Advanced Science and Technology Letters
Vol.28 (CIA 2013), pp.94-98
http://dx.doi.org/10.14257/astl.2013.28.18

Improved NC association security model based on Bluetooth 4.0

DaeHee Seo[1], DoHyueng Kim[1], ByungGil Lee[1], JangMi Baek[2]

[1] Electronics and Telecommunications Research Institute,
[2] SoonChunHyang University
{dhseo, dhkim516, bglee}@etri.re.kr
Bjm1453@sch.ac.kr

Abstract. In this paper, the potential security weaknesses in the process of Secure Simple Pairing which is introduced by Bluetooth 4.0 are analyzed, and an improved method of Secure Simple Pairing is proposed to compensate the security concerns.

Keywords: Bluetooth 4.0, NC association, Simple Pairing, Mutual Authentication.

1 Introduction

In this study, a reliable security protocol is proposed to compensate the vulnerabilities of the existing short-range wireless communications. When hierarchical piconets are formed on the basis of the proposed security protocol, a secure communication method is proposed for the devices in a variety of situations to offer more enhanced security services.

For this purpose, In Section 2, the existing Bluetooth scheme vulnerabilities are analyzed. In Section 3, an enhanced security model using SSP in Bluetooth v4.0 is proposed to provide protection against the BT-Nino-MITM attacks. Finally, conclusions are drawn in Section 4.

2 Technology Overview

2.1 Novel MITM attack

Keijo et al., proposed a novel Man-In-The-Middle (MITM) attack, known as a BT-SSP-Printer-MITM attack, based on Bluetooth 4.0 in 2008. In the Novel MITM attack, a MITM attack is made against Bluetooth-enabled USB printers that support Secure Simple Pairing (SSP) [1][5]. In the proposed scenario, a MITM attacker disrupts the PHY by hopping along with a piconet device and sending random data at the physical

ISSN: 2287-1233 ASTL

layer (PHY) in the 2.4 GHz band to make the device difficult to initiate a new connection with another Bluetooth device. As a result, the frustrated user thinks that something is wrong with the user device and then deletes link keys previously stored in the user Bluetooth device[3]. In particular, a Novel MITM attacker replaces the BD_ADDR of a user legitimate device with the different BD_ADDR of the MITM device by using the same 1-248 byte user-friendly string when the BD_ADDR is verified in the paring process of Bluetooth SSP. As a result, the MITM attacker becomes capable of capturing all Bluetooth data via a Bluetooth connection.

In the case of the bluetooth 2.0+EDR(SSP support) device, separate pretreatment is required in order to conduct such attacks.

2.2 BT-NiÑo-MITM attack

Konstantin, et al., proposed a BT-NiÑo-MITM attack (Bluetooth - No Input No Output - Man In The Middle) in 2007. The attacker considers the IO capabilities of the devices to intercept the information required during the first phase of SSP. This attacker controls an unauthenticated channel to intercept the important information in the communication between the devices by attacking data transmitted, connectivity, and association models [2][4]. In this attack, the link key is saved on two target devices during the IO capability exchange phase to use the devices later without IO capability exchange in the process of SSP, and there can be a MITM attack against the physical layer. Thus, two scenarios are possible for this attack.

- A MITM attack can proceed when a target device (A, B) initiates SSP.
- A MITM attacker first initiates SSP with a target device to perform its attack. Depending on the implementation of the target devices, it may be possible to perform SSP without asking the user to enter any message to accept the connection request message.

3 Improved NC association security model based on Bluetooth 4.0

3.1 System parameters

- PK_v: Device X's public key
- SK_v: Device X's private key
- DHkey: Diffie-Hellman key generated by Device X
- $nonce_v$: Device X's nonce value

- nonce: Device communication between the participation of the generated value for confidential communication (_ and _)

- a: Integer, a = 1 ... = 1 ... refinement to the factorization and one of the arguments is the ∈ ℕ(1 ≤ ≤ ,1≤ ≤).

- r_x: Random number of generated by the Device X

- C_x: Middle value of generated by Device X

- f1(): Ony-way Function

- f2():Ony-way Function for Link key

- f3(): One-way Function for verification value

- g(): One-way function for Middle value verification

- IOcapX: Device X's input/output capacity

- BD_ADDR: 48bit Bluetooth device address

- E(): Encryption function

3.2 Improved SSP protocol details

The protocol details for the improved NC association security model based on Bluetooth 4.0 are as follows.

