Bluetooth Technology: Security Issues And Its Prevention

Priyal Arora[1], Dinesh Swami[2]
[1]Dept of MCA
[2]Assoc. Professor, Dept of MCA
[1, 2] RIET Jaipur

Abstract- *Bluetooth is primarily used for establishing wireless Personal Area Networks (PANs) communication. It is a popular and commonly used technology for sending data from one device to another device. It allows the user to form ad hoc networks to transfer data among wide variety of devices. The current data transfer rate for a Bluetooth is 1 mbps. However, as Bluetooth technology is becoming widespread, vulnerabilities in its security are increasing which can be very dangerous to the users' personal information. Preventing such unauthorized access from secure communication plays a vital role to the pairing devices. This paper presents the malicious intervention about the attacks on the devices while connecting with other devices during the exchange of data using Bluetooth technology. It also discusses various security measures that can be involved during data exchange using Bluetooth technology.*

Keywords- Bluetooth Security, pairing, malicious attackers, network security and Man-in-the-middle attack (MIM)

I. INTRODUCTION

Bluetooth was designed as a cable replacement technology. It is a short range radio link designed to connect portable and/or fixed electronic devices. The effective range, to date, is thirty feet or ten meters. It is a combination of software and hardware 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.

The Bluetooth SIG (Special Interest Group) has developed to reduce the cost of implementation and speed up its adoption for various applications. The Bluetooth specifications provide for three basic security services:-

- *Authentication*: verifying the identity of communicating devices based on their Bluetooth device address. Bluetooth does not provide native user authentication.
- *Confidentiality*: protecting information from eavesdropping by ensuring that only authorized devices can access and view transmitted data.
- *Authorization*: allowing the control of resources by ensuring that a device is authorized to use a service before permitting it to doso.

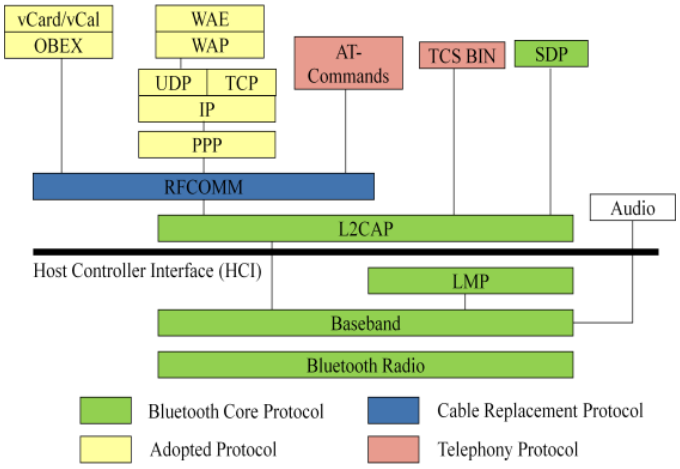
Bluetooth (BT) wireless technology provides an easy way for a wide range of devices to communicate with each other and connect to the Internet without the need for wires, cables and connectors. It is supported and used in products by over 3000 companies, including large corporations such as Sony Ericsson, Nokia, Motorola, Intel, IBM, Toshiba, Motorola, Apple, Microsoft, and even Toyota, Lexus and BMW. A variety of products available on the market have short range Bluetooth radios installed, including printers, laptops, keyboards, cars and the most popular type of Bluetooth enabled devices - mobile phones, driving 60% of the Bluetooth market. The technology has already gained enormous popularity, with more than 3 million Bluetooth-enabled products shipping every week. According to IDC, there will be over 922 million Bluetooth enabled devices worldwide by 2008. The technology seams to be very interesting and beneficial, yet it can also be a high threat for the privacy and security of Bluetooth users

Bluetooth devices are low-power and have a range of 10m distance from the device. Today Bluetooth technology is the implementation of the protocol defined by the IEEE 802.15 standard. The standard defines a wireless PAN (Personal Area Network) operable in an area of the size of a room or a hall. It is a protocol of choice to connect two or more devices that are not in direct line of sight to each other. A security association between two devices can be connected manually by pairing i.e. the user entered common PIN (Personal Identification Number) number to each of the devices. When two devices attempt to connect, unique key is generated based on the PIN number entered on both the devices.

II. PROTOCOL STACKS OFBLUETOOTH

A protocol stack is a combination of software/hardware implementation of the actual protocols specified in the standard. It also defines how the devices should communicate with each other based on the standard. The Bluetooth protocol stack is shown in Figure 1. Each component of the Bluetooth stack is explained below.

