BULETINUL INSTITUTULUI POLITEHNIC DIN IAŞI
Publicat de
Universitatea Tehnică „Gheorghe Asachi” din Iaşi
Tomul LX (LXIV), Fasc. 3, 2014
Secția
ELECTROTEHNICĂ. ENERGETICĂ. ELECTRONICĂ

ON THE ADVANCEMENTS OF BLUETOOTH SECURITY PROTOCOL

BY

ANA-DORINA MOCANU[1] and CRISTIAN ANDRIESEI[1,2,*]

[1]“Gheorghe Asachi” Technical University of Iaşi
Faculty of Electronics, Telecommunications and Information Technology
[2]AT&C TECHNOLOGY SRL, Iaşi, Romania

Received: July 10, 2014
Accepted for publication: July 31, 2014

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.

Key words: AES; Bluetooth; encryption; SAFER+; SHA-256.

1. Introduction

Bluetooth technology is a short-range wireless communication system intended to replace the cables. In this regard, it is similar to UWB (ultra wide band) 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 frequency band (2.4…2.483 GHz) as WiFi (IEEE 802.11 b/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.

[*]Corresponding author : *e-mail*: candriesei@etti.tuiasi.ro

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 Group developed the Bluetooth as resumed in Table 1, where EDR and HS refer to Enhanced Data Rate and High Speed.

Table 1
Adopted Bluetooth Core Specifications.

Specifications	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

Beyond its current use on mobile platforms, Bluetooth standard has many other interesting possible applications, less known to the public but reported in literature as well. One critical direction aims medical platforms, addressing orthodontic care (Mupparapu, 2006), stomatology (Kolahi & Fazilati, 2009), biomonitoring (Tay *et al.*, 2009) (ECG, SpO_2, temperature and blood pressure) and diabetes sensing (Silva *et al.*, 2012). The second one addresses exotic applications, such as wireless monitoring of the fuel cell buses (Hua *et al.*, 2009) and analysis of the spatiotemporal dynamics of human movement at mass events (Versichele *et al.*, 2012). Finally, other applications that can be reported consist of using Bluetooth technology in shipping industry (Tarn *et al.*, 2009), power applications equipped with wireless sensor networks (WSN) (Hsu, 2009) and in implementing mobile platforms interacting with smart things (Espada *et al.*, 2013).

Some of these Bluetooth systems mentioned above, the third direction in particular, usually transmit private data about users, manufacturers or patient accounts (medical applications), therefore being sensitive to security attacks. This problem had already been emphasized in (Reaves & Morris, 2012), where industry aspects were of primary interest and already studied in medical applications (Mišić & Mišić, 2007). In this regard, it is important to mention that, in order to provide information confidentiality, data security had been addressed from the very beginning, the Bluetooth network implementing security functionality such as data encryption and authentication on both application and link layers. This article is a short review of the security development for Bluetooth standard.

2. Bluetooth Encryption Scheme

Security aspects have been seriously taken into consideration in the first Bluetooth standard core (Bluetooth v1.0, 1999), the encoding scheme being shown in Fig. 1 (as found in the Specification of the Bluetooth System, v1.0).

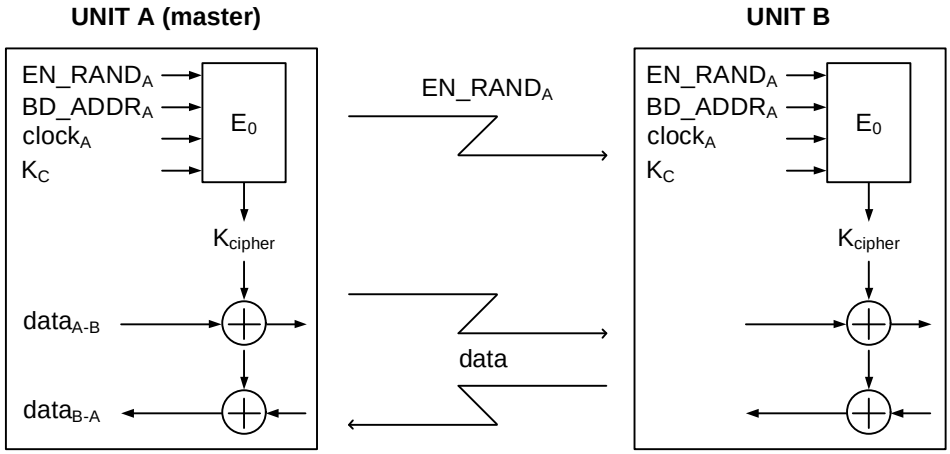

Fig. 1 – Encoding procedure.

