

Security of Bluetooth: An overview of Bluetooth Security

Marjaana Träskbäck

Department of Electrical and Communications Engineering
mtraskba@cc.hut.fi
52655H

ABSTRACT

The purpose of this paper is to give an overview of Bluetooth security and how it was designed. At the end there is also a short discussion of its weaknesses on a general level.

Keywords

Bluetooth, Security, Architecture, Authentication, Encryption

1. INTRODUCTION

Bluetooth is a new technology for wireless communication. The target of the design is to connect different devices together wirelessly in a small environment like in an office or at home. The BT range restricts the environment, which at the moment is about 10 meters. Before accepting the technology a close look at the security function has to be taken. Especially in office the information broadcasted over the Bluetooth piconet can be sensitive and requires a good security.

Bluetooth employs several layers of data encryption and user authentication measures. Bluetooth devices use a combination of the Personal Identification Number (PIN) and a Bluetooth address to identify other Bluetooth devices. Data encryption can be used to further enhance the degree of bluetooth security. [3]

Bluetooth uses transmission scheme that provides a level of security in itself. Instead of transmitting over one frequency within the 2.4 GHz band, Bluetooth radios use a fast frequency-hopping spread spectrum (FHSS) technique, allowing only synchronised receivers to access the transmitted data. [3]

2. BLUETOOTH SECURITY

BT uses authorisation and authentication to know who is the user and what are the devices and their rights. The terms are defined as follows:

Authentication:

The process of verifying 'who' is at the other end of the link. Authentication is performed for devices. In Bluetooth, this is achieved by the authentication procedure based on the stored link key or by pairing (entering a PIN). [12]

Authorisation:

This is the process of deciding if device X is allowed to have access to service Y. This is where the concept of "trusted" exist (explained below). [4 pg. 14]

Bluetooth uses link level security where each connection is given a unique secret authentication key and encryption key that is derived from the first one. More of these later in the paper.

Communication between different Bluetooth (BT) devices use fast frequency-hopping spread spectrum (FHSS) technique, which uses 79 different radio channels. Bluetooth uses the same frequency than other household machines, example microwave oven, which can cause interference. FHSS prevents this interference to cause too much harm, since it changes transmission frequency 1600

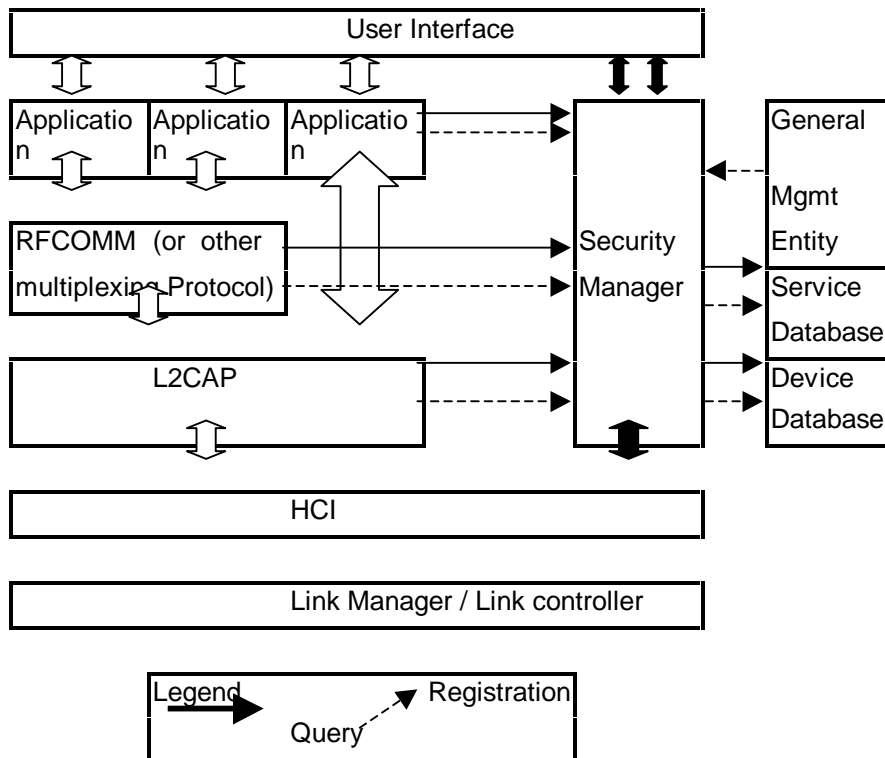


Figure 1. Security Architecture (based on [4])

times per second and if there is an interference at some frequency, only that one transmission is damaged. FHSS also add security on data transmission between devices since it makes it harder to eavesdrop.

