International Journal of Computing Academic Research (IJCAR)
ISSN 2305-9184 Volume 1, Number 2 (December 2012), pp. 88-95
© MEACSE Publications
http://www.meacse.org/ijcar

Analysis of Security Risks in Bluetooth

Manish Shrivastava
Department of Computer Science & Engineering, Institute of Technology,
Guru Ghasidas University, Bilaspur, CG, India

Abstract
There have been several versions of Bluetooth, with the most recent released definition being Bluetooth 4.0. The released versions differ greatly in bandwidth and the provided security. Since most of the available devices are still implemented according to Bluetooth 2.1 and earlier, this chapter will focus on their analysis. Like WiFi, Bluetooth (BT) operates in the unlicensed 2.4 GHz ISM frequency band. Therefore it is primarily vulnerable to all physical layer Denial of Service (DoS) attacks like channel jamming. As BT implements channel-hopping at a very high rate, changing frequencies about 3200 times per second, it shows some resistance against these DoS attacks.

Keywords: Bluetooth, Authentication, Security key.

1. Introduction

Bluetooth is a wireless technology that allows devices to communicate, or transmit data or voice, wirelessly over a short distance. Bluetooth is intended to provide a common communication medium for technologies in different industries (e.g., computers, mobile phones, and automotive devices). Bluetooth technology was designed primarily to support simple wireless networking of personal consumer devices and peripherals, including cell phones, PDAs, and wireless headsets. Wireless signals transmitted with Bluetooth cover short distances, typically up to 30 feet (10 meters). Bluetooth devices generally communicate at less than 1 Mbps. Bluetooth networks feature a dynamic topology called a *piconet* or *PAN*. Piconets contain a minimum of two and a maximum of eight Bluetooth peer devices. Devices communicate using protocols that are part of the Bluetooth Specification.

Although the Bluetooth standard utilizes the same 2.4 Ghz range as 802.11b and 802.11g, Bluetooth technology is not a suitable Wi-Fi replacement. Compared to Wi-Fi, Bluetooth networking is much slower, a bit more limited in range, and supports many fewer devices. Bluetooth is a specification (IEEE 802.15.1) for the use of low-power radio communications to link phones, computers and other network devices over short distances without wires. A key difference with other existing wireless technologies is that Bluetooth enables combined usability models based on functions provided by different devices.

A key characteristic of Bluetooth that differentiates it from other wireless technologies is that it enables combined usability models based on functions provided by different devices. Again, let us consider a connection between a PDA (computing device) and a cellular phone (communicating device) using Bluetooth and a second connection between the cellular phone and a cellular base station providing connectivity for both data and voice communication. In this model, the PDA maintains its function as a computing device and the phone maintains its role as a communication device - each one of these devices provide a specific function efficiently, yet their function is separate and each can be used independently of the other. However, when these devices are near each other they provide a useful combined function.

2. Bluetooth Specification & Architecture

The Bluetooth Specification defines the requirements ensuring interoperable operation between Bluetooth devices from different manufacturers. The Bluetooth Specification is work-in progress and any material presented here is preliminary and subject to change without notice.1 The Specification is composed of two sets of documents:

