Volume 2 No. 3, March 2012 ISSN 2223-4985

International Journal of Information and Communication Technology Research

http://www.esjournals.org

A Review on Key Agreement Protocols used in Bluetooth Standard and Security Vulnerabilities in Bluetooth Transmission

[1]Trishna Panse, [2]Vivek Kapoor, [3]Prashant Panse
[1,2]Institute of Engineering & Technology DAVV, Indore
[3]Swami Vivekanand College of Engineering RGPV, Indore

ABSTRACT

This paper gives an overview of protocols used in Bluetooth communication and security weaknesses and vulnerabilities of the Bluetooth system. Now days, Bluetooth is a frequently used technique for data transmission. Bluetooth standard was come under IEEE 802.15. Its basic features are ad hoc in nature, very low power consumption and low cost. It operates on radio propagation with 2.4GHZ. Various types of security protocols are used to prevent eavesdropping and message interception but still some security weaknesses like no integrity check, man in middle attack, Bluesnarf attack and many more are present in Bluetooth transmission. This paper gives broad overview of the security flaws in Bluetooth.

Keywords: *Bluetooth, Vulnerability, Eavesdropping, Piconet, Bluesnarf, Authentication, Encryption and E0 stream cipher*

1. INTRODUCTION

The size of transmitted data through Bluetooth technology is depend upon the version of Bluetooth and the range of transmission is up to 10m depending up on the power level. Bluetooth is basically a personal area network that enables devices to connect to each other and share data whenever we want. Devices that connect to each other creates Piconet, it is a dynamically created network which includes one master device and maximum seven slave devices. Bluetooth technology consists of radio technology, protocol stack and interoperability profiles. A Bluetooth enabled application can be either server or client. The process of connecting two devices and transmit data start from Bluetooth stack initialization, after initialization the client can discover for nearby device and then for services. A server first, registers device in service discovery data base, wait for incoming connection and make service available to client[1]. Here, the important thing is discovery mode of Bluetooth device, there are three mode of device discovery: non discoverable mode, limited discoverable mode and general discovery mode. In discoverable mode device does not respond to enquiries, in limited discoverable mode device respond to queries for a limited time period and it is visible continuously in general discovery mode. Here we discuss security weakness and protocols used in Bluetooth communication.

2. PROTOCOL USED IN BLUETOOTH TECHNOLOGY

Bluetooth technology uses various types of protocol as key agreement protocol. Generating keys for Bluetooth technology is very decisive part, so our main focus is on functioning of key agreement protocol . For example if two devices want to communicate securely to each other first of all they want to generate a secret key because initially they do not have shared secret key, because of this they use the key agreement protocol. When this protocol performed the link key and encryption keys are generated. The encryption key is used in E0 stream cipher and the link key is used in challenge response technique which is used for authentication in Bluetooth. Link key is of two types: unit key and combination key. Unit key: same key is use for authentication for all the connection. Combination key : is specific to one pair of Bluetooth device[2].

2.1 Unit key creation

Unit key is a type of link key and it can be generated by two ways either dynamically or by a pairing mode. This key is unique for every device and its is never changed. It is generated as follows: first, the device calculates a random number RAND. The unit key is based upon this random number and the Bluetooth address (which is a factory-established parameter unique for every device).

The authentication process uses E1 algorithm. This procedure is shown in Figure 1.[3]

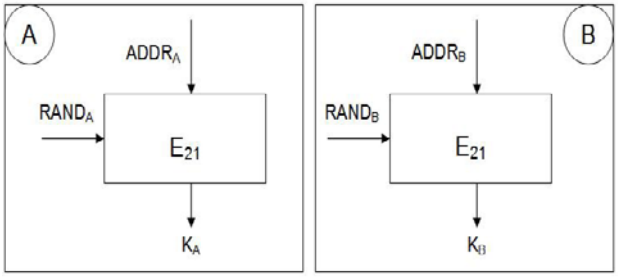

Figure 1: Unit key creation

2.2 Initialization key creation

An initialization key is based on Bluetooth addresses of two devices, random no. and pass key also called as PIN. An initialization key is generated using temporary key that is a function of a random number IN RAND (which is generated by the device that initiated the communication (let's suppose that A did this) and sent to the other device (B)), a shared PIN and the length L of the PIN. The PIN should be entered in both devices. The length of the PIN can be chosen between 8 and 128 bits. Typically, it consists of 4 decimal digits. If one of the devices does not have an input interface, a fixed PIN is used (often, the default value is 0000). This procedure is shown in Fig. 2. The result is a temporary shared key (the initialization key). This key is used in generation of link key [3].

