A Survey on Bluetooth Security Threats & Solutions

Ms.V.Priya

Lecturer
Department of Computer Science & Engineering
PSNA College Of Engineering & Technology,Dindigul,Tamil Nadu,India.

vpriyamalar@gmail.com

Abstract

Bluetooth technology has become an integral part of this modern society. The availability of mobile phones, game controllers a popular technology for short range wireless communication. However, as the Bluetooth technology becomes widespread, vulnerabilities in its security protocols are increasing which can be potentially dangerous to the privacy of a user's personal information. The security issues of Bluetooth have been an active area of research for the last few years. This paper presents the vulnerabilities in the security Protocols of this technology along with some past security threats and possible countermeasures as reported in the literatures which have been surveyed and summarized in this paper. It also presents some tips that end-users can implement immediately to become more cautious about their private information. Finally, the paper concludes with some recommendations for future security enhancements that can be implemented in the Bluetooth standard.

Keywords

Bluetooth, encryption, security protocols, security threats, countermeasures, Bluetooth enhancements

I. INTRODUCTION

Bluetooth technology has been considered as a cheap, reliable, and power efficient replacement of cables for connecting electronic devices. This technology was officially approved in the summer of 1999 [1]. Since then it has widely been used in various electronic devices. Bluetooth Special Interest Group (SIG) was formed to nurture and promote this technology. The SIG has over 14,000 members including some leading companies in the fields of telecommunications, computing, automotive, music, industrial automation, and network industries [2]. Bluetooth is a combination of hardware and software technology. The hardware is riding on a radio chip. On the other hand, the main control and security protocols have been implemented in the software. By using both hardware and software Bluetooth has become a smart technology for efficient and flexible wireless communication system. Bluetooth radio chip supports communication among a group of electronic devices. Once the hardware radio chips are installed into the International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012

128 electronic devices, wireless communication can be established among these devices. The operating distance between two Bluetooth devices ranges from 10 and 100 meters. By using a directional antenna and an amplifier the range of Bluetooth can be extended over a mile away. One of the major advantages of Bluetooth technology is that it operates in a license-free Industrial, Scientific and Medical (ISM) band ranging from 2.4 to 2.4835 MHz. This band is divided into 79 channels each being 1MHz wide. Using Fast Frequency Hopping Sequence (FFHS) a Bluetooth device hops from one channel to another channel up to 1600 times in one second [9]. Bluetooth also uses Adaptive Frequency Hopping (AFH) technique which is designed to cope with excessive packet losses due to packet collisions or external interferences.

Each Bluetooth chip has a unique identity code. The 'master-slave' concept is the core of a Bluetooth based network [5]. The 'master' works as the moderator during the communication between itself and the slave as well as among the slaves themselves. In Bluetooth a trusted relationship between two devices called 'pairing' are formed by exchanging shared secret codes referred to as PINs. A 'master' device has the option of pairing with up to seven 'slave' devices establishing a network called a piconet. Two or more piconets together form a scatternet, which can be used to eliminate Bluetooth range restrictions. A scatternet is formed when the devices act as 'master' or 'slave' devices in multiple piconets at the same time. A more detail description of Bluetooth technology can be found in [4].

Data Security Authentication key128 bit key Data Security-Encryption 8-128 bits(configurable) With each release of a new Bluetooth version, the manufacturers have upgraded different aspects of this technology to make it more secure and user-friendly to support a wide range of devices, a list of all the Bluetooth versions released to date is mentioned in [12]. The last version to be released was version 4.0 which had the most versatile design and was focused on low power usage [13]. Although the Bluetooth technology is undoubtedly considered a very popular technology, it has some security 'loop-holes' that make it vulnerable. In this paper, these vulnerability issues have been addressed. The security threats and solutions proposed in the literatures have been surveyed and summarized in this paper. The rest of the paper is organized as follows, Section II describes some related work done with Bluetooth security protocols and Section III explains the Bluetooth protocol stacks. The security architecture of Bluetooth technology has been explained in section IV. Section V contains the vulnerabilities International Journal of Distributed and arallel Systems (IJDPS) Vol.3, No.1, January 2012 129 of this technology. The security threats reported so far in the literatures have been complied in section VI. Counter measures against the security threats have been presented in section VII and section VIII presents some security tips for the users to create awareness among them to protect their private information while communicating, to mitigate the risks of being attacked. The paper is concluded with section.