Radio and Protocol definitions
Compliance requirements

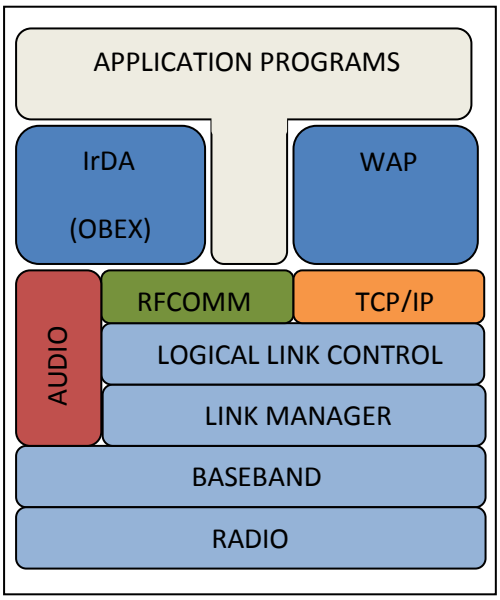

Fig. 1: Application Framework

Figure 1 outlines the application framework in the context of the radio and protocol stack. The Radio takes care of sending and receiving modulated bit streams. The Baseband (BB) protocol defines the timing, framing, packets, and flow control on the link [2]. The Link Manager (LM) assumes the responsibility of managing connection states, enforcing fairness among slaves, power management, and other management tasks. The Logical Link Control handles multiplexing of higher level protocols, segmentation and reassembly of large packets, and device discovery. Audio data is mapped directly on to the Baseband while audio control is layered above the logical link control. Above the data link layer, RFCOMM and network level protocols provide different

communication abstractions. RFCOMM provides serial cable emulation using a subset of the ETSI GSM 07.10 standard. Other parts of the Bluetooth Specification deal with interoperability with other protocols and protocol stacks. Defining TCP/IP over Bluetooth requires that bridging, address resolution, MTU definition, and multicast/broadcast mappings be solved. To accelerate the number of wireless-specific applications, the Bluetooth SIG contemplating interoperability with higher layer IrDA2 andWAP3 protocol stacks.4 For example, IrOBEX defines a transport independent format and session protocol for object exchange and is used as the basis for a variety of applications from exchanging files and business cards to synchronizing address book and calendar schedules. The other part of the Specification defines the compliance requirements. Due to the wide variety of possible Bluetooth devices, different sets of requirements are needed. For example, one would not expect an audio headset to have the same minimum requirements as a notebook computer. The goal of the Specification's compliance section is ensuring any device wearing a Bluetooth "logo" supports a minimum set of benefits for its user.

3. Bluetooth Security

Bluetooth (BT) operates in the unlicensed 2.4 GHz ISM frequency band. Therefore it is primarily vulnerable to all physical layer Denial of Service (DoS) attacks like channel jamming. As BT implements channel-hopping at a very high rate, changing frequencies about 3200 times per second, it shows some resistance against these DoS attacks[1][4]. The BT standard specifies the following three security services:

- **Authentication**: This service authenticates the communicating devices. User authentication is not natively provided by Bluetooth.
- **Confidentiality**: Ensuring that not only authorized devices can access transmitted data, and therefore prevents all kinds of eavesdropping.
- **Authorization**: As bluetooth allows the control connected resources (printers, headphones, etc.), this service assures a device's authorization before allowing it to do so.

The three security services offered by Bluetooth and details about the modes of security are described below. Bluetooth does not address other security services such as audit, integrity, and non-repudiation[1]; if such services are needed, they should be provided through additional means.

3.1 Bluetooth Security Modes

Cumulatively, the BT versions up to 2.1 define four modes of security. Each of these versions supports some of these modes but none of them supports all four.

3.1.1 Security Mode 1

This mode is insecure. Authentication and encryption are bypassed leaving this mode without any security measures at all. Mode 1 is only supported in BT 2.0 + EDR (Enhanced Data Rates) and earlier versions.

3.1.2 Security Mode 2 (service-level enforced)

Mode 2 is designed as a service-level enforced security-mode. It is possible to grant access to some services without providing access to others. It introduces the notion of authorization, the process of deciding if a specific device is allowed to have access to a specific service. A centralized security manager (as defined in the BT architecture) controls access to specific services and devices. The security measures take place after the physical link has been established. Security mode 2 is supported by all Bluetooth devices.

3.1.3 Security Mode 3 (link-level enforced)

This mode mandates authentication and encryption for all connections to and from the device. All security measures take place before the physical link is fully established. Security mode 3 is only supported in Bluetooth 2.0 + EDR and earlier devices.

3.1.4 Security Mode 4 (service-level enforced)

Similar to security mode 2, this mode is enforced on the service level, after the physical link has been established. The pairing mechanism uses Elliptic Curve Diffie Hellman (ECDH) techniques. Services supported by mode 4 must be classified as one of the following:

- Authenticated Link Key required
- Unauthenticated Link Key required
- No security required.

