Analysis and improvement of the Security Capability of Bluetooth System

Shengsheng Li 1*, Yongyan Cui 1
1Nari group corporation/state grid electric power research institute, Nanjing, China

*Corresponding author e-mail: lishengsheng@sgepri.sgcc.com.cn

Abstract: The security capability is a very important matter of the Bluetooth system. The factors that can affect the security of the system are manifold. The author of this paper makes a detail on the security capability of the Bluetooth system and analyzes the potential problems with the system. The author points out that because of the small value space of the initial key, it is vulnerable to the brute attack and that its key exchange protocol is very susceptible on the beginning phrase to the DOS attack due to time delay in the channel. Finally, the author proposed that the public key scheme introduced to solve the problem in the Bluetooth system.

1. Introduction

The goal of the Bluetooth system is to provide a unified interface for the transmission of personal data, so the security of data transmission becomes an important issue [1]. With the popularity of Bluetooth devices and the openness of wireless transmission, it is necessary for the Bluetooth system to provide an authentication process to ensure the security of the system. At every stage in communication, any unauthorized device should not be given sensitive data.

Bluetooth system authentication, data encryption and data modulation methods provide the security assurance for data transmission, however, most authentications is based on link layer security control, and it is difficult to achieve uniformity in the current application phase. This paper mainly discusses the security of the system from the generation of system keys and data encryption.

In order to ensure the security of the Bluetooth system, the system applies the following four variables: device address (48bit), authentication key (128bit), encryption key (8~128bit) and a random number. To ensure the security of the key, you cannot use direct inquiry. Then the following describes the key generation and exchange process:

(1) Through PIN (Personal Identity Number), the length of PIN and a random number yields the initial key.

(2) The authentication process uses the inquiry/response method, and the authenticator sends a
random number to the applicant. If the applicant's device address and initial key authenticator are known, then the returned number should be consistent with the results produced by the authenticator.

3. The applicant can also initiate reverse authentication to the authenticator.

4. Each Bluetooth device has a unit key. The party of the session gives the unit key to the other party by initial key encryption.

5. The other party sends its own unit key to the other party in the same way and generates a connection key through the unit key.

6. The data encryption key is generated directly from the unit key or generated by a composite. This connection key will be stored for use in future sessions.

2. Connection key generation

2.1. Initial key generation

In the Bluetooth system, the connection key is generated by the initialization key and the unit key at initialization [2]. Moreover, the initialization key is only used during the connection establishment process and is used only once. The generation of its initialization key is shown in Figure 1. L is the length of the PIN. RAND is a random number given by the authenticator. The connection to the Bluetooth system is most vulnerable when it is first established, because at this time, the generation of the initial key has a great relationship with the PIN. RAND is issued by the authenticator in clear text and is easily accessible to attackers. For PIN, it is generally no more than 16 bytes. For the average user, there may be not many digits of PIN. Therefore, an attacker can gain K-init by attacking the PIN, and then attack the system more deeply.

![Figure 1. Initialization key generation](image)

2.2. Certification process

In Bluetooth technology, device authentication is done through a shared key between two devices. This type of key is called a "connection key" in Bluetooth technology. The connection key is established through a dialogue between devices. A connection key is shared between the two communication devices. There are two types of connection keys, one called "unit key" and the other called "composite key". A device with a unit key as a connection key is generally small in storage. In this case, only the unit key of one device is used as the connection key. The composite key is unique to both devices communicating. The composite key ensures that communication is between the two devices. Communication with a composite key as a connection key is much safer than communication...
with a unit key as a connection key. When master communicates with server1, the key between them is k master, that is, the unit key of the master (UNIT KEY) is used as the connection key. When Master and server 2 communicate, the key between them is also k master, so when master and server 1 communicate, server 2 can listen.

Bluetooth authentication is through the method of "inquiry/answer", which is established by the algorithm. The algorithm used is an improved version of the grouping algorithm SAFER+ and the certification process is shown in Figure 2.

![Figure 2. Certification process](image)

A sends B a 128-bit random number AU- RAND, B puts the physical address of AU- RAND called BD- ADDR- B and LINK KEY into E1, then get SRES- B and send it to A. At the same time, A also inputs AU- RAN D and BD- ADDR- B as well as LINK KEY into E1 to get SRES- A. Compare SRES- A and SRES- B in A, if they are equal, the authentication from A to B ends. And authentication is two-way in Bluetooth systems.

2.3. Unit key generation

Each Bluetooth system has a unit key [3], which is generated when the device is first run and stored in the device's permanent memory. In general, this unit key is constant throughout the life of the device (of course, for security reasons, or for other reasons, may need to be changed). The unit key is generated as shown in Figure 3. The unit key is generated by a 128-bit random number and a device physical address of 48 bit through the algorithm E21.

![Figure 3. Unit key generation](image)
2.4. connection key generation

With the unit key, the connection key can be generated in two ways [4].

(1) If the system has limited memory space, then you can consider the unit key which is one of the conversation devices as the connection key. The process is shown in Figure 4.

![Figure 4. Unit key as the connection key](image)

The connection key between device A and device B is the unit key of device A.

(2) If the system memory allows and from a security point of view, the unit key of system A and system B generate a connection key through the composition.