II. RELATED WORK

Many security experts in the field of wireless technologies have conducted research on different aspects within the security architecture of Bluetooth and have provided amazing results with new tweaks that enhances the security of the device within a network. Some commendable research work is mentioned in [6]. [7] and [8]. In [6], the authors have presented a light weight protocol to provide location privacy in wireless body area network. The basic idea of their protocol is on the use of temporary pseudonyms instead the use of hardware addresses to communicate in the wireless body area networks. This allows protecting the source and the destination of mobile devices in the WBANs. Their protocol is efficient and also energy saving. In [7], the authors proposed the design of a device pairing simulator called “PSim”, they have felt the need to create this tool because most wireless systems are prone to security risks, such as eavesdropping and require different techniques as compared to traditional security mechanisms to test their security protocols. This tool can be used to perform test on different types of device pairing methods as well as generate new protocols for increased security measures. In [8], the authors have compared different techniques used for device pairing in wireless networks and have presented a comparative result of their findings on the security protocols used. Besides the work mentioned here, there are other numerous papers published and research work done which are beyond the scope of this paper to elaborate on all of them, but they all aim to improve wireless network security systems and since Bluetooth is a common wireless standard among almost all devices, its security must be given a high priority due to its widespread usage.

III. BLUETOOTH PROTOCOL STACKS

A protocol stack is a combination of software/hardware implementation of the actual protocols specified in the standard [11]. It also defines how the devices should communicate with each other based on the standard. The Bluetooth protocol stack is shown in Fig. 1. International Journal of Distributed and arallel Systems (IJDPS) Vol.3, No.1, January 2012 130 Fig. 1 Bluetooth Protocol Stack The protocols below the host controller interface (HCI) are built into the Bluetooth microchip and the protocols above the HCI are included in the host device's software package. The HCI ensures a secured communication between the host and the Bluetooth module. The radio layer transmits data in the form of bits by using a radio frequency. This function is defined by the radio layer. Bluetooth transceivers use Gaussian Frequency Shift Keying (GFSK) technique. The baseband layer performs the functions of frequency hopping for interference mitigation, medium access control and forming data packet. In addition, the baseband layer also controls link, channel, error correction and flow control. It establishes two kinds of link depending on the application and operating environment.

A synchronous connection oriented (SCO) link is established to emulate circuit switched connections for voice and data connection. While an asynchronous connection link (ACL) is defined for the data bursts. This link also supports broadcasting and data rate control by the master device. The link manager (LM) acts as a liaison between the application and the link controller (LC) on the local device. It is also used for communication with the remote LM via protocol data units (PDU) and the link manager protocol (LMP). The audio protocol is used for a real time two way voice communication. The audio protocol is carefully located in such a way so that the overhead of upper layer protocols does not cause any delays for real-time twoway voice connections. The logical link control and adaptation protocol (L2CAP) is a software module that normally resides in the host. It acts as a conduit for data on the asynchronous connection link (ACL) between the baseband and host applications. The L2CAP is used to ensure both connection oriented and connection less services. Connection oriented service is used for communication between the master to one slave. Connection less service is used for communication between a master and multiple slaves. The L2CAP can initiate security procedures when a connection oriented or a connectionless connection request is made. The Object Exchange Protocol (OBEX) is used to exchange objects such as calendar notes, business cards and data files between devices based on a client-server model. The telephony control specification (TCS) defines the call control signaling for the establishment/release of

Application specific security protocols

Bluetooth host security protocols

Security protocols on Bluetooth hardware chip

AT CommandsHCI

Applications OBEX TCP/IP

RFCOMM TCS SDPL2CAP

Link Manager (LM)Baseband

Bluetooth RadioAudioInternational Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012 131 speech and data calls between Bluetooth devices. It also provides functionality for exchanging signaling information not related to ongoing calls.The service discovery protocol (SDP) discovers the services that are available in the RF proximity and determines the characteristic of these available services. SDP is an essential protocol that enables the Bluetooth devices to form an ad hoc network. RFCOMM is a transport protocol used to emulate the RS-232 serial ports. This protocol enables a Bluetooth device to connect with external devices like printers and scanners. The RFCOMM protocol relies on the baseband protocol stack to provide reliable in-sequence delivery of bit stream.

