2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing

Pairing and Authentication Security Technologies in Low-Power Bluetooth

Junfeng Xu, Tao Zhang, Dong Lin, Ye Mao, Xiaonan Liu, Shiwu Chen, Shuai Shao, Bin Tian and Shengwei Yi
China Information Technology Security Evaluation Center, Beijing, China, 100085
Email: {Xujf, Zhangt, Lind, Maoy, Liuxn, Shaosh, Tianb, Yisw}@itsec.gov.cn

***Abstract*—With the release of up-to-date Low-Power (LP) bluetooth 4.0, Bluetooth Technologies are not only widely deployed on personal area devices such as the smart phone, the headset, the intelligent health-care equipment etc., but also are recommended as a standard communication protocol in the Internet of Things. However, due to the inherent limitation in the bluetooth protocol, the network designer must face critical vulnerabilities which might bring serious security issues. This paper describes the security features of the bluetooth 4.0 protocol and analyses pairing and authentication security technology in the LP bluetooth 4.0. The security vulnerabilities and security recommendations concerning to the pairing and authentication process of the bluetooth devices are presented. In the end, the countermeasures are proposed to mitigate the risk.**

Key words: Bluetooth 4.0, Information Technology Security, Low-Power, High Speed, vulnerability.

I. Introduction

With the Bluetooth short-range wireless technology becoming more sophisticated [1], a variety of wireless communication technologies play an increasingly important role in the field of information technology in automation control and family, and has become the cornerstone of the Internet of Things (IoT). Experts form industry and academia have been showing their concerns about Bluetooth security issues since the birth date of the Bluetooth technology.

Bluetooth 3.0 technology was released by Bluetooth SIG in April 2009 [2]. The technology can provide about $100M$ high-speed communication for Bluetooth devices. Then the official Bluetooth 4.0 technology was released on July 7, 2010. Unlike some other communication technologies, it is a zero cost technology, which means no royalty fee has to be paid for deploying the technologies[3], [4], [5]. Bluetooth SIG chief Suke Jawanda Chairman has said, Bluetooth connection is an important part of the Internet of Things in transferring data to the network services and applications[6], [7], [8].It is estimated that the cumulative shipments of Bluetooth devices will reach 20 billion by 2017. At present, the percentage of configuring Bluetooth devices in smart phones is close to 100%, and by 2014, 90% of the notebooks will also be fitted with Bluetooth devices. However, Low-Power Bluetooth 4.0 Security presents a new feature. Compared with the previous technical standards, Bluetooth 4.0 applies a Low-Power transformational technology.

In recent years, experts from academia have carried out a lot of research work. Bluetooth technology and related equipment suffer from vulnerable wireless network threats [9], such as denial of service attacks, eavesdropping, an intermediate device attack, message modification and resource abuse [10]. In addition, the Bluetooth devices are facing a more specific attack against themselves, such as: (1) Bluesnarfing [10], [11]. This attack is forced to connect to a Bluetooth device which allows to access storage devices including data on International Mobile Equipment Identification (IMEI).(2) Bluejacking [12]. Attacker via Bluetooth sends unsolicited messages to the user to start the Bluejacking program. When a user sends a response Bluejacking message, Bluejacking will start and harm the Bluetooth device. (3) Bluebugging [13]. This device attacking command notifies the user and allows attackers to access data and phone calls, to eavesdrop on phone calls, to send messages and use other services or functionality of the device. (4) Denial of Service [14]. Bluetooth is vulnerable to DoS attacks. As a result, Bluetooth device interfaces cannot be used anymore and batteries may be depleted. (5) Fuzzy Bluetooth attacks [15],which sends a malformed or other nonstandard data to the device's Bluetooth wireless Bluetooth devices, and then listens to how to react.

This paper summarizes the general security issues on the bluetooth technology. Especially, it describes the security features of the bluetooth 4.0 protocol and analyses pairing and authentication security technology in the LP bluetooth 4.0. The security vulnerabilities and security recommendations concerning to the pairing and authentication process of the bluetooth devices are presented. In the end, the countermeasures are proposed to mitigate the risk.

The remainder of this paper is organized as follows. In Section , II, the new security features of the LP Bluetooth 4.0 are described. Section presents LP Bluetooth 4.0 security vulnerabilities and proposes security recommendations for mitigating the vulnerabilities. Finally, the concluding remarks are given in Section IV.

