Volume 8, Issue 2, April 2021 ISSN: 2348-8565 (Online)
International Journal of Modern Engineering and Research Technology
Website: http://www.ijmert.org Email: editor.ijmert@gmail.com

Bluetooth Security Technology and its Different Prospects

Aptatim Pranshu
M.Tech Research Scholar
Computer Science and Engineering
Dr. A.P.J. Abdul Kalam University,
Indore (M. P.), India
Email: supercool.apratim@gmail.com

Lokendra Singh Songara
Assistant Professor
Department of Computer Science and Engineering
Dr. A.P.J. Abdul Kalam University,
Indore (M. P.), India
Email: lokendrasingh9229@gmail.com

ABSTRACT

Bluetooth is a wireless technology that facilitates short-distance information sharing over a network. It's a short range, low control application. Since Bluetooth is a communication protocol, it uses it to communicate with other Bluetooth-enabled devices. Bluetooth resembles some other correspondence convention that you utilize each day, for example, HTTP, FTP, SMTP, or IMAP. Bluetooth is designed to connect with monitor and mouse without any connection with CPU. Different kinds of Bluetooth gadgets are headsets, Bluetooth prepared printer, in-auto Bluetooth framework, Bluetooth gaps framework, Bluetooth console, Bluetooth prepared webcam and so on. Bluetooth advancement tends to an open entryway for the business to pass on remote arrangements that are unavoidable over an expansive scope of gadgets. The constraints and properties of Bluetooth scatter presents remarkable troubles in framing a system in which all devices communicate with each other directly. In this paper, detailed description of Bluetooth along with its working is given. Description also includes connection protocols of the Bluetooth, usage models, advantages and dis-advantages. Further, various applications of the Bluetooth wireless technology are portrayed.

Keywords:— *HTTP, FTP, SMTP, or IMAP. Bluetooth, L2CAP, ACL, SCO*

I. INTRODUCTION

Bluetooth is an innovation that offers information rates of up to 3 Mb/s for real-time two-way speech communication and short-range remote information sharing. Any device can be connected to another device using it. Bluetooth-empowered gadgets[5], for example, cell telephones, headsets, PCs, portable PCs, printers, mice, and consoles, are generally utilized everywhere throughout the world. As of now in 2006, the one billionth Bluetooth gadget was sent, and the volume is relied upon to increment quickly soon. The objective volume for 2010 is as high as two billion Bluetooth [5] gadgets. Hence, it is imperative to stay up with the latest. As an interconnection innovation, Bluetooth [5] needs to address all conventional security issues, no doubt understood from conveyed systems. Likewise, security issues in remote adhoc systems are a great deal more intricate than those of more customary wired or brought together remote systems. Besides, Bluetooth[5] systems are shaped by radio connections, which implies that there are extra security viewpoints whose effect is not yet surely knew. The L2CAP[2] (Logical Link Control and Adaptation Protocol) is a product module that typically lives on the host. The ACL[1] connection gives a parcel exchanged association between the expert and all dynamic slaves in the

piconet. Diffie-Hellman key[6] trade is taking into account the utilization of discrete logarithm. The L2CAP[2] (Logical Link Control and Adaptation Protocol) is a product module that typically lives on the host. The ACL[1] connection gives a bundle exchanged association between the expert and all dynamic slaves in the piconet. Diffie-Hellman key[6] trade is in view of the utilization of discrete logarithm

1.1 Bluetooth versions

The preparatory work for creating Bluetooth [5] innovation began in 1994, when Ericsson started exploring the conceivable methods for supplanting links in the middle of adornments and portable telephones with remote connections. Ericsson immediately understood the potential business for Bluetooth items, yet overall collaboration was required for the items to succeed. Along these lines, the Bluetooth SIG [Blu07b] was established in February 1998 by Ericsson, Nokia, IBM, Intel and Toshiba. 3Com, Lucent, Microsoft and Motorola joined the Bluetooth SIG in December 1999.These nine individuals from the Bluetooth SIG are known as the Bluetooth SIG Promoters. They are in charge of upper-level SIG organization, and for giving labor to run the advertising, capability and lawful procedures. At present, the Bluetooth SIG has more than 10000 part organizations.

1.1.1 First Version

The primary open adaptation of Bluetooth [5] particular, Bluetooth 1.0A [Blu99a], was discharged in July 1999. Numerous gadget producers experienced issues in making their Bluetooth 1.0A good items interoperable. Consequently, the Bluetooth 1.0B particular [Blu99b] was discharged later around the same time (December 1999) to alter the interoperability issues. The Bluetooth 1.1 particular [Blu01] was discharged in February 2001. It altered numerous mistakes that were found in the Bluetooth 1.0 B particular and included backing for decoded correspondence and additionally bolster for RSSI (Received Signal Strength Indicator). RSSI is an estimation of the got radio sign quality that is utilized for controlling power as a part of Bluetooth gadgets. It can likewise be utilized for Bluetooth situating purposes, for instance.

