*International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)*
*August 2015, PP 69-75*
*ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)*
*www.arcjournals.org*

# A Review on Bluetooth Security Vulnerabilities and a Proposed Prototype Model for Enhancing Security against MITM Attack

**Vimalesh Kumar Dubey[1], Kumari Vaishali , Nishant Behar* and Manish Shrivastava**

Department of Computer Science and Engineering, Guru Ghasidas Vishwavidyalya
Institute of Technology, Bilaspur, C.G.
* *nishant.behar@gmail.com*

**Abstract:** *Bluetooth has emerged as an optional radio frequency communication over short range. Today Bluetooth has been implemented in billions of devices including mobile phones, personal computers, cars, medical devices and many more. Bluetooth works over a wide range of fixed devices. From security point of view this technology seems more secure. It is due to frequency hopping technique used in Bluetooth communication. Actually Bluetooth works over 79 channels and during its communication there is frequent hopping over 79 channels. It merely allows any MITM (man in the middle) attack. No doubt Bluetooth is a useful and valuable wireless communication but still has weakness in its security architecture. Due to this Bluetooth technology has a number of security vulnerabilities. The privacy of a user's personal information may at high risk due to increasing vulnerabilities in its security protocols. The most considerable weakness in its pairing mechanism is pin guessing attack, which is responsible for many security problems. This attack reveals the Initialization, Link and Encryption keys which are cardinal parameter for Bluetooth security. In this paper we have discussed about the most common Bluetooth vulnerabilities and related security problems and also about initiatives taken to improve the major security problems and key security features of latest Bluetooth v4.2.We present here a prototype model of proposed methodology to ensure simple secure pairing mechanism to make Pin Guessing attack difficult to crack the link keys . This method uses two shared secret parameters, which makes the pairing process more secure from man in the middle attack also.*

**Keywords:** *Bluetooth, security, pairing, vulnerability, MITM, pin, key generation.*

## 1. INTRODUCTION

In today's world Bluetooth technology has become ubiquitous. It was developed [5] by a group called Bluetooth Special Interest Group (SIG), formed in May 1998[3]. The founding members were Ericsson, Nokia, Intel, IBM and Toshiba. Since then, almost all of the biggest companies in the telecommunications business (e.g. 3Com, Microsoft, Motorola) have joined the Bluetooth SIG. Now SIG has over 14000 members who works on development of this technology. Bluetooth is an ingenious amalgamation of hardware and software technology. The hardware is implemented on a radio chip while control and security protocols have been implemented in the software. Using Fast Frequency Hopping Sequence (FFHS) a Bluetooth device hops from one channel to another channel up to 1600 times/sec for data/voice links and 3200 times/sec during page and inquiry scanning. A particular channel is used only for a very short time (625 ms), followed by a hop designated by a pre-determined pseudo-random sequence to another channel. Bluetooth is also facilated with Adaptive Frequency Hopping (AFH) technique which is designed to manage excessive packet losses in the case of packet collisions or external interferences. The Bluetooth special technical specification are shown below. You can get more detailed information at [3].

| Connection | Spread spectrum frequency |
|---|---|
| Frequency band | 2.4 Ghz ISM |
| Transmission power | >20 dbm |
| Modulation technique | Gaussian frequency shift |
| Mac scheduling scheme | FH-CDMA |
| Aggregate data rate | 0.721-1 mbps |
| Range | 10-100 m |
| Voice channels | 3 |

| | |
|---|---|
| Supported stations | 8 stations (per piconet) |
| Data security | 128 bit key |
| Data security and encryption | 8-128 bits configurable |

**Table 1.** *Bluetooth Technical Specification*

The last released version v4.2 had the most versatile design, low power usage and enhanced with the best security mechanism. But still it has some security 'loop-holes' that make it vulnerable to many security attacks. In this paper, these vulnerability issues have been addressed. The security threats have been surveyed and summarized in this paper. The rest of the paper is organized as follows, Section II describes some Bluetooth security vulnerabilities and past works over these vulnerabilities. Section III describes the security features and section IV describes the proposed method over SSP (simple secure pairing). Section V describes the future of Bluetooth technology.

