Available online www.jocpr.com

Journal of Chemical and Pharmaceutical Research, 2014, 6(6):1380-1386

Research Article

ISSN : 0975-7384
CODEN(USA) : JCPRC5

The security analysis and improvements of link connection mechanism for mobile phone bluetooth transmission

Rui Zhang[1], Jian Wei Wang[1], Yaobin Xie[2] and Lizhong Wang[2]

[1]North China University of Water Resources and Electric Power, Zhengzhou, Henan, China
[2]Information Engineering University, Zhengzhou, Henan, China

---

ABSTRACT

The development of mobile communication technology has become a dazzling star in the information field. Especially for the third-generation mobile communication, Mobile phone Bluetooth is a highly-anticipated technology, with wide application prospects and potential economic value. Bluetooth mobile phone is incredibly good at connecting wirelessly to other terminal equipments and transferring data between devices very near each other. Meanwhile, the security of mobile phone Bluetooth transmission becomes the concern of the current users, and ensuring the security of Mobile phone Bluetooth transmission is also a problem to be solved urgently. In this paper, the file transport mechanism of Mobile phone Bluetooth is the main research object. Based on link protocol, using the security analysis of link connection mechanism, this paper improved the Personal Identification Number (PIN) input from the user interface, in order to enhancing the security of link connection mechanism of the underlying file transfer protocol.

Key words: mobile phone Bluetooth, Link Management Protocol (LMP), Personal Identification Number, attack

---

INTRODUCTION

With the development of information technology, convenient, fast, efficiently has become the basic requirement of all kinds of information equipment. The using of mobile communication devices has a great effect on people's study, work and life. To realize resource communion between Mobile phone and other electronics is the electrifying dynamics of the production of Bluetooth mobile phone. Bluetooth mobile phone really provides us great convenience, which can realize the interconnection between terminal facilities from different manufacturers. Across the space constraints is the biggest advantage of Bluetooth network. Nevertheless, people suffered from the security threats of Bluetooth system while enjoying the convenience and efficiency brought by the Mobile phone Bluetooth network. In the range of Bluetooth network, the important confidential information can be issued by the users of Bluetooth mobile phone, and Secret unit faces a serious risk of information leakage; in addition, at begging of the connection establishment of file transfer, malicious attackers can attack the Bluetooth mobile phone, which weaken security of file transfer mechanism. Consequently, to ensure the security of the Bluetooth mobile phone file transmission is particularly important and urgent.

The date stored in the Bluetooth mobile phone can be sent without any Security leak prompts. The emergence of FM technology and PIN code authentication improved the security of mobile phone Bluetooth transmission. Nevertheless, in the influence of the realization of application development and the habits of users, malicious attackers can damage the link protocol security by monitoring all messages of link layer authentication between different Bluetooth devices.

RESEARCH STATUS

Bluetooth network and the internet have the same security target. In order to realize the security feature, similar to the wired communication, three types of data transmission safe modes were defined in the underlying and the top Bluetooth network. But these works cannot ensure that the Bluetooth network leaks hardly and keeps safe from attacks. In the application of Bluetooth, with irregular dynamic variation of Bluetooth network topology and non-directional data transmission, ensuring effective data security is the challenge for Bluetooth networks.

The Bluetooth network security policy mainly aims at four secure entities contained in link layer of Bluetooth protocol: Bluetooth device address, two user private keys and random number [1]. There are serious securities threats remain, through these four secure entities provide certain security arrangements for Bluetooth security. The two reasons [1]: (1) the starting point of the product design was cost-effectiveness and efficiency, safety protection was a less pressing consideration in this instance; (2) with the irregular dynamic variation of Bluetooth network topology, the typical security arrangements cannot be realized simply. For these reasons above, there are certain defects in Bluetooth network:

(1) Modification of the Bluetooth mobile phone address

By using particular technology, malicious attackers can modify the world's sole address of Bluetooth device, to destroy the security of Bluetooth network.

(2) The security of personal identification number (PIN)

In order to using Bluetooth mobile phone simply, the users set up PIN with Simple character or number or use the default PIN set up in factory-fresh condition. All these can threaten the security of PIN.

(3) The security of link key

In condition that the connection with the same link key among three devices being established at the same time, then one of these devices can steal the communications between the other two devices.

(4) The security of authentication process

Link layer authentication process between Bluetooth mobile phone is simple, malicious attackers can steal the communications, and destroy the authentication process of Bluetooth network. Security concerns of Bluetooth mobile phone have attracted an increasing attention of Information security researchers.