1.1.2 Further Version

The Bluetooth 2.0+EDR (Enhanced Data Rate) determination [Blu04a] was discharged in November 2004. The fundamental change was the presentation of EDR, which gives information rates up to 3 Mb/s. The first Bluetooth information rate before EDR was 1 Mb/s. As per the Bluetooth SIG, EDR has the accompanying impacts on Bluetooth correspondence: [Blu04a, Blu04b]

- Three times better transmission speed (up to 10 times in certain cases).
- Lower power consumption by a reduced duty cycle.
- Simplification of multilink scenarios due to more present bandwidth
- Further improved BER (Bit-Error-Rate) performance.

1.2 Bluetooth communication

Connection sorts define the ways Bluetooth devices can exchange data. Bluetooth has three connection sorts: ACL[1] (Asynchronous Connection-Less), SCO[1] (Synchronous Connection -Oriented) and eSCO.

SCO connections are symmetric (greatest of 64 kb/s for both headings) and are utilized for transferring realtime two-way

voice. Retransmission of voice bundles is not utilized. Accordingly, when the channel BER is high, voice can be twisted.

eSCO connections are likewise symmetric (most extreme of 864 kb/s for both headings) and are utilized for exchanging realtime two-way voice. Retransmission of bundles is utilized to guarantee the trustworthiness of information (voice). Since retransmission of parcels is utilized, eSCO connections can likewise convey information bundles. Then again, they are basically utilized for exchanging realtime two-way voice. Bluetooth 1.2 (or later) gadgets can utilize eSCO joins, yet they should likewise bolster SCO connections to provide backward-similarity.

ACL connections are for symmetric (greatest of 1306.9 kb/s for both bearings) or unbalanced (greatest of 2178.1 kb/s for send and 177.1 kb/s for get) information exchange. Retransmission of parcels is utilized to guarantee the honesty of information.

Level of obstacles:	n:	TX power (dBm):	RX sensitivity (dBm):	PL:	Range (m):
None	2.0	0	-70	70	32
None	2.0	0	-80	80	100
None	2.0	20	-70	90	316
None	2.0	20	-80	100	1000
Light	2.5	0	-70	70	16
Light	2.5	0	-80	80	40
Light	2.5	20	-70	90	100
Light	2.5	20	-80	100	251
Moderate	3.0	0	-70	70	*10*
Moderate	3.0	0	-80	80	*22*
Moderate	3.0	20	-70	90	*46*
Moderate	3.0	20	-80	100	*100*
Heavy	4.0	0	-70	70	6
Heavy	4.0	0	-80	80	10
Heavy	4.0	20	-70	90	18
Heavy	4.0	20	-80	100	32

Figure 1: Range of Bluetooth Devices

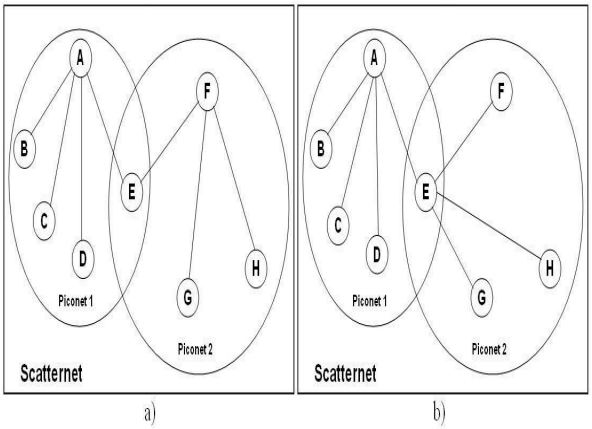

Figure 2: a) Bluetooth topology when ACL links are used. b) Bluetooth topologywhen SCO or eSCO links are used.

1.3 Special characteristics of the Bluetooth medium

Bluetooth is a remote RF correspondence framework utilizing chiefly omni-directional antennas. Communication with other Bluetooth gadgets is conceivable inside of the reach, and no direct line-of-sight between the imparting Bluetooth gadgets is needed. This capacity makes Bluetooth correspondence much simpler to use than the conventional link based correspondence or short range direct viewable pathway infrared correspondence, however then again it too makes spying much less demanding. Bluetooth devices can create ad-hoc networks of several devices in which no fixed infrastructure is required.

There are three Bluetooth gadget classes: class 1, class 2 and class 3. The greatest transmit powers for class 1, class 2 and class 3 gadgets are 100 mW (20 dBm, i.e. 20 decibels relative to one milliwatt), 2.5 mW (4 dBm), and 1 mW (0 dBm) individually. As indicated by the Bluetooth particular [Blu07a], the reference affectability Bluetooth gadget needs to be -70 dBm or better.