## 2. BLUETOOTH VULNERABILITIES

Due to implementation of millions and millions of Bluetooth devices in use, malicious security violations are now common events these days and expected to be increase in upcoming future. On the contrary, the increased usage of Bluetooth devices makes security concerns even more alarming. Like any other wireless communication system Bluetooth transmission can be deliberately jammed or intercepted. False or modified information could be sent to the users by the attacker. The problems regarding Bluetooth security have been reported since its inception. 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.[16]
- 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.[17]
- In January 2005, a mobile malware called 'Lasco' was detected. Lasco was a self-replicating worm, which was successful in rendering a mobile device unstable before infecting another device.[18]
- In April 2005, Cambridge University published a paper documenting actual passive attacks by implementing off-line PIN cracking.[19]
- In August 2005, Bluetooth enabled phones were used to track other mobile device left inside of cars. [20]
- 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.[21]
- 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.[22]

Some important common vulnerabilities are listed below:

**1)** **Blue jacking**: Blue jacking is the process of sending unsolicited messages to Bluetooth-enabled devices. It is a passive attack in which victim is flooded with anonymous messages. This attack can easily be carried out in a crowded area where a number of unsuspecting victims are easily found. This attack uses the “***obex push attack***” vulnerability. Many of the noika, sony and motorolla mobile phones have been targeted with this attack.

2) **Bluebugging**: It uses the AT(address translation) commands available in GSM phones. An attacker exploits these commands and steal personal information like phonebook and message. Even phone call can be initiated. Unwanted messages, viruses, worms can be sent from victim device to any other device.

3) **Backdoor attack**: In backdoor attack attacker get access of victim device without alarming it. By exploting pairing mechanism one can connect to victim device without being available in

its registered user.Attacker uses all services of victim like it were legitimate user of it. To carry this attack the victim device has to be vulnerable to a backdoor attack.

4) **Dos** attack

**BD_ADDR duplication attack:** An attacker places a 'bug' in the range of the Bluetooth device. The bug duplicates the BD_ADDR of the target device. When any Bluetooth device tries to make a connection with the target device, either the target device or both devices (i.e., the target device and the bug) will respond and jam each other. In this way, the attacker can cause denial of access from the legitimate device. The most effective way to perform this attack is to duplicate the BD_ADDR of the Piconet master device, because all information within the Piconet goes through the master Device.

**SCO/eSCO attack:** It is based on a real-time two-way voice. It reserves a great deal of a Bluetooth Piconet's attention so that the legitimate Piconet devices are not allowed to get the service within a reasonable period of time. The most effective way to perform this type of attack is to establish a SCO or an e-SCO link with the Piconet master

**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. It is also used as a battery exhaustion attack.

5.) **Worm attack [16-20]**

Bluetooth technology is also effected with viruses and worms. Due to their self repeating nature they spread from one Bluetooth device to another Bluetooth device. *Lasco* worm, *Kabir* worm, *Skulls* worm etc. are some common frequently used malicious programs. These worms were mainly written for Symbian series 60 user interface platform. These are malicious SIS (Symbian Installation System) Trojan file that pretends to be Macromedia Flash player for Symbian Mobile devices .When worm is activated, it automatically searches for another Bluetooth devices in range and transfers .SIS file on victim device. Since these are Trojan files so attacker can do all legitimate activities with phone what a legitimate user can do.

6.) **Pin cracking attack: [22]**

This is most important security vulnerability in the Bluetooth technology. Security of Bluetooth communication is totally dependent on the user defined shared secret i.e. pin number. This is the only parameter which is unknown to an attacker. A dictionary attack or a simple pin guessing attack can be successful to crack the Bluetooth communication link keys. Guessing the exact pin attacker can easily authenticate itself illegally. Most research on Bluetooth security are focused towards this issue.

