Preventing mitm attack in secure simple pairing in Bluetooth

[1]Nishant Mishra
[1]Vishal. Gupta

[2] Naina Mittal

[1]Ambedkar Institute of Advanced Communication Technologies & Research, New Delhi, India

[2] C-DAC NOIDA

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.

Key Words- *MITM , Bluetooth Security, Privacy, SSP, Authentication, Encryption.*

I. INTRODUCTION

- Bluetooth is a short range wireless communication technology developed to use for home, office and mobile Personal Area Networks [3]. Today, Bluetooth is successfully integrated into mobile phones, Personal Digital Assistants (PDAs) and other consumer devices to communicate them. Bluetooth technology was invented in
- 1994 by Ericson but version 1.0 of Bluetooth came out in1999. Today, more than one billion Bluetooth devices are used by the consumers all over the world. Some key benefits of Bluetooth technology are :(1)Cable replacement. Bluetooth technology replaces a variety of cables, such as those traditionally used for peripheraldevices (e.g.,mouseandkeyboard connections), printers, and wireless headsets and ear buds that interface with personal computers (PC) or mobile telephones.(2)Ease of file sharing.: A Bluetooth-enabled device can form a piconet to support file sharing capabilities with other Bluetooth devices, such as laptops.(3)Wirelesssynchronization:.Bluetooth provides automatic synchronization between Bluetooth-enabled devices. Forexample, Bluetooth allows synchronization of contact information contained in electronic address books and calendars[4] 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 conclude the paper

II. SECURE SIMPLE 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 uitilized 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[1,2,6]

STEPS OF SSP:

(1)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 some reason
(2)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
(3) AUTHENTICATION STAGE 1: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.
(4) AUTHENTICATION STAGE 2: This phase is same in all association models. It affirms that ublic key exchanged took successfully.
(5) 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.
(6) LINK MANAGER PROTOCOL AUTHENTICAION AND ENCRYPTION: This is the last phase in the ssp where the encryption are brought forth.It is similar to one utilized in legacy.

III.MAN IN THE MIDDLE ATTACK IN SSP

In the man in the 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. Secure simple 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[7].

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 publickey. 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, BlueSpooof and bthidproxy.[6,7]

(a) 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. TheBT-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.

(b) BLUESPOOF: By BlueSpooof tool, The attacker can act as another Bluetooth device by using its BT

address .