Currently, the research on the security of Bluetooth mainly focuses on two aspects below:

(1) Improving the key generation algorithms used in the progress of link layer connection of Bluetooth, Xilinx Company proposed a design concept of the full transformation of Bluetooth security algorithm. This design concept substitutes the existing E0 stream cipher for DES block cipher.

(2) Research on the security system of the existing Bluetooth, mainly aims at improve the existing Bluetooth bluetooth protocol protocol with loopholes, literature[4] points out that the safety recommendations proposed by Lucent Lab and Wetzel exert a greater influence on the research of this field.

Research on the two aspects described above mainly aims at the security system of the Bluetooth itself, the Bluetooth mobile phone faces threats in the channel of information sharing, such as file transfer in Bluetooth network, was not considered. The research on Bluetooth mobile phone security starts relatively late, and few reports of the Bluetooth security were appeared. This paper will proceed with the security of file transfer contained in the security system of the existing Bluetooth, in order to resolve the security problems of link layer protocol in Bluetooth network protocol.

BLUETOOTH SYSTEM STRUCTURE

Bluetooth system structure consists of three parts: the underlying hardware module, protocol layer, application layer.

3.1 protocol layer

Bluetooth protocol is a group of protocol specifications defined by SIG, with the purpose of realizing the mutual operation among Bluetooth devices by utilizing Bluetooth protocols of each layer. Complete Bluetooth protocol stack [6] as shown in Fig.1.

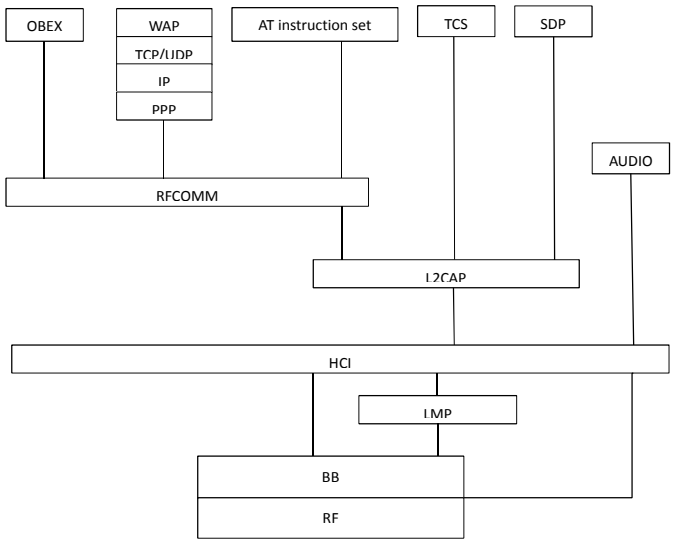

Fig.1 Complete Bluetooth protocol stack

3.2 Link layer protocol and security mechanism

The LMP is mainly responsible for the establishment and management of the connecting link. LMP realizes requesting and responding, encryption and authentication of messages with Bluetooth devices on both sides. The authentication among Bluetooth device was realized in link protocol layer, the security of this link layer plays an important role in the complete Bluetooth protocol stack.

Link level security mechanism of Bluetooth protocol has two main functions: authentication among devices and encryption of data transmission[7]. In the link layer, Bluetooth specification designs three types of security model[8]:

(1) Model with no security mechanism (model1): this model enable no security measure during data communication, in this condition, any types of date can be transferred among devices.
(2) Model with service levels security mechanism (model2): this model applies security measures for data communication, when the channel of communication being established, such as access allowed, encryption, identity verification etc.
(3) Model with Link level security mechanism (model3): this model applies security measures for data communication, before the channel of communication being established, in this condition, access allowed, encryption and identity verification are necessary for all servers and applications.

Three types of model apply different security levels for the communication among Bluetooth device.

SECURITY ANALYSIS OF LINK MECHANISM OF MOBILE PHONE BLUETOOTH

4.1 The connection establishment of mobile phone Bluetooth link

Realizing communication among different Bluetooth devices needs two steps: i the initialization of communication channel; ii the negotiation and the matching of the same PIN code. Yaniv Shaked and Avishai Wool proposed specific achievements for the PIN attack[9], this method can obtain the correct PIN code within 0.27seconds.

Being the only parameter in key generation generated by the consultation of both sides, PIN code affect the link key, the generation and security of encryption key directly. Meanwhile, the main method of PIN attacks protection is improving the safety consciousness of the users. Users do not use the Bluetooth device in public place or use Bluetooth device with high level security mechanism and enter longer PIN simultaneously. The method described above, bring great inconvenience to users of mobile phone Bluetooth devices. This paper mainly aims at using PIN code safely and conveniently.