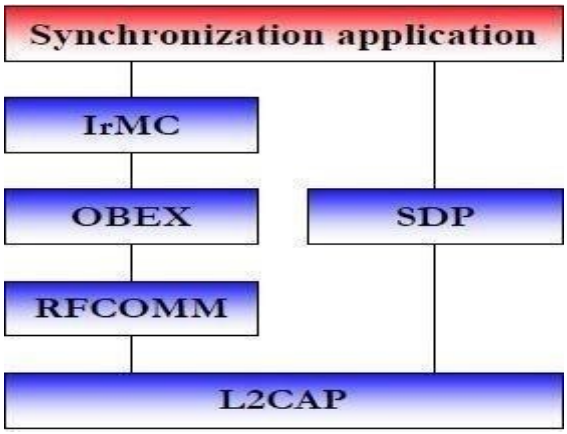

Figure 4: Synchronisation Application

1.4 Bluetooth Application Profiles Using OBEX

Synchronization: Basically, the synchronization means comparing two object stores, deciding their differences, and then binding these two object stores.

File Transfer: At the least, the File Transfer profile is intended for sending and retrieving generic files to and from the Bluetooth gadget.

Object Push: The Object Push profile is the extraordinary case of the File Transfer Profile for bearing objects and alternatively pulling the default objects

II. BLUETOOTH MODULES

2.1 Bluetooth Connectivity (Pairing)

The RFCOMM protocol copies the serial cable line settings and status of an RS-232 serial port and is used for providing serial data transfer. RFCOMM joins the lower layers of the Bluetooth protocol stack through the L2CAP layer.

2.2 Bluetooth Key Authentication

Basically, the synchronization means contrasting two object stores, determining their differences, and then binding these two object stores.

2.3 Bluetooth Data Transmission

There are two sorts of OBEX operations: a PUT and a GET. The PUT operation is to send an article from the customer to the server and the GET operation is to give back an item from the server to the customer.

Figure 5: Comparing pairing codes between two devices.