<Step 1> Public key exchange

① Device A transmits 1 , 1 and 1 to Device B after calculating 1 by using the public key and public key certificate i.

$$1 = (,1,1\_,1)$$

② Device B checks the integrity of 1 transmitted from Device A. If it is valid, Device B calculates 2 ~ 2 and then transmits them to Device A.

$$2 = (, 2, 2\_,2)$$

<Step 2> Authentication 1

① Device B transmits C_B to the Device A after selecting a random number R_B and calculating C_B.

$$C_B = f1(PK_B, PK_A, nonceD\_L, R_B)$$

② Device A temporarily stores C_B transmitted from Device B, and it transmits M_A and R_A to Device B.

$$M_A = (R_A EDnonce_{o1\_R})$$

③ Device B calculates the following based on M_A and R_A transmitted from Device A. Device B calculates M_B and transmits M_B to the Device A after

generating a nonce by using $nonce_{D1\_B}$ and $nonce_{D2\_L}$

$$M_A\ ED\ R_A = nonce_{1\_R}$$

Device A and Device B generate the following DHKey based on the previous data.

Device A'sDHKey = (PK$_B$, SK$_A$, nonce),
Device B's DHKey = (PK$_A$, SK$_B$, nonce)

After the created DHKey is stored, the verification process is performed on the value H in <Step 1>. If the value is valid, the value v for mutual verification is checked by using the nonce in <Step 2>.

$$v = g(PK_A, PK_B, R_A, R_B, nonce)$$

<Step 3> Authentication 2

① Device A calculates E_A as follows and transmits E_A to Device B.

$$E_A = f3(DHK\ ey, b_j, 0, 10\ capA, A, B)$$

② Device B calculate E_B and then transmit E_B to Device A after receiving E_A

Device A and B performs the verification process of b_j and c_j as follows.

$$E_A = f3(DHK\ ey, c_j, 0, 10\ cap\ B, B, A)$$

<Step 4> Link key generation
Device A and B mutually generates the following link key.

4 Conclusion

With the rapid development of information-oriented society represented by Smart devices, users no longer use new applications and services available passively, but they actively create and distribute information by themselves. At the same time, there has been considerable interest on the short-range wireless communication

technologies.

In particular, Bluetooth is being applied to many wireless devices due to its fast transmission speed and convenience, and it has been used in various fields due to its ad-hoc networks. However, the security concerns have been raised in the initial process of Bluetooth SSP.

In this paper, the existing security vulnerabilities of SSP are analyzed and an improved NC association security model is proposed to compensate the problems. The proposed method guarantees the integrity and confidentiality of the information transmitted at each stage in the process of SSP and provides protection against the MITM attacks. For future research, the proposed method can actually be applied to the network formation of a hierarchical model and thereby its effectiveness can be verified. As a result, a secure personal area network can be developed.

References

1. Kalia M, Garg S, Shorey R., “Scatternet structure and inter-piconet communication in the Bluetooth system,” IEEE national conference on communications 2000, New Delhi.
2. Sharmila, D., Neelaveni, R.and Kiruba, K., "Bluetooth Man-In-The-Middle attack based on Secure Simple Pairing using Out Of Band association model," INCACEC 2009, pp.1-6, 2009.
3. Sanna Pasanen, Keijo Haataja, Niina Paivinen, Pekka Toivanen, "New Efficient RF Fingerprint-Based Security Solution for Bluetooth Secure Simple Pairing," hicss, pp.1-8, 2010 43rd Hawaii International Conference on System Sciences, 2010.
4. Konstantin Hypp¨onen, Keijo M.J. Haataja, ""NiÑo” Man-In-The-Middle Attack on Bluetooth Secure Simple Pairing," 2007 Third IEEE/IFIP International Conference in Central Asia on Internet, pp.1-5, 2007.
5. Keijo M.J. Haataja, Pekka Toivanen, “Practical Man-in-The-Middle Attacks against Bluetooth Secure Simple Pairing,” WiCom’08, pp. 1~5, 2008.