IV. SECURITY ARCHITECTURE

Security issues have played a major role in the invention of Bluetooth technology. The Bluetooth SIG has put much effort into making Bluetooth a secured technology. Several security measures have been implemented at different protocol levels, but the basic Bluetooth security configuration depends on the user’s Bluetooth device, who decides about the discoverability and connection options. In general, Bluetooth discoverability and connection options are divided into three 'modes' of operation [14], which are as follows:

• Silent: The device will never accept any connections. It simply monitors the Bluetooth traffic.

• Private: The device cannot be discovered. A connection will be accepted only if the Bluetooth device address (BD_ADDR) of the device is known to the prospective master. A 48-bit BD_ADDR is normally unique and it refers globally to only one individual Bluetooth device.

• Public: The device can be both discovered and connected to. It is, therefore, called a discoverable device. In addition to these modes, there are also four different security modes that a device can implement. These are as follows-

• Non-secure: The Bluetooth device does not initiate any security measures.

• Service-level enforced security mode: Two Bluetooth devices can establish a nonsecure ACL. Security procedures are initiated after an L2CAP connection oriented or an L2CAP connection-less channel request is made.

• Link-level enforced security mode: Security procedures are initiated when an ACL link is established and before any channel request is made.

• Service-level enforced security mode (SSP): This mode is similar to mode 2, except that only Bluetooth devices using secure simple pairing (SSP) can use it. There are three main steps in Bluetooth security procedures, which are as follows

• Authentication: It involves proving the identity of one Piconet device to another. The objective of the authentication procedure is to determine the client's authorization level. The authentication is verified by checking the link keys. The sender encrypts the Bluetooth device address of the receiver using the link key and a random number to produce a signed response authentication result (SRES). The SRES is sent to the receiver and the connection is established if the two link keys are equal.

• Authorization: It is the process of granting or denying access to a network resource. International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012 132

• Optional Encryption: It is the encoding of information being exchanged between Bluetooth devices in a way that eavesdroppers cannot decode its contents. The encryption is an essential part of Bluetooth security. The encryption key can vary between 8 and 128 bits. The user does not have access to change the size of the encryption key as the key size must be specified by the manufacturers according to the countries' regulations. A random number must be sent from one device to the other when any two Bluetooth devices wish to start the communication. The receiving device must also have knowledge of the PIN from the sending devices. With these two sets of information, a link key is generated on both devices.

Bluetooth security is based on building a chain of events. None of these events provides any meaningful information to an eavesdropper. All the events must occur in a specific sequence for the enforcement of secured communication between two Bluetooth enabled devices. Two Bluetooth devices begin pairing with the same PIN code that is used for generating several 128-bit keys. The same PIN code can be used for all Bluetooth enabled devices in a trusted network. For example, in a conference environment where two people meet for the first time and they want to create a Bluetooth network between their electronic devices, the PIN selection should be done by using a different PIN codes for that master-slave pair. Otherwise all other Bluetooth connections that are using the same PIN code may be compromised. Fig. 2 shows the detailed pairing process of two Bluetooth enabled devices. International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012 133

