International Journal of Electronics, Electrical and Computational System
IJEECS
ISSN 2348-117X
Volume 6, Issue 7
July 2017

Academic Science

eSSP : Bluetooth Security Value Addition

Sumesh Raman
Adi Shankara Institute of Engineering and Technology
Murali Parameswaran
Adi Shankara Institute of Engineering and Technology

ABSTRACT

The importance of secure data transfer in Bluetooth is growing with the rapid development of short range wireless communication devices that use Bluetooth as the primary option for communication. The proliferation of the Bluetooth devices in the workplace exposes organizations to security risks. Bluetooth technology is sensitive to wireless networking threats like Man-In-The-Middle Attack(MITM),eavesdropping. The security issues inherent in Bluetooth are mainly due to the process of pairing one device to another. All severe attacks are carried out in between the Bluetooth pairing procedure. The use of Public key exchange in Secure Simple Paring(SSP) is a generic cause that leads to Man in the Middle attacks. This paper proposes enhanced Secure Simple Pairing(eSSP) that reinforce SSP so that it could effectively restrict MITM attacks. eSSP applies a new key agreement protocol on top of the Public Key exchange phase of SSP, that uses Crypto-Credentials provided by a Bluetooth Cryptographic Service Provider.

Keywords

Bluetooth Security, Secure Simple Pairing, Bluetooth Cryptographic Service Provider, Man In The Middle Attack

1. INTRODUCTION

Security has become a major concern in the usage of Bluetooth for short range wireless communication. Bluetooth runs in a Wireless Personal Area Network(WPAN). Bluetooth Cryptographic Service Provider(CSP) is own by WPAN Administrator and shall be deployed in all the devices[1]. ForBluetooth Core Specification up to 2.0+Enhanced Data Rate(EDR), pairing is performed exclusively by both devices sharing the same Personal Identification Number (PIN) or Passkey. Authentication is done at Link level and therefore it is called Link Level pairing or Legacy pairing. From Core Specification 2.1+EDR onwards, a service level pairing; Secure Simple Pairing (SSP) has been introduced as the default pairing mechanism. SSP is designed to secure the pairing procedure by adopting suitable Cryptographic algorithms and multiple protocol handshakes that provide protection against Man In The Middle Attack(MITM) and passive eavesdropping. However, SSP could not conclusively protect against MITM as certain modes Pass Key entry, Numerical Comparison and Just Works are unguarded to MITM attacks.

In this work we are modifying SSP mechanism by introducing a new Key agreement protocol. Enhanced SSP (eSSP) targets effectively safeguarding Bluetooth devices from MITM attacks in closed environment like in WPAN.

The rest of the paper is organized as follows. Section 2 briefly introduces SSP. Related work is described in Section 3. eSSp, along with motivation assumption and other details are provided in Section 4. eSSp specific HCI Commands and other protocol specific Events are described in Section 5. Section 6 lists result and analysis, and Section 7 concludes the paper.

2. SECURE SIMPLE PAIRING - SSP

Bluetooth versions 2.1+EDR (Enhanced Data Rate) has adopted a new protocol for the pairing procedure, namely Secure Simple Pairing (SSP)[2]. It endorse Elliptic Curve Diffie-Hellman (ECDH) Public Key Cryptography as the source of entropy for building link key instead of short pass key. The Link key is constructed using Public-Private key pairs, Bluetooth addresses of the devices and a number of nonces. Passive eavesdropping is effectively countered by running an exhaustive search on a Private key with approximately 95 bits of entropy which is currently considered to be in-feasible in short time [12]. For protecting MITM attacks, SSP uses an Out-Of-Band (OOB) channel [3] that used NFC handover mechanism. SSP introduces the concept of IO Capabilities. The protocol takes in account of the devices' Input and Output Capabilities and choose the Pairing Model based on these Capabilities.

