Proc. of the Intl. Conf. on Recent Trends In Computing and Communication Engineering -- RTCCE 2013
Copyright © Institute of Research Engineers and Doctors. All rights reserved.
ISBN: 978-981-07-6184-4

A Survey of Bluetooth Security in Smart Phone

[Vijendra Singh Bhamu]

Abstract: **Bluetooth technology has become an integral part of this modern society. The availability of mobile phones, game controllers, Personal Digital Assistant (PDA) and personal computers has made Bluetooth a popular technology for short range wireless communication. However, as the Bluetooth technology becomes widespread, vulnerabilities in its security Issue/problem are increasing which can be potentially dangerous to the privacy of a user's personal information. The security issues/problem of Bluetooth has been an active area of research for the last few years.**

This paper presents the unprotected in the security Issue/problem of this technology along with some past security threats and possible countermeasures as reported in the literatures which have been surveyed and summarized in paper. It also presents some tips that end-users can implement immediately to become more cautious about their private information.

Keywords: **Bluetooth Version & Range, Specification, Security Threats, Security Procedures, Problem Formulation.**

I. INTRODUCTION

Bluetooth technology has become an integral part of this modern society. The availability of mobile phone, game controllers, Personal Digital Assistant (PDA) and personal computers has made Bluetooth a popular technology for short range wireless communication. Bluetooth is a short range low power wireless technology designed especially for compact handheld devices. Bluetooth is a short range low power wireless technology designed especially for compact handheld devices. Among various other applications that are enabled through this short range connectivity, an important one is the possibility for handhelds to connect to a network access point[8]. This access point may provide location specific services, such as airline information at an airport, enable transactions at kiosks, or act as a gateway to the Internet or other local networks. The basic usage model is that mobile handhelds enter public places such as supermarkets, airports, museums or cafeterias and connect to access points installed at these places, using Bluetooth.

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. 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. 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.

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. A summary of the other key features of Bluetooth technology has been presented:-

Table I. Bluetooth Technical Specification

Connection	Spread Spectrum(Frequency)
Frequency band	2.4 GHZ ISM
Modulation Technique	Gaussian Frequency Shift
MAC Scheduling scheme	FH-CDMA
Transmission Power	>20 dBm
Aggregate Data Rate	0.721-1 Mbps
Range	10m-300m
Supported Stations	8 devices (per Piconet)
Voice Channels	3
Data Security	128 bit key
Data Security-Encryption	8-128 bits(configurable)

The methods used for handoff should be optimized for the Bluetooth physical and Medium Access Control (MAC) layers to reduce handoff delay.

Bluetooth links use optional pre-shared key authentication and encryption algorithms that are widely considered acceptably strong when both implemented and used correctly. The strength of Bluetooth security relies primarily on the length and randomness of the passkey used for Bluetooth pairing, during which devices mutually authenticate each other for the first time and set up a link key for later authentication and encryption. Also important for overall Bluetooth security are discoverability and connect-ability settings.
These settings control whether remote Bluetooth devices are able to find and connect to a local Bluetooth device. Optional user authorization for incoming connection requests provides additional security.

Bluetooth allows adhoc connections to be set up between devices without the users having to know the device addresses or configurations. However, Bluetooth does not provide for seamless handoff when a mobile handheld moves from the range of one access point to another.

Advantage:-

Bluetooth is actually inexpensive:-The technology of Bluetooth is cheap for companies to implement, which results in lower costs for the company.

Bluetooth is automatic:- Bluetooth doesn't have set up a connection or push any buttons. When two or more devices enter a range of up to 300 meter of each other, they will automatically begin to communicate without we having to do anything.

Low interference:- Bluetooth devices almost always avoid interference from other wireless devices. Bluetooth uses a technique known as frequency hopping, and also low power wireless signals.

Low energy consumption:- As a result of Bluetooth using low power signals, the technology requires very little energy and will use less battery or electrical power as a result. This is an excellent benefit for mobile devices, as Bluetooth won't drain the battery.

Sharing voice and data:-The standard for Bluetooth will allow compatible devices to share data and voice communications. This is great for mobile phones and headsets, as Bluetooth simplifies driving and talking on your cell phone.

II. Version & Range

Bluetooth is first released in 1998, Bluetooth was designed for low power consumption and moderate data transfer rates over short ranges[1]:

- Class 1: 1 meters
- Class 2: 10 meters
- Class 3: 100 meter
- Class 4: 300 meter

The technology forms a mobile ad hoc network, or piconet, between two or more wireless devices. The connecting devices establish a master–slave relationship in which the master device is in charge of the network. Devices are identified by a unique 48-bit string address; a user- or manufacturer-assigned human-readable name; and a class—identifying the device type, such as a cell phone, computer, printer, or video game console.