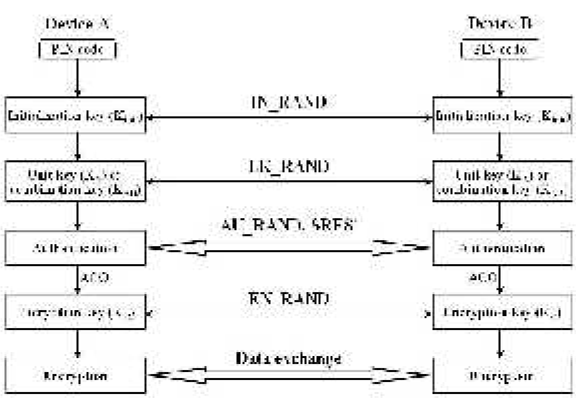

Fig. 1 Illustration of Bluetooth security operations

An initialization key (Kinit) is generated when two Bluetooth devices meet for the first time and it is used for generating more secured 128-bit keys, which are generated during the next phases of the security chain of events. The Kinit is derived from a 128-bit pseudorandom number IN_RAND, an L-byte (1 ≤ L ≤ 16) PIN code, and the BD_ADDR. It is worth noting to mention that the IN_RAND is sent via air in unencrypted form. The The K is the Kinit if the devices create a link key for the first time together. The K is the KA if the link key is a unit key, and it is the KAB if the link key is being upgraded to a combinationkey. Device B decrypts the LK_RANDA with the K, (i.e., LK_RANDAK K=LK_RANDA), and can now produce the KA. Correspondingly, device B encrypts the LK_RANDB with the K (i.e., LK_RANDBK), and sends it to device A. Device A decrypts the LK_RANDB with the K (i.e., LK_RANDBK K=LK_RANDB), and produces the key KB. Finally, both devices can produce the KAB by using KA and KB(i.e., KAB=KAKB). The next phase of the security chain of events is the challenge response authentication in which a claimant's knowledge of a secret link key is checked as illustrated in Fig. 3. During each authentication, a new 128-bit pseudorandom number AU_RAND is exchanged via air in an unencrypted form. Other inputs to the authentication function E1are the BD_ADDR of the claimant and the current link key (KA or KAB). Fig. 3 Bluetooth challenge-response authentication A 32-bit SRES and a 96-bit authenticated ciphering offset (ACO) are produced in both devices by E1(AU_RANDA, BD_ADDRB, Link key) function, where the Link key is the KAor the KAB. The claimant sends the SRES' (i.e., the SRES value produced by the claimant), via air in unencrypted form to the verifier. Even with longer 16-character alphanumeric PINs full protection against active eavesdropping cannot be achieved and Man-In-The-Middle (MITM) attacks on Bluetooth communications can easily break the protection. The Bluetooth version 2.1+EDR and higher version adds a new i for the pairing procedure called secure simple pairing (SSP). Its main goal is to improve the security of pairing by providing protection against passive eavesdropping and MITM attacks. Instead of using (often short) passkeys as the only source of entropy for building the link keys, SSP employs ECDH public-key cryptography. To construct the link key, devices use public-private key pairs and the Bluetooth addresses of the devices. Passive eavesdropping is effectively blocked by the SSP, as running an exhaustive search on a private key with approximately 95 bits of entropy is currently considered to be infeasible in a short time.

V. BLUETOOTH NETWORK VULNERABILITIES

Since there are now billions of Bluetooth devices in use, malicious security violations are common events now and it is expected to increase in the near future.

On the contrary, the increased usage of Bluetooth devices makes security concerns even more alarming. Hence, Bluetooth security architecture needs a constant upgrading to prevent new unknown threats. Like any other wireless communication system Bluetooth transmission can be deliberately jammed or intercepted. False or modified information could be passed to the devices by the cyber criminals. Security threats in Bluetooth can be divided into three major categories [15] as follows:

• Disclosure threat: The information can leak fromthe target system to an eavesdropper that is notauthorized to access the information.

• Integrity threat: The information can be deliberately altered to mislead the recipient.

• Denial of Service (DoS) threat: The users can be blocked to get access to a service by making it either unavailable or severely limiting its availability to an authorized user.

Bluetooth security is currently a very active research area in both academia and industry.

VI. EXISTING REPORTS OF BLUETOOTH THREATS

The problems regarding Bluetooth security have been reported since its inception. But, it has not been considered as a significant problem until its adaptation into mobile devices. A brief overview of some of the real incidents is listed below:

• In 2003, Bend and Adam from A.L. Digital Ltd Discovered and published serious flaws in Bluetooth technology regarding the protocol. Their investigations concluded that the security flaws could lead to loss of personal information of a user [15].

• In 2004, the first bluetooth virus was reported in the literatures as a 'proof-of-concept'. It was proved as a potential threat to the Bluetooth technology [16].