978-0-7695-5046-6/13 $26.00 © 2013 IEEE
DOI 10.1109/GreenCom-iThings-CPSCom.2013.185

II. The new security features of the Low-Power Bluetooth 4.0

Due to limited computing and storage ability of Low-Power Bluetooth devices, its security technology is different with traditional BR/EDR/HS Bluetooth. One difference is that the Low-Power Bluetooth pairing results in Long-term Key (LTK), instead of the link key, which fundamentally performs the same secret key function as a link key. LTK is established in different ways. It is generated by using a key transport protocol, rather than using the BR/EDR negotiation. In other words, the Bluetooth device determines LTK. The pairing process will be sent to another Bluetooth device, rather than generating separate keys for the same two devices. A Bluetooth specification, the Low-Power Bluetooth first describes how to use the Advanced Encryption Standard-Counter with CBC-MAC (AES-CCM). In addition to providing a strong, standard-based encryption, AES-CCM for local Low-Power Bluetooth devices FIPS-140 validation paves roads of the future.

The Low-Power Bluetooth device also introduces a dedicated device address and signature functions. Called identity to solve key (IRK) and connect the new encryption key signatures solve key (CSRK) to support these functions. IRK is used to solve the public address mapping to the specialized equipment. This allows trusted devices to determine from the public (random) device into a dedicated device address. The new security features for a particular device provides secure privacy. Prior to this, the device will be assigned a static address in the search process. If the device remains can be found, its location can be opponents track. CSRK used data from a specific device authentication cryptographic signature frame. Bluetooth connectivity which allows the use of the data signature (integrity and authentication) to protect the connection instead of the connection data encryption, the AES-CCM provides confidentiality, integrity and authentication.

A. Security mode and level of the Low-Power Bluetooth 4.0

Low-Power Bluetooth security mode is similar to the level of security of the BR/EDR mode (Security Mode 2 and 4), which can have its own security requirements for each service. However, Low-Power Bluetooth also specifies each service request can have its own security requirements. Equipment to enforce the service following the appropriate security mode and level of security requirements.

Low Power Security Mode 1 has a plurality of encryption-related level. Level 1 does not specify the security, which means that no authentication and encryption. Level 2 requirements to unauthenticated paired encryption. Level 3 requirements with encrypted authentication.

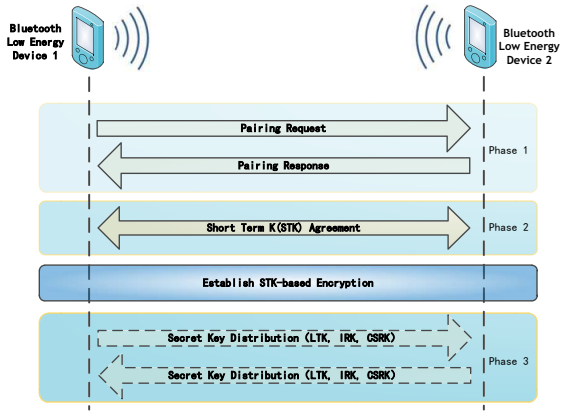

Figure 1. Pairing process of two LP Bluetooth devices

The low power security mode 2 has a signature associated with the data at multiple levels. Data signature provides a powerful data integrity, but not confidentiality. Level 1 requirements unauthenticated data signature matching. Level 2 requires an authenticated signature matching and data.

If a service request and related services with different security model and (or) levels, and more powerful security requirements. For example, if any demand need security mode level 3, then Security Mode 1 Level 3 requirements be enforced.

B. Pairing of Low-Power Bluetooth 4.0

Although the Low-Power Bluetooth BR / EDR SSP similar pairing method name, but Low-Power Bluetooth pairing based on ECDH encryption technology, and provides no eavesdropping protection. Therefore, if the attacker can capture Low-Power Bluetooth pairing frame, you may be able to determine generates LTK. Because Low-Power Bluetooth pairing key transport key agreement is adopted instead of a key agreement, key distribution steps are required in the Low-Power Bluetooth pairing. Figure 1 two devices, low power Bluetooth pairing start reaching the temporary key (TK), its value depends on the the pairing method being used. Then switching equipment random value, generated based on these short-term value and TK key (STK). Link and then use the STK encryption, which allow secure key distribution IRK LTK and CSRK.

