of both circuit switching and packet switching. Therefore, it supports both synchronous voice channels and asynchronous data channels. Bluetooth communicates by frequency hopping spread spectrum (FHSS) using 79 different radio channels, each of the channels is 1 megahertz (MHz). It hops 1600 times per second which decreases transmission interference and provides a minimum extent of transmission security.

Bluetooth exchange data between two devices in the form of packet. A packet consists of Access Code, Header, Payload. In order to establish a connection between two devices the first and foremost step is to look for another Bluetooth device within the range. This is done by sending a ID Packet. Any device interested to establish a link will respond by sending a Frequency Hop Synchronization (FHS) Packet. The device which initiate the connection is called the master device. Bluetooth devices communicate by forming an ad-hoc networks, known as piconets. Every piconet has its own timing clock and frequency hopping sequence so that the communication of one piconet is not overlapped with the other nearby piconets. Each piconet has only one master device and number of slave devices. Bluetooth provides a half-duplex communication channel. Slaves of a specific piconet cannot communicate among themselves directly, they depend on the master device for transit. A Bluetooth device of a particular piconet may carry out communication with multiple piconets at the same time by using time division multiplexing (TDM). A collection of piconet is called scatternet. Two or more piconets can share information forming a scatternet.

There are mainly two types of Bluetooth devices: (i) Basic Rate/Enhanced Data Rate (BR/EDR) device which is also called "Classic Bluetooth device", and (ii) Bluetooth Low Energy (LE) device which is also called "Smart Bluetooth device". These two types of devices have different architectures and cannot communicate to each other. To overcome this issue, dual mode (consisting of chipsets of both BR/EDR and LE devices) was introduced that enables communications between both types of Bluetooth devices.

3.2. *Bluetooth core architecture*

The core components of Bluetooth architecture are (i) Bluetooth Controller, (ii) Host Controller Interface (HCI) Transport Layer, and (iii) Bluetooth Host. Bluetooth core architecture is shown with a block diagram in Fig. 1 (Bluetooth core system).

3.2.1. *Bluetooth controller*

Bluetooth controller is a hardware on which the Bluetooth technology stands. It consists of three layers (i) Link Manager layer, (ii) Baseband Layer, (iii) Radio Layer. Each layer has its own protocol implementation and provides different applications and services. Bluetooth controller is responsible for establishing connection to the host through Host to Controller Interface (HCI) (Alcorn, 2011). The main protocols are the radio (RF) protocol, link control (LC) protocol, and link Manager (LM) protocol.

- Link Manager Layer: This layer is responsible for initiating a link between two Bluetooth devices.

Link Manager communicates with link manager of remote Bluetooth device and creates link between two devices. It also modifies or terminates the link if required.

Device Manager does not take active part in data transmission but it is responsible for maintaining all other functions of the device. It looks for nearby Bluetooth devices and controls whether the device will be discoverable by other devices.

- Baseband Layer: This layer is responsible for establishing a link between Bluetooth devices by using radio frequency. Baseband Resource Manager controls the access to the Bluetooth channel. It also schedules the data packets. Link Controller controls acknowledgement and retransmit request signal. It also encodes and decodes the data packets.
- Radio Layer: The responsibility of this layer is to send and receive Bluetooth data packets.

3.2.2. *Host controller interface (HCI)*

Transport Layer: This layer acts as a liaison between Bluetooth host and Bluetooth controller. Bluetooth host communicates with Bluetooth controller by sending and receiving commands through HCI layer.

3.2.3. *Bluetooth host*

Bluetooth Host constructs the logical layers of Bluetooth technology. This component of the Bluetooth architecture is responsible for connecting and exchanging data with Bluetooth Host of another peripheral device. Bluetooth Host contains Logical Link Control and Adaptation Protocol (L2CAP) which detects error in data transmission and if error is detected it retransmits data. It consists of (i) Bluetooth Stack, and (ii) Bluetooth Profile.

There still exist some extent of vulnerability in the Bluetooth architecture. Link Manager Layer can be breached and attacker can establish link with the victim device. Data packets encoded by the Baseband Layer can be deciphered by the attacker and information can be extracted. Radio Layer can be manipulated and data transmission can be intruded.

4. Bluetooth security threats

Any action that is pernicious to a system can be termed as a threat. Threats are danger that might cause harm to the system.

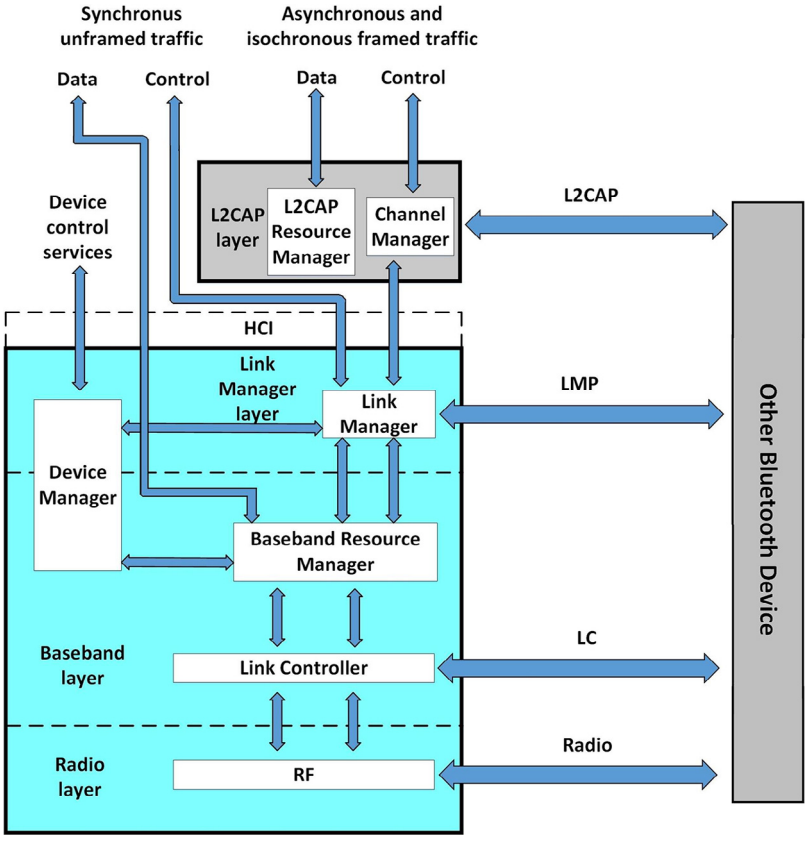


Fig. 1 – Bluetooth core architecture (Bluetooth core system).

They are constantly evolving and changing their methods of penetration. Different threat leaves different effects on the system.

According to the glossary of key information security terms by National Institute of Standards and Technology (NIST), threat is defined as "Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service" (Kissel).

There are a number of security threats for Bluetooth and they can be broadly divided into two types: (i) Attacks and (ii) Malware.

4.1. *Attacks*

Attack is an attempt to gain unauthorized access to victim device without the knowledge of the victim. It is meant to destroy, alter, disable, or steal data from the victim. Attacks on Bluetooth devices may be active or passive. Attacker may directly breach the security system of the device and gain control of the victim device. Again attackers may manipulate the victim or apply different schemes to gain control of the victim device.

In the glossary of key information security terms by NIST, attack is defined as "An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity." or "Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself" (Kissel).

4.1.1. *Evolution of bluetooth attacks*

Since most of the Bluetooth attacks are undetected and unreported, it is not specifically known when and how the first Bluetooth attack was carried out. But there are some information regarding the detection of some of the attacks. In 2001, researchers at Nokia Bell Labs detected flaws in the pairing mechanism and mentioned that Bluetooth communication can be intruded. The first PIN cracking attack was detected in April 2005 by researchers at Cambridge University. Surveillance attack using Bluetooth device was first reported in August 2005 by police department at Cambridgeshire, England.