• In January 2005, a mobile malware called 'Lasco' was detected. Lasco was a selfreplicating worm, which was successful in rendering a mobile device unstable before infecting another device [17].

• In April 2005, Cambridge University published a paper documenting actual passive attacks by implementing off-line PIN cracking [18].

• In August 2005, Bluetooth enabled phones were used to track other mobile device left inside of cars [19].

• In April 2006, researchers from Secure Network and F-Secure published a report addressing that a large number of devices were left in a visible state that posed the possibility of spread of a Bluetooth worm [20].

• In October 2007, Kevin Finistere and Thierry Zoller demonstrated the first Bluetooth and link key cracking technique at a conference. A remote root shell via Bluetooth on Mac OS X v10.3.9 and v10.4 was used in that demonstration [21]. Bluetooth devices are exposed to malicious intervention during the process of pairing with another device. These weaknesses are primarily due to flaws in the link key establishment protocol, which is required for devices to pair, and the fact that the encryption of a session is optional and created at the end of the pairing process. It means that the various types of attacks can be performed well before pairing is complete. Even after the pairing is complete, the attackers can still sniff the airwaves to gain enough information to steal link keys so that they can deceptively authenticate or perform Man-in-the-Middle (MITM) attacks to impersonate other devices. Some other reported attacks on the Bluetooth security are

(1) MAC spoofing attack,

2) PIN cracking attack,

(3) Man-in-the-Middle/Impersonation attack,

(4) BlueJacking attack,

(5) BlueSnarfing attack,

(6) BlueBugging attack,

(7) BluePrinting attack,

(8) Blueover attack,

(9) International Journal of Distributed nd Parallel Systems (IJDPS) Vol.3, No.1, January 2012 138 off-line PIN recovery attack,

(10) brute-force attack, (11) reflection attack,

l2) backdoor attack,

13) DoS attack,

14) Cabir worm,

(15) Skulls worm, and

(16) Lasco worm [22-25].

1) *MAC spoofing attack* :Among all passive attacks, the most frequently reported attacks are classified as MAC spoofing and PIN cracking attacks. Malicious attackers can perform MAC spoofing during the link key generation while Piconets are being formed. Assuming the attack is made prior to successful pairing and before encryption is established attackers can easily intercept data intended for other devices. Attackers, with specialized hardware, can easily use spoofing to terminate legitimate connections or capture and/or manipulate data while in transit. Bluetooth SIG did not provide a good solution to prevent this type of attack. They only advised the users to do the pairing process in private settings. They also suggested that a long, random, and variable PIN numbers should be used.

2. *PIN Cracking attack* :Using a Bluetooth frequency sniffer (or protocol analyzer) and acquisition of a FHS packet, attackers can attempt to acquire IN_RAND, LK_RAND and the initialization key during the entire pairing and authentication processes. The attacker would have to list all of the possible permutations of the PIN. Using the acquired IN_RAND and BD_ADDR they would need to try possible permutations as input in the E22 algorithm.
3. Man-in-the-Middle/Impersonation Attack Man-in-the-Middle and impersonation attacks actually involve the modification of data between devices communicating in a Piconet. A Man-in-the-Middle attack involves relaying of authentication message unknowingly between two devices in order to authenticate without knowing the shared secret keys. By forwarding the message of two devices trying to pair, an attacker will relay two unique link keys. By acting between two devices an attacker can trick two devices into believing they are paired when in fact they have paired with the attacker. The suggested solutions to this kind of attack involve incorporating more Piconet specific information into the pairing process. For example, timestamps and nested mutual authentication can be used to determine the legitimacy of a device's challenge before responses are sent in return.