The Bluetooth Special Interest Group is an industry consortium that specifies and licenses the technology. Major specification **versions and release dates** are as follows:

Table II. ***Bluetooth Versions and release dates***

Version	*Details*	*Release year*
1.0		2001
2.0	EDR(Enhanced Data Rate)	2004
3.0	HR(High Speed)	2009
4.0		2009

III. Bluetooth Security Threats

A. Low range

Bluetooth is a short and low range power wireless technology devices. Bluetooth working in present time something 10 to 300 meters.

B. Network conjunction

Bluetooth data transferring then network conjunction some case is high and some case data lose probability is very high.

C. MAC (Medium Access Control) spoofing attack

Among all passive attacks, the most frequently reported attacks are classified as MAC spoofing attacks. Hateful 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.

D. PIN cracking attack

Personal Identification Number (PIN). The PIN code is 1-8 bytes long (8128 bits). However, most devices use PIN sizes of 4 decimal digits.

Solution:- The proposed solutions for these types of attacks involve different pairing and authentication schemes that involves using a combination of public/private keys.

E. Man-in-the-Middle attack

Man-in-the-Middle and impersonation attacks actually involve the modification of data between devices communicating in a Piconet.

Solution:- The suggested solutions to this kind of attack involve incorporating more Piconet specific information into the pairing process.

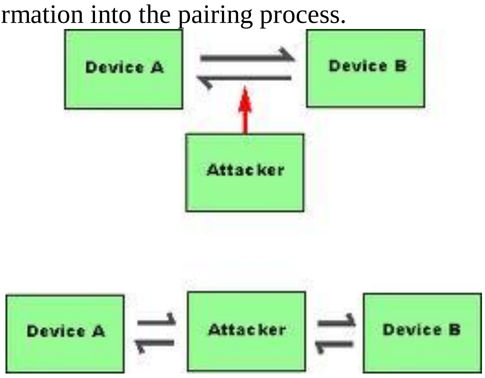

Figure 1. Main-in-the-Middle attack

F. Blue Jacking attack

Blue jacking is the process of sending unwanted messages to Bluetooth- enabled devices. This does not involve altering any data from the device, but nonetheless, it is unsolicited.

G. Blue Snarfing attack

Blue snarfing 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.

H. Blue Bugging attack

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.

I. Blue Printing attack

A Blue Printing 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. Blue Print 0.1 is a tool for performing Blue Printing attack. It runs on Linux and it is based on the Blue Z protocol stack. BluePrinting attacks work only when the BD_ADDR of the target device is known.

J. 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.

K. 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.

L. 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 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.

M. 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.

N. 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 established. 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.

O. 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. Cabir worm that uses Bluetooth and Multimedia Messaging Service(MMS) to replicate.

P. 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.

Q. 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. It arrives in the target mobile phone via Bluetooth in a similar way as Cabir and Skulls.D do. When the user opens the velasco.sis file and chooses to install it, the worm will be activated and it will immediately starts searching for new Bluetooth devices to infect. In addition to sending itself via Bluetooth, it is also capable of inserting itself into other SIS files in the target device. Therefore, if infected SIS files are copied to another device, Lasco worm will also affect the other device too.

R. Blue spamming

An extended version of bluejacking where contacts on a phone can be sent messages without the user noticing the spamming.

S. Bluetoothing

The Bluetoothing which is just like social engineering; the hacker can use methods like harassment or luring the victim to fall his prey to his intentions.

IV. 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.

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.

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.

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.

V. BLUETOOTH SECURITY PROCEDURES

There are three main steps in Bluetooth security procedures:-

- **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.
- **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.

VI. PROBLEM FORMULATION

The Bluetooth device has importance in technical life but Bluetooth devices has not secure till date. Bluetooth came up as one of the major breakthroughs in close range wireless transfer of data and communication standard between mobile devices. Although the GSM standard itself is a wireless standard operating on licensed bands, yet transfer of large amount of data is not feasible especially if you want to share a file may be with your friend near by. Mobiles did have the Infrared technology which was used for such applications.

Bluetooth has become a very basic feature of mobiles and now every mobile be it from a branded vendor or to may be a Chinese clone of such mobiles; all have this feature embedded in them. Many Bluetooth application therefore have emerged that allow peering of users, however people least give importance to the security issues that arise when radio spectrum is used in such a way.