On the other hand the low transmission power prevents the transmission to propagate far and makes it harder to cut between the transmission.

The information on a BT packet can be protected by encryption. Only the packet payload is encrypted, never the access code and the packet header. The encryption is done with a stream cipher E0, which is synchronised for each payload.

2.1 Security Architecture

The Bluetooth architecture is shown in figure 1. The security manager stores information about the security of services and devices. It decides on accepting the access or disconnection and requires authentication and encryption if they are needed. Security manager also initiates setting up a trusted relationship and pairing and asks for PIN code from the user.

2.2 Security Levels

Bluetooth has several different security levels that can be defined for devices and services. All the devices get a status when they connect the first time to another device.

2.2.1 Device Trust Level

The devices can have two trust levels; trusted and untrusted. The trusted level requires a fixed and trusted relationship and it has unrestricted access to all services. The device has to be previously authenticated. The untrusted device doesn't have fixed relationship and its access to services is limited. An untrusted device can also have a fixed relationship, but it's not considered as trusted. A new device is labelled as unknown device and it is always untrusted.

2.2.2 Security Modes

Bluetooth has three different security modes build in it and they are as follows:

Security Mode 1 A device will not initiate any security. A non-secure mode. [12]

Security Mode 2 A device does not initiate security procedures before channel establishment on L2CAP level This mode allows different and flexible access policies for applications, especially running applications with different security requirements in parallel. A service level enforced security mode. [12]

Security Mode 3 A device initiates security procedures before the link set-up on LPM level is completed. A link level enforced security mode. [12]

This paper exploits most the security mode 2.

2.2.3 Security Level of Services

The need for authorisation, authentication and encryption changes. When the connection is set there are different levels of security where the user can choose from. The security level of a service is defined by three attributes:

Authorisation required: Access is only granted automatically to trusted devices or untrusted devices after an authorisation procedure. [4 pg. 15]

Authentication required: Before connecting to the application, the remote device must be authenticated. [4 pg. 15]

Encryption Required: The link must be changed to encrypted mode, before access to the service is possible. [4 pg. 15]

On the lowest level the services can be set to be accessible to all devices. Usually there is a need for restrictions so the user can set the service so that it needs authentication. When the highest level of security is needed the service can require authorisation and authentication. At this level trusted device has access to the services, but untrusted device needs manual authorisation.

2.3 Link Layer

At the link layer, authentication of the peers and encryption of the information maintain security. For basic security we need a devices unique public address (BD_ADDR), two secret keys (authentication keys and encryption key) and a random number generator. BD_ADDR is used in the authentication process. When a challenge is given. The device has to response with it's own challenge that is based on the incoming challenge, its BD_ADDR and a link key shared with the two devices. Other devices' BD_ADDRs are stored in the device database for further use.

2.4 Random number Generation

Each Bluetooth device has a random number generator to be used in the security functions. This generator is usually implemented with software. BT devices use random numbers for contacting other devices and for the authentication and encryption.

3. KEY MANAGEMENT

There are several kinds of keys in the Bluetooth system to ensure secure transmission. The most important key is the link key, which is used between two BT devices for authentication purpose. Using the link key an encryption key is derived. This secures the data of the packet and is regenerated for all new transmissions.

3.1 Link key

There are four link keys to cover the different applications it is used for. All the keys are 128-bit random numbers and are either temporary or semi-permanent.

Unit key, K_A , is derived at the installation of the Bluetooth device from a unit A. The storage of K_A requires little memory space and is often used when device has little memory or when the device should be accessible to a large group of users.

Combination key, K_{AB} , is derived from two units A and B. This key is generated for each pair of devices and is used when more security is needed. This requires more memory, since device has to store one combination key for each connection it has.

The master key, K_{master} , is used when the master device wants to transmit to several devices at ones. It over rides the current link key only for one session.

The initialisation key, K_{init} , is used in the initialisation process. This key protects initialisation parameters when they are transmitted. This key is formed from a random number, an L-octet PIN code, and the BD_ADDR of the claimant unit.

