On the advancements of Bluetooth security protocol

A. D. Mocanu, C. Andriesei
Faculty of Electronics, Telecommunications and Information Technology
"Gheorghe Asachi" Technical University
Iași, Romania

Abstract—**Bluetooth security represents a major chapter of the standard core. Therefore, it is not surprising to notice that the security protocol knows a continuous improvement with each new Bluetooth core, a fact imposed, more or less, by the technology development that facilitates network security attacks. This article aims to review the development of the Bluetooth security functionality from the first Bluetooth version to the last Bluetooth Core V4.1 adopted in December 2013.**

Keywords- AES; Bluetooth; encryption; SAFER+; SHA-256

I. INTRODUCTION

Bluetooth technology is a short-range wireless communication system intended to replace the cables. In this regard, it is similar to UWB in-door systems thought to replace the cable connectivity between computers. Its major advantages are robustness, low power consumption and low cost. In addition, sharing the same 2.4–2.483 GHz bandwidth as WiFi (IEEE 802.11b/g) favored its wide integration onto popular portable devices, such as smartphones and tablets. Right now, all new smartphones support the Bluetooth Core V4.0 specifications.

The Bluetooth history starts in 1994 when two engineers from Ericsson developed the first wireless connectivity as cable replacement. Its specifications were formalized by the Bluetooth Special Interest Group in 1998, a group including now thousands of companies all over the world. This Interest Group developed the Bluetooth versions mentioned in Table 1:

TABLE I. ADOPTED BLUETOOTH CORE SPECIFICATIONS

Specification	Adopted date
Core Version 1.0	1999
Core Version 1.1	2001
Core Version 1.2	2003
Core Version 2.0 + EDR	2004
Core Version 2.1 + EDR	2007
Core Version 3.0 + HS	2009
Core Version 4.0	2010
Core Version 4.1	2013

In order to provide information confidentiality, the Bluetooth network has to implement security functionality, such as data encryption and authentication, both at the application and link layers. Both aspects are discussed in the following sections.

II. BLUETTOH ENCRYPTION SCHEME

Security aspects have been seriously taken into consideration in the first Bluetooth standard core [1], the encoding scheme being shown in Fig. 1.

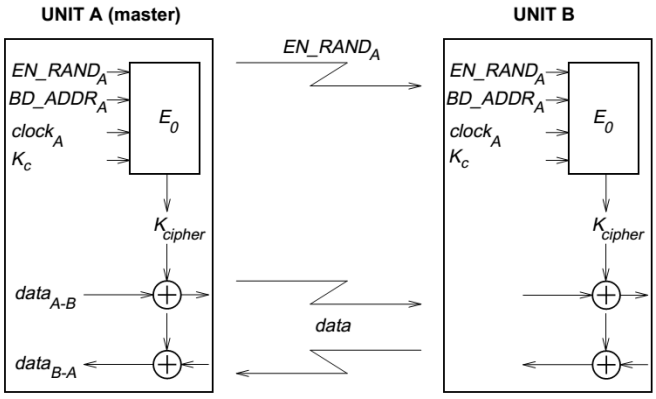

Figure 1. Encoding procedure (Bluetooth v1.0)

As can be noticed, the cipher is symmetric, decryption being performed in the same way and with the same key used for encryption. The encryption routine is applied to the data stream after the CRC bits are appended and prior to the FEC encoding. Moreover, the entire process is based on the cipher algorithm E_0, a hardware structure containing 4 linear feedback shift registers (LFSR), derived from the summation stream cipher generator attributable to Massey and Rueppel, that uses the following four distinct data to generate the binary keystream K_{cipher}:

- 128 bit random number EN_RAND_A issued by the master before entering encryption mode and publicly known since it is transmitted as plaintext over the air;
- 48 bit Master Bluetooth device address (BD_ADDR);
- 26 bit master real-time clock ($clock_A$ or CLK_{26-1});
- 8-128 bit K_C encryption key generated by E_3 (64 bits were enough in 1999).

K_{cipher} is further used to encrypt the data by bit-wise modulo-2 addition. E_0 algorithm is reinitialized at the start of each new packet.

Studying the Core Version 1.2 [2] adopted four years later, it can be noticed that chapter dedicated to security aspects has been moved from Baseband Specification (Part B, Core V1.0) to a distinct Security Specification chapter (Part H, Core V1.2), clearly split in several distinct sections: Random number generation, Key management, Encryption, Authentication, Authentication and Key-generating functions. This new structure reveals the significant importance gained by the security functionality within the Bluetooth standard. However, the entire security functionality remains unchanged in this newer version even though some improvements are proposed.

Security protocol and functionality remain unchanged for Bluetooth Core V2.0 + EDR [3], the main attractiveness of this new version being its superior data rate (up to 3 Mb/s for Enhanced Data Rate mode).