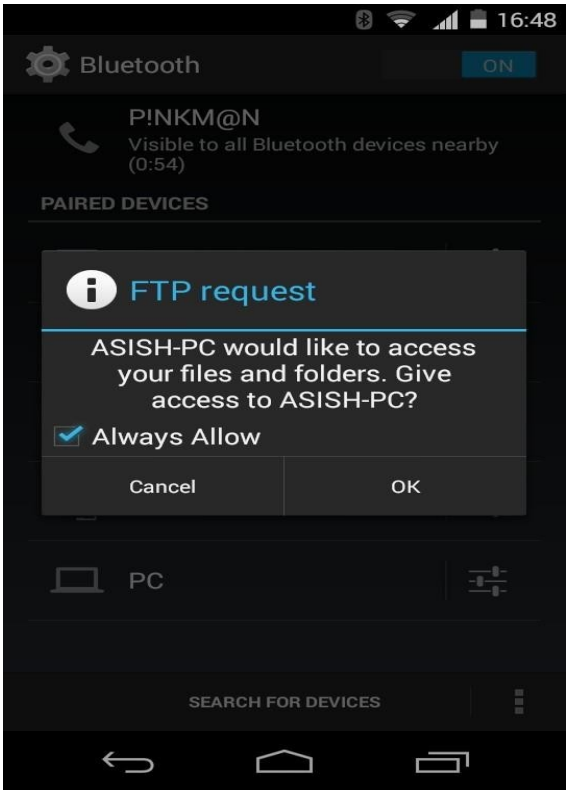

Figure 6: Determining their inequalities and unifying these two object stores

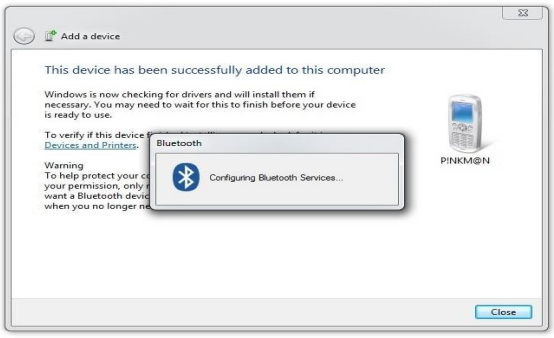

Figure 7: Synchronization

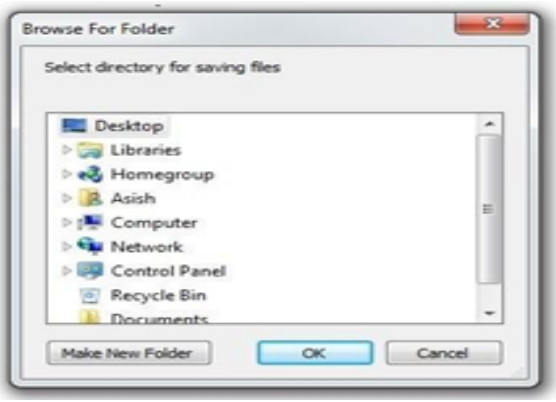

Figure 7: File Transfer

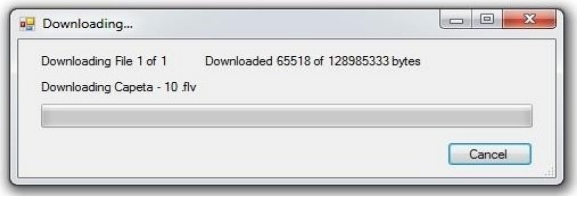

Figure 8: Sending generic files

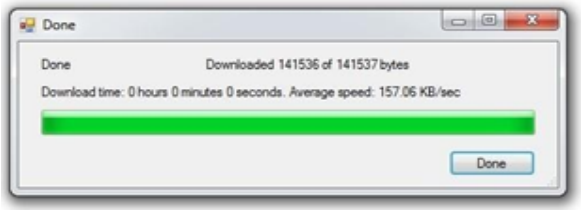

Figure 9: Retrieving generic files from Bluetooth Devices

Figure 10: Bearing objects and optionally pulling the default objects

III. The Bluetooth Security Issue

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 its content.

Despite all the defence mechanisms in place, usage of Bluetooth might result in exploits and data loss from the device through the following methods:-

3.1 MAC spoofing attack:

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].

3.2 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].

3.3 BlueJacking 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.

3.4 BlueSnarfing attack:

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

3.5 BlueBugging attack:

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

3.6 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].

3.7 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 II installed.

3.8 Fuzzing Attacks:

It consists of sending malformed or otherwise non- standard data to 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].

3.9 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].

3.10 Backdoor attack:

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

3.11 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.

3.12 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].

3.13 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 as Redfang, to sniff for accessible phones.

3.14 Eavesdropping:

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

IV. FUTURE SCOPE AND CONCLUSION

To better understand the total impact of Bluetooth on future pervasive computing applications (e.g., performance, reaction to noise, and interferences in a piconet or

scatternets), to create Bluetooth Transmission safer

4.1 Security Analysis

Due to inclusion of Authentication mechanism, the improved Diffie-Hellman [6] Key exchange protocol can stand up to replay attack, impersonation attack and man-in-the-middle attack. The simulation outputs in the LAN prove that authentication using hash function has the fewer computing quantity and the faster computing speed than the other public key and symmetric key encryption algorithm. It has a high practical worth in creating a secure communication channel of symmetric key.

4.2 Performance Evaluation

As long as the Diffie-Hellman[6] problem is difficult to decode, no eavesdropper can make out the secret key from the publicly known intelligence.

REFERENCES:

[1] Kapoor, R., Ling-Jyh Chen, Lee, Y. -Z., Gerla, M. "Bluetooth: carrying voice over ACL links" Mobile and Wireless Communications Network, 2002. 4th International Workshop on DOI: 10.1109/ MWCN.2002.1045792 Publication Year: 2002

[2] Yang Hua; Yuexian Zou; "Analysis of the packet transferring in L2CAP layer of Bluetooth v2.x+EDR" Information and Automation, 2008. ICIA 2008. International Conference on DOI:10.1109/ ICINFA.2008.4608099 Publication Year: 2008

[3] Choonhwa Lee, Helal, A "Ns-based Bluetooth LAP simulator" Local Computer Networks, 2001.Proceedings. LCN 2001. 26th Annual IEEE Conference on DOI: 10.1109/LCN.2001.990832 Publication Year: 2001

[4] Pek, E.; Bogunovic, Nikola; "Formal verification of logical link control and adaptation protocol" Electrotechnical Conference, 2004. MELECON 2004. Proceedings of the 12thIEEE Mediterranean Volume:2 DOI: 10.1109/MELCON.2004.1346997 Publication Year: 2004

[5] Bluetooth, S. I. G. "Specification of the Bluetooth System, version 1.1." http://www. bluetooth. com (2001).

[6] Research on Diffie-Hellman Key Exchange Protocol, Nan Li, "Information Engineering Teaching and research section", The People's Armed Police Force cadAemy of China, Langfang Hebei 065000, China

[7] Papakonstantinou, Yannis, Hector Garcia-Molina, and Jennifer Widom. "Object exchange across heterogeneous information sources." Data Engineering, 1995. Proceedings of the Eleventh International Conferenceon. IEEE, 1995.

* * * * *