4.2. *Malware*

Malware is a malicious software that is programmed with an intention to do harm. The term malware was coined by Yisrael Radai in 1990. Malware comes in various forms.

In the glossary of key information security terms by NIST, malware is defined as "A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victims data, applications, or operating system or of otherwise annoying or disrupting the victim." (Kissel). Bluetooth malware can further be divided into two types (i) Trojan and (ii) Worms.

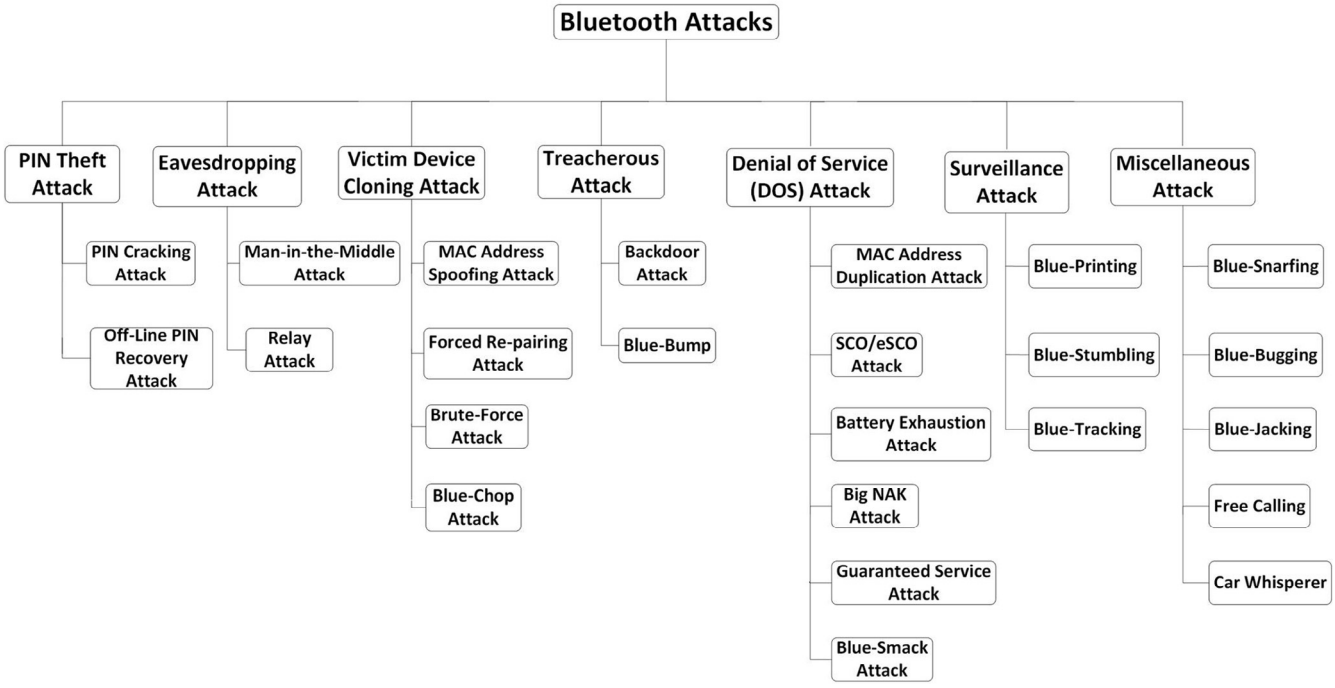


Fig. 2 – Classification of bluetooth attacks.

4.2.1. *Evolution of bluetooth malware*

The first Bluetooth worm was Cabir which was reported to infect Symbian OS in 2004 almost 7 years after the invention of Symbian OS. Cabir took epidemic form during the 10th World Athletics Championship in August 2005 which took place at Helsinki, Finland (Peng et al., 2014). It took such a severe form that warning was displayed on the big screen of the stadium. Comm-Warrior was first detected in March, 2005 (Hypponen, 2006). Other worms like skull, Drever, Card-Block etc. were reported in the consecutive years. The latest Bluetooth Trojan reported is Obad which was discovered on 4th June 2013 (Cortes, 2013). There is no recent report on Bluetooth attacks or malwares, but this does not mean that Bluetooth is absolutely secure.

5. Bluetooth attacks

Bluetooth attacks are classified in Fig. 2. Attacks which follow similar method of penetration or leave same effect on the victim are grouped under one single title. Severities of attacks are listed in Table 1. These attacks are classified as high, medium and low based on the extent of effects they leave on the victim. Attacks that gain full control of the victim device and can steal, alter or delete data from the memory or external storage of the victim device are categorized as high severity attacks. These threats may also cause financial damage to the victim. Attacks that steal data and extract information from the victim device during the transmission of data between two or more Bluetooth devices are categorized as medium severity attacks. Attacks that track the victim, monitor the activities of the victim or create disturbance to the victim are categorized as low severity attacks.

The security threats are described and illustrated in the following subsections chronologically as they are represented in Fig. 2.

5.1. *Pin theft attack*

These attacks involve stealing the PIN and subsequently establishing a connection with the victim device with an intention to carry out malicious activities.

5.1.1. *PIN cracking attack*

In order to start communication between two Bluetooth devices, a trusted relationship must be established. This process is known as pairing which is done by exchanging secret codes, a.k.a., Personal Identification Number (PIN). The PIN can be 1 to 8 bytes long. Then pairing is completed in 4 steps.

1. Initialization key Generation
2. Link key Generation
3. Authentication
4. Encryption

The attacker eavesdrops the entire process of pairing and authentication and collects all the messages. Next, the

Table 1 – Severity of bluetooth attacks.

High severity	Medium severity	Low severity
PIN Cracking Attack	Man-in-the-Middle 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	Brute-Force Attack	Blue-Tracking
Blue-Bugging	Blue-Bump	Blue-Jacking
Free Calling		
Car Whisperer		

attacker uses a brute force algorithm to find the PIN used. Then the attacker lists all the possible permutations of the PIN. If the MAC Address of Bluetooth Device is already known then by using a 128-bits random number, correct initialization key can be detected. The next step is to find the shared session link key using all the collected data. If all the collected information is correct PIN can be easily cracked (Nilsson et al., 2007; Shaked and Wool, 2005). Once the attacker cracks the pin, then he can pair with the victim device and can steal data without the consent of the victim.

5.1.2. *Off-line PIN recovery attack*

Off-line PIN recovery attack is the method of intercepting the PIN in order to get access to the victim device. First of all an initialization key, IK (128 bits) is generated by using a device MAC Address (48 bits) and the PIN code with its length. Using this initialization key the devices generate two random values RAND-1 (128 bits) and RAND-2 (128 bits). These two random values are used by the devices to create the link key in-order to establish connection. By using a decryption algorithm the PIN is calculated. It is shown with illustration in Fig. 3. In this method it is not certain that an attacker can discover the PIN correctly, but there is a possibility of discovering the PIN code if the PIN is short in length (Minar and Tarique, 2012; Shaked and Wool, 2005). Once the attacker recover the pin, then he can pair with the victim device and can steal data without the consent of the victim.

5.2. *Eavesdropping attack*

In the eavesdropping attack, the attacker taps into the communication between the two victim devices and steals information. The following subsection explains two of the eavesdropping attacks.

5.2.1. *Man-in-the-middle attack*

This is the method of accessing and modifying the data that are transmitted between the Bluetooth devices by using a fake Access Point. The first and foremost job of the attacker is to persuade both the victim devices to use same hopping sequence, so that attacker can easily breach the transmission security (Herfurt and Mulliner, 2005). The communication between two devices is intercepted by the attacker and then the attacker manipulates the obtained data as shown in Fig. 4. The attacker intercept between the two devices in such a way that the victims think nothing is wrong. In this attack, the attacker has no access to the victim devices. The attacker can only access the data that are transmitted.