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 (cyclic redundancy error check) are appended and prior to the FEC (forward errors correcting) 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}:

a) 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;

b) 48 bit Master Bluetooth device address (BD_ADDR);

c) 26 bit master real-time clock ($clock_A$ or CLK_{26-1});

d) 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 (Bluetooth v1.2, 2003) adopted four years later, it can be noticed that the 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 were addressed.

Security protocol and functionality remain unchanged for Bluetooth Core v2.0 + EDR (Bluetooth v2.0, 2004), 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 (Bluetooth v2.1, 2007), 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 using high resynchronization frequency are suggested to disrupt security attacks.

Version 3.0+HS (Bluetooth v3.0, 2009) comes with new enhancements to security for AMP (alternate MAC/PHY). It encompasses the verification of the random number generator against 16 statistical tests, in accordance with FIPS SP800-22.

Version 4.0 (Bluetooth v4.0, 2010) comes with a major improvement for Bluetooth LE (low energy version), AES-CCM cryptography for encryption algorithm, a block cipher defined in NIST publication FIPS-197 and used to encrypt the plaintext data.

Version 4.1 (Bluetooth v4.1, 2013) improves the Secure Simple Pairing by using P-256 elliptic curve. As in previous case, AES-CCM (Cipher Block Chaining Message Authentication Code) is still used whereas the encryption scheme remains unchanged.

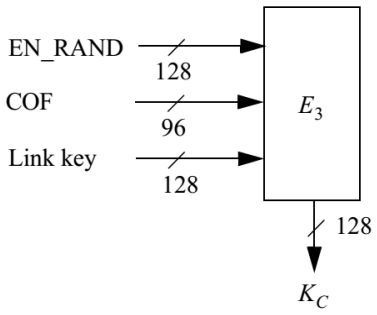

Fig. 2 – Generating the encryption key K_C.

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.

Because the algorithm E_0 uses the K_c key derived by algorithm E_3, the attention will be primarily focused on the encryption key function E_3, as proposed in the first Bluetooth core v1.0 and shown in Fig. 2. As can be noticed, similar to other key generation functions (E_1, E_2), E_3 is a hash function that generates a 128 bit encryption key from the current 128-bit link key, a 96-bit ciphering offset number (CFO) and a 128-bit random number (EN_RAND). Its implementation remains unchanged for all newer Bluetooth versions.

3. Input Entities of the Security Subsystem

To ensure the link layer security, four entities are required to compute different keys (for authentication and encryption), as shown in Table 2.

Table 2
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 which becomes more complex and difficult to deal with.

It is important to notice 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 (and simple) as possible while implementing stronger and optimized encryption algorithms thanks to the increased computing power of portable devices (but with the price of extra power consumption).

4. Authentication Procedure

The authentication procedure based on a challenge-response scheme, as implemented by the first Bluetooth version, is illustrated in Fig. 3. Its main goal

is to check whether the claimant computes the same signed response (SRES) 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, Asynchronous Connection-Oriented (logical transport), is further used to generate the ciphering key by E_3 (COF is ACO if the link key is not the master key).

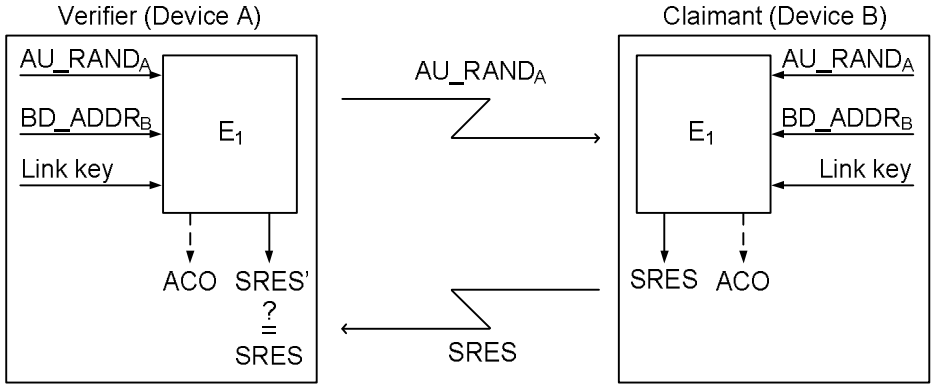

Fig. 3 – Authentication procedure.