- **Bluetooth Radio:** specifics details of the air interface, including frequency, frequency hopping, modulation scheme, and transmission power.
- **Baseband**: concerned with connection establishment within a piconet, addressing, packet format, timing and power control.
- **Link manager protocol (LMP)**: establishes the link setup between Bluetooth devices and manages ongoing links, including security aspects (e.g. authentication and encryption), and control and negotiation of baseband packet size.



- **Logical link control and adaptation protocol (L2CAP)**: adapts upper layer protocols to the baseband layer. Provides both connectionless and connection-oriented services.
- **Service discovery protocol (SDP)**: handles device information, services, and queries for service characteristics between two or more Bluetooth devices.
- **Host Controller Interface (HCI):** provides an interface method for accessing the Bluetooth hardware capabilities. It contains a command interface, which acts between the Baseband controller and link manager
- **TCS BIN (Telephony Control Service)**: bit- oriented protocol that defines the call control signaling for the establishment of voice and data calls between Bluetooth devices.
- **OBEX (Object EXchange)** : Session-layer protocol for the exchange of objects, providing a model for object and operation representation
- **RFCOMM**: a reliable transport protocol, which provides emulation of RS232 serial ports over the L2CAPprotocol
- **WAE/WAP**: Bluetooth incorporates the wireless application environment and the wireless application protocol into its architecture.

III. APPLICATION DOMAINS FOR BLUETOOTH TECHNOLOGY

Here we discuss the application domain of Bluetooth Technology. Bluetooth allows a maximum of Eight devices to communicate in a small network called a piconet. The maximum number of Bluetooth wireless devices that can be paired varies depending on which model of the unit is used. In the Bluetooth radio, ten piconets can coexist in the same coverage range. To provide secure connection, each link is encoded and protected against snooping and interference. Using short-range wireless property Bluetooth provides support for 3 general application areas: information and voice access points- Bluetooth permits voice and information transmissions by providing wireless association of stationary and moveable communication devices, Cable replacement- Bluetooth eliminates the necessity for varied, typically proprietary cable attachments for the association of much any quite communications device.

IV. PICONETS ANDSCATTERNETS

The basic unit of Bluetooth networking is a piconet. The terms„piconet "and „scatternet" are typically applied to Bluetooth wireless technology. A brief description of each of the two terminologies is given below:

- Piconet - It is a Bluetooth network that can have up to eight stations, one of which is called as master and the rest are called as slaves as shown in Figure2.

Fig 2: Piconet [5]

- Scatternet - It is computer network comprising of two or more piconets as shown in Figure 3. A scatternet has the advantage of supporting communication between more than eight devices. However, currently there are only few implementations of scatternets and various researches are being done related toit.

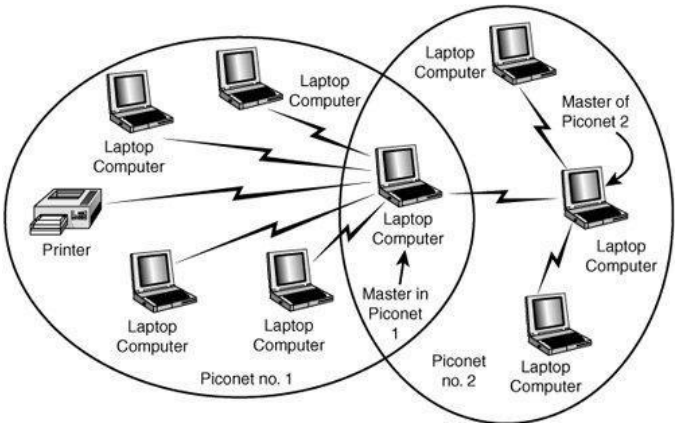


Fig 3: Scatternet [5]

V. WHAT ARE THE BLUETOOTHSECURITY ISSUES?

Bluetooth offers several benefits and advantages, but the benefits are not provided without risk. It includes authorisation, authentication and optional encryption. Authentication is the proving of identity of one Bluetooth-enabled device to another. Authorisation is the granting or denying of Bluetooth connection access to resources or services from the requesting device. Encryption is the translating of data into secret code so that eavesdroppers cannot read itscontent. Despite all the defence mechanisms in place, usage of Bluetooth might result in exploits and data loss from the d*MAC spoofingattack:*

Malicious attackers can perform MAC spoofing during the link key generation while Piconet is being formed. 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[6].
device through the following methods:-

- *Cabir Worm:*

It is a kind of malicious software that uses Bluetooth technology to seek out available Bluetooth devices and sends itself to them. 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[1].

