http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 6 (6): 938-940, 2007
ISSN 1812-5638
© 2007 Asian Network for Scientific Information

Bluetooth Authentication and Personal Identification Number Estimation by Attacker

Pushpa R. Suri and Sona Rani
Department of Computer Science and Applications, Kurukshetra University, Kurukshetra, India

Abstract: This research deals with the mechanisms used in Bluetooth Link-level security Mode. In this mode, a Bluetooth device will initiate security measures before a channel is established. This is a built-in mechanism that is used regardless of the application layer security that may also be used. In this study we have discussed about the estimation of personal identification number by the attacker and demonstration of how the security of the Bluetooth devices is disturbed.

Key words: Pairing, personal identification number, initialization key, link key

INTRODUCTION

Bluetooth, a short-ranged wireless technology, was originally designed to be a cable replacement. Due to its energy efficient nature and its low cost of production, Bluetooth has become a popular way for small mobile devices to connect to each other wirelessly. Today, most of mobile phone models support Bluetooth and most of the palm pilots provide Bluetooth connection. As more and more important personal information is stored within these gadgets, Bluetooth will become an increasingly important gateway that mobile phones and palm pilots manufacturers need to guard. Although Bluetooth technology has been around for more than 10 years, its design may not be secured enough for some potential applications. Most mobile phones have their Bluetooth features turned off by default so that only knowledgeable users will turn them on. Mobile phone manufactures also recommend users not to turn on the Bluetooth connections on their mobiles when they are not in use in order to minimize the risk of being attack by hackers. Bluetooth designers also recommend people not to bond Bluetooth devices in public places. All these facts are reinforcing the fact that the Bluetooth security (SIG, Part B, 2001) design is insufficient for many applications.

THE BLUETOOTH PAIRING AND AUTHENTICATION PROCESS

The Bluetooth pairing procedures consist of 3 or 4 steps:

- Creation of an initialization key (K_{init}).
- Creation of a link key (K_{AB}).
- Authentication.

After the 3 pairing steps are completed, the devices can derive an encryption key to hide all future communication in an optional 4th step.

Creation of Kinit: The K_{init} key is created using the E_{22} algorithm, whose inputs are:

- A BD_ADDR.
- The PIN code and its length.
- A 128 bit random number IN_RAND.

This algorithm outputs a 128-bit word, which is referred to as the initialization key (K_{init}).

Figure 1 describes how K_{init} is generated using E_{22}.

The PIN code is available at both Bluetooth devices. One hundred and twenty eight bit IN_RAND is transmitted in plain text.

This initialization key (K_{init}) is used only during the pairing process. Upon the creation of the link key (K_{AB}), the K_{init} key is discarded.

Creation of K_{AB}: After creating the initialization key, the devices create the link key K_{AB}. The devices use the initialization key to exchange two new 128 bit random words, known as RND_A and RND_B(SIG, Part B, 2001). Each device selects a random 128 bit word and sends it to the other device after bitwise xoring it with K_{init}. Since both devices know K_{init}, each device now holds both random numbers RND_A and RND_B. Using the E_{21} algorithm, both devices create the link key K_{AB}. The inputs of E_{21} algorithm are:

- A BD_ADDR.
- The 128 bit random number RND.

E_{21} is used twice is each device, with two sets of inputs. Figure 2 describes how the link key K_{AB} is created.

Corresponding Author: Sona Rani, Department of Computer Science and Applications, Kurukshetra University, Kurukshetra, India