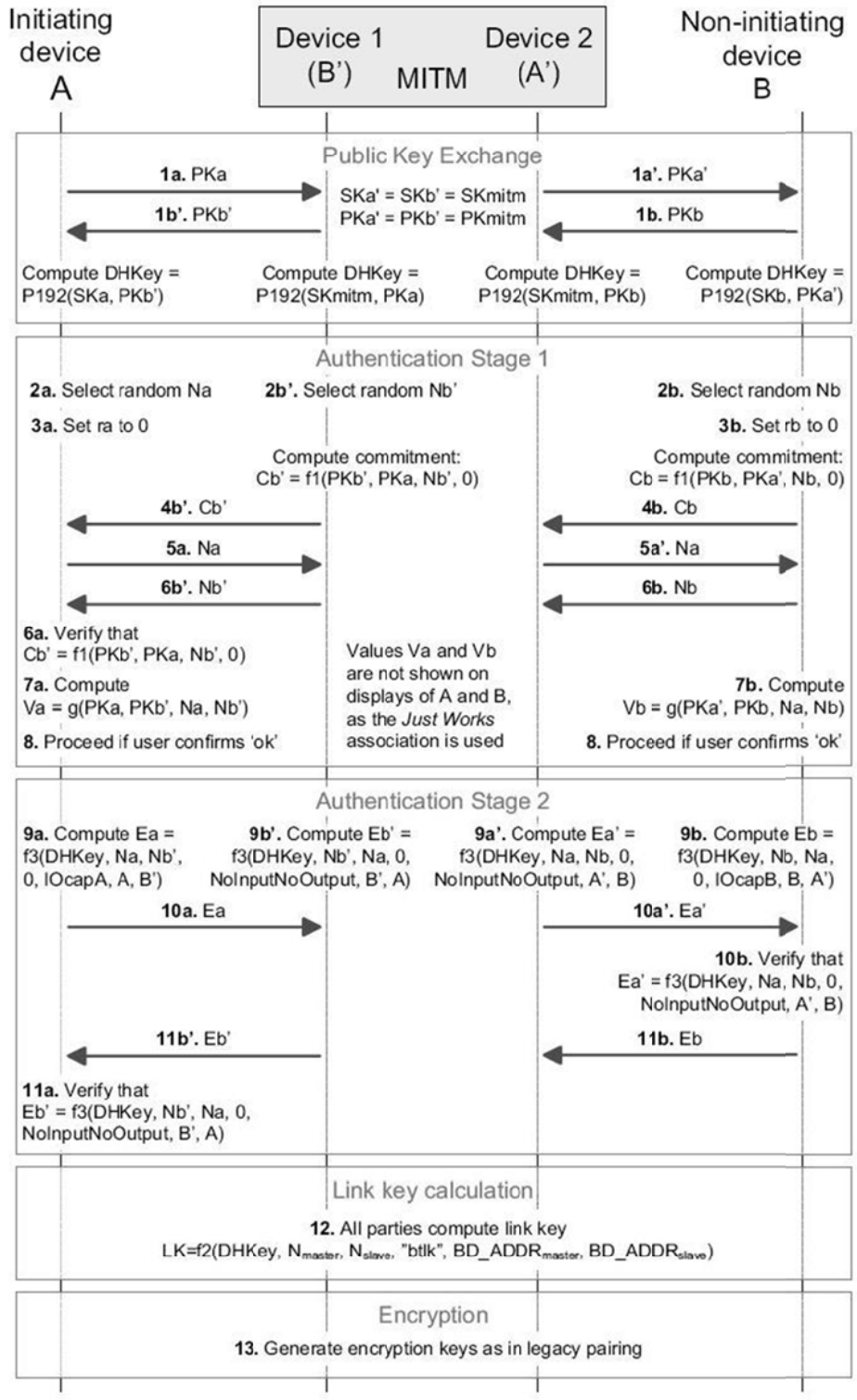
(C) Bthidproxy

Bthidproxy is yet another handy piece of software. Using it MITM attack canbe 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 performedwhen either the device or host are allowing anyone to take their place.

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)[2,5] .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 Elliptic Curve Diffiee-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 over unauthenticated channel

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



IV.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 to "Stop". The problem of such proposal is when a hacker tries to

mislead the user that the devices he/he 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[2].

It is also suggested to utilize OOB as amandatory 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 userthat triggered a connection using Bluetooth technology and would like to apply OOB for validation during a connection.[6,7]

V.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 :
Attacker insert his own public key during the phase of public key exchange and later on he become successful to find out the link key which is used for checking the authentication. On successfully getting the link key a user can simply access the device of victim without any difficulty. For the verification of the user commitment value is encrypted with the function which is known to both user in the advance. With the help of that function we can calculate key which is used for encrypting the commitment value

Take a example suppose difffie hellman key with the help of P192(Skx,Pkx) is 5 and the function is $f(x)=x^3+x+21$..then with the help of this value of function is 151This value 151 is used to encrypt the commitment value .Other device will decrypt this value before verification .An attacker will not be able to decrypt the value because he does not know the function. Now the step of authentication stage 1 will be modificated:
After the calculation of commitment value (in step IV of authentication stage 1)it is encrypted with the help of the function which is known to both user in advance. this encrypted value is send to other user. Attacker won't be able to decrypt it because he don't had any idea about function.If attacker will send its own commitment value then user can easily detect because attacker don't know the value of cryptographic function

VI.CONCLUSION

IN this paper we had presented an efficient way to defend against man in middle attack. Man in middle attack is taking to a great extent in today world. we had proposed a new step in simple secure pairing .With the help of this technique we can easily defend man in middle attack since attacker won't be able to intercept cryptographic function in this way we can easily defend man in middle attack

REFERNCES

[1] K. Haataja and P. Toivanen. Two practical man-in-the-middle attacks on bluetooth secure simple pairing and countermeasures. Wireless Communications, IEEE Transactions on, 9(1):384{392, Jan. 2010.
[2] Kugler and Dennis. man in the middle attacks" on Bluetooth . In Financial Cryptography, volume 2742 of Lecture Notes in Computer Science, pages 149-161. Springer Berlin / Heidelberg, 2003.
[3] Scarfone, K. and J. Padgette, 2008. Guide toBluetooth Security, Technical Report Special Publication SP 800-121, National InstituteofStandards and Technology (NIST).
[4] Bluetooth Special Interest Group-"Simple PairingWhitepaper";http://www.bluetooth.com/NR/rdonlyres/0A0B3F36-D15F-4470-85A6F2CCFA26F70F/0/SimplePairing_WP_V10r00.pdf
[5] E. Ferro and F. Potorti. Bluetooth and Wi-Fi Wireless Protocols: A Survey and A Comparison. IEEE Wireless Communications, 12(1):12–26, Feb. 2005.
[6] K. Haataja and K. Hypponen. Man-In-The-Middle attacks on Bluetooth: A Comparative Analysis, A Novel Attack, and Countermeasures. In 3rd International Symposium on Communications, ControlandSignal Processing,ISCCSP'08, pages 1096–1102, March 2008.
[7] K. Haataja and P. Toivanen. Practical Man-in-the-Middle Attacks Against Bluetooth Secure Simple Pairing. In 4th International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM'08, pages 1–5, Oct. 2008.