## Work related to the Bluetooth security

As per the above mentioned security problems, many research work and studies have been done. These all activities are mainly focused on providing an efficient, short and effective pairing mechanism between Bluetooth devices. Many of them are focused towards providing security facilities like integrity and confidentiality. Some commendable research work has been mentioned in [6][7][8]. Most of the works are categorised as follows:

1) Many of the researchers are agree to use the DES and RSA to be used in Bluetooth communication to provide integrity and confidentiality, but some researchers are against this because these protocols are too lengthy and will increase the communication delay.

2.) Some researchers have suggested that pairing mechanism is not secure because there is only one user shared secret key. So we should use the concept of two shared secret parameters.

3.) Some scholars have suggested that most vulnerabilities are only because Bluetooth address of devices are easily cracked by attackers, so we should use an alias of Bluetooth address for Bluetooth communication.

4.) **Markus Jakobsson and Susanne Vitzel, 2008:** He published an articles in which he mentioned the different ways of generating link keys and initialisation keys keeping major vulnerabilities in mind. One of his suggested procedure was later used in Bluetooth specifications. [12]

5.) **jun-Zhao, Douglas Howie, Antti and Jaakko sauvola:** He proposed many link key management, authentication and encryption schemes to make Bluetooth more secure and robust. He also proposed many countermeasures to handle security issues. [13]

6.) **Wuling Ren, Zhejiang Gongshang, 2010:** In 2010 wuling and et al. proposed that the current Encryption and authentication algorithm are prone to MITM and pin cracking attacks. He suggested a hybrid system of DES and RSA. Since DES is symmetric and RSA is asymmetric, both together can provide confidentiality and integrity [10].

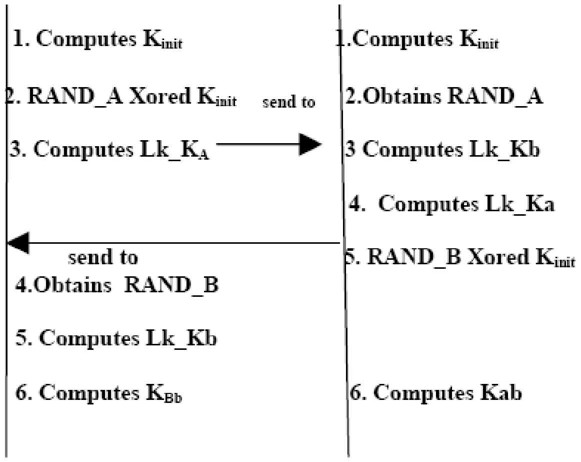
7.) **Li juan Chen Bin, Li Kun, 2009:**

He proposed that des cannot be alone able to provide all security services. Because in des only one key is shared which can easily be cracked.so we need a more robust security mechanism and authentication procedure [11]

## 3. Pairing Mechanism

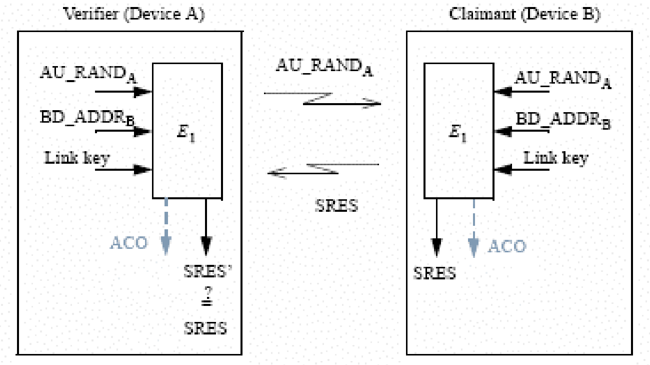
Current pairing mechanism can be described as follows:

First of all Initialization key is generated using the three parameters: Bluetooth address, random number and pin. This key is used to generate combination key $k_{ab.}$ This can be easily visualize as follows:



[redacted]

To final process of pairing mechanism is to authenticate the devices. This authentication is done using the combination link key. The authentication process can be illustrated as follows:



This process is actually a challenge–response scheme. Each device calculates the SRES using the LINK KEY, BD_ADDR and AU_RAND. If the SRES value for both devices match each other then the two devices are said to be paired.