3. RELATED WORKS

Ever since the roll out of SSP (Secure Simple Pairing), there have been a lot of studies published focusing on how to improve SSP security. MO Kui et al, [4] and Peter Dell et al, [5] made few statistical analysis and come up with certain findings and generic suggestions to resist Bluetooth vulnerabilities. CM Fan et al[6], Guang Liang et al[7], Priyanka et al[8] Md. Ariful Alam et al [9] suggested additional Cryptographic methods on top of SSP to strengthen security. However, these researches has not addressed the issue of insecure Public Key Exchange of SSP. Bandyopadhyay et al[10], M. Othman et al[11] have tried to attain MITM protection by maintaining an exhaustive Database of different parameters pertaining to remote devices. Kumar et al[12] proposed a mechanism to detect MITM adopting a tamper detection mechanism by means of a device called BlipTrack Bluetooth Detector (BBD). Pasanen et al [13] suggested a novel mechanism to enhance Secure Simple Pairing exploiting the concept of RF-Fingerprints and keeping them in a Database.

4. ENHANCED SSP - eSSP

The analysis of related works reveal that MITM can only be protected by securing Public Key Exchange. eSSP recommend to encrypt the Public Key of each device using known Cryptographic function along with Trusting the Key with a Certificate. That is, essentially there must be Certification Authority to verify if the key belongs to a device is a trusted one. eSSP proposes a new concept of Bluetooth Cryptographic Service Provider (CSP) as the Certification Authority.

Though there is a master in the Piconet, due to the dynamic nature of wireless radio and short demographic range, the topology often works in an Ad-hoc manner, for instance, Wireless Personal Area Network (WPAN). A typical WPAN environment consist of a WPAN Admin Center and a list of WAN capable devices those are connected to an Intranet/Internet via WiFi hub or any other means. The fundamental and necessary requirement that attributes eSSP to enforced shall be on a WPAN network.

4.1 MOTIVATION

During Public key exchange phase of SSP, the two pairing devices generates its own ECDH Public-Private key pair, exchange Public key and calculate DHKey on both devices. The public key and the DHKey will be used in all the later phases, so the security vulnerabilities in this phase may threaten all the later phases. Generally the attacker targets the public Key exchange and captures the Public key by intervening between the two communicating devices to proceed for MITM. The motivation is to propose a solution eSSP (enhanced SSP), that effectively restricts MITM attacks by securing Public Key Exchange of SSP.

4.2. ASSUMPTIONS

eSSP shall assume below requirements.

- Targeting Wireless Personal Area Network (WPAN).
- WPAN should have a WPAN Admin .
- Applicable only to Bluetooth enabled WAN Devices.

Bluetooth devices should be WAN capable that WPAN Admin can connect and communicate over a secure link, preferably WiFi.

4.3. CRYPTOGRAPHIC SERVICE PROVIDER - CSP

Bluetooth CSP is a software entity having two role as CSP Source and CSP Sink. The Source role shall be running in WPAN Admin center and the Sink role shall be deployed in all the Bluetooth devices in WAPN. The Source Role at Admin center shall define the Certificates (Crypto-credentials) for WPAN devices that need security. The Certificates shall be sent to Bluetooth WAN devices and they cache Certificates in a Database, namely CSP Database. Instead of defining a device address based Certificate, eSSP shall be defining a Certificate based on three parameters,

1. Bluetooth Friendly Name
2. Bluetooth UAP - Upper Address Part.
3. Bluetooth CoD – Class of Device

Therefore, Bluetooth CSP database shall have four fields < Device Name, Class of Device, UAP, Certificate> corresponding to a remote device or series of remote devices. The Device Name shall be the mandatory field. The Certificate will be retrieved in a Database query, if the Name field, and either one of CoD or UAP matches to that of remote pairing device. This approach is smart enough to avoid probable overhead of maintaining huge database for database updates and refresh calls from WPAN Admin. All the Database management APIs can be implemented by either CSP or Host as per the design call. A diagrammatic representation of Bluetooth WPAN that eSSP can be practiced is given in below Figure 1.

