DEFENCE AGAINST MAN IN MIDDLE ATTACK IN SECURE SIMPLE PAIRING

Nishant Mishra and Vishal. Gupta

1Research scholar, Dept. of computer, Ambedkar Institute of Advanced Communication Technologies & Research, New Delhi, India
mishnmishant@gmail.com

2Assistant professor ,Dept. of computer science, Ambedkar Institute of Advanced Communication Technologies & Research, New Delhi, India
vishalg26@rediffmail.com

Abstract- Secure simple pairing has been adopted by Bluetooth version “Bluetooth 2.1+EDR (ENHANCED DATA RATE). It should be noted that for establishing Bluetooth connection that uses Diffie hellman public cryptography in its communication, SSP is a secure method. But it is still prone to attack regardless of the high security mechanism it provides, for example man in middle attack. In this paper we provide a efficient method to prevent man in the middle attack.

Keywords- MITM, Bluetooth Security, Privacy, SSP, Authentication, Encryption.

INTRODUCTION

For real-time voice exchange and short range wireless data transmission in billion of devices and consumer electronics, Bluetooth is an affordable wireless class technology. It function in the license free 2.4-2.835 GHz frequency band, which corresponds to the Industrial, Scientific and medical band by utilizing frequency hopping spread spectrum[1]. A piconet is formed by the Bluetooth devices that communicate with each other. The device that begins a connection is known as piconet master. There could be a maximum of seven active slave devices and one master device in one piconet [2]. A Bluetooth personal area network (PAN) is formed by a piconet master and piconet slave. As in other technologies, Bluetooth technology also faces different type of problem from attackers who are attempt to trespass data transmission by various means. Secure simple pairing process is a dependable method for demonstrating the Bluetooth linking by using Diffie-Hellman Public key cryptography in its intercommunication In place of employing a CA, Bluetooth standard chose a secure simple pairing. During recent days man in middle attack start taking place in simple secure pairing. In this attack attacker control the communication between devices. Devices think that they are communicating to each other but their communication is controlled by attacker. In this paper we will provide some background information about simple secure pairing, man in the middle attack. We will also describe previously provided solution to defend from man in the middle attack.

The remainder of the paper is organized as follows. Section II contains overview of simple secure pairing in Bluetooth section III tells man in middle attack in simple secure pairing. Section IV tells various previously proposed solutions for preventing MITM in simple secure pairing. section V contain proposed solution to prevent man in middle attack. section VI give security analysis of paper.

SIMPLE SECURE PAIRING

Before any Bluetooth device start transmitting, pairing must be done. As a result of this two devices would form a trusted pair and a link key is constituted. There are four association models that are utilized in SSP. Selecting an association model reckons on the device potentialities. The first one is Numeric comparison where both devices have the capability to exhibit six digit and enter “yes” or “no”. The second one is just works which is utilized when at least one device has exhibiting abilities but no keyboard for figuring six digit. Out of band is third association model that is utilized for scenarios using OOB mechanism for both detecting the devices and replacing the cryptographic number utilized in the pairing method. Passkey entry model is used when out of two devices one has no input capability only display capabilities and other has only input capability [1].

Steps of ssp:

a. Capabilities Exchange: During this stage devices interchange their Input/output capabilities to find out the best association model used. This phase happens when the devices had never encountered earlier or when they want to reperform the pairing process for the same reason.

b. Public key exchange: During this stage public private key is exchanged with each other. Diffie Hillman key is also calculated which is used in calculation of link key.

c. Authentication Stage I: This stage taget to render protection versus MITM attacks. It is accomplished by exchanging commitment to the nonces, set of nonces and the exchanged public key to check their integrity.
d. **Authentication Stage 2:** This phase is same in all association models. It affirms that aubic key exchanged took successfully.

e. **Link Key Calculation:** Once pairing is affirmed by both devices, the link key is computed using their Bluetooth address, nonce value and diffie hellman key.

f. **Link Manager Protocol Authenticaion And Encryption:** This is the last phase in the ss where the encryption are brought forth. It is similar to one utilized in legacy. [1]

**MAN IN MIDDLE ATTACK IN SSP**

In the man in middle attack an attacker try to establish connection with both devices and communication will be controlled by attacker. user think that they are communicating with each other but their communication is controlled by an attacker which control the entire communication. Simple secure pairing was unable to prevent man in middle attack completely. Input output capabilities is exchanged over unauthenticated channel. Attacker can modify the capability information which can made a compulsion for user to use a less secure association model such as just work model in which there is no authentication. Just work model provide no protection against man in middle attack [3,4].

Suppose Alice wishes to communicate with Bob. Meanwhile, Mallory wishes to intercept the conversation to eavesdrop and possibly deliver a false message to Bob. First, Alice asks Bob for his public key. If Bob sends his public key to Alice, but Mallory is able to intercept it, a man-in-the-middle attack can begin. Mallory sends a forged message to Alice that claims to be from Bob, but instead includes Mallory’s public key.

Alice, believing this public key to be Bob’s, encrypts her message with Mallory’s key and sends the enciphered message back to Bob. Mallory again intercepts, deciphers the message using her private key, possibly alters it if she wants, and re-enciphers it using the public key Bob originally sent to Alice. When Bob receives the newly enciphered message, he believes it came from Alice. In this way mitm attack took place.

MITM attacks place an attacking device between two connected devices to act as a relay (the attacker uses obfuscation to hide the attacking device). Previously paired devices send their information to the attacking device, which then relays MITM Attacks it to its intended destination. The threats under MITM attacks are BT-SSP-Printer-MITM, BlueSpoof and bthidproxy.