### Problem in Pairing Mechanism

Thus the Bluetooth pairing mechanism is totally dependent on some random numbers and Bluetooth address and pin. Except pin all the parameters can be guessed or can be captured from the air. A simple MITM attack can be enough to reveal the secret keys. Pin guessing attack as describes earlier becomes more dangerous when it is carried with MITM attack.

## 4. Prototype of Proposed Method

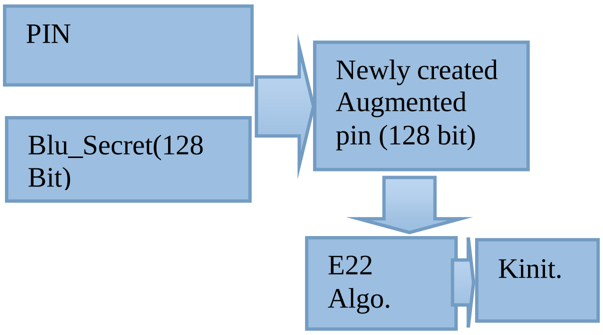
In order to provide full proof security we need an efficient pairing mechanism because most of the security problems arises due to improper and insecure pairing mechanism. If we observe the pairing mechanism of two Bluetooth devices, it is clear that there is only one unknown parameter that is user defined secret pin. In that case security can be breached by just a guessing or brute force attack.

To enhance the security further we can use the concept of DUAL SHARED SECRET KEY. Now instead of single shared secret key pin we will use Another shared secret parameter which we called Blu_Secret, which would be used in E22 Algorithm to generate initialization key. Blu_Secret (128 bit) is a shared parameter which can be exchanged between the two devices using Diffie Hellman key exchange method which has been accepted by Bluetooth SIG as a method to exchange keys. Blu_Secret would be used to augment pin number as follows:

PIN'= PIN[ 0…L-1], L=16

PIN'=PIN[0—L-1]UBlu_Secret[0—15-L]

Where L<=16



Where,

Kinit =initialization key,

This augmented PIN' can be directly used as input to the key schedule to compute round sub keys. This augmented PIN' adds more robustness to key schedule, as the PIN guessing attack only reveals PIN number , since round sub keys are computed from two shared parameters, it is difficult to compute round sub keys .

In the current pairing procedure, we find that Initialization key is used to exchange key generation parameters. Now since Kinit would be updated in two devices (using new value of Blu_secret), so the receiver with updated value would be only able to recover key generation parameters. This would further perform the task of authenticating the receiver, that only the recipient with valid Key would be able to recover the key generation parameters. Further, if the two known devices establish connection again, they will authenticate themselves with challenge response mechanism where the verifier sends a random value, AU_RAND to the claimant unit. The claimant unit then sends a response, SRES which is computed via the following parameters as inputs:-

i) BD_ADDR_claimant

ii) AU_RAND

iii) Kab

Since two devices will have updated value of Kab, which would further enhance the current challenge response mechanism.

This approach promises increased security, as the attacker may observe the number of sessions between two devices, but he may not be able to guess, the number of transactions between two devices, hence the current value of Blu_secret would remain as a secret between two devices. Further , since the keys are also updated with new value of Blu_Secret, this ensures security from man in the middle attack.

## 5. BLUETOOTH V4.2 'THE SKY'S THE LIMIT'[1]

Bluetooth SIG has recently adopted the newest version of Bluetooth v4.2.

Bluetooth 4.2 makes Bluetooth Smart even smarter, faster and the ideal wireless technology for the Internet of Things (IoT). Some speciality of v4.2 is as follows:

1.) low-power IP connectivity

2.) Bluetooth smart technology gateways (GATT) architecture

3.) Its speed is 2.5 time more than v4.0 [3] and capacity is increased by 10 times than that of v4.0.

4.) It is implemented upon industry leading privacy mechanisms. It is highly secure, more powerful and efficient.