4. *BlueJacking Attack*: Blue jacking is the process of sending unsolicited messages to Bluetooth-enabled devices. This does not involve altering any data from the device, but nonetheless, it is unsolicited. Devices that are set in non-discoverable mode are not susceptible to Bluejacking. In order for Bluejacking to work, the sending and receiving devices must be within 10 meters of each other. While this method has been widely used for promotional purposes, Bluetooth device owners should be careful about not adding the contacts to their address books. Bluejacking is usually not done with malicious intent. Repetitive spam messages can be annoying to the user. In some cases, Bluejacking can render the product inoperable. This can also open the door to a variety of other attacks. International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012 139

5. *BlueSnarfing Attack:* Bluesnarfing is a method of hacking into a Bluetooth-enabled mobile phone and copying its entire contact book, calendar or anything else stored in the phone's memory. By setting the device in non-discoverable a user can minimizes the chance of this kind of attack. However, the software tools required to steal information from Bluetooth enabled mobile phones are widely available in the Web. Leading telecommunication giants like Nokia and Sony Ericsson are ensuring that new phones coming to market will not be susceptible to Bluesnarfing attack.

6. *BlueBugging Attack:* A BlueBugging attack means that an attacker connects to the target device (typically a Bluetooth mobile phone), without alerting its owner, and steals some sensitive information. Assuming an attacker has full access to the address translation (AT) command set available in GSM (Global System for Mobile) an attacker can exploit the AT commands. It means that the attacker can, in addition to stealing information, send text messages to premium numbers. Hence the attacker can initiate phone calls to premium numbers, write to phonebook entries, connect to the Internet, set call forwards, try to slip a Bluetooth virus or worm to the target device.

7. *BluePrinting Attack*: A BluePrinting attack is used to determine the manufacturer, device model and firmware version of the target device. An attacker can use Blueprinting to generate statistics about Bluetooth device manufacturers and models, and to find out whether there are devices in the range of vulnerability that have issued with Bluetooth security, for example. BluePrint 0.1 is a tool for performing BluePrinting attack. It runs on Linux and it is based on the BlueZ protocol stack. BluePrinting attacks work only when the BD_ADDR of the target device is known.

8. *Blueover attack* :Blueover and its successor Blueover II are derived from Bluetooth. However, because they run on handheld devices such as PDAs or mobile phones and are capable of stealing sensitive information by using a BlueBugging attack. A Blueover attack can be done secretly, by using only a Bluetooth mobile phone with Blueover or

Bluover II installed. Bluleover and Bluover II run on almost every J2ME (Java 2 Micro Edition) compatible handheld device. They are intended to serve as auditing tools which can be used for checking whether Bluetooth devices are vulnerable or not, but they can be used for attacking against Bluetooth devices as well. A Blueover attack is dangerous only if the target device is vulnerable to BlueBugging. Moreover, an attacker has to know the BD_ADDR of the target device.

9. *Off-Line PIN Recovery Attack* :An off-line PIN recovery attack is based on intercepting the IN_RAND value, LK_RAND values, AU_RAND value and SRES value, and after that trying to calculate the correct SRES value by guessing different PIN values until the calculated SRES equals the intercepted SRES. It is worth noting that SRES is only 32 bits long. Therefore, a SRES match does not necessarily guarantee that an attacker has discovered the correct PIN code, but the chances are quite high especially if the PIN code is short.

10. *Brute-Force Attack: A* brute-force BD_ADDR scanning attack uses a brute-force method only on the last three bytes of a BD_ADDR, because the first three bytes are publicly known and can be set as fixed. A International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012 140 brute-force BD_ADDR scanning attack is perhaps the most feasible attack when target devices are Bluetooth mobile phones, because millions of vulnerable Bluetooth mobile phones are used every day all over the world.

11. *Reflection Attack*: Reflection attacks (also referred to as relay attacks) are based on the impersonation of target devices. An attacker does not have to know any secret information, because the attacker only relays (reflects) the received information from one target device to another during the authentication. Hence a reflection attack in Bluetooth can be seen as a type of a MITM attack against authentication, but not against encryption. The only information needed is the BD_ADDRs of the target devices.

12. *Backdoor Attack*: The backdoor attack involves establishing a trust relationship through the pairing mechanism, but ensuring that it no longer appears in the target's register of paired devices. In this way, unless the owner is actually monitoring their devices at that moment, a connection is stablished. The attacker may continue using the resources that a trusted relationship with that device grants access to until the users notice such attacks. The attacker can not only retrieve data from the phone, but other services such as modems, Internet, WAP and GPRS gateways may be accessed without the owner's knowledge or consent. A backdoor attack works only if the BD_ADDR of the target device is known. Moreover, the target device has to be vulnerable to a backdoor attack.