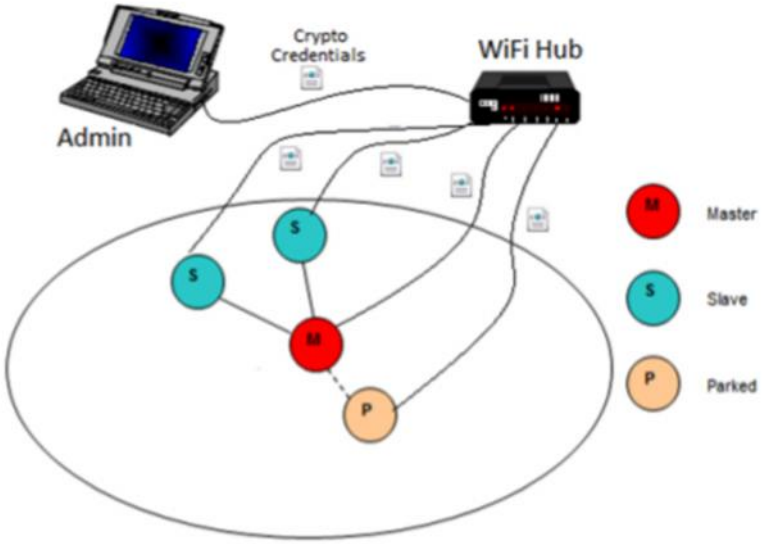

Figure 1: eSSP -Static View

4.4. eSSP SYSTEM MODEL

Secure Simple Pairing (SSP) is a 6 -Step process implemented in LMP layer of Host Controller. eSSP introduced one more step to SSP, entitled as 'Public Key Encryption' that encipher Diffie- Helman Public Key before exchanging public key with remote device. Step 2 of 7 is enhanced by eSSP and all other steps belongs to SSP. The Step by step process of eSSP is given below

1. IO Capability Exchange: defines the devices regarding their input and output capabilities, for instance ‘DisplayYesNo’, ‘NoInputNoOutput’, ‘Display Only’ and ‘KeybpardOnly”

2. Public Key Encryption: specific to eSSP, in this Step, we perform the follow ing operations in LMP Layer of Host Controller.

• GetSecurity Mode: The mode can be either SSP or eSSP

• Crypto-Credentials Request to Host: if eSSP is set, Certificate request is indicated with incoming device address to to Host stack.

• Reply/Neg Reply of Crypto-Credentials from Host: Host will run Database query and if Certificate is queried, inform Controller with HCI Command else send Negative reply command.

• Extract Random values from Credentials: parse the certificate to get the inputs to Key Agreement Protocol

• RSA Algorithm use Random values to encrypt Public Key: This paper recommend RSA encryption for Key Agreement Protocol and Pub lic key is encrypted using RSA algorithm.

3. Encrypted Public Key Exchange: Public key is exchanged over air.

4. Authentication Phase 1: This protocol is determined based on the mode of SSP.

5. Authentication Phase 2: Exchange of values (Keys and random numbers) have been completed

6. Link Key Generation: Link key is computed at both end and indicated Host stack with Link key notification event.

7. Link Management Protocol Authentication and Encryption: Encryption keys are calculated.

In Step 2 of 7, eSSP shall read its enable status set in LMP and if eSSP Mode is not set, default SSP shall be used for pairing. eSSP shall use a newly defined HCI Event to request Crypto-Credentials from Bluetooth Host, and the host shall reply using newly defined HCI Commands. The Credentials will be processed to extract the Random inputs that shall be given as inputs to enciphering algorithm. Any suitable ciphering algorithm can be adopted and published for encrypting Public Key. However this paper recommend RSA algorithm with two Random number for eSSP.

5. eSSP SPECIFIC HCI COMMANDS AND EVENTS

HCI Interface has to be enhanced with new eSSP specific HCI Commands, HCI Event and HCI Error codes (Status Parameters).

Proposed Command shall be included in Link Controller Command group and the Op-Code Group Code (OGF) will be 0x01, and adopt the same packet format from Bluetooth standard. The Commands shall be acknowledged by HCI Command Status Event with different event code in which success shall be always noted as 0x0000 of size 2 octet.