C. The key generation and distribution of Low-Power Bluetooth 4.0

Once the link is encrypted using the STK, two equipment distribution key as LTK, IRK, and CSRK. Two options are specified before distribution key generation. The device may simply generate a random 128-bit value, and stores them in the local database. Another option is, with each of the 16 different (DIV) only trusted device to generate a key, use

of a single 128-bit static but random values, it is called the encrypted root (ER). This option is referred to as the key hierarchy. For example, the key can be derived from the ER and DIV using the following formula:
$LTK = d1(ER, DIV, 0)$
$CSRK = d1(ER, DIV, 1)$
$IRK = d1(IR, 1, 0)$
Where $d1$ is known as the diversified functions based AES 128 encryption. Use this key hierarchy, the Bluetooth device does not require more than 128 trusted Bluetooth devices stored for each key equipment; contrary, it only needs to store each device its ER and unique DIV. During reconnect, remote device sends its DIV. Local device can then be regenerated from the ER and through the DIV LTK and/or CSRK of. If data encryption or signature is successfully set up, it can verify that the correct remote devices LTK or CSRK of. If unsuccessful, the link will be discarded.

D. Low-Power Bluetooth 4.0 confidentiality, authentication and integrity

AES-CCM in the Low-Power Bluetooth is used to provide confidentiality, and each packet authentication and integrity. No separate authentication challenge / response steps and BR/EDR/HS used to verify whether they have the same LTK or CSRK of. LTK provide implicit authentication is used as input the encryption key, successful encryption settings. The same, although it does not provide confidentiality, but the success of the data signature remote device to provide implicit authentication holds correct CSRK. Versions of Bluetooth technology, in addition to many well-known vulnerabilities such as PIN too short, PIN management deficiencies, encryption key stream recycling vulnerability, but also there are some little-known loophole. These loopholes to bring the convenience of the user, and gave the attacker a shortcut.

- Modes weak protection: ”Just Works” associated mode during pairing provides MITM protection, which will result in unauthenticated link key. In order to obtain the highest level of security, Bluetooth devices in the SSP during MITM protection, and refused to accept the ”Just Works” unauthenticated link key pairs generated upon request.
- Weak password generated: SSP ECDH key may be static or weak generation. Weak ECDH key SSP eavesdropping protection minimized, which allow the attacker can determine the secret link key. All equipment shall have a unique, strong generates ECDH key pair.
- Password static: static SSP key to MITM attacks facilitated. Key MITM protection during the SSP, even when you do not need to re-key Bluetooth devices, while still using the last connection key. Bluetooth devices for each pair is connected using the random, unique key. Allowed to fall back to any other security mode? Mode switching vulnerabilities: security mode devices connection does not support security mode 4 Bluetooth devices. Then, the worst case will fall device to return to the security mode, it provides no security authenticated connection.
- Key compromise: connection authentication attempts repeatable. Bluetooth devices need to include a mechanism to prevent unrestricted identity verification request. Bluetooth specification requires that the wait interval between attempts to exponential growth in continuous identity verification. However, it does not require the kind of waiting interval of authentication the suspect requests, so the attacker can collect a large number of suspected response (which the confidential link key encryption), may leak information about the secret link key information.
- Broadcast secret sharing: for broadcast encryption master key is shared between all the micro-network equipment. Secret key shared between two or more of the Parties to provide favorable conditions for the simulated attack.
- The vulnerability: encryption algorithm used for E0 stream cipher algorithm Bluetooth BR/EDR encryption more vulnerable. Bluetooth BR/EDR FIPS-approved encryption stratified by application-level FIPS-approved encryption available. User information leaks ”If the Bluetooth device address (BD_ADDR) is captured and associated with a particular user, privacy may be affected. Once (BD_ADDR) associated with a specific user, the user’s activities and locations may be tracked.
- Equipment certification attack: device authentication is simple shared key suspect in the response. One-way-only suspect that the response to the authentication part of MITM attacks. Bluetooth provides mutual authentication, it should be used as a verification device and network legitimacy.

III. Security vulnerabilities and Recommendations in Low-Power Bluetooth 4.0

Pairing of Low-Power Bluetooth technology providing eavesdropping protection; ”Just Works pairing method does not provide MITM protection. If the wiretap was successful, the eavesdropper can capture in Low-Power pairing process allocation key (for example, LTK, CSRK, IRK). In addition, MITM attacker can capture and tamper with data transmitted between trusted devices. The Low-Power devices should be paired in a security environment, to minimize the risk of of pairing eavesdropping and MITM attack.