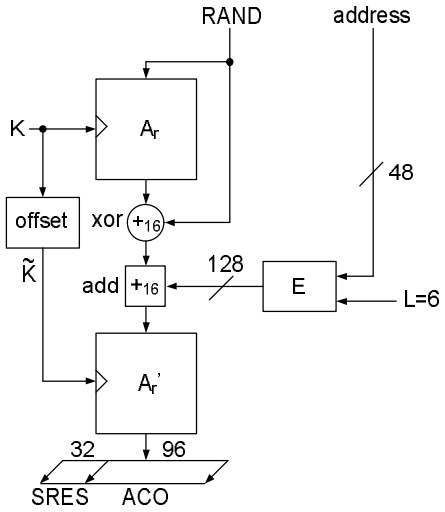

Fig. 4 – Flow of data for the computation of E_1.

The function A_r is identical to SAFER+ (an enhanced version of an existing 64 bit block ciphers SAFER-SK128) 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 unchanged for all newer versions, is shown in Fig. 5. As specified in this core, the cryptographic function E_2 is used to create either a

128 kink key for creating unit and combination keys (algorithm E_{21}) or a 128 bit link key (algorithm E_{22}) for initialization key (K_{init}) or generation of the master key (K_{master}). E_{21} uses a 128 RAND value and 48-bit address (BD_ADDR) while E_{21} uses a 128 RAND value and an L octet user PIN. In the second mode, PIN′ is composed from the L octets in the user PIN augmented with BD_ADDR if $L < 16$, otherwise PIN′ and PIN are identical.

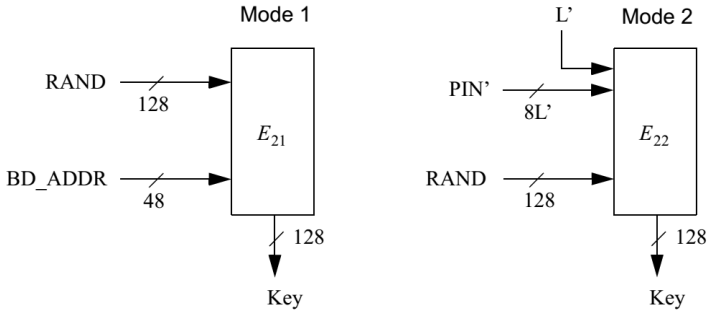

Fig. 5 – Flow of data for the computation of E_2 (Bluetooth v3.0, page 953).

The key hierarchy particular to Bluetooth v4.1 is shown in Fig. 6. As can be noticed, the entire security layer needs at least 6 input parameters for device authentication and BR/EDR encryption key generation prior to/with secure connections: DHKey (Diffie-Hellman key), N_1 and N_2 (streams of 128 bits), "btlk"/"btdk" (Bluetooth link/device key), BD_ADDR_m (Bluetooth

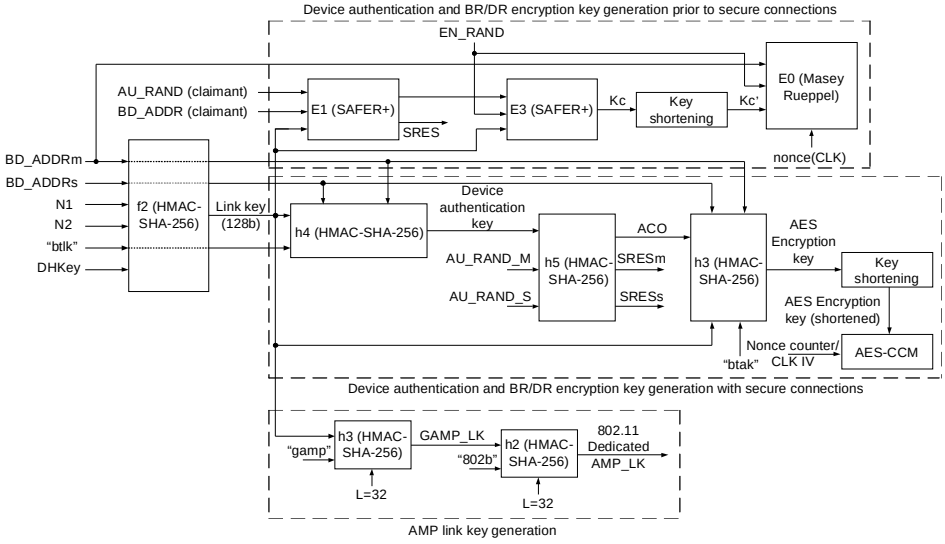

Fig. 6 – BR/EDR and AMP key hierarchy (Bluetooth v4.1).

address of the Master), BD_ADDR_s (Bluetooth address of the Slave). Regarding the authentication process, beside E_0, E_1 and E_3 functions, the hash functions

$h_2 \ldots h_5$ are used to generate different keys and responses while AES-CCM is inserted as final encryption process (in conjunction with P-256 for pairing process).

As can be noticed, the security scheme is greatly improved for this last Bluetooth core, being sufficient complex to resist at two different attacks (passive eavesdropping and man-in-the-middle attacks/active eavesdropping).