Identity authentication of device is the precondition of the communication among Bluetooth device, Including matching and authentication. Communication process in link layer is shown as follows:

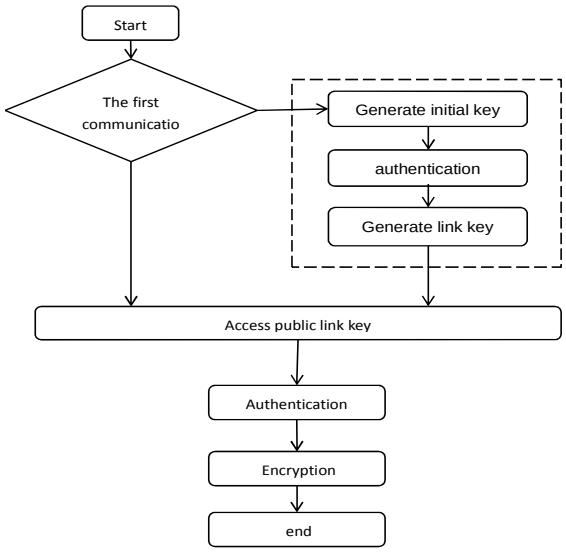

Fig.2 Communication process in link layer

The first step of communication process is the authentication of devices, then using an encryption key to encrypt data transmission, and completing the process data transmission.

In the default condition, though most of the mobile phone Bluetooth devices transfer date with no security mechanism (in Model1), the recommendation of this paper is using mobile phone Bluetooth devices which support model3. In Bluetooth specification, though model3 has the highest security level, there are security risks in data transmission using model3.

4.2 The analysis of PIN code matching

In technology standard of Bluetooth, the communication operational principle of mobile phone Bluetooth devices is as follows: two users input two same PIN code after discussion, in order to generate a random number as an initialization key, and this initialization key will lose efficacy after the first using, then a 128 bit random number will be generated as the link key. The link key will be stored in Bluetooth device, and then these two devices can connect to each other by authentication only next time. During matching and authentication, these two Bluetooth devices will check the paired PIN code all the time.

The initial key generation, link key generation and authentication are the main parts of Bluetooth pairing.

(1) Link key

The initial key is a type of link key. The Bluetooth specification definite four types of link key for different applications. All of link key is described as a 128 bit number, and the link key can be a temporary or semi-permanent key. The initial key and group key will be describe in detail:

1) Initial key (Kinit)

As parameters, the Bluetooth device address (BD_ADDR) (An only 48 bit address), PIN and random number (IN_RAND) (a 128 bit random number) are operated by E22, and Kinit is the result of this operate process with the length 128 bit. BD_ADDR, IN_RAND and E22 are public, and the PIN code is the only one input by users after discussion, as a result, the PIN code plays an important influence to the security of initial key generation.

2) Combinational key (KAB)

The main device (A) and the slave device (B) randomly generate a random number with the length 128 bit separately. Each number will do the XOR operation with Kinit, after this operation, the two results of XOR will be exchanged, and analyzed by A and B separately, then the random number as LK_RANDA and LK_RANDB are obtained. The main device (A) and the slave device (B) obtain the corresponding device address (BD_ADDRA, BD_ADDRB) through sending query messages. The parameters as LK_RANDA, BD_ADDRA and LK_RANDB, BD_ADDRB are corresponding to A and B. The two devices generate two temporary keys: K_A and K_B, through E21 respectively. In the end, the KAB is obtained by K_A XOR K_B.

Though Kinit will not be used after the generation of KAB, determining the input parameters of KAB has inseparable relations with Kinit. Being a input parameter of Kinit, the security of PIN has indirect effects on the

security of KAB.

(2) Authentication

Different from CA of internet, the purposes of authentication between Bluetooth devices are described as follows: 1) ensuring that parameter transmission in the process of link connection is successful or not; 2) used for carrying on the authentication between Bluetooth devices. The authentication between Bluetooth devices is realized by the mode of request-response. Show as Fig.3

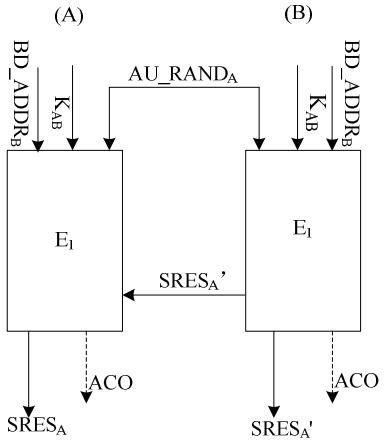

Fig.3 The authentication between Bluetooth devices

4.3 PIN attack

In the process of authentication, the algorithms of link key as E22, E21 are public, and the information exchanged between mobile phone Bluetooth devices is described as plaintext. Through network sniffer, the attackers can obtain the communication information in pairing and authentication process[3][4] (shown as TABLE 1), after this step, once the PIN is attacked, and obtained by attacker, the security of the whole Bluetooth will be suffer serious threat.