In Raphael and Phan (2012) and Sandhya and Devi (2012), authors mentioned that Man-in-the-Middle attack may also occur due to flaws in pairing process, when a device wants to connect to a device but mistakenly connects to a different device.

5.2.2. *Relay attack*

In relay attack, attacker connects two dummy devices to both the victim devices. Victims are unaware of this and they think that they are communicating between each other. But actually victims are transmitting information to the attacker devices. Attacker devices eavesdrop the communication and continuously give feedback to the victim devices (Nilsson et al., 2007). As a result, the attack is not detected. Relay attack is also called Reflection attacks.

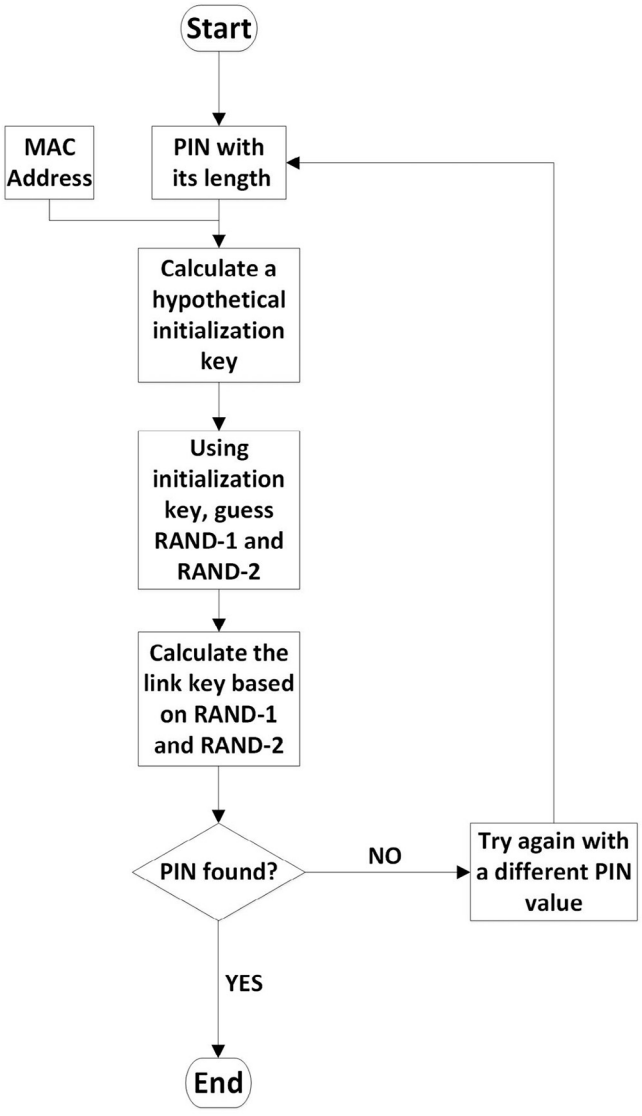


Fig. 3 – Off-line PIN recovery attack.

5.3. *Victim device cloning attack*

These attacks are done by stealing the device address of the victim. Then the attacker clones itself as that of the victim and pursue the attack.

5.3.1. *MAC address spoofing attack*

Bluetooth MAC address consists of 48-bits identifier which uniquely defines a Bluetooth device. Out of these 48-bits, first 24-bits are manufacturer identifier, which is unique to the manufacturer of the device. And the last 24-bits are random but unique values assigned by the manufacturer. This can be represented as MM:MM:MM:XX:XX:XX. Here M refers to the manufacturer of the device and X refers to random values that uniquely define a device.

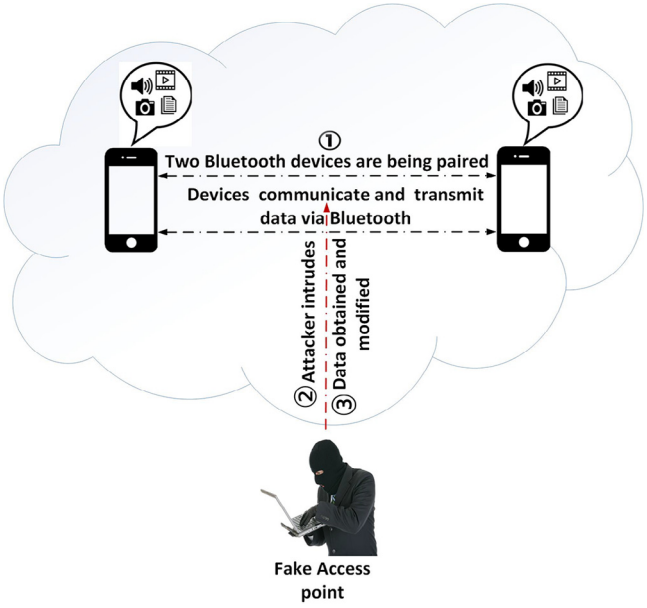


Fig. 4 – Man-in-the-middle attack.

In Cross et al. (2008), authors divided 48-bits the MAC address into 3 parts. The first 16-bits are non-significant address part (NAP) and the next 8-bits are the upper address part (UAP). NAP and UAP together form the manufacturer identifier. The last 24-bits are lower address part (LAP).

MAC Address Spoofing Attack is done with an intention to steal data from the device. MAC addresses of two Bluetooth devices can be detected by eavesdropping the communication. This is because the header of the transmitted data contains the MAC addresses of both the sender and the receiver devices. In this attack, the MAC address of a Bluetooth device is changed to some other value to that of the victims device. In other words, the attacker device is cloned as the victim device, as shown in Fig. 5. As a result, data sent to the victim reach the attacker before it gets to the victim. The attacker gets the data and then he may forward the data to the victim's device so that the attack is undetected (C. PGP, 2016).

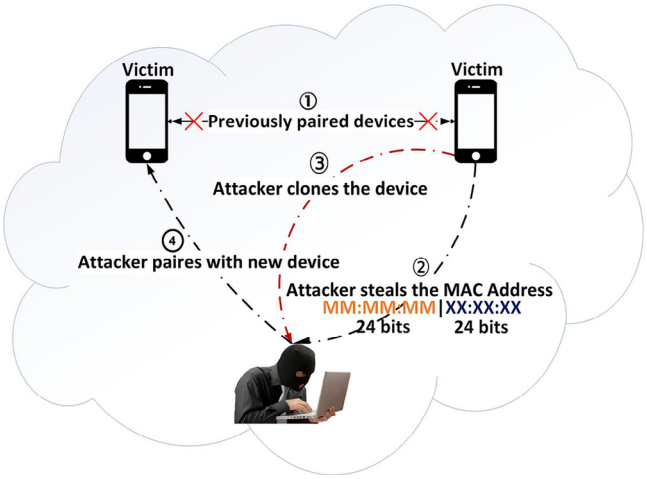


Fig. 5 – MAC address spoofing attack.

5.3.2. *Forced re-pairing attack*

When two Bluetooth devices want to communicate, they share a link key by the pairing process. This link key is saved into the device so that next time they try to communicate, they do not need authentication because the link key is saved in both the devices. In forced re-pairing attack, the attacker spoofs the MAC address of any one of the already paired devices. So, next time when the victims try to communicate the victim whose MAC Address is not spoofed will be forced to re-pair with the attacker device.