5. Security Overview

It is worth reviewing the evolution of the Bluetooth security algorithms up to fourth version, as shown in Table 3. As the last core specifies, some obvious strong improvements are proposed, such as using four supplementary cryptographic functions:

a) f_1: the simple pairing commitment function;
b) g: the simple pairing numeric verification function;
c) f_2: the simple pairing key derivation function;
d) f_3: the simple pairing check function.

Table 3
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

6. 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 opened 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.

This article was presented at Workshop on Circuits, Systems and Information Technology, WCSIT 2014, a joint event organized by "Gheorghe Asachi" Technical University of Iasi (ETTI) and IEICE Communications Society (technical cosponsor).

REFERENCES

Espada J.P. *et al., Using Extended Web Technologies to Develop Bluetooth Multi-Platform Mobile Applications for Interact with Smart Things.* Information Fusion, Elsevier, **21**, 30-41 (2013).

Hsu C.L., *Constructing Transmitting Interface of Running Parameters of Small-Scaled Wind-Power Electricity Generator with WSN Modules*. Expert Syst. with Appl., Elsevier, **37**, *5*, 3893-3909 (2010).

Hua J. *et al.*, *Bluetooth wireless monitoring, diagnosis and calibration interface for control system of fuel cell bus in Olympic demonstration*. J. of Power Sources, Elsevier, **186**, *2*, 478-484 (2009).

Kolahi J., Fazilati M., *Bluetooth Technology for Prevention of Dental Caries*. Medical Hypotheses, Elsevier, **73**, *6*, 1067-1068 (2009).

Mišić J., Mišić V. B., *Implementation of Security Policy for Clinical Information Systems over Wireless Sensor Networks*. Ad Hoc Networks, Elsevier, **5**, *1*, 134-144 (2007).

Mupparapu M., *Bluetooth: The Invisible Connector. Short-Range Wireless Technology for the Contemporary Orthodontic Practice*. Amer. J. of Orthodontics a. Dentofacial Orthopedics, Elsevier, **131**, *6*, 805-808 (2007).

Reaves B., Morris T., *Analysis and Mitigation of Vulnerabilities in Short-Range Wireless Communications for Industrial Control Systems*. Internat. J. of Critical Infrastructure Protection, Elsevier, **5**, *3-4*, 154-174 (2012).

Silva S. *et al.*, *A Bluetooth Approach to Diabetes Sensing on Ambient Assisted Living Systems*. Procedia Comp. Sci., Elsevier, **14**, 181-188 (2012).

Tarn J.M. *et al.*, *Exploring the Implementation and Application of Bluetooth Technology in the Shipping Industry*. Computer Standards & Interfaces, Elsevier, **31**, *1*, 48-55 (2009).

Tay F.E.H. *et al.*, *MEMSWear-Biomonitoring System for Remote Vital Signs Monitoring*. J. of the Franklin Inst., Elsevier, **346**, *6*, 531-542 (2009).

Versichele M. *et al.*, *The Use of Bluetooth for Analysing Spatiotemporal Dynamics of Human Movement at Mass Events: A Case Study of the Ghent Festivities*. Appl. Geograhy, Elsevier, **32**, *2*, 208-220 (2012).

*** Bluetooth v1.0, *Specification of the Bluetooth System. Version 1.0* (1999).

*** Bluetooth v1.2, *Specification of the Bluetooth System. Version 1.2* (2003).

*** Bluetooth v2.0, *Specification of the Bluetooth System. Version 2.0 + EDR* (2004).

*** Bluetooth v2.1, *Specification of the Bluetooth System. Version 2.1 + EDR* (2007).

*** Bluetooth v3.0, *Specification of the Bluetooth System. Version 3.0 + HS* (2009).

*** Bluetooth v4.0, *Specification of the Bluetooth System. Version 4.0* (2010).

*** Bluetooth v4.1, *Specification of the Bluetooth System. Version 4.1* (2013).

DESPRE EVOLUŢIA PROTOCOLULUI DE SECURITATE LA STANDARDUL BLUETOOTH

(Rezumat)

Securitatea informației reprezintă un capitol important din specificațiile standardului Bluetooth. Deci, nu este surprinzător de remarcat că protocolul de securitate cunoaşte o continuă îmbunătățire cu fiecare nouă versiune a acestui standard, fapt impus, într-o măsură mai mare sau mai mică, de dezvoltarea tehnologiei care uşurează atacurile informatice. Acest articol îşi propune să treacă în revistă dezvoltarea securității standardului Bluetooth de la prima variantă a standardului Bluetooth până la ultima variantă v4.1 adoptată în Decembrie 2013.