TABLE 1. THE INFORMATION EXCHANGED AMONG BLUETOOTH DEVICES

#	source	Destination	Message	Length
1	A	B	IN_RAND	128bit
2	A	B	LK_RANDA XOR Kinit	128bit
3	B	A	LK_RANDB XOR Kinit	128bit
4	A	B	AU_RANDA	128bit
5	B	A	SRESA	32bit
6	B	A	AU_RANDB	128bit
7	A	B	SRESB	32bit

The attack process as shown in Fig.4:

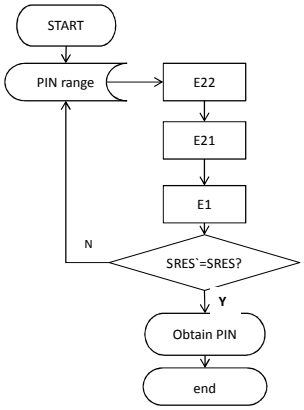

Fig.4 The attack process of PIN attack

1) The attackers obtain the message exchanged in table.1 as IN_RAND, and then obtain the Kinit through the E22 algorithm.

2) The malicious attackers obtain LK_RANDA and LK_RANDB by XOR, using the second and the third piece of

message in table.1 and Kinit.
3) Using LK_RANDA and LK_RANDB and the addresses of two devices (BD_ADDRA and BD_ADDRB), the malicious attackers obtain KAB by E21 algorithm.
4) According to the authentication between Bluetooth devices, through E1 algorithm and many input parameters such as AU_RANDA, AU_RANDB, BD_ADDRA and BD_ADDRB which were obtained in table.1 and step3, the malicious attackers obtain two SRES separately. Then comparing this two SRES with message5 and message7 in table.1. In condition that the attackers succeed in cracking PIN with brute force, the two SRES are equal to message5 and message7 separately, and rather the contrary.

IMPROVEMENT OF LINK CONNECTION MECHANISM FOR MOBILE PHONE BLUETOOTH

In the process of two Bluetooth's connection, through exchanging the PIN value before E22 algorithm, the complexity of PIN is increased, which will solve the security problem of PIN code. Show as Fig.5.

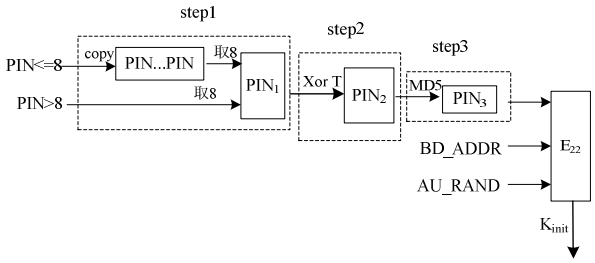

Fig.5: Kinit generation process after improvement

First of all, PIN1 can be got by sorting PIN values with any length. When two mobile phone Bluetooth devices are connecting each other, two sides input PIN values with any length, which will be sorted to a fixed size of 8 bytes, thereby getting PIN1. When the length of PIN values, inputted by two sides, is less than 8 bytes, based on 8 bytes, it will be sorted into a PIN value with the length of 8 bytes. The sorting algorithm usually uses duplication algorithm. When the length of PIN value is less than or equal to 8 bytes, its length will become greater than 8 byte through duplicating or continually duplicating. For example, 'abcdeabcde' can be got by duplicating 'abcd'; while 'abcabcabc' can be got by continually duplicating 'abc'. In contrast, when the length of PIN value is greater than 8 bytes, this algorithm will select 8 bytes located in the middle. When the length of PIN value is odd, the algorithm select will select from the next position of the middle. With above algorithm, it is possible that two PIN values with different length match successfully. To avoid this, a flag is used when PIN codes are input through two sides of Bluetooth. The flag is used as an identifier, which will be sorted into 8 bytes together with PIN value. Finally, we get a new PIN value, named as PIN1.

In addition, the exclusive-OR result of instant time T and PIN1 is PIN2. The system time of the mobile phone Bluetooth divide by a given time period, we can get a result. The instant time T is the last 2 bytes of it. Tests and experiments show that it is reasonable to assume the given time period is 10 minutes. Here, the system time of Bluetooth is a time period; it is the deviation of current time from one time basis.

Finally, by using MD5 algorithm, PIN2 is changed into PIN3. Then PIN3.is used as the input parameter of E22 algorithm.