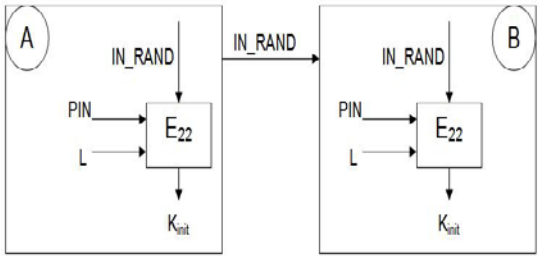

Figure 2: Initialization key creation

2.3 Link key creation

The link key will be stored on both devices so that it can be used for future communication.

If the unit key of device A is the link key, it is transmitted encrypted from A to B. This encryption is done by XOR'ing with the initialization key. If the link key is a combination key, then both devices first generate a random number .These random numbers are encrypted with the initialization key and sent to the other device. Now they both can calculate K_{unit} and K_{link}. This is shown in Figure 4. The key generation algorithm E21 is the same as the algorithm used for the generation of the unit key. After the generation of the link key, the old temporary initialization key is definitively discarded and a mutual authentication is started with the exchanged link key[3]. The Bluetooth Mutual authentication scheme uses a challenge-response strategy, where a 2-move protocol is used to check whether the other party knows the secret key. The protocol uses symmetric keys, so a successful authentication is based on the fact that both participants share the same key. The authentication scheme generates the value ACO (Authenticated Ciphering Offset) as a result[4].

The procedure shown in Figure 4 is also executed when a new link key is calculated. The only difference is that the random numbers are encrypted with the old link key. The result is a new link key which will replace the old link key (this old link key will be discarded).

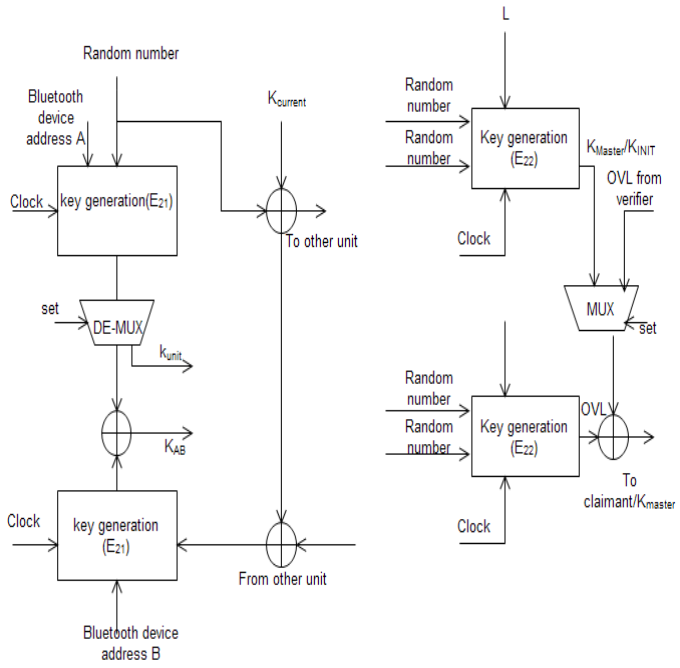

Figure 4: Link Key generation function unit

2.4 Encryption key creation

The encryption key is generated from the current link key, a 96-bit Ciphering Offset Number (COF) and a 128-bit random number. The COF is based on the Authenticated

Ciphering Offset (ACO), which is generated during the authentication process[4]. When the Link Manager (LM) activates the encryption, the encryption key is generated. It is automatically changed every time the Bluetooth device enters the encryption mode.