Security mode 4 is mandatory for communication between devices in compliance to Bluetooth 2.1 + EDR or newer versions.

4. Bluetooth Key Management

The various defined Bluetooth security mechanisms require several different keys. Depending on the used security mode, some of them are used to establish the connection and derive a Link Key between two devices. This Link Key can be semi-permanent or temporary. A semi-permanent key might be stored in the nonvolatile memory of a device and therefore used for multiple sessions, while the lifetime of a temporary key is limited to the current session[4][5].

- **K_{AB} - Combination Key**

The Combination Key is derived from information in both connecting devices A and B. It therefore depends on two devices. KAB is derived for each new combination of two devices.

- **K_A - Unit Key**

Contrary to KAB, KA is only derived from the information of a single device. It is generated at the installation of the device and usually very rarely changed.

- **K_{master} - Master Key**

In a point-to-multipoint (Broadcast or Multicast) scenario, a common encryption key (Kmaster) may be used to replace the current Link Keys.

- **K_{init} - Initialization Key**

The Initialization Key should be used to as the Link Key during the initialization process, when no combination or unit keys have been exchanged yet. It protects the transfer of initial parameters. In security modes 2 and 3, this key is derived from the triple of a random number, a PIN code and the device's hardware address.

- **K_{link} - Link Key**

The Link Key is usually a 128-bit random number which is shared between two or more parties as the basis for all cryptographic transactions. It is used in the authentication routine and to derive the Encryption Key K_c.

- **K_c - Encryption Key**

The Encryption Key is used for encrypting all transmissions during a session. It is usually derived from the Link Key Klink.

5. Authentication

The Bluetooth device authentication procedure is in the form of a challenge–response scheme. Each device interacting in an authentication procedure is referred to as either the claimant or the verifier. The *claimant* is the device attempting to prove its identity, and the *verifier* is the device validating the identity of the claimant. The challenge–response protocol validates devices by verifying the knowledge of a secret key—the Bluetooth link key. Figure 2 conceptually depicts the challenge–response verification scheme. The steps in the authentication process are as follows:

Step 1. The verifier transmits a 128-bit random challenge (AU_RAND) to the claimant.
Step 2. The claimant uses the E1 algorithm11 to compute an authentication response using his or her unique 48-bit Bluetooth device address (BD_ADDR), the link key, and AU_RAND as inputs. The verifier performs the same computation. Only the 32 most significant bits of the E1 output are used for authentication purposes. The remaining 96 bits of the 128-bit output are known as the Authenticated Ciphering Offset (ACO) value, which will be used later as input to create the Bluetooth encryption key.
Step 3. The claimant returns the most significant 32 bits of the E1 output as the computed response, the Signed Response (SRES), to the verifier.
Step 4. The verifier compares the SRES from the claimant with the value that it computed.
Step 5. If the two 32-bit values are equal, the authentication is considered successful. If the two 32-bit values are not equal, the authentication fails.