- *Blue Jacking attack:*

This attack is initiated by an attacker sending unsolicited messages to a user of a Bluetooth- enabled device. Does not allow any adversary access to any data.

- *Blue Snarfing attack:*

In this case, attackers can access the data without the consent from the owner.

- *Blue Bugging attack:*

Attacker can remotely change the data without the permission from the users.

- *Blueprinting attack:*

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[1].

- *Blueover attack:*

A Blueover attack is dangerous only if the target device is vulnerable to BlueBugging. BlueBugging attack is capable of stealing sensitive information from your friend. A Blueover attack can be done secretly, by using only a Bluetooth mobile phone with Blueover or Bluover IIinstalled.

- *Fuzzing Attacks:*

It consists of sending malformed or otherwise non-standard datato a device‟s Bluetooth radio and observing how the device reacts. When a device‟s response is slowed or stopped by these attacks, this indicates that a serious vulnerability potentially exists in the protocol stack[5].

- *Reflection attack:*

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 [1].

- *Backdoor attack:*

Attacker may continue using the devices for extracting the data without the consent from the owner until the user notices such attacks.

- *Denial of Service:*

Malicious attackers can damage your devices, block them from receiving phone calls and drain your battery. Switch off the Bluetooth if not necessary.

- *Man-in-the-Middle/Impersonation Attack:*

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. Actually involve the modification of data between the pairing devices communicating in a Piconet[6].

- *War Nibbling:*

War Nibbling is an attack in which a phreaker attempts to find and access as many vulnerable Bluetooth phones as possible. They typically use laptops or PCs with high gain antennas and special software, such asRedfang, to sniff for accessible phones.

- *Eavesdropping:*

It is all about wireless communications. Just like with Wi-Fi, Bluetooth encryption is supposed to stop criminals listening in to your data.

VI. SECURITY FEATURES ANDMODES

The various versions of Bluetooth specifications define four security modes. Each version of Bluetooth supports some, but not all, of the four modes. Each Bluetooth device must operate in one of the four modes, which are described below:-

- *Security Mode1*

It is non-secure. In effect, Bluetooth devices in this mode is “Promiscuous” and do not employ any mechanisms to prevent other Bluetooth-enabled from establishing connections.

- *Security Mode2*

The centralized security manager maintains policies for access control and interfaces with other protocols and device users. All Bluetooth devices can support Security mode 2.

- *Security Mode3*

A Bluetooth device initiates security procedures before the physical link is fully established. Bluetooth devices operating in Security Mode 3 mandates authentication and encryption for all connections to and from the device. This mode supports authentication (unidirectional or mutual) and encryption [7].

To generate this key, a pairing procedure is used when the two devices communicate for the first time.

The link key is generated during an initialization phase, while two Bluetooth devices that are communicating are “associated”. Per the Bluetooth specification, two associated devices simultaneously derive link keys during the initialization phase when a user enters an identical PIN into both devices. The PIN entry, device association, and key derivation are depicted conceptually in Figure 4. After initialization is complete, devices automatically and transparently authenticate and perform encryption of the link. It is possible to create a link key using higher layer key exchange methods and then import the link key into the Bluetooth modules. The PIN code used in Bluetooth devices can vary between 1 and 16 bytes. The typical 4-digit PIN may be sufficient for some applications; however, longer codes may be necessary[7].

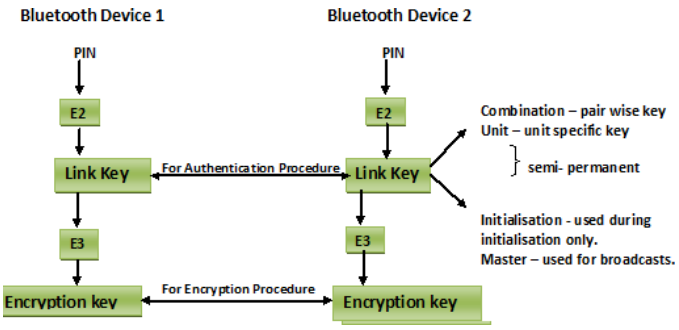


Figure 4: Bluetooth Generation Key from PIN [7]

- *Security Mode4*

This mode is similar to Security mode 2. Security mode 4 is a service level enforced security mode in which security procedures are initiated after link setup. Secure

Simple Pairing uses Elliptic Curve Diffie Hellman (ECDH) techniques for key exchange and link key generation. Security requirements for services protected by Security Mode 4 must be classified as one of the following: authenticated link key required, unauthenticated link key required, or no security required.