As it is written, users use shorter PIN code of any length can ensure safety in data transmission. Bluetooth users need not to worry about the insecurity since the PIN code is short. Under the control of the given time period, within 10 minutes, it is difficult for attackers to crack PIN1. Experiments show that it is about 45 minutes. For crack PIN2, the attack firstly needs to obtain accurate T, which depends on the system time and current time period. At this stage, attackers are very difficult to obtain the source PIN code of Bluetooth. By using MD5 algorithm, PIN2 is changed into PIN3. PIN3 consists of characters and digitals and its length is 16 bytes. Testing and experiments show that it is impossible for attackers to crack the source PIN value even though they knew the MD5 algorithm clearly. This plan can defend the attack on PIN code and improve the link layer safety of mobile phone network.

The main drawback to this strategy is mainly that the system time of two Bluetooth is not synchronized. Assuming two mobile phones were not within the same given time period, their match cannot successful. This can be resolved by matching upper and lower time automatically, particularly, to move up or down 2 time period. If they still could not match within this effective time period, the matching process should be started again.

THE SECURITY ANALYSIS OF IMPROVED STRATEGY

In the condition of having obtained communication message shown as table 1, we have a test, which try to attack the

improved PIN code by using brute force, simulating the attack principle shown as Fig 5. There are three testes under three different situations: 1) we have an attack test when we have known that PIN codes consist of characters and digitals, and then have an attack test; 2) we have the test when the MD5 algorithm is known; 3) we have the test when T XOR PIN1 and MD5 algorithm are known. Testing results are shown in table2 and table 3. The PIN lengths of testing data are 4, 5, 6 and 7. For comparing easily, we also list the brute force time before improvement.

TABLE 2 THE CRACKING TIME BEFORE IMPROVEMENT

Attacking method	Length of PIN(byte)	Approximately exhaustive time(s)
Original attack	4	1
	5	10
	6	102
	7	103

TABLE 3 THE CRACKING TIME UNDER THREE DIFFERENT SITUATIONS AFTER IMPROVEMENT

Attacking method	Length of PIN(byte)	Approximately exhaustive time(s)
1)	4	---
	5	---
	6	---
	7	---
2)	4	25.68*104
	5	25.68*104
	6	25.68*104
	7	25.68*104
3)	4	104
	5	104
	6	104
	7	104

From the above analysis, the difficulty of cracking PIN becomes bigger after improvement, the complexity of PIN and exhaustive time increase with every transformation. After three steps, the difficulty of cracking PIN has been raised remarkably, which effectively defends the PIN attacking in the matching process of two mobile phone Bluetooth devices.

CONCLUSION

For mobile phone Bluetooth devices, the article analyzed the link connection mechanism of link layer, discussed 3 kinds of safe modes of data transmission. The matching process of two mobile phone Bluetooth devices in the third safe mode was mainly discussed, which contains the production and matching process of the link key. From customer perspective, we can increase the complex of PIN code by analyzing the process of cracking PIN code and exchanging the length of PIN code. Even though users inputted shorter PIN code, the safety of data transmission could also be ensured, which compensated, at least in part, some hidden trouble of Bluetooth underlying protocol.

REFERENCES

[1] Wang Wenchun. The Safety Research of Bluetooth Technology[D]. *Dalian University of Technology,* **2006**.
[2] Wu Fan. Design and Realization of Wireless File Transmission System on Bluetooth Technology[D]. *Wuhan University of Technology*,**2007**.
[3] Mamoon Hamid. *Global Electronics China* **2011**, 22(8): 44-46.
[4] Shi Jianghong. The Research of Communication Security Problem in *Wireless Personal Area Networks*[D]. XiaMen University,**2002.**
[5] Zhang Lulin, Lei Chunjuan, Lang Xiaohong. *Bluetooth Protocol And Realization* [M]. BeiJing: The People's Posts and Telecommunications Press, **2009**.
[6] Ma Jiancang, Luo Yajun, Zhao Yuting. *Bluetooth Core Technology and Application*[M]. BeiJing: Science Press, **2006**.
[7] Ollie Whitehouse. War nibbling: *Bluetooth in security*[EB/OL]. http://www.atstake.com /research/ reports/acrobat/atstake_war_nibbling.pdf, April 15, **2009**.
[8] Bluetooth SIG. *Specification of the Bluetooth system*, "Baseband specification", Version1. 0[S/OL]. http://www. bluetooth. com/,July 24,**1999**.
[9]Nikos Mavrogiannopoulos. On Bluetooth™ security[EB/OL]. http://www. bluez.org/, **2009.**