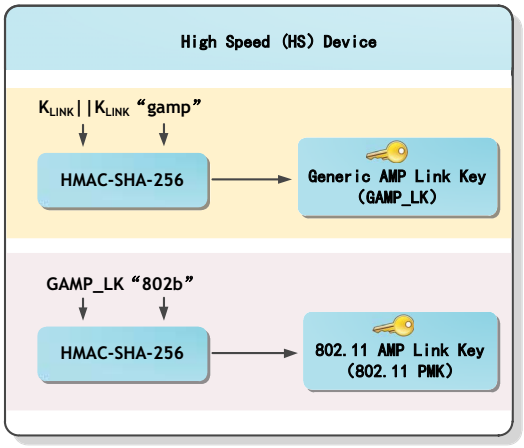

Figure 2. ($GAMP\_LK$) using Bluetooth link key series and extended the ascii code key identifier (keyID).

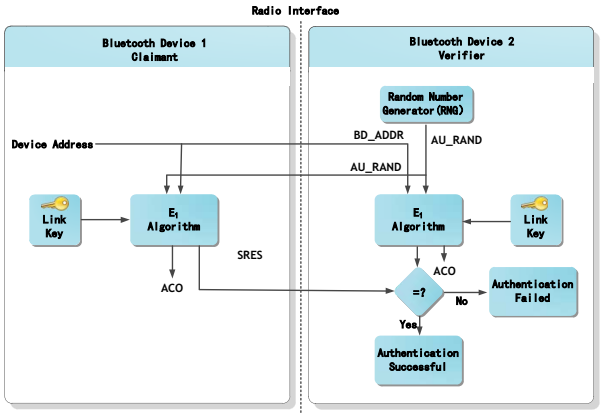

Figure 3. The challenge-response authentication scheme.

Low-Power security mode level 1 does not require any security mechanism (ie no authentication or encryption). Essentially this is unsafe, any attacker can freely in this mode level access to the Bluetooth device is similar to the BR/EDR security mode.

(1) Bluetooth link key AMP link key derivation Derived from Bluetooth link key link security for AMP, AMP link security key (for example, IEEE 802.11) Bluetooth version 3.0 is introduced. Whenever the Bluetooth link key is created or changed by the generic AMP link key ($GAMP\_LK$), is generated the AMP manager in the host stack. As shown in Fig. 2, ($GAMP\_LK$) using Bluetooth link key series (and itself) and extended the ascii code key identifier (keyID), "gamp" as the input function HMAC-SHA-256. Then the generic AMP link key and keyID of derive a special AMP link key (for specific AMP and trusted combination of equipment). 802.11 AMP link key, keyID "802b". IEEE 802.11 AMPs, AMP dedicated link key to use as 802.11 Pairwise Master Key.

(2) Bluetooth authentication and key management The verification process of the Bluetooth device is in the form of a challenge-response strategy. Each interaction device called the applicant in the process of authentication or verification procedures. The applicant is an attempt to prove its identity verification process is an authentication application equipment. Challenge-response protocol verification equipment through a secret knowledge of the validation key - the Bluetooth link key. Fig. 3 depicts the challenge-response authentication scheme.

Table I provides five security vulnerabilities associated with Low-Power Bluetooth 4.0. It also provides a Bluetooth security checklist with guidelines and recommendations for creating and maintaining secure Bluetooth piconets. For each recommendation or guideline in the checklist, a justification column lists areas of concern for Bluetooth devices, the security threats and vulnerabilities associated with those areas, risk mitigations for securing the devices from these threats, and vulnerabilities.

IV. Concluding Remarks

In this paper, we investigate the security features of the bluetooth 4.0 protocol and analyse pairing and authentication security technology in the LP bluetooth 4.0. Addressing the pairing and authentication process of the bluetooth devices, the security vulnerabilities and security recommendations are proposed. In order to mitigate the risk, we also propose the countermeasures.

References

[1] M. Tan and K. Masagca, "An investigation of bluetooth security threats," in *2011 International Conference on Information Science and Applications (ICISA)*, pp. 1–7, Apr. 2011.

[2] C. Douligeris and D. Serpanos, "Current status and future directions," *Network Security*, pp. 608 – 616, 2010.

[3] C. Hager and S. Midkiff, "An analysis of bluetooth security vulnerabilities," in *2003 IEEE International Conference on Wireless Communications and Networking (WCNC 2003)*, pp. 1825–1831, Mar. 2003.