Some notable improvements can be found in Bluetooth Core V2.1+EDR [4], such as: encryption pause and resume, secure simple pairing (using Elliptic Curve Diffie Hellman – ECDH public key cryptography), security mode 4. In addition, it emphasizes on periodical refreshing of the encryption keys and using better pseudo random number generators compliant with FIPS PUB 140-2 and capable of succeeding 14 statistical tests. In addition, replacing SHA-1 with SHA-256 function and high resynchronization frequency are suggested to disrupt security attacks.

Version 3.0+HS [5] comes with new enhancements to security for AMP. It encompasses the verification of the random number generator against 16 statistical tests, in accordance with FIPS SP800-22.

Version 4.0 [6] comes with a major improvement for Bluetooth LE (low energy version), AES-CCM cryptography for encryption algorithm, block cipher defined in NIST publication FIPS-197 and used to encrypt the plaintext data.

Version 4.1 [7] improves the Secure Simple Pairing by using P-256 elliptic curve. As in previous case, AES-CCM is still used whereas the encryption scheme remains unchanged.

Starting with Bluetooth V2.0, a common recommendation addressing passive eavesdropping proposes using an alphanumeric digit PIN as long as possible, 16 character alphanumeric case sensitive PIN offering 95 bits of entropy whereas 16 numeric PIN achieves about 53 bits of entropy. In this regard, using large PIN codes clearly improves the communication security.

The key generation function for encryption E_3, as proposed in Bluetooth V1.0, is shown in Fig. 2.

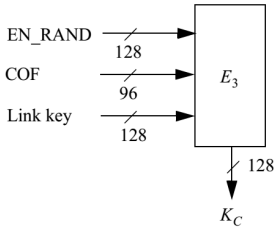

Figure 2. Generation of encryption key

As other key generation functions (E_1, E_2), E_3 is a hash function that produces a 128 bit encryption key. Its functionality remains unchanged for all newer Bluetooth versions.

III. Input Entities of the Security Subsystem

To insure the link layer security, four entities are required to compute different keys (for authentication and encryption):

TABLE II. ENTITIES USED IN AUTHENTICATION AND ENCRYPTION PROCEDURES

Entity	Size
BD_ADDR	48 bits
Private user key, authentication	128 bits
Private user key, encryption	8-128 bits
RAND	128 bits

BD_ADDR is the Bluetooth device address, unique for each Bluetooth unit and publicly known. The secret keys are set during the initialization procedure and are never disclosed. The key used in authentication algorithm is always 128 bits whereas the key length for encryption algorithm varies between 1 and 16 bytes (8-128 bits). Bluetooth core V1.0 stipulates that 64 bits for encryption key gives satisfying protection (perfectly right in 1999), remark that is missing in other Bluetooth cores, therefore proving that the continuous technology development pushes much pressure over the network security.

It is important to notice here that these four inputs remain unchanged for all Bluetooth cores even though the network security is continuously improved. This means that the primary goal behind the security protocol was to keep the user inputs as simple as possible while implementing stronger and optimized encryption algorithms thanks to the increased computing power of portable devices.

IV. Authentication Procedure

The basic authentication procedure based on a challenge-response scheme, as implemented by the first Bluetooth version, is illustrated in Fig. 3. Its main scope is to check whether the claimant computes the same SRES (signed response) based on a random sequence and link key. A new AU_RAND_A is issued during each authentication procedure. The algorithm E_1 is illustrated in Fig. 4, where ACO response is further used in the generation of the ciphering key by E_3.