5.3.3. *Brute-force attack*

Brute-Force involves scanning the MAC address of a Bluetooth device. Brute-Force is used on the last 24 bits of MAC address, assuming that the first 24 bits are already known and fixed (Minar and Tarique, 2012). There are approximately 16.8 million possible combinations which will require an average of 8.4 million attempts to guess. But by using a smart toolkit and free open source software, it is not difficult for an attacker to find it. Once the MAC address of the victim device is determined, the attacker changes his MAC address to that of the victims MAC address and eavesdrops the victim.

In Cross et al. (2008), authors proposed a faster and effective Brute-Force methodology which scans the paging channels associated with the MAC addresses. As a result, it can determine the MAC address of non-discoverable Bluetooth devices.

5.3.4. *Blue-chop*

Blue-Chop attack is the method of creating disturbance in the Bluetooth piconet. It is not meant to harm the victim by stealing or altering files. The attacker spoofs the Bluetooth device address of a random device that is already participating in the piconet. This attack is only possible if the master device of the piconet supports multiple connections (Herfurt and Mulliner, 2005). Once the attacker makes his way inside the piconet, it continuously sends a connection request to all the devices causing a disturbance. Therefore, it clogs the piconet and hampers the regular flow of communication of that piconet.

5.4. *Treacherous attack*

These attacks are based on establishing a trusted relation between the devices and then breaking the trust. Therefore the attacker can take full control of the victim device.

5.4.1. *Backdoor attack*

The backdoor attack is the method of gaining trust of the victim device through the pairing mechanism. It ensures that the attacker's device does not appear on the victims list of paired devices. In this way, the attacker can monitor the activities of the victim device, shown in Fig. 6. The attacker can retrieve data from the victim device and access services such as modems, Internet, WAP and GPRS gateways etc. without the concern of the victim (Colleen, 2006; Minar and Tarique, 2012).

5.4.2. *Blue-bump*

Blue-Bump is a social engineering technique. First, the attacker sends a text, image, video or business card to the victim device and gain the faith of the victim. Then the attacker

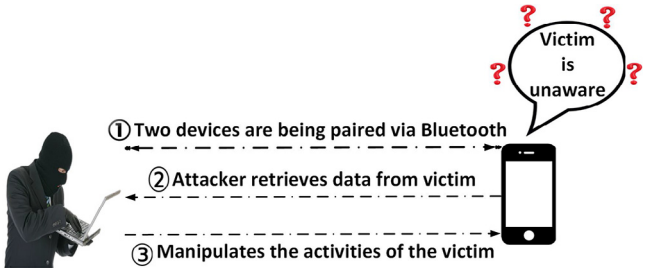


Fig. 6 – Backdoor attack.

persuades the victim to delete the link key that was established during the transaction by keeping the connection open. While the victim is unaware of the open connection, the attacker requests the victim to initiate another link-key. Now, the attacker device remains concealed in the paired list of the victim device and remains connected with the victim. To the victim the attacker device seems a complete new device (Herfurt and Mulliner, 2005).

5.5. *DoS attacks*

DoS attack stands for Denial of Service attack. DoS attack does not cause any harm to the victim by stealing or altering information from the victim device. It temporarily paralyzes the victim device by making resources unavailable to the victim. It creates unnecessary traffic to the network and jams the network. DoS attack is simply meant to cause disturbance to the victims. It is almost impossible to prevent DoS attack. There can be six different types of DoS attacks which are listed below. A comparative study of the DoS attacks are shown in the Table 2.

5.5.1. *MAC address duplication attack*

MAC Address duplication attack is the method of hacking the device address of the victim. Then the attacker clones itself using the stolen MAC Address and the attacker device is placed in the communication range of the victim device. Whenever any device tries to establish a communication with the victim they mistakenly connect to the attacker.

5.5.2. *SCO/eSCO attack*

SCO stands for Synchronous Connection Oriented link. It is a radio link that maintains a set of reserved timeslots on an existing piconet. And eSCO stands for Enhanced Synchronous Connection Oriented link. It is an advanced version of SCO. SCO/eSCO attack reserves a great portion of a Bluetooth Piconet. As a result, the devices connected in that piconet will not receive the desired service in due time.

5.5.3. *Battery exhaustion attack*

Bluetooth devices operate on battery. So it is important to conserve the battery power of these devices. Battery exhaustion attack does hot harm the victim or damages the victim device. It attacks the processor of the victim device and engages the processor making the system unstable. As a result, battery power is drained out from the victim device (Premnath and Kasera, 2008). This attack is also called sleep deprivation attack.

5.5.4. *Big NAK attack*

Big NAK (Negative Acknowledgment) attack puts the victim device in an infinite loop of re-transmission as a result the performance of the victim device slows down. The attacker requests data from the victim and when the victim responds, the attacker pretends that he did not receive any reply by sending back a negative acknowledgment. Therefore, the victim keeps re-transmitting over and over again and the victim remains busy throughout.

5.5.5. *Guaranteed service attack*

In this attack, attacker obtains all the attention from the victim by requesting the maximum data rate with minimum delay from the victim device. As a result, all other devices connected to the victim device are ignored. This attack is meant to cause disturbance in the piconet.

5.5.6. *Blue-smack attack*

Bluetooth's L2CAP protocol provides connection-oriented as well as connectionless data services. L2CAP requests and receives data from other Bluetooth devices through L2CAP ping. The size of L2CAP ping of each Bluetooth device is limited. If it receives an L2CAP ping packet which is beyond the size of the L2CAP ping size, the system will crash. The crash may lead to injection of malicious codes (Strobel, 2007).

5.6. *Surveillance*

These attacks are meant to observe the victim closely and extract information about the victim device. These attacks are not directly harmful, rather information gathering for future attacks.

5.6.1. *Blue-printing*

Blue-Printing is the method of determining the details of a device, such as International Mobile Equipment Identity (IMEI) number, manufacturer name, manufacturer details, device

Table 2 – Analogy among DoS attacks.

	Attacking protocol	Jamming piconet	Paralyzing device	Cloning victim device
MAC Address Duplication Attack				✓
SCO/eSCO attack	✓			
Battery Exhaustion Attack			✓	
Big NAK Attack		✓	✓	
Guaranteed Service Attack		✓	✓	
Blue-Smack Attack	✓			

model, and firmware version of the victim (Minar and Tarique, 2012). This attack is not meant to steal any information or do any harm to the victim device. The attacker collects the information about a victim device by using the Blue-Printing attack to plan a further attack on that device.

5.6.2. *Blue-stumbling*

Blue-Stumbling is the method of randomly searching for Bluetooth devices to pursue attack. It is mostly done in crowded place where a large number of Bluetooth devices are available. Attacker mainly searches victim and marks the device with more security flaw that would be easy to hack. It does not cause any harm to the victim, it is only the first step to initiate an attack.

5.6.3. *Blue-tracking*

Blue-Tracking is the method of tracing the location of the victim by following the signal of their Bluetooth Device. It is not meant to steal information from the victim. The attacker has no access to any content of the victim device. Attacker may follow the victim and find his/her house address or workplace address. A data set may also be prepared by observing the location of the victim for some days and the whereabouts of the victim can be predicted at different periods of the day.

5.7. *Miscellaneous attack*

These attacks involve stealing the data from the victim device, bugging the victim device and taking full control of it, conducting spam attack by sending unwanted messages, tapping the Bluetooth based car multimedia kit,hacking the headset, initiating calls etc.

5.7.1. *Blue-snarfing*

Blue-Snarfing has been identified by Marcel Holtmann in September 2003 (Herfurt and Mulliner, 2005). Blue-Snarfing is a method of gaining unauthorized access to a Bluetooth device without the consent of the user. It hacks the device and steals its resources like contact book, text messages, calendar, emails, document files, pictures, and videos or any contents of the phone memory (Minar and Tarique, 2012). It may also divert incoming call or text message from the victim device to another device without the consent of the victim. Blue-Snarfing is illustrated in Fig. 7. An advanced version of Blue-Snarfing is called Blue-Snarfing++. Blue-Snarfing++ can steal resources and can even alter the stored files in the victim device without the consent of the victim, shown in Fig. 8. It may also acquire the international mobile equipment identity (IMEI) of the victim device and divert incoming call or text message from the victim device to many other devices.