3.2 Encryption key

Encryption key is derived from the current link key. Each time encryption is needed the encryption key will be automatically changed. The purpose of separating the authentication key and encryption key is to facilitate the use of a shorter encryption key without weakening the strength of the authentication procedure. [1 pg. 152]

3.3 PIN code

This is a number, which can be fixed or selected by the user. The length is usually 4 digits, but it can be anything between 1 to 16 octets. The user can change it when it wants to and this adds security to the system. The PIN can be used entering it into one device (fixed PIN), but it is safer to enter it to both units. Example the latter one can be used when there is a laptop and a phone to be connected.

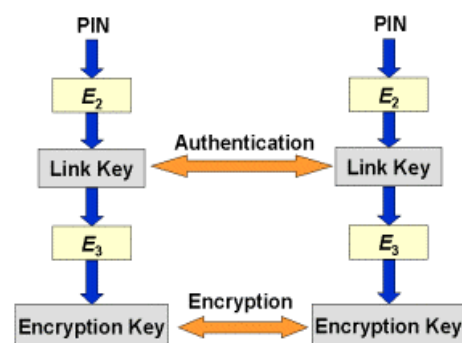


Figure 2. Encryption and key control [5]

3.4 Key Generation and Initialisation

The exchange of the keys takes place during an initialisation phase, which has to be carried out separately for each two units that want to implement authentication and encryption. All initialisation procedures consists of the following five parts:

- Generation of an initialisation key
- Authentication
- Generation of link key
- Link key exchange
- Generating of encryption key in each unit

[1 pg. 153]

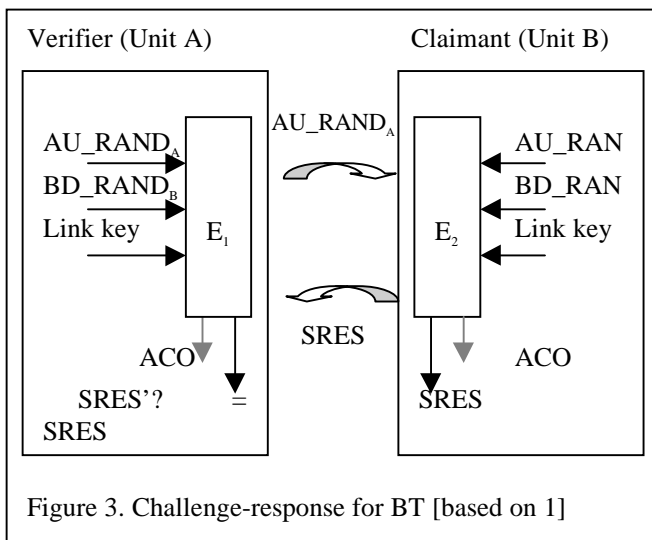
After this procedure the connection is build or the link can be aborted.

4. AUTHENTICATION

Authentication starts by issuing a challenge to another device and it has to then send a response to that challenge which is based on the challenge, it's BD_ADDR and link key shared between them. After authentication, encryption may be used to communicate. [10]

Without knowing the PIN, one unit can't logon to the other unit if authentication is activated. To make matters easier, the PIN can be stored somewhere inside the unit (in Memory/Hard Drive etc.) so if you wish to establish the connection, a user may not have to manually type in the PIN (Note: the level of security is none in this case). [14]

Bluetooth uses a challenge-response scheme in which a



claimant's knowledge of a secret key is checked through a 2-move protocol using symmetric secret keys. [1 pg. 169] It has been represented in figure 3. The unit A sends a random input, denoted by AU_RAND_A , with an

authentication code, denoted by $E1$ for the unit B. Unit B calculates $SRES$ as stated in Figure 4 and returns the result to unit A. Unit A will derive $SRES'$ (in figure 4) and will authenticate the Unit B if $SRES$ and $SRES'$ are equal. $E1$ consist of the tuple AU_RAND_A and the BT device address (BD_ADDR) of the claimant. On each authentication a new AU_RAND_A (a random number) is issued. [1 pg. 169]

The challenge-response scheme for the symmetric keys used in the bluetooth are shown in figure 4. The application indicates who has to be authenticated by whom. Certain applications only require a one-way authentication. However, in some peer-to-peer communications one might prefer a mutual authentication in which each unit is subsequently the challenger (verifier) in two authentication procedures. The Link Manager coordinates the indicated authentication preferences by the application to determine in which direction(s) the

