Bluetooth Security - Need to Increase the Efficiency in Pairing

Pushpa R Suri
Kurukshetra University,India
Sona_malhotra@yahoo.com

Sona Rani
Kurukshetra University,India
Sona_malhotra@yahoo.com

Abstract

This paper focuses on the mechanism of bluetooth authentication. When two units want to communicate in a secure way, they need to be paired to each other. In the pairing process units are exchanging keys and authenticate each other. We have mentioned about bluetooth security breaks and holes used by the attacker. Finally this paper ends with countermeasures of the attack.

1. Bluetooth Pairing Introduction

When Bluetooth devices come within range of another, an electronic conversation takes place to determine whether the devices in range are known or whether one needs to control the other. Most Bluetooth devices do not require any form of user interaction for this to occur. If devices within range are known to one another, the devices automatically form a network – known as a pairing.

Authentication addresses the identity of each communicating device. The sender sends an encrypted authentication request frame to the receiver. The receiver sends an encrypted challenge frame back to the sender. Both perform a predefined algorithm. The sender sends its findings back to the receiver, which in turn either allows or denies the connection[1].

The steps of calculating the keys in the bluetooth pairing process are as under.

Step 1. Each device creates a random number and encrypts it together with its hardware address.

Step 2. The random number is XORed with initialization key and sent away to the other unit.

Step 3.Now the two units have the other's random number. The hardware address is public so each unit can calculate their counter part's encrypted random number together with hardware address.

Step 4.Both units now do a bitwise modulo2 addition to combine the two units encrypted values.

Step 5.The result of the modulo2 addition is the combination key of the two units.

Step 6.A mutual authentication is required in order to confirm that both units have the correct combination key. After a successful authentication the old link key can be discarded.

2. Bluetooth Authentication

The Bluetooth Authentication procedure is based on the challenge-response scheme. Authentication addresses the identity of each communicating device. The sender sends an authentication request frame to the receiver. The receiver sends an challenge frame back to the sender. Both perform a predefined algorithm. The sender sends its findings back to the receiver, which in turn either allows or denies the connection [3].Two devices interacting in an authentication procedure are referred to as the claimant and the verifier. The verifier is the Bluetooth device validating the identity of another device. The claimant is the device attempting to prove its identity. The authentication verification scheme is depicted in Figure 1. One of the Bluetooth devices (the claimant) attempts to reach and connect to the other (the verifier).

The steps in the authentication process are the following:

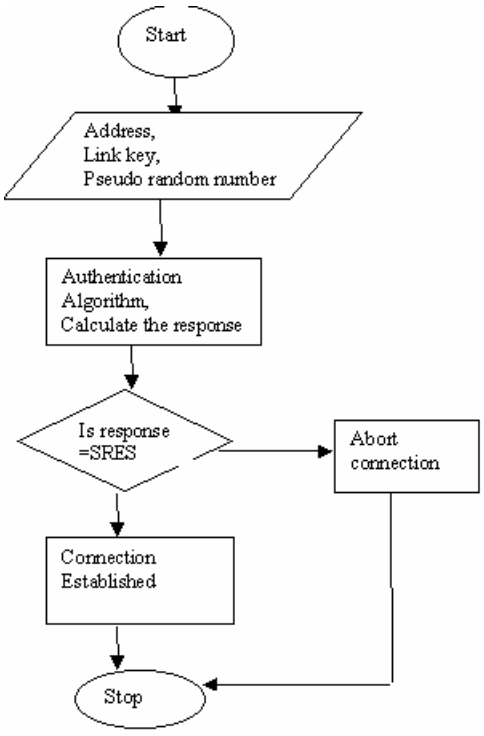

Figure 1 Existing Authentication Process

Step 1. The claimant transmits its 48-bit address (BD_ADDR) to the verifier.

Step 2. The verifier transmits a 128-bit pseudo random challenge (AU_RAND) to the claimant.

Step 3. The verifier uses the authentication

algorithm to compute an authentication response using the address, link key, and random challenge as inputs. The claimant performs the same computation.

Step 4. The claimant returns the computed response' SRES' to the verifier.

Step 5. The verifier compares the SRES from the claimant with the SRES that it computes.

Step 6. If the two 32-bit SRES values are equal, the verifier will continue connection establishment.

The Bluetooth address is a public parameter that is unique to each device. This address can be obtained through a device inquiry process. The link key is a secret entity. The pseudo random challenge is designed to be different on every transaction.The random number is derived from a pseudo-random process within the Bluetooth device.