Bluetooth v4.2 was brought to life by some of the brightest minds and companies in technology(Global Mission Control Team).Their mission -To provide you with the freedom to create anything you can imagine(Internet of things).

## 6. CONCLUSION

Even though SSP (secure simple pairing) improves the security of Bluetooth pairing, it has been shown that MITM attacks against Bluetooth 2.1+EDR, 3.0+HS, and 4.0 devices are possible by forcing victim devices to use the Just Works association model. Moreover, at least one of the proposed MITM attacks against Bluetooth SSP has already been implemented and mounted in practice. Thus, the security of SSP should be further improved. We need a simple and efficient method to authenticate two Bluetooth devices such that no mitm can take place. If pin cracking attack is resolved many of the security problems will be solved and thus we can give a bright secure future to the most attractive and amazing Bluetooth technology.

## REFERENCES

[1]. www.bluetooth.org

[2]. J. Dunning. Taming the Blue Beast: A Survey of Bluetooth Based Threats. IEEE security and privacy magazine 2010

[3]. Bluetooth SIG, Bluetooth Specification Version 2.1 +EDR, 2007. (http://www.bluetooth.com/Bluetooth/Technology/Building/Specifications/Default.htm)

[4]. Bluetooth SIG, Simple Pairing Whitepaper, 2006.(http://bluetooth.com/nr/rdonlyres/0a0b3f36d15f447085a6f2ccfa26f70f/0/simplepairing wp v10r00.

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

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

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

[8]. 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

[9]. 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

[10]. "Wuling Ren, Zhiqian Miao, College of Computer and Information Engineering, Zhejiang Gongshang University, "*A Hybrid Encryption Algorithm Based on DES and RSA" in Bluetooth Communication* Second International Conference on Modeling, Simulation and Visualization Methods, 2010.

[11]. Li Juan, Chen Bin, Li Kun, Electronic Engineering College, Naval University of Engineering Wuhan, China, "Study on the Improvement of Encryption Algorithm of Bluetooth", 2009 International Conference on Networking and Digital Society

[12]. Markus Jakobsson and Susanne Vitzel, Lucent Technologies – Bell Bell Labs, Information Science Research Center, Murray Hill,USA,Security Weakness in Bluetooth”.

[13]. Jun-Zhao Sun, Douglas Howie, Antti Koivisto and Jaakko Sauvola, Media Team, Machine Vision and Media Processing unit, InfoTech Oulu, University of Oulu, Finland, “Design Implementation and Evaluation of Bluetooth security.

[14]. *Bluetooth Version 4.0 Released*. Bluetooth SIG, available at: http://www.bluetooth.com/Pages/High-Speed.aspx

[15]. Keijo Haataja, “*Security Threats and Countermeasures in Bluetooth Enabled Systems*”, Kuopio University Library, 2009, pp. 55-62

[16]. *“The BlueBug*”, a Bluetooth virus, available at :http://trifinite.org/trifinite_stuff_bluebug.html

[17]. John Oates, “*Virus attacks mobiles via Bluetooth*”, available at: http://www.theregister.co.uk/2004/06/15/symbian_virus8/

[18]. F-Secure Article on Lasco. A Worm, available at: http://www.f-secure.com/v-descs/lasco

[19]. Ford-Long Wong, Frank Stajano, Jolyon Clulow, “*Repairing the Bluetooth pairing protocol*”. University of Cambridge Computer Laboratory, available at: http://www.cl.cam.ac.uk/research/dtg/~fw242/publications/2005-WongStaClu-bluetooth.pdf

[20]. *Phone pirates in seek and steal mission*", Cambridge Evening News, available at:

[21]. http://www.cambridge-news.co.uk/news/region_wide/2005 /08/17/

[22]. "*Going Around with Bluetooth in Full Safety*”, available at: http://www.securenetwork.it/ricerca/whitepaper/download/ bluebag_brochure.pdf

[23]. Yaniv Shaked, Avishai Wool, “*Cracking the Bluetooth PIN*” School of Electrical Engineering Systems, Tel Aviv University, available at: http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/