13. *DoS Attacks* :The DoS threats can be roughly divided into two parts: (1) attacks against the physical (PHY) layer, and (2) attacks against protocols above the PHY layer. At the PHY layer, an attacker can jam the Piconet entirely or capture the channel from the legitimate Piconet device. A jammer can disrupt the PHY layer by hopping along with the Piconet devices and send random data in every timeslot. Some typical DoS attacks are described below:

L2CAP Guaranteed Service attack: An attacker requests the highest possible data rate or the smallest possible latency from the target device so that all other connections are refused, and the throughput is reserved for the attacker.

14. *Cabir worm* :The Cabir worm is a kind of malicious software that uses Bluetooth technology to seek out available Bluetooth devices and sends itself to them. The Cabir worm currently only affects mobile phones that use the Symbian series 60 user interface platform. Furthermore, the user has to manually accept the worm and install the malware in order to infect the phone. It is usually done by disguising the Cabir worm impersonating another application and the user is unaware of it. The Cabir worm shows that it is achievable to write mobile viruses that spread via Bluetooth and may cause other hackers to explore the possibilities of writing Bluetooth viruses. The Mabir worm is essentially a variant of the Cabir worm that uses Bluetooth and Multimedia Messaging Service messages (MMS) to replicate.

15. *Skulls worm: Skulls.D* (also referred to as SymbOS/Skulls.D) is a malicious SIS (Symbian Installation System) trojan file that pretends to be Macromedia Flash player for Symbian mobile phones which support the Series 60 platform. It arrives in the target mobile phone via Bluetooth in a similar way that Cabir follows. When the user opens the SIS file and chooses to install it, the SymbOS/Cabir.M worm (i.e., a variation of the Cabir worm) will be installed in the target mobile phone. Both the system applications and the third party applications needed to disinfect viruses and worms will be disabled. An animation showing a flashing skull picture will also

be displayed on the background of the target device's display at the time of using the application by the user. When the worm is activated, it immediately starts searching for new Bluetooth devices to infect.

16.*Lasco Worm* :Lasco (also referred to as SymbOS/Lasco.A or EPOC/Lasco.A) is a Bluetooth worm and a SIS file infecting virus running in Symbian mobile phones which support the Series 60 platform.

VII. COUNTER MEASURES

As technology makes progress, new attacks are being developed by the attackers. It is not possible to take counter measures against all the weaknesses and the security holes of Bluetooth. The weakest part of the Bluetooth technology involves the pairing process in which it establishes trusted relationships with other devices. Table 2 below provides an overview of some of the known security vulnerabilities with Bluetooth communication [26].

1. Unit key sharing can lead to eavesdropping. Attacker may be able to compromise the security between two users if the attacker has communicated with either of the other two users. This is because the link key (unit key), derived from shared information has been disclosed

2. Short PINs are allowed. Weak PINs, which are used for the generation of link and encryption keys, can be easily cracked. People have a tendency to select short PINs.

3. PIN management is lacking. Establishing use of adequate PINs in an enterprise setting with many users may be difficult. Scalability problems frequently yield security problems.

4. Attempts for authentication are repeated. A limiting feature needs to be incorporated in the specification to prevent unlimited requests. The Bluetooth specification currently requires a time-out period between repeated attempts that will increase exponentially.

5. Strength of the challenge response pseudo-random generator is not known. The Random Number Generator (RNG) may produce static number or periodic numbers that may reduce the effectiveness of the authentication scheme.

6. Encryption key length is negotiable. The specification allows devices to negotiate encryption keys as small as one byte. A more robust encryption key generation procedure needs to be incorporated.

7. The master key is shared. A better broadcast keying scheme needs to be incorporated into the specification.

8. No user authentication exists. Only device authentication is provided by the specification. Application level security, including user authentication, can be added via overlay by the application developer.

9. Privacy may be compromised if the Bluetooth device address (BD_ADDR) is captured and associated with a particular user. Once the BD_ADDR is associated with a particular user, that user’s activities could be logged, resulting in a breach of privacy.