3. Problem in the Current System

When connection is made between the Bluetooth devices, an intruder device can be there in different ways . An intruder can act as the fake device in the different roles. The fake device can behave as false slave or false master. Similarly the intruder can be a active (changing the contents of the information) intruder or passive one (simply coping the information and sending the same information to the another end).It can continue the connections to the both communicating (original) devices or detach the one end (the another end is considering the intruder as the real one communicating device)[2]. Messages sent by device A and device B are shown in figure 2.

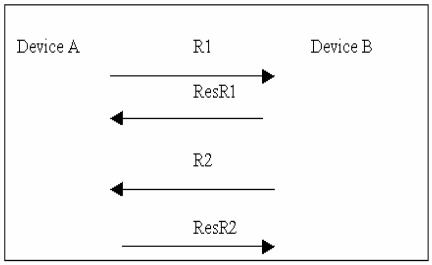

Figure 2 Messages in existing authentication

In the existing authentication scheme of bluetooth technology, mutual authentication is performed. First one device sends the random number for authentication to device second. Then the second device sends the response and sends another random number for the verification of first device. Then the first device sends the response of random number send by second device. In this way the identification of both the devices is done.

4. Improved Authentication Method

In this section, we propose the solution to detect the attacks. We propose to include piconet-specific information in SRES calculation. Such information could be hop sequence parameters or channel access code, which is added to each packet sent within the piconet.

We consider master's clock and some address part values in SRES calculation. To do so, the AU_RAND values could be XORed with the concatenation of clock and part of

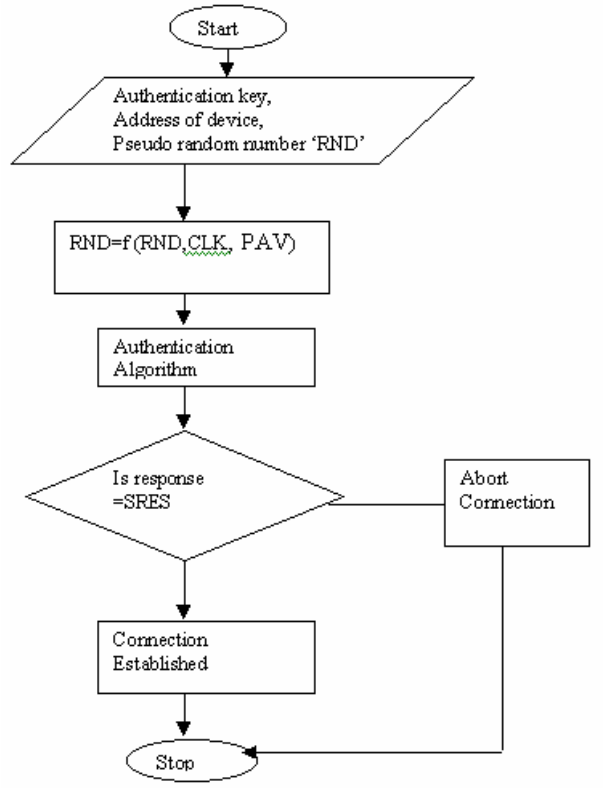

Figure 3 Improved method of pairing

Address values (PAV) at each piconet for SRES calculation and verification. Real A and B use different clock and/or PAV values since the attacker cannot enforce the same values, because otherwise messages of two piconets mix up. The updated authentication mechanism is shown in Figure 3. The original Bluetooth authentication scheme does not have the XOR part, i.e. pseudo random number is directly fed into authentication process.

The attacker need not obtain any secret (like PINs or current keys) of the victims attacks on Bluetooth authentication method. The attacker simply transfers some messages from one victim to another without alteration. Authentication attacks are based on a deception that both victims think they are in the same piconet. They are actually in different piconets. If the victims can include some information about their actual piconets in SRES, then authentication attacks could be detected. If they are close, then inclusion of PAV (address part) of the master

BD_ADDR and master clock in SRES messages solves the problem.

5. Conclusion

We describe the solution to secure against the attack on bluetooth authentication protocol. In the existing system the attacker does not need to guess or obtain a common secret known to both victims in order to set up these attacks, merely to transfer the information it receives from one victim to the other during the authentication process. If an unknown device wants to make connections or request for a service, then proper authentication is followed by authorization and encryption. We propose that the authentication process should be such that to add information about the piconet in response message so that the authentication attack could be detected.

6. References

[1] A. Laurie. "Serious flaws in bluetooth security lead to disclosure of personal Data", 2003.

[2] Armknecht.."An Algebraic attack on the Bluetooth Key Stream Generator", 2004.

[3] Gehrmann, J. Persson , B. Smeets. "Bluetooth Security". Artech House, Inc.. 2004.