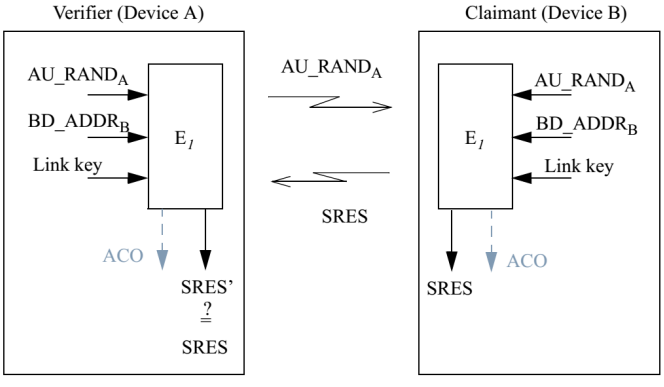

Figure 3. Authentication procedure

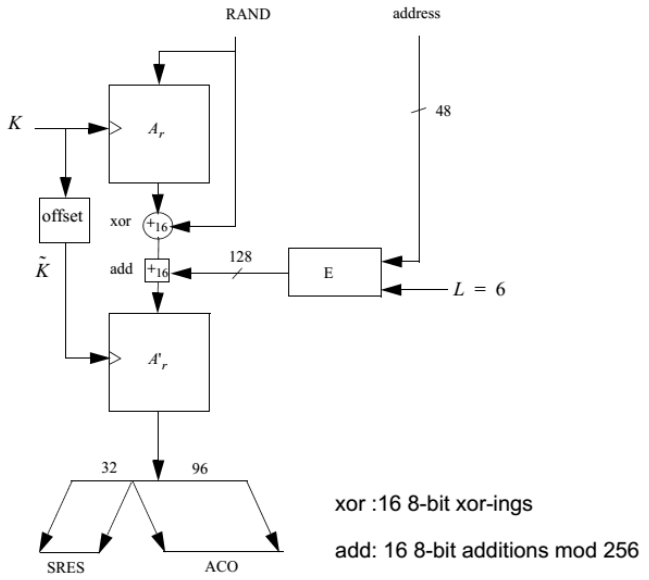

Figure 4. Flow of data for the computation of E_1

The function A_r is identical to SAFER+ whereas A_r' is a slightly modified version of A_r. E_1 remains unchanged for all Bluetooth versions.

The key generation function for authentication, E_2, as proposed in Bluetooth V1.0 and remained unchanged for all newer versions, is shown in Fig. 4. As it is well known, E_2 is used to produce either a 128 link key (when creating unit keys and combination keys) or a 128 bit link key (when initialization or master key is necessary).

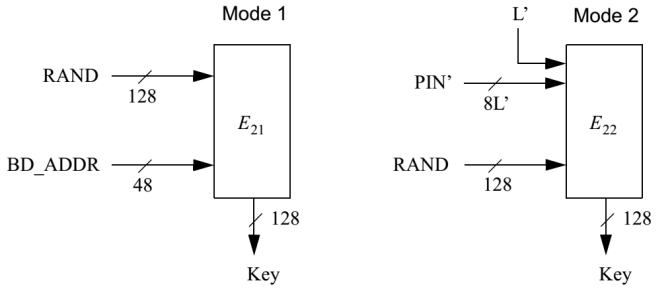

Figure 5. Flow of data for the computation of E_1

The key hierarchy characteristic to Bluetooth V4.1 is shown in Fig. 6.

V. Security Overview

It is worth reviewing the evolution of the Bluetooth security algorithms up to fourth version, as shown in Table III. As the last core specifies, some obvious strong improvements are proposed, such as using four supplementary cryptographic functions:

- f_1: the simple pairing commitment function;
- g: the simple pairing numeric verification function;
- f_2: the simple pairing key derivation function;
- f_3: the simple pairing check function.

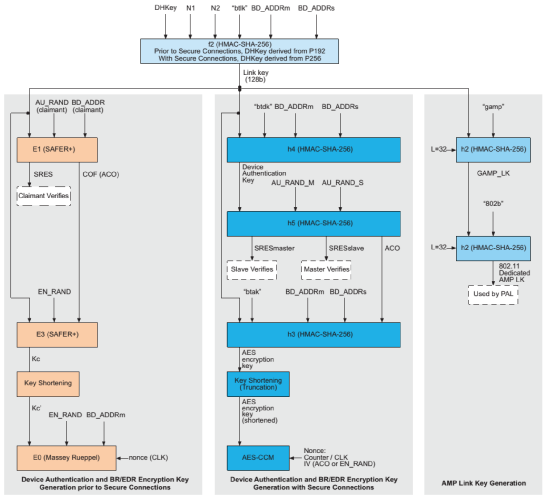

Figure 6. BR/EDR and AMP key hierarchy (Bluetooth v4.1)

TABLE III. ENTITIES USED IN AUTHENTICATION AND ENCRYPTION PROCEDURES

Security mechanism	Legacy	Secure simple pairing	Secure connections
Encryption	E_0	E_0	AES-CCM
Authentication	SAFER+	SAFER+	HMAC-SHA-256
Key generation	SAFER+	P-192 ECDH HMAC-SHA-256	P-256 ECDH HMAC-SHA-256

VI. Conclusion

The main aspects related to Bluetooth security evolution were reviewed in this article. It is important to notice a significant improvement of the security algorithms, fact facilitated by the technology development that opens the path to faster operations and smarter security facilities. However, the valuable security performances achieved by the last Bluetooth core can only be exploited when the paired devices support this last version, otherwise the communication becomes less secure.

References

[1] Specification of the Bluetooth System. Version 1.0, 1999.
[2] Specification of the Bluetooth System. Version 1.2, 2003.
[3] Specification of the Bluetooth System. Version 2.0 + EDR, 2004.
[4] Specification of the Bluetooth System. Version 2.1 + EDR, 2007.
[5] Specification of the Bluetooth System. Version 3.0 + HS, 2009.
[6] Specification of the Bluetooth System. Version 4.0, 2010.
[7] Specification of the Bluetooth System. Version 4.1, 2013.