In Bluejacking a hacker might send unsolicited messages to the victim in the form of a business card or a mobile contact with a text that may look intimidating to read. In many cases hacker may also send sounds like a ring tone. The victim’s mobile could then be infiltrated and he might never know what has hit him. Bluejacking messages can also be viewed as spam messages with emails. There have also been reports about people getting hacked by Trojan Horse’s which could mean a serious compromise.

Bluesnarfing is considered a serious compromise in the category of Bluetooth hacking especially if the information vulnerable, is quite critical, as such attacks can allow the hacker access to victims; contact list, text messages, emails and even private photos and videos. The hacker can use brute force attack even if the device is invisible to guess the victims MAC address.

Bluebugging in which the hacker uses sophisticated attacks to gain control of victims mobile. It works just like Trojan horses, where the hacker can manipulate the users phone the way he desires by executing commands on the victims phone. The hacker could forward mobile calls from the victim’s mobile to his own device and can even manipulate the mobile to follow a Bluetooth headset instructions like; receive call, send messages etc.

Bluetoothing which is just like social engineering; the hacker can use methods like harassment or luring the victim to fall his prey to his intentions.

VII. CONCLUSION

This Survey 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. Due to limitations in time and resources, only a comprehensive literature survey has been presented in this paper. Emerging devices all have Bluetooth as a mandatory feature and its potential applications are increasing, so its future vulnerabilities needs to be explored through further research in this field. The bottom line is, we need technology to survive and technology needs us to evolve ensuring our safety first.

ACKNOWLEDGMENT

First of all I feel great pleasure in acknowledging my deepest gratitude to my revered guide and mentor, **Ms. Anu Garg**, Ass. Professor, Computer Science and Engineering Department, Lovely Professional University, under whose firm guidance, motivation and vigilant supervision I succeeded in completing my work. He infused into me the enthusiasm to work on this topic. His tolerant nature accepted my shortcomings and he synergized his impeccable knowledge with my curiosity to learn into this fruitful result.

Finally, I also wish to thank my friends **Mr. Tarun Singh (Software Engineer), Er. Sunil Gill, Er. Ankur Kumar Sharma and Rohan Kumar** for supporting me during my whole project work.

Words are inadequate to express my heartfelt gratitude to my affectionate parents who have shown so much confidence in me and by whose efforts and blessings I have reached here.

I find it hard to express my grateful to the Almighty in words for bestowing upon me his deepest blessings and providing me with the most wonderful opportunity in the form of life of a human being and for the warmth and kindness he has showered upon me by giving me life's best.

I wish to express heartiest thanks to my friends and colleagues for their support, love and inspiration.

REFERENCES:-

Research papers

[1] Mohammed Mana, Mohammed Feham, and Boucif Amar Bensaber, *"A light weight protocol toprovide location privacy in wireless body area networks",* International Journal of Network Security and its Applications (IJNSA), Vol.3, No.2, March 2011

[2] 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

[3] Kumar, A., et al. Caveat eptor, *"A comparative study of secure device pairing methods*", IEEE International Conference on Pervasive Computing and Communications (PerCom-09). 2009.

[4] K. Scarfone and J. Padgette, NIST SP 800-121 Guidelines for Bluetooth Security, Whitepaper, September 2008

[5] NSA IAD SNAC, Bluetooth Security, I732016R-07

Websites:-

[6] *"The Bluetooth Blues*", available at

http://www.information-age.com/article/2001/may/the_bluetooth_ blues

[7] 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

[8] www.free4notes.in/reserchpaper/what-is-introduction-Andriod& Bluetooth

[9] http://www.sysopt.com/features/ network/article.php/3532506 (1999-12- 14).

[10] The Bluetooth Special Interest Group:-

www.bluetooth.com www.bluetooth.org

[11] www.aircces.org/journal/ijdps/papers/0112ijdps_10.pdf

[12] www.ieeexplore.iee.org/stamp/stamp.jsp?#p=&arnumber=617053

About Author (s):

Vijendra Singh Bhamu is currently studying from Lovely Professional University Punjab(India) in the Department of Computer Science and Engineering. He completed his M.Sc(CS) from JNR University, Udaipur in the year 2011 in the Department of Computer Science and Engineering. He pursing his engineering post-graduation from Lovely Professional University, Pujab(India) in the Department of Computer Science and Engineering.