**BT-SSP-Printer-MITM:**

The BT-SSP-Printer-MITM attack shows possible vulnerabilities in the newer Bluetooth standards. This attack focuses on the JW connection option in four association models of SSP, which lets devices pair without authentication. The BT-SSP-Printer-MITM attack sets the attacker’s device as a relay point between the user’s device and a printer. When the user device connects to the printer using the JW method, the attacker breaks the connection by using some form of DoS.[2]

**Bluespoof:**

By BlueSpoof tool, The attacker can act as another Bluetooth device by using its BT address.

**Bthidproxy**

Bthidproxy is yet another handy piece of software. Using it MITM attack can be possible on Bluetooth connections by using two dongles and spoofing the host and device addresses. Because of virtual cabling, a one to one connection is made between device and host. This means that almost all attacks must be performed when either the device or host are allowing anyone to take their place [3].

In Bluetooth versions up to 2.0+EDR, pairing is based exclusively on the fact that both devices share the same Personal Identification Number (PIN) or passkey. As the PINs often contain only four decimal digits, the strength of the resulting keys is not enough for protection against passive eavesdropping on communication. It has been shown that Man-in-the-Middle attack (MITM) attacks on Bluetooth communications (versions up to 2.0+EDR) can be performed. Bluetooth versions 2.1+EDR (Enhanced Data Rate) and 3.0+HS (High Speed) add a new specification for the pairing procedure, namely Secure Simple Pairing (SSP). Its main goal is to improve the security of pairing by providing protection against passive eavesdropping and MITM attacks. Instead of using (often short) passkeys as the only source of entropy for building the link keys, SSP employs EllipticCurve Diffie-Hellman public-key cryptography. To construct the link key, devices use public-private key pairs, a number of nonces, and Bluetooth addresses of the devices. But attacker make advantage of the first phase of SSP where input/output capability is exchanged on unauthenticated channel [4]

**MITM ATTACK TAKE PLACE AS SHOWN IN figure:**

Various notation are as follows:

- PKx: Public key for device X
- Skx: Private key for device X
- DHKey: Diffie-hellman key of device
- Nx: Nonce created by device x
- Rx: Random number created by device X;
  - Equal to zero in numeric comparison model
- Cx: Commitment value given by device X
- f 1: one way function to find commitment value
- f 2: one way function to find out the link key
- g: one way function used to calculate numeric check value
- IOcapx: input/output capabilities for device
- BD_ADDR: 48 bit Bluetooth address
PREVIOUSLY PROPOSED SOLUTION FOR DEFENCE AGAINST MITM

Haataja and Hypponen suggested contributing an extra message to the SSP to be used when Just works association model is utilized. This message says “The second device has no display and keyboard! Is this true?”, then the user may prefer either to “Proceed” or “Stop”. The problem of such proposal is when a hacker tries to mislead the user that the devices he/she is transmitting with has not any 10 abilities although it may have, if that device is far away may be the user will consent the connection.[6]

It is also suggested to utilize OOB as a mandatory affiliation model. The trouble in such proposal is that in OOB, the devices need to be near each other every time they require to communicate and initiate the SSP six phases. Moreover, the devices should have special abilities to back up OOB links which make it restricted in its use. Finally, OOB does not back up a user that triggered a connection using Bluetooth technology and would like to apply OOB for validation during a connection [4,8].

PROPOSED SOLUTION

As we had seen attacker intercept public key in simple secure pairing we try to protect public key with the help of newly added step before ssp

a. We encrypt the public key of each device with the help of known cryptographic function which is known to each user in advance
b. Transfer the public key of one device to other and vice versa. This public key is decrypted with known cryptographic function
c. In this way each device will have public key of each other

Now initiate simple secure pairing. If an attacker will try to change its public key during public key exchange then user can check their database whether there is change in the public key or not. In this way we can easily prevent man in middle attack.
Now the steps of pairing are as follows:
Suppose there are two device A & B.

a. Encrypt the public key of A device with the help of known cryptographic function
b. Transfer the public key of A device to B. This public key is decrypted with known cryptographic function
c. This public key is stored in the database of B device
d. Encrypt the public key of B device with the help of known cryptographic function
e. Transfer the public key of B device to A. This public key is decrypted with known cryptographic function
f. This public key is stored in the database of A device.

Now initiate the simple secure pairing as follows[3,4]

g. Capabilities exchange: Devices that have never met before or want to perform repairing for some reason, first exchange their IO (Input /Output) capabilities to determine the proper association model to be used. Attacker make advantage of this phase as no authentication is performed during this stage

h. Public key exchange: The devices generate their public-private key pairs and send the public keys to each other. They also compute the Diffie-Hellman key.

i. Authentication stage 1: The protocol that is run at this stage depends on the association model. One of the goals of this stage is to ensure that there is no MITM attack. It is achieved by exchanging set of nonces, commitments to the nonces and the exchanged public keys to check their integrity.

j. Authentication stage 2: This phase is the same in all association models. It confirms that the public keys exchange ended successfully.

k. Link key calculation: Once pairing is affirmed by both devices, the link key is computed using their Bluetooth address, nonce value and diffie hellman key

l. Link manager protocol authentication and encryption: This is the last phase in the ssp where the encryption key are generated

**SECURITY ANALYSIS OF PROPOSED STEP:**

Attacker insert his own public key during the exchange of public key phase. When they insert their own public key they can easily calculate the link key which is used for pairing. In our proposed solution we had stored the public key before the simple secure pairing initiate. In this way each device has got the public key of each other device in advance before ssp initiates. If an attacker try to change the public key during the public key exchange then device can check his database to compare the value of public key stored and public key received if the value matches then we can say there is no attack if the value did not match then terminate the connection as there is possibility of mitm attack

**REFERENCES**


