Bluetooth Communication using Hybrid Encryption Algorithm based on AES and RSA

Komal Rege, Nikita Goenka, Pooja Bhutada, Sunil Mane
Department of Computer Engineering and Information Technology
College of Engineering, Pune.
Wellesley Road, Pune, Maharashtra, India – 411005

ABSTRACT

A hybrid encryption algorithm based on AES and RSA is proposed to enhance the security of data transmission in Bluetooth communication. E0 algorithm is currently used in transmission of data via Bluetooth between two or more devices. E0 is a 128-bit symmetric stream cipher used in the bluetooth protocol. Several attacks and attempts at cryptanalysis of E0 and the Bluetooth protocol have shown that it may be broken in 2^{64} operations [4]. In the proposed hybrid encryption algorithm, instead of the E0 encryption, AES algorithm, known for of its higher efficiency in block encryption is used for data transmission and RSA algorithm is used for the encryption of the AES key due to its key management advantages. Thus the dual protection using AES and RSA algorithm will make the data transmission using Bluetooth more secure. Moreover, the hybrid encryption algorithm provides a very easy and convenient technique for the encryption of transmitted data. The confidentiality of the hybrid encryption algorithm is also discussed.

General Terms

Security, Encryption Algorithm, Bluetooth

Keywords

Bluetooth, E0 cipher, hybrid encryption algorithm, data transmission, AES Algorithm, RSA Algorithm

1. INTRODUCTION

Bluetooth technology is a wireless protocol that connects electronic devices while they are close to each another. In addition to being paired with cell phones, short-range blue-tooth technology is also compatible with personal computers, laptops, printers, GPS receivers, digital cameras, telephones, video game consoles and more. Bluetooth being a wireless technology is susceptible to spying and remote access. It introduces a number of potentially serious security vulnerabilities. Data-leaking frequently arises in bluetooth which may lead to the compromise of the device and the networks to which it connects. Thus security is a big concern in bluetooth technology.

At present the E0 stream cipher is being used for encryption of data in bluetooth technology. However, 128-bit E0 stream cipher has a few weaknesses. It can be cracked in some cases in 2^{64} operations.

In this paper, the Bluetooth mechanism is discussed along with its advantages. Finally, a hybrid encryption scheme is

proposed to solve the security risk in Bluetooth data transfer.

2. ENCRYPTION ALGORITHM IN BLUETOOTH

2.1 Bluetooth Security

The Bluetooth security mechanism has three defined modes [1]:

(1) Safe Mode 1: No security except against casual eaves-droppers.

(2) Safe Mode 1: Provides security at service level which is established after creating the channel, above datalink layer.

(3) Safe Mode 3: Provides security at data link level. It is initiated before establishing channel, by the Link Man-ager, as well as by the Service Level.

In every Bluetooth device, there are four entities used for maintaining the security at the link level:

(1) A unique 48-bit Bluetooth device address (BD_ADDR) allocated by the Institute of Electrical and Electronics Engineers (IEEE).

(2) Private authentication key, which is a 128-bit random number used for authentication purposes.

(3) Private encryption key, 8-128 bits in length that is used for encryption.

(4) A frequently changing 128-bit random or pseudo-random number called Random number (RAND) made by the Bluetooth device itself.

Authentication key and encryption key (secret key) are generated during the initialization process. Secret key is derived from the authentication key during the certification process.

Both the keys are different and during every encryption process a new key is generated. Whereas in the case of authentication key, the concrete application of Bluetooth device decides whether to change it as it is more stable. The random numbers generated cannot be duplicated and also have to be significantly lesser than random numbers' zero probability estimate in the authentication key life.

2.2 Authentication And Encryption Process

Bluetooth security-mechanism provides authentication, encryption and key management functions in Link layer [4]. It uses E0, E1, E2 and E3 algorithms. 4-bit PIN entered by the user produces Link key using E2 algorithm which is then used by the E3 algorithm to generate the encryption key. Then the

key stream generated by E0 algorithm along with the encryption key is used to encrypt the plaintext to generate the ciphertext. The Bluetooth encryption process is demonstrated by Figure 1.

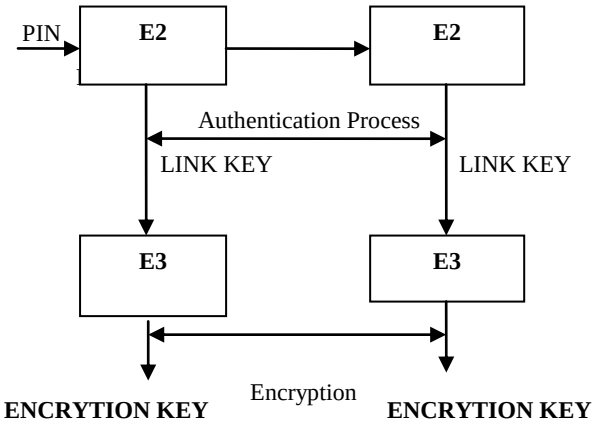

Figure 1: Bluetooth Encryption Process

The 3 modules consist of:

(1) Key generation module comprises of generating the Link key using E2 algorithm and then generating the Encryption key using E3 algorithm.

(2) In the Encryption module, the plaintext is encrypted by the key stream generated using the E0 algorithm.

(3) Authentication module requires the two devices to compare their respective identification words generated using E1 algorithm thus completing the authentication process.