- HCI Commands

1. HCI_Set_eSSP_Authentication: Command shall Set the eSSP Mode of Security at LMP layer. The parameters shall be of Size 2 Octet with below defined values. 0x0000 - Enable eSSP and 0x0001 - Disable eSSP
2. HCI_ eSSP_Certificate_Reply: Command shall be used to notify LMP with the Crypto-Credentials (Certificates) stored in database corresponding to remote Bluetooth device name, CoD, and UAP. The parameters shall be defined as Remote_address of Size 6 Octet and Certificate of Size 16 Octet.
3. HCI_eSSP_Certificate_Negative_Reply: This command shall be used to notify LMP that a valid Crypto-Credentials (Certificates) does not exist in database and eventually the pairing shall be rejected. The Parameters shall be remote_address of Size 6 Octet

- HCI Events

1. HCI_eSSP_Certificate_Request_Event: LMP will trigger this Event to fetch the Certificate corresponding to the Bluetooth device address of incoming pairing request. The Parameters shall be remote_address of Size 6 Octet.

Description: This Event shall be propagated to the Host and host will reply with HCI_ eSSP_Certificate_Reply or a HCI_eSSP_Certificate_Negative_Reply Command.

6. RESULT

Bluez-5.44 Simulator has been used to verify eSSP. We have implemented eSSP Public Key Encryption on top of Emulator LMP component and tested over emulator. In addition, the Bluez host module has been enhanced with new HCI Commands, Events and their handler routines. The CSP Crypto-Credentials were generated in Emulator module and the DH Public Key is encrypted using this Credentials. The emulators at each peer were able to decipher the Exchanged Public Key and successfully executed pairing.

Table 1. eSSP Results

Scheme	MITM Attacks	Eavesdropping Attacks
BT White-paper	No	Yes
[7] [8] [10]	No	Yes
eSSP	Yes	Yes

7. CONCLUSION

In this paper we bring forth the concept of Cryptographic Service provider, which is a kind of Certification authority issues Credentials to the proposed Key Agreement protocol. eSSP is specifically targeted to WPAN Networks, where a WPAN Admin, and CSP Module are the mandatory requirements. Therefore, we propose this as an additional Security option to effectively protect against MITM attacks. From users perspective, eSSP shall be a configurable feature that can be enabled or disabled by CSP kind of Application or from a Host application.

REFERENCES

[1] A S Diallo A Wajddi and F Sado. Secure Autehntication Scheme for Bluetooth Connection. IEEE International Conference on Computer and Communication Engineering, 2014.

[2] Christian Gehrmann. Bluetooth Security White Paper. Bluetooth SIG Security Expert Group, 2002. Simple Pairing White Paper. 2006-08-03.

[3] MO Kui and Cuo Xiuying. Research in Bluetooth security Manager . IEEE Int. Conf. Neural Networks and Signal Processing, 2003.

[4] Peter Dell and Khwaja Shan ul Hasan Ghori. A Simple Way to Improve the Security of Bluetooth Devices. International Symposium on Applications and the Internet, 2008.

[5] CM Fan S Sheih and BH LI. Security of password based pairing protocol in bluetooth. Network Operations and Management symposium-APNOMS, 2011.

[6] Guangliang Xu and Bin Yu. Security Enhanced Design of the Bluetooth Simple PairingProtocol. IEEE International Conference on Computer Science and Network Technology, 2008.

[7] Sharon Priyanka S and B Nagajayanthi. Enhancing Security In Bluetooth Networks. IEEE Personal Communication, 2013.

[8] Md Ariful Alam and Mohammad Ibrahim Khan. Security Enhancement of Pairing and Authentication Process of Bluetooth. IJCSNS International Journal of Computer Science and Network Security, 2010.

[9] Subhansu Bandyopadhyay and Anirban Majumdar. A Proposal for Improvement in Service-Level Security Architecture of Bluetooth. IEEE International Conference, 2008.

[10] M Othman W H Hassan, AH, and Abdalla Kulliyyah. Developing A Secure Mechanism for Bluetooth-based Wireless Personal Area Networks(WPANs). IEEE Personal Communication, 2007.

[11] Monu Kumar and B K Gupta. Security for Bluetooth enabled devices using BlipTrack Bluetooth Detector. International Conference on Advances in Computer Engineering and Applications (ICACEA), 2015.

[12] Sanna Pasanen Keijo Haataja Niina Päivinen and Pekka Toivanen. New Efficient RF Fingerprint-Based Security Solution for Bluetooth Secure Simple Pairing. Proceedings of the 43rd Hawaii International Conference on System Sciences, 2010.