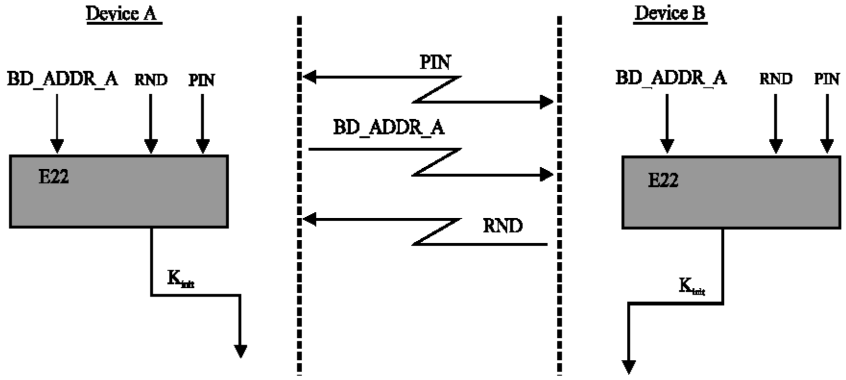

Fig. 1: Generation of K_{init} using E_{22}

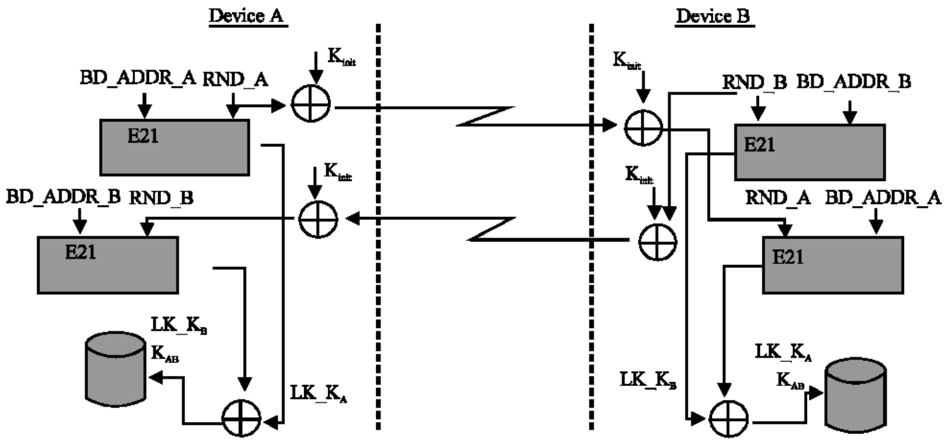

Fig. 2: Generation of K_{AB} using E_{21}

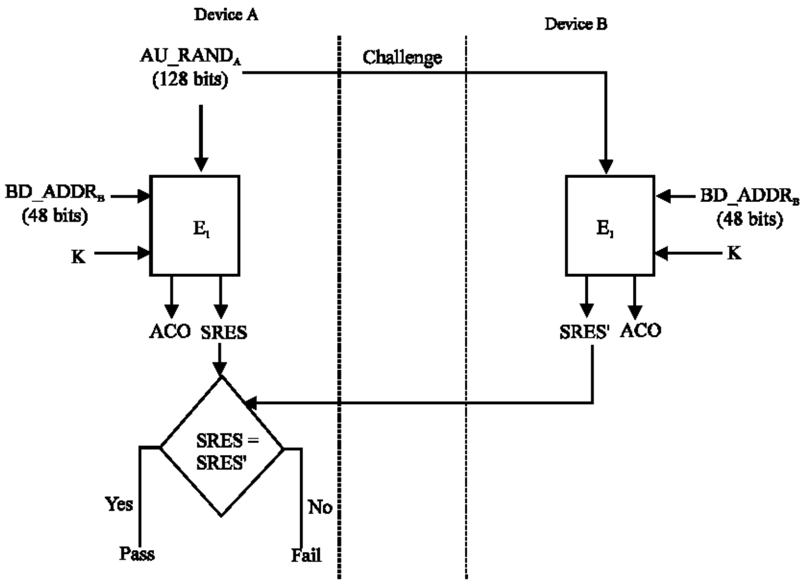

Fig. 3: Mutual authentication

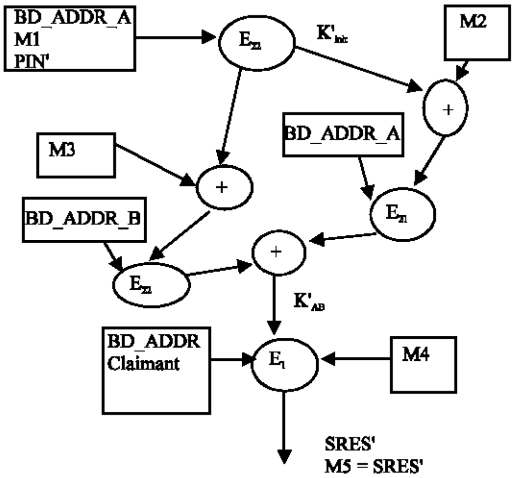

Fig. 4: Estimation the PIN by attacker

MUTUAL AUTHENTICATION

Upon creation of the link key $K_{AB,}$ mutual authentication is performed. This process is based on a challenge-response scheme (SIG, Part H, 2001). One of the devices, the verifier, randomizes and sends (in plain text) a 128 bit word called AU_RAND$_A$. The other device, the claimant, calculates a 32 bit word called SRES using an algorithm E_1. The claimant sends the 32 bit SRES word as a reply to the verifier, who verifies (by performing the same calculations) the response word. If the response word is successful, the verifier and the claimant change roles and repeat the entire process. Figure 3 describes the process of mutual authentication. The inputs to E_1 are:

- The random word AU_RAND$_A$.
- The link key K_{AB}.
- Its own Bluetooth device address (BD_ADDR$_B$).

BLUETOOTH CRYPTOGRAPHIC PRIMITIVES

Bluetooth PIN Guessing: The basic attack assume that the attacker eavesdropped on an entire pairing and authentication process and saved all the messages (Table 1) the attacker can now use a brute force algorithm to find the PIN used. The attacker enumerates all possible values of the PIN. Knowing IN_RAND and the BD_ADDR, the attacker runs E_{22} with those inputs and the guessed PIN and finds a hypothesis for K_{init}. The attacker can now use this hypothesis of the initialization key, to decode messages 2 and 3.

Table 1: List of messages sent during the pairing and authentication process. ``A'' and ``B'' denote the two Bluetooth devices