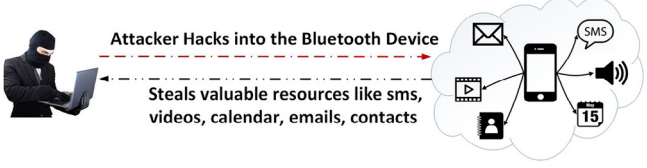


Fig. 7 – Blue-snarfing.

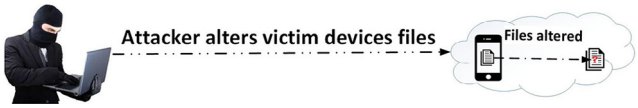


Fig. 8 – Blue-snarfing++.

5.7.2. *Blue-bugging*

Blue-Bugging was unfolded in 2004, by German researcher Martin Herfurt (Herfurt and Mulliner, 2005). It is the method of taking full control of the victim device, shown in Fig. 9. Now the attacker can do anything he wishes. He can steal information without the consent of the victim. The attacker can do even more severe things.

- An attacker can initiate phone calls.
- An attacker can set call forward.
- An attacker can monitor phone calls.
- An attacker can send text messages.
- An attacker can read text messages.
- An attacker can access the Internet and may expose the device to malware infection.
- An attacker can access Global Positioning System (GPS) Service and can track the location of the victim.
- An attacker can edit phone book, calendar, files etc.
- An attacker can reset the entire device settings.
- An attacker can block the network operator and paralyze the device.

Blue-Bugging is an invasion of the privacy of the victim. It may also lead to resource loss and financial damage to the victim (Legg, 2005; Minar and Tarique, 2012).

5.7.3. *Blue-jacking*

Blue-Jacking is the method of sending uninvited messages to Bluetooth devices. This attack does not steal or alter any data from the device. Blue-Jacking is harmless, it is not done with malicious intention, it is done for promotional purposes. It was invented with a view to carry out guerrilla marketing, to advertise about products or services by spending less money. In this attack text message, image, small sound clip, small video clip or electronic business card is sent to the victim device, shown in Fig. 10. This attack is mostly carried out in crowded places like a shopping mall, cinema hall, train station or restaurants. When Bluetooth devices were newly invented it was

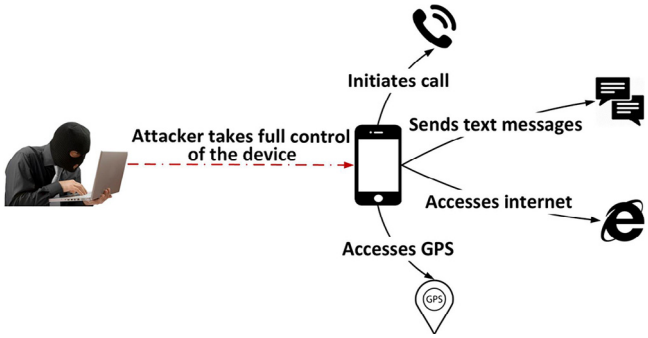


Fig. 9 – Blue-bugging.

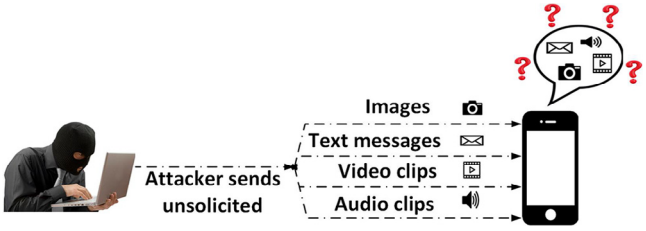


Fig. 10 – Blue-jacking.

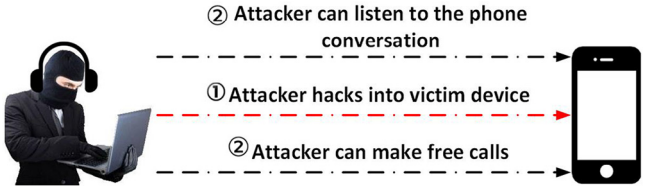


Fig. 11 – Free calling.

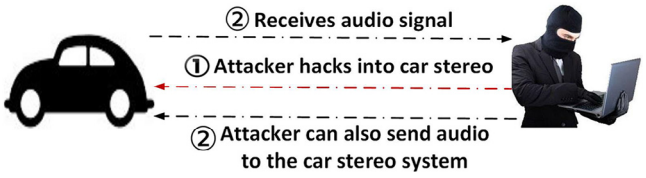


Fig. 12 – Car whisperer.

used to prank people. It is actually a spam and creates annoyance to the victim (Minar and Tarique, 2012; Tan and Masagca, 2011).

5.7.4. *Free calling*

Attacker hacks the victims Bluetooth device and pairs a headset with a Bluetooth system in order to make free phone calls. This attack causes financial damage to the victim as the victim has to pay the cost of the call (Jabra). In addition to that, the attacker can listen to the conversation of the victim using that headset as illustrated in Fig. 11.

5.7.5. *Car whisperer*

Car Whisperer attack is done on Bluetooth car kits. Car Whisperer is actually the name of a software or hardware device by which attacker can receive audio from a Bluetooth enabled car stereo (Panse and Panse, 2013). The attacker can also misguide the victim by sending in audio to the car stereo system like fake traffic information and wrong navigation, shown in Fig. 12. An attacker can also listen to the conversations of the people chatting inside the car.

6. Bluetooth malware

Bluetooth malware are of two types (i) Trojan and (ii) Worms. Types of malware are shown in Fig. 13. Each type has its own method of infection and intention. A detailed overview of known Bluetooth technology malware is presented in Table 3. In the table malware are leveled as high or low based on their severity. Malware that steal data and cause financial damage to the victim are leveled as high severity malware. On the other hand, malware that paralyze the device and cause disturbance to the victim are leveled as low severity malware.

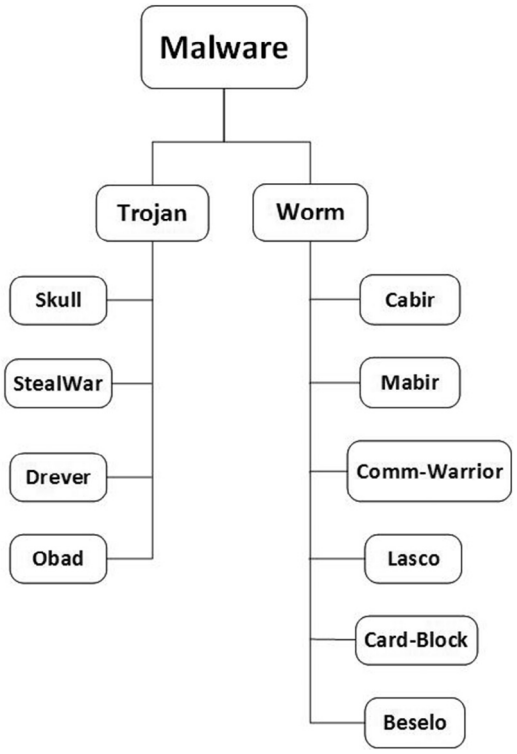


Fig. 13 – Types of bluetooth malware.

6.1. *Trojan*

A Trojan is a malware that tricks the user to gain access to the system and run malacious activities. Trojan is named after the wooden horse that the Greet used to trick Troy. Trojan cannot propagate itself. It may steal sensitive information and may give access to the attacker. Trojan attack is illustrated in Fig. 14.