VII. RISK MITIGATION AND COUNTER MEASURE

Risk mitigation can be achieved in Bluetooth systems by applying countermeasures to address specific threats and vulnerabilities. Organizations should applying countermeasures to address specific threats and vulnerabilities to Bluetooth network. First solution is to provide an adequate level of knowledge and understanding for those who will deal with Bluetooth- enabled devices. Organizations using Bluetooth technology should design and document security policies that address the use of Bluetooth-enabled devices and users‟ responsibilities. Organizations should also include awareness-based education to support staff to enhance their understanding and knowledge of Bluetooth.

Bluetooth security checklist with guidelines and recommendations for creating and maintaining secure Bluetooth piconets:-

- Need to develop an organizational wireless security policy that addresses Bluetooth technology.
- Need to ensure that Bluetooth users on the network are made aware of their security-related responsibilities regarding Bluetooth use.
- Comprehensive security assessments at regular intervals to fully understand the organization Bluetooth security posture.
- Need to ensure that wireless devices and networks involving Bluetooth technology are fully understood from an architecture perspective and documented accordingly.
- Users should be provided with a list of precautionary measures they should take to better protect handheld Bluetooth devices from theft.
- Change the default setting of the Bluetooth device to reflect the organization ‟security policy.
- Bluetooth devices should be set to the lowest necessary and sufficient power level so that transmissions remain within the secure perimeter of the organization.
- Choose PIN codes that are sufficiently random and long. Avoid static PINs, such as all zeroes.
- If Bluetooth devices is lost or stolen, users should immediately unpaired the missing device from all other Bluetooth devices with which it was previously paired.
- Need to install antivirus software on Bluetooth- enabled hosts that are frequently targeted by malware.
- Need to fully test and deploy Bluetooth software patches and upgrades regularly.
- Users should not accept transmissions of any kind from unknown or suspicious devices. These types of transmission include message, files, and images.

VIII. PREVENTIVE MEASURE FORBLUETOOTH USAGE

Bluetooth Technology has many security vulnerabilities in its various configurations. Let us talk about how we can secure ourselves in spite of these vulnerabilities in Bluetooth:-

- The discoverable mode on your device is only meant to be used to “pair” two Bluetooth-enabled devices. When the pairing process is done, the discoverable mode can be turned off as the devices should remember each other.
- Refrain from communicating or transmitting sensitive and personal information using the Bluetooth-enabled device as it might be sniffed.
- Use strong passkey that is randomly generated when pairing Bluetooth devices and never enter passkeys when unexpectedly prompted for them.
- Maintain physical control of devices at all times. Remove lost or stolen devices from paired device lists.
- Avoid accepting attachments or applications received on your phone or device if you were not expecting it no matter how legitimate it may be. If your device asks to pair and you didn't initiate the pairing, deny it and check that your 'discoverable' setting is set to off or hidden.

IX. CONCLUSION

This paper discusses about the unique way of utilizing this amazing Bluetooth technology to achieve efficient ways of communication. It also covers up various important topics such as some background information related to the Bluetooth system, its applications and various security issues involved in Bluetooth. Vulnerabilities in Bluetooth technologies and threats against those vulnerabilities are also discussed. 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 users personal information becomes the primary objective. The latest improvements and innovations related to Bluetooth technology will be studied for our future work.

REFERENCES

[1] Nateq Be-Nazir Ibn Minar and Mohammed Tarique,"Bluetooth Security Threats and Solution" A Survey. In International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012

[2] Dieter Gollmann., "Computer security", 2nd Edition, paperback January1,2007.

[3] Satwant Kaur First Lady of Emerging Technologies Silicon Valley, USA,2014.

[4] TarunKumar, "Improving pairing mechanism in Bluetooth security" International Journal of Recent Trends in Engineering, Vol 2, No. 2, November 2009

[5] Karen Scarfone and john Padgette, "Guide to Bluetooth Security", paperback June30,2012.

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

[7] Praveen kumarmishra, "Bluetooth Security Threats." International Journal of Computer Science & Engineering Technology(IJCSET)

[8] Tzu-Chang Yeh, Jian-Ren Peng, Sheng-Shih Wang, and Jun-Ping Hsu, "Securing Bluetooth communication" International Journal of Network Security, Vol.14, No.4, PP.229-235, July2012.