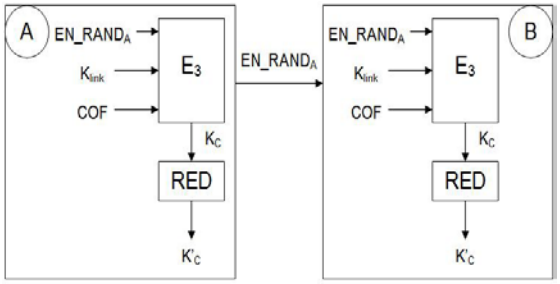

Figure 5: Encryption key creation

3. SECURITY VULNERABILITIES IN BLUETOOTH TECHNOLOGY

There are many security weaknesses in the Bluetooth Technology. Some of these are practical and some are theoretical. We have given overview of some problems.

3.1 Low credibility of PIN

Bluetooth technology uses non-standard 4-digit PIN code and another variable to generate the link key and encryption key. Actually, 4-digit PIN code is the only variable which is the real key generated, resulting only one key (a random number) transport in the air.

3.2 High probability of non-link key cheat

Along with the use of the link key takes new problems. Authentication and encryption set up on the basis of the link key. All the other Information used in this connection usually is public.

3.3 Address Spoofing

Every Bluetooth device has a unique Bluetooth device address. However, its uniqueness raises new problems. Once the ID links with a certain fixed person, this person can be tracked and their activities can easily be recorded. In this case, the individual's privacy will be violated.

3.4 The weakness of E0 stream cipher algorithm

The main weakness of stream cipher algorithm is that if a pseudo-random sequence make an error, it will make the whole cipher text mistake happen, it also bring about the cipher text cannot restore back to plaintext in decipherment.

3.5 Denial of service attack

Bluetooth networks are vulnerable to denial of service attacks. They consist of mobile devices and these devices are often battery fed. Bluetooth is no exception. An attacker can send dummy messages to a mobile device. When this device receives a message (a real of a fake one), it consumes some computation (and battery) power. After some time, all battery power will be consumed and the device won't be available anymore. This exhaustion of the battery power is called the sleep deprivation attack. There are a lot more denial of service attacks.

3.6 Bluesnarf

It is possible, that some of Bluetooth enabled devices connect to the devices without knowing the authenticated user and they gain access to restricted portion ,including the entire phonebook (and any image or other data associated with the entries), this is only possible if the device is in discoverable mode[5].

4. CONCLUSION

In this paper we have emphasized on protocols used in Bluetooth communication in terms of key exchange protocols. This is the most critical part of Bluetooth transmission because it is very important that before transmission of data, security capabilities are established properly. Disappointingly, there are many security flaws present in this type of transmission. Some of them we have discussed in this paper.

5. FUTURE WORK

Whenever Bluetooth is used for secure transmission of data in any application where confidentiality is the major concern, added cryptographic techniques should be used to achieve the high security. In existing Bluetooth system, attacker can easily hack the key through Man- in-middle attack and the brute force attack is not prevented. Some researchers proposed a system with additional cryptographic algorithm like single DES and RSA. The size of key used in DES is 56-bit only that is

more vulnerable to brute force attack and the problem of key distribution is also present in their system. After lots of research on this ground and find that there is no any system that gives confidentiality, authentication and integrity check all together. So we want to propose a system that enhances the security system of existing Bluetooth communication.

REFERENCES

[1] *C. Enrique Ortiz*, *December 2004* Using the Java APIs for Bluetooth Wireless Technology, Part 1 - API Overview

[2] Jeffrey B. Hall, Brush up on Bluetooth, SANS Institute Reading Room site.

[3] Dave Singel´ee, Bart Preneel, Security Overview of Bluetooth, COSIC Internal Report, June, 2004

[4] Paraskevas Kitsos, Nicolas Sklavos,Kyriakos Papadomanolakis, and Odysseas Koufopavlou, Hardware Implementation of Bluetooth Security,*University of Patras, Greece*

[5] Trishna Panse,Vivek Kapoor, A Review paper on Architechture and Security system of Bluetooth Transmission, Department of Information Technology, Institute of Engineering & Technology, DAVV Indore, India,2012