Some of the Trojans that are spread through Bluetooth are listed as follows:

a) Skull: Skull is a Trojan. If a device is infected with skull, all the phone application icons are replaced with images of a skull. It also makes all phone applications useless and if any application is opened it displays a flashing skull animation. Skull spreads via Bluetooth or SMS (Bose and Shin, 2006). It may also send text messages containing malicious links to all contacts which may cause financial damage to the victims.

b) StealWar: When a device is infected with StealWar, it displays that the device is attacked by some untrusted source and need to install some files to restore the system. Once user clicks install button the Trojan is installed into the system. It may steal personal information from the device. It can transmit via both Bluetooth and MMS.

c) Drever: Drever is a Trojan. It tricks victim by showing that an update of Symbian OS is available and asking the victim

Table 3 – Overview of bluetooth malwares.

Name	Origin	Type	Method of infection	Effects	Operating system	Severity level
Cabir	2004	Worm	Spreads by sending .sis files via Bluetooth	Blocks the UI and drains the battery	Symbian OS	Low
Skull	2004	Trojan	Spreads via Bluetooth or SMS	Makes all phone applications useless and replaces all phone applications with an image of skull	Symbian OS	Low
Mabir	2005	Worm	Spreads by sending .sis files via Bluetooth and MMS	Causes financial damage by sending MMS	Symbian OS	High
Comm-Warrior	2005	Worm	Spreads via Bluetooth and MMS	Causes financial damage by sending MMS	Symbian OS	High
Card-Block	2005	Worm	Spreads via Bluetooth	Corrupts the memory card	Symbian OS	Low
Lasco	2005	Worm	Spreads by sending velasco.sis files via Bluetooth	Infects files and corrupts the system	Symbian OS	Low
Drever	2006	Trojan	Spreads by sending OS update installation file via Bluetooth	Disables Symbian antivirus	Symbian OS	Low
StealWar	2006	Trojan	Spreads via Bluetooth and MMS	Steals personal information	Symbian OS	High
Beselo	2008	Worm	Spreads by sending common media file extensions (e.g., .jpeg, .mp3, .mp4) files via Bluetooth and MMS	Causes financial damage by sending MMS	Symbian OS	Low
Obad	2013	Trojan	Spreads via Bluetooth	Steals information and opens the system to other malicious attacks	Android OS	High

to install the update. It sends the installation file as a .sis file. If the victim installs the file it gets infected. Once a device is infected it can infect other and via Bluetooth. This worm affects the device by disabling Symbian antivirus (Bose and Shin, 2006).

d) Obad: Obad was discovereed in 2013 by Kaspersky Labs at Russia. It is designed for Android Operating System. It is available over the Internet specifically in malicious websites. If user visits those sites Obad automatically downloads into the system. Once a device is infected with Obad it is capable of downloading other malicious programs. It may steal information, send SMS to premium numbers causing financial damage and gain network access (F-secure labs, 2013). The deadly fact is that it remain concealed in the system so it is almost impossible to delete it.

6.2. *Worms*

A worm is a malware that spreads among other devices by self-replicating. An illustration of spreading worm from the infected device to all other nearby devices is shown in Fig. 15. Bluetooth worms were known to widely infect Symbian OS. Some of the worms that are replicated through Bluetooth are listed as follows:

a) Cabir: Cabir worm was originated from Czech Republic and Slovakia in 2004 and known to be the first computer worm that can infect mobile phones. Before that worms were only known to infect computers. An infected device displays, the message "Caribe" on the device's display, and it is displayed every time the phone is turned on. Cabir is a self-replicating worm. Once a device is infected with cabir it continuously scans for nearby Bluetooth devices and spreads among other devices in its range by sending .sis files via Bluetooth. The victim will receive popups asking them to install it. Cabir re-send itself and blocks the UI until installation request is accepted. Once installed the device become infected (Gostev, 2006). Since cabir requires user interaction, it could not infect a large number of devices.

b) Mabir: A derivative of Cabir worm is Mabir worm. It infects the device in the same way as Cabir. The only difference is it replicates both via Bluetooth and Multimedia Messaging Service messages (MMS) (Colleen, 2006). Since MMS charges money, Mabir also causes financial damage to the victim.

c) Comm-Warrior: Comm-Warrior was originated from Russia. If a device is infected by Comm-Warrior it remains silent and inactive in the device. It becomes active on the 14th of every month and resets the phone deleting all personal data. Comm-Warrior is the first known mobile worm that spreads via both Bluetooth and MMS. Once a device is infected it repeatedly scans for nearby Bluetooth devices and

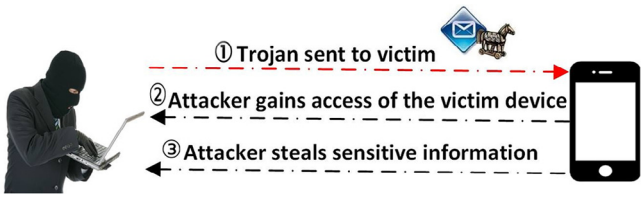


Fig. 14 – Trojan attack.

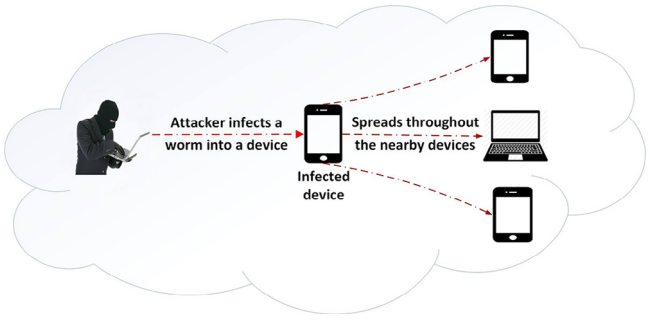


Fig. 15 – Worm propagation.

spread to other devices in its range via Bluetooth. It may also spreads by sending MMS to random numbers from the phone book of victim device and thereby causing monetary loss to the victim (Bose and Shin, 2006).

d) Lasco: Lasso was programmed in 2005 by Marcos Velasco from Rio de Janeiro, Brazi. It infects system files. Once a device is infected it repeatedly scans for nearby Bluetooth devices and spreads to other devices in its range by sending velasco.sis files via Bluetooth.

e) Card-Block: Card-Block attacks the memory card of the device, if there is any memory card available in the device. When a device is infected with this worm, it corrupts the memory card. Once a device is infected it repeatedly scans for nearby Bluetooth devices and spreads to other devices in its range by via Bluetooth (Bose and Shin, 2006). An updated version of Card-Block attack may even permanently block the memory card and destroy it.

f) Beselo: When people became aware of .sis extension of worms then Beselo was introduced with common media file extensions (e.g., .jpeg, .mp3, .mp4). It is a self-replicating worm that spreads through Bluetooth connections and MMS messages (La Polla et al., 2013). Beselo is dangerous as victim gets tricked easily. Victim accepts it thinking that it is a common media file containing pictures, audio or video clips.

7. Probable solutions

Many users are victims of Bluetooth threats. Recently, Bluetooth threats have been reduced due to the fact the manufacturers of Bluetooth devices have taken preventive measures against the threats. Bluetooth version v2.1 released in 2007, introduced "Secure Simple Pairing (SSP)" which improved the prevention against threats. The latest version of Bluetooth v4.2 released in December 2014, introduced "Secure Connections Only mode", which further improved the security. The antivirus softwares these days are also very efficient. But these still does not make Bluetooth a secure technology. Bluetooth devices are continuously increasing and with that hackers are also increasing and getting smarter.