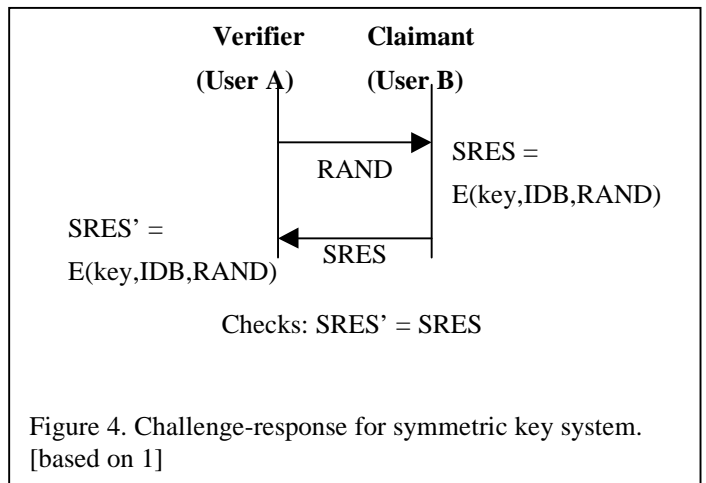


Figure 4. Challenge-response for symmetric key system. [based on 1]

authentication(s) has to take place. [1 pg. 170]

5. ENCRYPTION

The Bluetooth specification 1.0 describes the link encryption algorithm as a stream cipher using 4 LFSR (linear feedback shift registers). The sum of the width of the LFSR is 128, and the spec says the effective key length is selectable between 8 and 128 bits. This arrangement allows Bluetooth to be used in countries with regulations limiting encryption strength, and "facilitate a future upgrade path for the security without the need for a costly redesign of the algorithms and encryption hardware" according to the Bluetooth specification. Key generation and authentication seems to be using the 8-round SAFER+ encryption algorithm. [3] [6]

The information available suggests that Bluetooth security will be adequate for most purposes; but users with higher security requirements will need to employ stronger algorithms to ensure the security of their data. [3] [6]

6. SECURITY LIMITATIONS

Bluetooth security is not all satisfactory and it has some limitations. First about the authentication: only the device is authenticated, not the user. If this feature is needed it have to be accomplished with application level security. Secondly BT doesn't define authorisation separately for each service either. This can be applied in the Bluetooth architecture without changing the BT protocol stack, but changes in the security manager and the registration processes would be necessary.

At the moment BT only allows access control at connection set-up. The access check can be asymmetric, but once a connection is established, data flow is in principle bi-directional. It is not possible within the scope of this architecture to enforce unidirectional traffic. [4 pg. 11]

There is no support of legacy applications: It will not make calls to the security manager. Instead Bluetooth-aware "adapter" application is required to make security-related calls to the BT security manager on behalf of the legacy application. [4 pg. 11]

7. CONCLUSIONS AND FURTHER WORK

Bluetooth security is not complete, but it seems like it wasn't meant to be that way. More security can be accomplished easily with additional software that is all ready available. More detailed information can be found from chapter 14 of the Specification of the Bluetooth System.

Further work will be done in the other seminar papers on the Bluetooth security.

8. REFERENCES

1. Specification of the Bluetooth System, volume 1B, December 1st 1999
2. Knowledge Base for Bluetooth information
<http://www.infotooth.com/>
3. General information on bluetooth
<http://www.mobileinfo.com/bluetooth/>
4. Thomas Muller, Bluetooth WHITE PAPER: Bluetooth Security Architecture, Version 1.0, 15 July 1999
5. Annikka Aalto, Bluetooth
<http://www.tml.hut.fi/Studies/Tik110.300/1999/Essays/bluetooth.html>
6. Bluetooth information,
<http://www.bluetoothcentral.com/>
7. Oraskari, Jyrki, Bluetooth 2000
<http://www.hut.fi/~joraskur/bluetooth.html>
8. How Stuff Works, information on BT
<http://www.howstuffworks.com/bluetooth3.htm>
9. Information on Bluetooth (Official Homepage)
<http://www.bluetooth.com/>
10. Bluetooth Baseband
<http://www.infotooth.com/tutorial/BASEBAND.htm>
11. Bluetooth - an inferior LAN concept?
<http://www.infotooth.com/knowbase/othernetworks/71.htm>
12. Bluetooth Glossary
<http://www.infotooth.com/glossary.htm#authentication>
13. Authentication process in Bluetooth
<http://www.infotooth.com/knowbase/security/66.htm>
14. Authentication in Bluetooth
<http://www.infotooth.com/knowbase/security/80.htm>