In this process, both sides of the session generate a random number, and then generate the respective unit key of 128 bit through the E21 algorithm. After the initial password is encrypted, it is exchanged with the other party, then the unit key of the other party is different from its own unit key, and the connection key is obtained.

3. Encryption key generation and data encryption

The encryption key is generated by the current used connection key, the calculation of the offset number (COF) and random number of 128 bit generated by algorithm E3[6]. If the current used connection key is the server's key, the COF is obtained from the server's device address; otherwise it is obtained by the authentication calculation offset. And its production is shown in Figure 5.

![Figure 5. Generation of encryption keys](image)

However, in Bluetooth systems, data encryption does not directly use the encryption key generated. Instead, the data is encrypted by the manner shown in Figure 6, and the key stream
changes with the transmission of each packet due to the participation of time variables.

![Figure 6. Encryption of the data stream](image)

Each Bluetooth system has a 128-bit clock that beats 3,200 times per second. This clock is never adjusted and will never be turned off. The accuracy of this clock is generally ± 20ppm. If it is in low energy state, its accuracy will drop to ±250ppm. Based on this, the attacker can adjust the clock of the system through low-energy laser or electromagnetic pulse, thus destroying the normal operation of the system[7].

4. System security performance improvement

As can be seen from the above statement, the security risks of the Bluetooth system mainly come from the process of generating the session key. Because of the characteristics of the symmetric key, it is convenient for the opponent's exhaustive attack (dictionary attack) against PIN. In order to overcome this drawback, it can be done using a key exchange protocol based on a public key system. Suppose that server 1 and server 2 share a common password P:

1. Server 1 generates a random public key/private key pair. Encrypt the public key K obtained randomly with P, and send the encrypted result to server 2:

   \[ A_{\text{server}1}, E_P(K) \]

2. Since server 2 knows P, it can decrypt the message K, then randomly generate the session key X, encrypt X with the public key and P obtained from server 1, and send it to server 1:

   \[ E_P(E_K(X)) \]

3. Server 1 decrypts to get X, then generates a random number \( R_{\text{server}1} \), encrypts it with X, and sends it to server 2:

   \[ E_X(R_{\text{server}1}) \]

4. Server 2 decrypts this message, then generates another random number \( R_{\text{server}2} \), encrypts the two random numbers \( R_{\text{server}1}, R_{\text{server}2} \) with X, and gives the result to server 1:

   \[ E_X(R_{\text{server}1}, R_{\text{server}2}) \]

5. Server 1 decrypts the message to get \( R_{\text{server}1} \), \( R_{\text{server}2} \), and confirms whether \( R_{\text{server}1} \) is sent by itself. If it is sent by itself, encrypt \( R_{\text{server}2} \) with X and send it to server 2:

   \[ E_X(R_{\text{server}2}) \]

6. Server 2 decrypts and compares whether \( R_{\text{server}2} \) is sent by itself. If yes, the protocol is completed, and both parties use X as the session key to communicate.

Between server 1 and server 2, if the third party Eve is eavesdropping, then what he gets is only \( E_P(E_K(X)), E_P(K) \), and some messages encrypted with X. Eve can guess P, but the
correctness of the guess cannot be confirmed without deciphering the public key algorithm. The implementation of this protocol can be implemented by RSA which is based on large number decomposition, or by EL Gamal based on discrete logarithm.

Of course, if an authentication server is added to the network as a public key management and distribution center, the system session key generation will be more efficient and convenient, but this will bring unnecessary hardware overhead.

5. Conclusion

From the above analysis of the key generation and data encryption of the Bluetooth system, it can be seen that the weakest link of the whole system is vulnerable to attack during the establishment phase of the session. If the system uses the unit key as the connection key, it is also vulnerable. Therefore, although it is relatively simple to use the unit key as the connection key, from a security perspective, the SIG does not agree with this approach. After the session is established, the connection key will not change anymore, even if the two devices communicate in the future, the connection key established at the first session will be used, and this also provides conditions for replay attacks. Therefore, the security of the Bluetooth system still needs to be improved.

Acknowledgments

This work is supported by Science and Technology Project of State Grid Corporation of China.

References

[1] Zhuang Yuqi. Bluetooth - Dreams and Reality[M] . Beijing: Mechanical Industry Press, 2002, 195-199.
[2] Gareth Barlow. Bluetooth security[C]. Network and internet work security report, April, 2000: 10-17.
[3] Thomas. Moller. Bluetooth security[C]. Proceedings Bluetooth '99, London, June 1999: 2-18.
[4] Anita Jones. A case study of wireless personal area network security [J]. Bluetooth security. April, 2001,253-268.
[5] Jin Chun, Xu Guangchen. Bluetooth technology[M]. Beijing: Publishing House of Electronics Industry, 2001, 69-75.
[6] Bellovin SM , Merritt M . Encrypted key exchange: password-based protocols secure against dictionary attacks [C]. Proceedings of the 1992 IEEE computer society conference on research in security and privacy, 1992, 72-84.
[7] (US) Schneier B, Wu Shizhong translation. Applied Cryptography[M]. Beijing: Mechanical Industry Press, 2001, 371-373.