Message No.	Source	Destination	Message signal	Length of message in bits	Message format
M 1	A	B	IN_RAND	128 bit	Plaintext
M 2	A	B	LK_RAND$_A$	128 bit	XORed with K_{init}
M 3	B	A	LK_RAND$_B$	128 bit	XORed with K_{init}
M 4	A	B	AU_RAND$_A$	128 bit	Plaintext
M 5	B	A	SRES	32 bit	Plaintext

Messages 2 and 3 contain enough information to perform the calculation of the link key K_{AB}, giving the attacker a hypothesis of K_{AB}. The attacker now uses the data in the last 4 messages to test the hypothesis: Using K_{AB} and the transmitted AU_RAND$_A$ (message 4), the attacker calculates SRES and compares it to the data of message 5. Figure 4 describes the entire process of PIN estimating.

Note that the attack, as described, is only fully successful against PIN values of under 64 bits. If the PI N is longer, then with high probability there will be multiple PIN candidates, since the two SRES values only provide 64 bits of data to test against.

CONCLUSIONS

This study describes the implementation of an attack on the Bluetooth security mechanism. Specifically, we describe a attack, in which an attacker can find the PIN used during the pairing process.

Since Bluetooth is a wireless technology, it is very difficult to avoid Bluetooth signals from leaking outside the desired boundaries. Therefore, one should follow the recommendation in the Bluetooth standard and refrain from entering the PIN into the Bluetooth device for pairing as much as possible. This reduces the risk of an attacker eavesdropping on the pairing process and finding the PIN used.

REFERENCES

Bluetooth SIG, 2001. Specification of the Bluetooth System: Core, Part B Baseband specification. Version 1.1. http://www.bluetooth.com/.

Bluetooth SIG, 2001. Specification of the Bluetooth system: Core, Part H: 1 Host Controller Interface Functional Specification. Version 1.1. http://www.bluetooth.com/.