[4] C. Hager and S. Midkiff, "Demonstrating vulnerabilities in bluetooth security," in *2003 IEEE Global Telecommunications Conference (GLOBECOM 2003)*, pp. 1420– 1424, Dec. 2003.

[5] E. Vergetis, R. Guerin, S. Sarkar, and J. Rank, "Can bluetooth succeed as a large-scale ad hoc networking technology," *IEEE Joural on Selected Areas in Communications*, vol. 23, no. 3, pp. 644–656, 2005.

Table I
SECURITY VULNERABILITIES, RECOMMENDATIONS AND JUSTIFICATIONS IN LOW-POWER BLUETOOTH 4.0

	Security Vulnerability	Security Recommendation	Security Need, Requirement, or Justification
1	Encryption key length is negotiable.	Choose PIN codes that are sufficiently random, long and private. Avoid static and weak PINs, such as all zeroes.	PIN codes should be random so that malicious users cannot easily guess them. Longer PIN codes are more resistant to brute force attacks. For Bluetooth devices, an eight-character alphanumeric PIN should be used, if possible. The use of a fixed PIN is not acceptable.
2	End-to-end security is not performed.	Invoke link encryption for all Bluetooth connections.	Link encryption should be used to secure all data transmissions during a Bluetooth connection; otherwise, transmitted data are vulnerable to eavesdropping.
3	Security services are limited.	Service and profile lockdown of device Bluetooth stacks should be performed.	Many Bluetooth stacks are designed to support multiple profiles and associated services. The Bluetooth stack on a device should be locked down to ensure only approved profiles and services are available for use.
4	LE pairing provides no eavesdropping protection. Further, the Just Works pairing method provides no MITM protection.	For v2.1 and later devices using SSP, avoid using the "Just Works"?association model. The device must verify that an authenticated link key was generated during pairing.	The Just Works?association model does not provide MITM protection. Devices that only support Just Works should not be procured if similarly qualified devices that support one of the other association models are available.
5	LE Security Mode 1 Level 1 does not require any security mechanisms	LE devices and services should use Security Mode 1 Level 3 whenever possible. LE Security Mode 1 Level 3 provides the highest security available for LE devices	Other LE security modes allow unauthenticated pairing and/or no encryption.

[6] H. Chun-Liang, Y. Sheng-Yuan, and W. Wei-Bin, "Constructing intelligent home-security system design with combining phone-net and bluetooth mechanism," in *2009 International Conference on Machine Learning and Cybernetics*, pp. 3316–3323, Jul. 2009.

[7] M. Othman, W. Hassan, and A. Abdalla, "Developing a secure mechanism for bluetooth-based wireless personal area networks (wpans)," in *2007 International Conference on Electrical Engineering (ICEE 2007)*, pp. 1–4, Apr. 2007.

[8] X. Li, R. Lu, X. Liang, X. Shen, J. Chen, and X. Lin, "Smart community: an internet of things application," *IEEE Communications Magazine*, vol. 49, no. 11, pp. 68–75, 2011.

[9] N. Anand, *An Overview of Bluetooth Security*. SANS Institute 2000-2002, 2001.

[10] P. Suri and S. Rani, "Bluetooth security - need to increase the efficiency in pairing," in *2008 IEEE Southeastcon,*, pp. 607–609, Apr. 2008.

[11] S. Liong and P. Barnaghi, "Bluetooth network security: A new approach to secure scatternet formation," in *2005 IEEE Region (TENCON 2005)*, pp. 1–6, Nov. 2005.

[12] T. OConnor and D. Reeves, "Bluetooth network-based misuse detection," in *2008 Annual Computer Security Applications Conference (ACSAC 2008)*, pp. 377–391, Dec. 2008.

[13] A. Aragues, J. Escayola, I. Martinez, P. Valle, P. Munoz, J. Trigo, and J.Garcia, "Trends and challenges of the emerging technologies toward interoperability and standardization in e-health communications," *IEEE Communications Magazine*, vol. 49, no. 11, pp. 182–188, 2011.

[14] M. Chaudhry, S. Murawwat, F. Saleemi, S. Tariq, M. Saleemi, and F. Chaudhry, "Power optimized secure bluetooth communication," in *IEEE International Multitopic Conference (INMIC 2008)*, pp. 182–188, Dec. 2008.

[15] J. Padgette, "Bluetooth security in the dod," in *IEEE Military Communications Conference (MILCOM 2009)*, pp. 1–6, Oct. 2009.