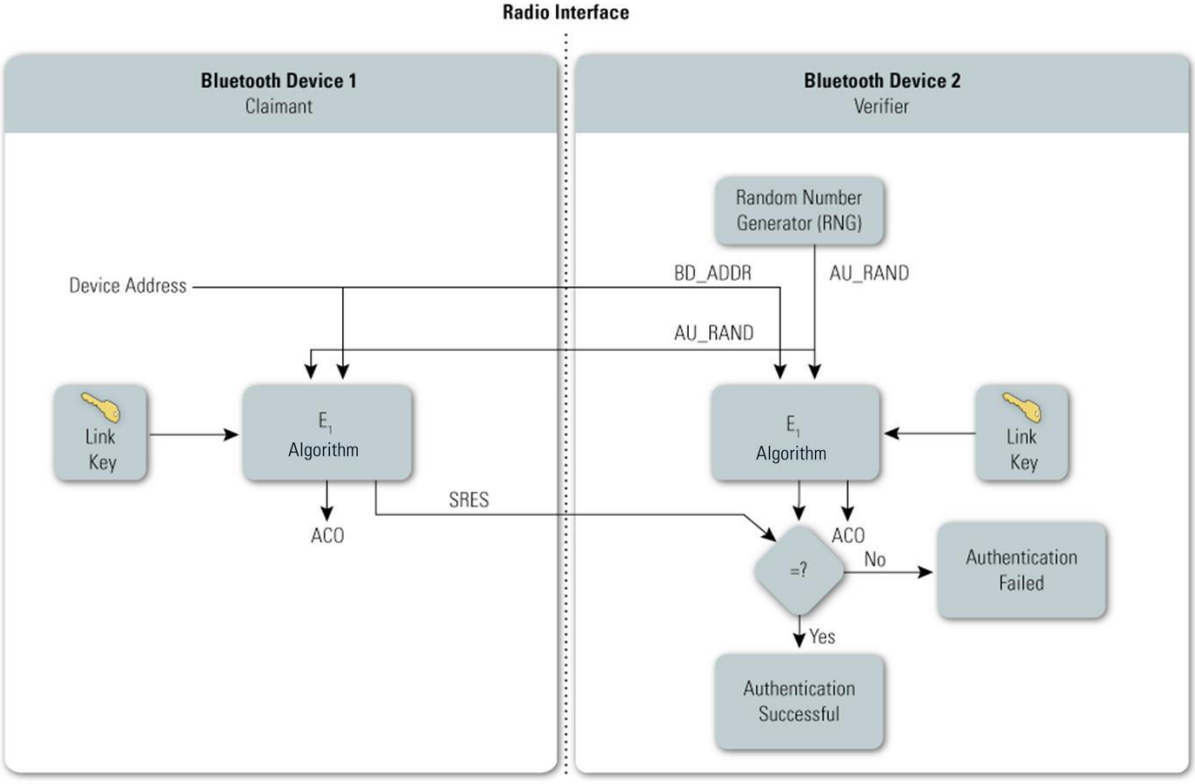

Fig. 2. Bluetooth Authentication

Performing these steps once accomplishes one-way authentication. The Bluetooth standard allows both one-way and mutual authentication to be performed. For mutual authentication, the above process is repeated with the verifier and claimant switching roles. If authentication fails, a Bluetooth device waits an interval of time before making a new attempt. This time interval increases exponentially to prevent an adversary from attempting to gain access by defeating the authentication scheme through trial-and-error with different link keys. It is important to note that this technique does not provide security against offline attacks to determine the link key using

eavesdropped pairing frames and exhaustively guessing PINs. Note that the security associated with authentication is solely based on the secrecy of the link key. While the Bluetooth device addresses and random challenge value are considered public parameters, the link key is not[3]. The link key is derived during pairing and should never be disclosed outside the Bluetooth device or transmitted over wireless links. However, the link key is passed in the clear from the host to the controller (e.g., PC to USB adapter) and the reverse when the host is used for key storage. The challenge value, which is a public parameter associated with the authentication process, must be random and unique for every transaction. The challenge value is derived from a pseudo-random generator within the Bluetooth controller.

6. Confidentiality

In addition to the Security Modes for pairing and authentication, Bluetooth provides a separate confidentiality service to thwart attempts to eavesdrop on the payloads of the packets exchanged between Bluetooth devices. Bluetooth has three Encryption Modes, but only two of them actually provide confidentiality[6]. The modes are as follows:

Encryption Mode 1—No encryption is performed on any traffic.
Encryption Mode 2—Individually addressed traffic is encrypted using encryption keys based on individual link keys; broadcast traffic is not encrypted.
Encryption Mode 3—All traffic is encrypted using an encryption key based on the master link key.

Encryption Modes 2 and 3 use the same encryption mechanism. Security Mode 4 introduced in Bluetooth 2.1 + EDR requires that encryption be used for all data traffic, except for service discovery. The encryption key provided to the encryption algorithm is produced using an internal key generator (KG). The KG produces stream cipher keys based on the 128-bit link key, which is a secret that is held in the Bluetooth devices; a 128-bit random number (EN_RAND); and the 96-bit ACO value. The ACO is produced during the authentication procedure.