Padgette et al. (2012), Panigrahy et al. (2011) and Dunning (2010) suggested security recommendation from the technical point of view. National Security Agency (NSA) released a paper providing guidlines for Bluetooth developers (Bluetooth for unclassified use: Guidelines for developers, 2015). Philip and Das (2011) proposed a security architecture to fight MITM attack. Here authentication is done using key and chaotic image encryption, which makes the pairing mechanism robust. Albazrqaoe et al. (2016) proposed a Bluetooth packet sniffer called BlueEar, which can increase the packet capture rate to 90%. Singelée and Preneel (2006) proposed advanced pairing protocol which enhances the pairing mechanism. No matter what security measures manufacturer are taking, it is always better to be safe from the user side. Bluetooth device with default setting provides a very minimum level of security. So, it is essential for users to personalize the default setting to obtain the maximum possible security. Here are some solutions that every user should follow.

7.1. Basic prevention

7.1.1. Turn Bluetooth off

Always turn off the Bluetooth port. Turn it on only when it is needed and turn it off as soon as the necessity is finished.

7.1.2. Remain undiscoverable

Keep the device in non-discoverable mode. Whenever needed turn on to discoverable mode use the Bluetooth and as soon as the need is finished again turn it to non-discoverable mode.

7.1.3. Protect the device

Install anti-virus, firewall and anti-spam software and make sure they are updated to the latest version. This helps to prevent malware infection.

7.1.4. Download from trusted source

Be careful not to install any unknown software in the device. Do not download software or files from unknown source.

7.1.5. Use device appropriately

Inappropriate exception handling, buffer overflows, and integer underflows make the Bluetooth technology prone to attacks. Users should always avoid these (Bose and Shin, 2006).

7.1.6. Be aware of social engineering

Social Engineering is the method of manipulating people and acquiring sensitive information. User should have basic knowledge of Social Engineering techniques.

7.2. Configure default settings

7.2.1. Change device name

By default the Bluetooth device name consists of the device manufacturer name and the model number. This gives the attacker an idea about the type of the device. User should change the default device name to something else.

7.2.2. Disable unused services

Bluetooth provides a number of services. Bluetooth services include file transfer to other Bluetooth device, audio or voice signal transfer to Bluetooth compatible headset. User should know which service is being used and disable all other unused services.

7.3. Pairing guide

Pairing guide helps to prevent Pin Theft Attack (PIN Cracking Attack and Off-Line PIN Recovery Attack).

7.3.1. Use strong PIN

When pairing the device use long and unpredictable PIN key consisting of alphanumerical and symbols. User should not use the default PIN.

7.3.2. Update the PIN

User should change the PIN every after a regular interval. Changing the PIN frequently makes it harder for the attacker to track

the PIN. Changing PIN will also prevent previously paired device from gaining access with notification.

7.3.3. *Secure pairing*

Pairing maybe made secured by using the concept of cookies.

7.3.4. *Pair in short range*

Always pair devices within a short range to keep the transmission within the secure perimeter.

7.3.5. *Avoid unknown pairing*

Always pair the device with a known device. Never pair with unknown devices. Do not respond to any unexpected pairing requests.

7.3.6. *Pair in private*

Avoid pairing in public areas like a shopping mall, railway station, cinema hall etc.

7.3.7. *Monitor paired list*

Keep eyes on the list of paired devices on the phone to discover any suspicious connections. Remove lost or stolen devices from paired device list. And it is better to keep the paired device list short.

7.4. *Observe device behavior*

By observing the device behavior user can easily prevent Eavesdropping Attack (Man-in-the-Middle Attack and Relay Attack), Malware and DDoS attack.

7.4.1. *Be aware abnormal activities*

If transmission of data between two Bluetooth devices gets slower than regular, then communication may be eavesdropped. If strange message pop up or if the system crashes frequently. Then the phone may be attacked.

7.4.2. *Monitor battery life*

If the device consumes more power, if the battery life is drained out quickly or if device becomes slower than usual, then it may be attacked.

7.4.3. *Observe anti virus activities*

If the anti virus of the device crashes or becomes deactivated automatically, then device may be attacked because some malware turns off the anti virus while some malware may totally corrupt the anti virus.

7.4.4. *Monitor data usage*

Pay attention to the application log of the device. It clearly shows which applications are used and how much data is consumed. If data use rate becomes abruptly higher, then it may be attacked.

If user experience any of these activities are going wrong. Then user should quickly disconnect the Bluetooth connection and isolate the device. The next step would be to clean up the virus. The best way would be to take back up of important data and reset the device to default factory setting.

8. Conclusion and future works

Bluetooth is a very popular and efficient wireless medium for exchanging data. In this paper, we have presented a comprehensive survey on the security flaws of Bluetooth technology with illustrations. Users are not much aware of these security threats. Hence, most of the Bluetooth attacks go undetected or unreported. A hackers greatest advantage would be the lack of concern for Bluetooth threats. With a bit of knowledge about these threats, users may remain safe.

This survey work can help researchers discover new type of threats that are still unknown through the knowledge of these existing threats and further analysis and possible combinations of manipulations. The research and development departments on Bluetooth devices may work on these threats and develop better in-built security measures for their devices. Anti-virus and anti-malware researchers can attain knowledge regarding the methods of Bluetooth infection and impacts of Bluetooth malwares, thereby upgrading their anti-malware/anti-virus software to prevent these infections.

We have grouped different Bluetooth attacks together that can be helpful for the vendors to develop solutions capable of protecting against similar group of attacks. Although there are many software and hardware solutions to fight against DoS attacks for workstations, there is no specific product to prevent DoS attacks of Bluetooth. This survey may give knowledge and motivation to develop an application to prevent DoS attacks in Bluetooth technology. Finally, this survey will inspire Bluetooth headset developers and car stereo system developers to come with a minimum level of preventive measures to ensure the integrity of their products.

Recent research is being carried out to improve the application Layer of the Bluetooth architecture for better exchange of link key and robust data encryption during communication. Researchers are also focusing on topology change issues and are also working on the improvement the frequency hopping sequence during data transmission for better security in Bluetooth network.

REFERENCES

Albazrqaoe W, Huang J, Xing G. Practical bluetooth traffic sniffing: Systems and privacy implications, in 14th Annual International Conference on Mobile Systems, Applications, and Services. New York, USA: ACM, pp. 333–345, 2016.

Alcorn E. Bluetooth architecture overview, Technical report, Microsoft Corporation, March 2011.

Babamir SM, Nowrouzi R, Naseri H. Mining bluetooth attacks in smart phones, in International Conference on Networked Digital Technologies, Prague, Czech Republic, July 7–9, pp. 241–253, 2010.

Bluetooth, What is bluetooth? Available from: https://www.bluetooth.com/what-is-bluetooth-technology/bluetooth-fact-or-fiction. [Accessed March 29, 2017].

Bluetooth core system. Available from: http://www.programgo.com/article/40951019534/. [Accessed March 29, 2017].

Bluetooth for unclassified use: Guidelines for developers, Technical Report, National Security Agency (NSA), Information Assurance Directorate, May 2015, [Accessed March 29, 2017].