10. Device authentication is simple shared-key challenge-response. One-way-only challenge-response authentication is subject to MITM attacks. Bluetooth provides for mutual authentication, which should be used to provide verification that users are legitimate.

11. End-to-end security is not performed. Only individual links are encrypted and authenticated. Data is decrypted at intermediate points. End-to-end security on top of the Bluetooth stack can be provided by the use of additional security controls.

12. Security services are limited. Audit, non-repudiation, and other services are not part of the standard. These services can be incorporated in an overlay fashion by the application developer.

13. Discoverable and connectable devices are prone to attack.Any device that must

go into discoverable or connectable mode to pair should only do so for a minimal amount of time. A device should never be in discoverable or connectable mode all the time.

VIII. RISK MITIGATION

Risk mitigation can be achieved in Bluetooth systems by applying countermeasures to address specific threats and vulnerabilities. Some of these countermeasures cannot be achieved through the security features built into the Bluetooth specifications. The countermeasures recommended in the Table 2 do not guarantee a secure Bluetooth environment and cannot prevent all attacks. It should be noted that the development of improved security comes at a cost—financial expenses related to security equipment, maintenance, and operation, which should also be considered during development of new security features. The first line of defense is to provide an adequate level of knowledge and understanding for the users of Bluetooth-enabled devices. Users should understand the security policies that address the use of Bluetooth enabled devices and their own responsibilities. The Bluetooth security experts should include awareness based education to support user's understanding and knowledge of Bluetooth security. Policy documents should include a list of approved uses for Bluetooth, and the type of information that may be transferred over Bluetooth networks. The security policy should also specify a proper password usage scheme. Most users do not pay attention while assigning strong pass codes because most of them are not aware of the proper techniques. The general nature and mobility of Bluetooth enabled devices increases the difficulty of employing traditional security measures. Nevertheless, a number of countermeasures can be enacted to secure Bluetooth devices and communications, ranging from distance and power output to general operation practices. International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012 144 Table 3 provides a Bluetooth security measure with recommendations for creating and maintaining secure Bluetooth Piconets. These recommendations are applicable for most of the Bluetooth profiles [10] that requires information exchange over Piconets. Note that some comercially available Bluetooth devices cannot be configured to meet the recommendations as they do not provide encryption and often use a four-digit PIN with a default value like "0000" that cannot be changed.

IX. CONCLUSION

This paper presented an overview of some of the major attacks that Bluetooth has faced over the years along with some possible solutions. Some safety tips for the users have also been provided to instantly create awareness among them to be more cautious about their personal information. Although a vast majority of devices now communicate using this technology, the risks are far greater if the security threats are overlooked by our peers in this industry. Bluetooth security specialists need to provide automatic updates to its security protocols and user privacy protection methods for every new security breach so that protection of the device user's personal information becomes the primary objective.

REFERENCES

[1]"The Bluetooth Blues", available at http://www.information-age.com/article/2001/may/the_bluetooth_blues

[2]Bluetooth SIG, Specification of the Bluetooth System: Volume 2, Profile, Version 1.1, Feb. 22, 2001. available at: https://www.bluetooth.org/About/bluetooth_sig.htm

[3]"The History of Bluetooth", available at: http://www.bluetomorrow.com/about-bluetoothtechnology/history-of-bluetooth/bluetoothhistory.html

[4]Monson, Heidi - "Bluetooth Technology and Implications" available at: http://www.sysopt.com/features/ network/article.php/3532506 (1999-12- 14).

[5]"How Bluetooth Works", available at: http://en.kioskea.net/contents/bluetooth/bluetooth-fonctionnement.php3.

[6]Mohammed Mana, Mohammed Feham, and Boucif Amar Bensaber, "A light weight protocol to provide location privacy in wireless body area networks", International Journal of Network Security and its Applications (IJNSA), Vol.3, No.2, March 2011 International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012 147

[7]Yasir Arfat Malkani and Lachhman Das Dhomeja, "PSim: A tool for analysis of device pairing methods", International Journal of Network Security & Its Applications (IJNSA), Vol.1, No.3, October 2009