The Bluetooth encryption procedure is based on a stream cipher, E0. A key stream output is *exclusive-OR-ed* with the payload bits and sent to the receiving device. This key stream is produced using a cryptographic algorithm based on linear feedback shift registers (LFSRs).12 The encryption function takes the following as inputs: the master device address (BD_ADDR), the 128-bit random number (EN_RAND), a slot number based on the piconet clock, and an encryption key, which when combined initialize the LFSRs before the transmission of each packet, if encryption is enabled. The slot number used in the stream cipher changes with each packet; the ciphering engine is also reinitialized with each packet while the other variables remain static.

7. Analysis of Security Measures in Bluetooth

Security matters differ very strongly between the single versions of Bluetooth. Bluetooth security always depends on the weakest BT device in the communication chain[7]. As legacy-standard devices are still widespread this section will take their vulnerabilities in account as well as of state-of-the-art implementations.

7.1.1 Versions before Bluetooth 1.2

Unit Key and Link Key vulnerability

The Unit Key is reusable and becomes public after once used. This could be circumvented by using temporary broadcast keys, derived from the Unit Key which is kept secret. The same

problem occurs if a corrupt or malicious device that has communicated with either device of a new communication pair, wants to eavesdrop on this communication. The Link Key stays the same for the same device. Various kinds of replay attacks are possible.

7.1.2 Versions before Bluetooth 2.1

This section presents vulnerabilities in Bluetooth standards prior to version 2.1 + EDR. As newer versions, namely 3.0 and 4.0, are still in the process of being standardized, no vulnerabilities have been published yet.

• Short PIN codes are allowed

Short PIN codes can easily be guessed and all derived Link end Encryption keys compromised.

• No PIN management

It is hardly possible to use adequate PINs in an enterprise setting as no PIN management capabilities are defined.

• Keystream reoccurrence

The keystream repeats after 23.3 hours due to a clock overrun allowing various cryptographic attacks on the ciphertext.

8. Conclusion

No User Authentication by default, no user authentication is defined by BT standards. Application level security and authentication needs to be added. The used stream cipher function SAFER+ has been subject to vulnerabilities and needs to be replaced by a more robust solution to prevent cryptographic attacks. One-way challenge-response authentication can easily be exploited by man in-the-middle (MITM) attacks. Mutual authentication should be enforced. No end-to-end encryption is provided in multi-hop scenarios. Transmissions are only encrypted between two nodes. Higher level solutions need to be deployed. Services such as non repudiation are not defined by BT standards. They can only be implemented in an overlay fashion. the occurrence of vulnerabilities is too high to allow its implementation in security-critical systems. The deployment of Bluetooth poses a serious security risk especially for enterprise settings. Even though BT can be regarded secure if all devices are configured properly.

References

[1] J. Dunning. Taming the Blue Beast: A Survey of Bluetooth Based Threats. IEEE Security & Privacy Magazine, 2010.

[2] J. Hallberg, M. Nilsson, and K. Synnes. Positioning with Bluetooth. In 10th International Conference on Telecommunications, 2003, pp.954-958, 2003.

[3] G. Hancke and M. Kuhn. An RFID Distance Bounding Protocol. In Security and Privacy for Emerging Areas in Communications Networks, pp.67-73, 2005.

[4] IEEE. 802.15.1 IEEE Standard for Information technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements Part 15.1: Wireless medium access control (MAC) and physical layer (PHY) specific , 2005.

[5] P. Kitsos, N. Sklavos, K. Papadomanolakis, and O. Koufopavlou. Hardware Implementation of Bluetooth Security. IEEE Pervasive Computing, 2003.

[6] A. Kotanen, M. Hannikainen, H. Leppakoski, and T. Hamalainen. Experiments on local positioning with Bluetooth. In Proceedings ITCC 2003, International Conference on Information Technology: Coding and Computing, pp. 297-303, 2003.
[7] S. Pasanen. New Efficient RF Fingerprint-Based Security Solution for Bluetooth Secure Simple Pairing Security, pp.1-8, 2010.