Bose A, Shin KG. On mobile viruses exploiting messaging and Bluetooth services, in International conference on Security and Privacy in Communication Networks (Securecomm), Aug 28-Sept. 1, 2006.
C. PGP, MAC address spoofing for bluetooth, Blog; 2016. Available from: http://computersecuritypgp.blogspot.com/2016/02/mac-address-spoofing-for-bluetooth.html. [Accessed March 29, 2017].
Chen L, Cooper P, Liu Q. Security in Bluetooth networks and communications. Wire Netw Sec 2013;77–94.
Colleen R. Bluetooth security, Technical Report, East Carolina University, pp. 6–9, 2006.
Cortes S. Android.obad; 2013. Available from: https://www.symantec.com/security_response/writeup.jsp?docid=2013-060411-4146-99&tabid=2. [Accessed March 29, 2017].
Cross D, Hoeckle J, Lavine M, Rubin J, Snow K. Detecting non-discoverable bluetooth devices. Int Fedr Inform Process 2008;253:281–93.
Dunning JP. Taming the blue beast: a survey of bluetooth-based threats. IEEE Secur Priv 2010;8(2):20–7.
F-secure labs, Threat Report; 2013. Available from: https://www.f-secure.com/documents/996508/1030743/Threat_Report_H2_2013.pdf. [Accessed March 29, 2017].
Gostev A. Mobile malware evolution: An overview, part 1, Web page; 2006. Available from: https://securelist.com/analysis/malware-evolution-monthly/36109/mobile-malware-evolution-an-overview-part-1. [Accessed March 29, 2017].
Haataja K, Hyppnen K, Pasanen S, Toivanen P. Bluetooth security attacks: comparative analysis, attacks, and countermeasures. Berlin: Springer; 2013.
Herfurt M, Mulliner C. Bluetooth security vulnerabilities and bluetooth projects, Web page; 2005. Available from: http://trifinite.org/trifinite_stuff.html. [Accessed March 29, 2017].
Hypponen M. Malware goes mobile. Sci Am 2006;295(5):70–7.
Iqbal MMW, Kausar F, Wahla MA. Attacks on bluetooth security architecture and its countermeasures. Inform Secur Assur 2010;76:190–7.
Jabra, Bluetooth security, Technical white paper. Available from: http://www.jabra.com/support/technical-whitepapers. [Accessed March 29, 2017].
Kissel R. Glossary of key information security terms. Available from: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf. [Accessed March 29, 2017].
Kumar P. Bluetooth quality issues, threats and security tips. Int J Comput Sci Commun 2011;2(1):211–13.
La Polla M, Martinelli F, Sgandurra D. A survey on security for mobile devices. IEEE Commun Surv Tutor 2013;15(1):446–71.
Lawton G. Is it finally time to worry about mobile malware ? IEEE Comput 2008;41(5):12–14.
Legg G. The bluejacking, bluesnarfing, bluebugging blues: Bluetooth faces perception of vulnerability; 2005. Available from: http://www.eetimes.com/document.asp?doc_id=1275730. [Accessed March 29, 2017].
Mark P. Bluetooth SIG 2014 annual report; 2014. Available from: https://www.bluetooth.org/en-us/Documents/Annual_Report_2014.pdf. [Accessed March 29, 2017].
McFedries P. Bluetooth cavities. IEEE Spectr 2005;42(6):88.
Minar NB-NI, Tarique M. Bluetooth security threats and solutions: a survey. Int J Distrib Parallel Syst 2012;3(1).
Mutchukota TR, Panigrahy SK, Jena SK. Man-in-the-middle attack and its countermeasure in Bluetooth secure simple pairing. In: Vanugopan KR, Patnaik LM, editors. Computer networks and intelligent computing, communication in computer and information science, vol. 157. Berlin: Springer; 2011. p. 367–76.
Nilsson DK, Porras PA, Jonsson E. How to secure Bluetooth-based pico networks, in International Conference on Computer Safety, Reliability, and Security. Nurmberg, Germany: Springer, Sept 18–21, pp. 209–223, 2007.
Padgette J, Scarfone K, Chen L. Guide to bluetooth security. NIST Spec Pub 2012;800(121):25.
Padgette JD. Bluetooth security in the DoD, in IEEE Military Communications (MILCOM), Boston, MA, Oct 18–21, 2009.
Panigrahy SK, Jena SK, Turuk AK. Security in Bluetooth, RFID and wireless sensor networks, in International conference on communication, computing & security. Odisha, India: ACM, Feb 12–14, pp. 628–633, 2011.
Panse T, Panse P. A survey on security threats and vulnerability attacks on bluetooth communication. Int JComput Sci Inform Technol 2013;4(5):741–6.
Peng S, Yu S, Yang A. Smartphone malware and its propagation modeling: a survey. IEEE Commun Surv Tutor 2014;16(2):925–41.
Philip M, Das A. A new bluetooth security architecture, in Trends in computer science, engineering and information technology. Tamil Nadu, India: Springer, Sept 23–25, pp. 507–515, 2011.
Premnath SN, Kasera SK. Battery-draining-denial-of-service attack on Bluetooth devices, Technical poster, 2008.
Raphael PM, Phan C-W. Analyzing the secure simple pairing in bluetooth v4.0. Wirel Pers Commun 2012;64(4):719–37.
Sandhya S, Devi KAS. Contention for man-in-the-middle attacks in Bluetooth networks, in International conference on computational intelligence and communication networks. Mathura, Uttar Pradesh, India: IEEE, Nov 3–5, pp. 700–703, 2012.
Shaked Y, Wool A. Cracking the Bluetooth PIN, in 3rd international conference on mobile systems, applications, and services. New York, USA: ACM, pp. 39–50, 2005.
Singelée D, Preneel B. Improved pairing protocol for bluetooth, in International conference on ad-hoc networks and wireless. Ottawa, Canada: Springer, August 17–19, pp. 252–265, 2006.
Strobel D. IMSI catcher, Technical report, Ruhr-Universit Bochum, 2007.
Tan M, Masagca KA. An investigation of bluetooth security threats, in International conference on information science and applications. Jeju Island, Republic of Korea: IEEE, 26–29 April, 2011.
Ullah MZ. An analysis of the Bluetooth technology, Master Thesis, School of Computing, Blekinge Institute of Technology, Sweden, 2009.
Zanero S. Wireless malware propagation: a reality check. IEEE Secur Priv 2009;7(5):70–4.



Shaikh Shahriar Hassan received his B.Sc. degree from Ahsanullah University of Science and Technology (AUST), Dhaka, Bangladesh in 2016 in Computer Science and Engineering. Currently he is a Graduate Researcher in the Department of Computer Science at Bangladesh University of Engineering and Technology (BUET), Dhaka, Bangladesh. His research interests include Computer Networks, Wireless Communications, Network Security & Privacy, Satellite networks and Internet of Things.



Soumik Das Bibon received his B.Sc. degree from Ahsanullah University of Science and Technology (AUST), Dhaka, Bangladesh in 2016 in Computer Science and Engineering. Currently he is a lecturer in Department of Computer Science and Engineering at Daffodil International University (DIU), Bangladesh. His research interests include Computer Networks, Wireless Communications, Network Security & Privacy, Satellite networks and Internet of Things.



Md. Shohrab Hossain received his B.Sc. and M.Sc. in Computer Science and Engineering from Bangladesh University of Engineering and Technology (BUET), Dhaka, Bangladesh in the year 2003 and 2007, respectively. He obtained his Ph.D. degree from the School of Computer Science at the University of Oklahoma, Norman, OK, USA in December, 2012. He is currently serving as an Associate Professor in the Department of CSE, BUET. His research interests include mobility of IPv6 networks, security, scalability and survivability of mobile networks, Software defined networking and Internet of Things.



Mohammed Atiquzzaman obtained his M.S. and Ph.D. from the University of Manchester. He currently holds the Edith Kinney Gaylord Presidential professorship at the University of Oklahoma. Dr. Atiquzzaman is the Editor-in-Chief of Journal of Networks and Computer Applications and founding Editor-in-Chief of Vehicular Communications. He received the NASA Group Achievement Award, and has over 300 refereed publications which are accessible at www.cs.ou.edu/~atiq. His research interests are in wireless and mobile networks, satellite networks, and vehicular communications. His research has been funded by National Science Foundation (NSF), NASA, U.S. Air Force, Cisco, Honeywell, etc. through grants totaling over $9M.