2.3 Analysis Of E0 Algorithm

The Bluetooth encryption system uses the stream cipher E0 to encrypt the payloads of the packets which is re-synchronized for every payload. The E0 stream cipher consists of the payload key generator, the key stream genera-tor and the encryption/decryption part. The input bits are combined by the payload key generator and are shifted to the four Linear Feedback Shift Registers (LSFR) of the key stream generator. The key stream bits are then generated which are used for encryption. The Exclusive-OR operation is then performed on the key stream bits and data stream bits to generate the ciphertext. Similarly the Exclusive-OR operation is performed on the ciphertext to get back the plaintext during the decryption process.

3. VULNERABILITIES OF BLUETOOTH SECURITY SYSTEM

3.1 Low reliability of PIN

The PIN is the only secret used for the key generation that is not transferred by wireless communication [8]. For many applications, the PIN will be a relatively short string of numbers. Typically, it may consist of only four decimal digits. If the PIN is small then an exhaustive search can derive the initialization of security keys. Therefore, the credibility of the PIN code is lower, 4 bits PIN code only has 10,000 possibilities. This problem can be overcome by using a longer PIN as it becomes difficult for the attacker but at the same time it becomes inconvenient for the user to enter the PIN every time when the connection is established.

3.2 Weakness of E0 Algorithm

Random Number Generator (RNG) may produce static or periodic numbers that may reduce the effectiveness of the authentication scheme. Thus the strength of the pseudo random generator may not be known [4]. If the random number comes out to be a sequence of zeros then the cipher text will be the same as the plaintext and the whole process would be worthless.

3.3 Address Spoofing

Addresses are not validated, so the addresses can be spoofed which is similar to IP address spoofing. If the unique blue-tooth address assigned to each device is known, the user can be tracked. Address spoofing also enables the tracker to monitor the activities of the user if his bluetooth address is known thus hampering the user's privacy.

3.4 Limited Resource Capacity of LFSR

LFSR (Linear Feedback Shift Register) is used to generate the pseudo random numbers in E0 algorithm [6]. Four LF-SRs are used in E0 stream cipher. If the generated cycle by LFSR is shorter than the key then there can be a threat from the attacker using divide and conquer attack. The probability of the attack however is very low since the divide and conquer technique requires access to the key stream extending over periods of partial input. This, however, has been taken into account in the Bluetooth specifications. The above mentioned divide-and-conquer attack needs access to the key stream extending over periods of partial input. Since the resynchronization frequency of bluetooth is very high, such an attack is impossible.

3.5 Low credibility of link key

Another problem lies in the unit key scheme [6]. Information used during data transmission is public except for the link key which is assumed to be the participant's shared secret. Now, consider during communication between two devices A and B, A's unit key is used as the link key. Simultaneously, devices A and C communicate using A's unit key as link key. Now, device B, knowing A's unit key can decrypt the data transmitted between devices A and C. Device B can also fake itself as device A to C or as C to A.

The above mentioned problems clearly show how vulnerable the bluetooth security system is. If the data transmitted using bluetooth is not that important the problems mentioned above won't pose a threat. However, for sensitive data and in complex networks where security of data is a must, a more reliable security system is needed. To eliminate the problems currently faced by the bluetooth security system a hybrid encryption technique using AES and RSA algorithms has been proposed.

4. PROCESS OF HYBRID ENCRYPTION ALGORITHM

RSA is the first public key algorithm used for data encryption and digital signature algorithms. It is based on the difficulty of factoring large numbers, the factoring problem. RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key.

The AES algorithm is based on permutations and substitutions. Permutations are rearrangements of data, and

substitutions replace one unit of data with another. AES performs permutations and substitutions using several different techniques. AES does not make use of Feistel network un-like DES. AES is a block cipher with a block length of 128 bits. It allows for three different key lengths: 128, 192, or 256 bits. The number of rounds differ according to the key length as follows:

(1) 10 rounds of processing for 128-bit keys.

(2) 12 rounds of processing for 192-bit keys.

(3) 14 rounds of processing for 256-bit keys.

The first step is Add round key stage which is followed by 9 rounds of four stages and a tenth round of three stages applicable for both encryption and decryption with the exception. Each stage of a round in the decryption process is the inverse of its corresponding part in the encryption process. Substitute bytes, shift rows, mix columns and add round key are the four stages.

Except for the last round in each case, all other rounds are identical. The mix columns stage does not take place in the last round. The tenth round simply leaves out the Mix Columns stage. The decryption process consists of inverse shift rows, inverse substitute bytes, inverse add round key and inverse mix columns. Like the decryption process the inverse mix columns stage is omitted in the tenth round.

Considering the efficiency of both AES and RSA, AES is faster than RSA for encryption and decryption of large messages while RSA is suitable for key management as it is based on the difficulty of factoring large numbers. RSA can distribute the encryption key openly and it always keeps the decryption keys secret. While in AES, the encryption key has to be distributed secretly before communication.

Taking into account the advantages of both AES and RSA and avoiding their shortcomings, hybrid encryption algorithm based on AES and RSA has been proposed in which AES is used for encryption of message and RSA is used to encrypt the AES key. This hybrid encryption algorithm can be used in Bluetooth Technology to avoid the current risks.

The entire hybrid encryption process is as follows: Let A and B be the sender and receiver respectively. Let eb be the public key of B and dB its private key. Let us suppose that the AES encryption session key is K. The public key of RSA is known to both the sender and the receiver.

4.1 Process of Encryption

During the process of sending encrypted information, the random number generator produces 128-bit AES key only once, it encrypts the plaintext to produce cipher text. In RSA, p and q are randomly generated depending on the millisecond measure of the ma- chine. This is used to en-crypt the AES key. Finally the encrypted message is send along with the encrypted AES key, private key and Big Integer n each separated by a semicolon and the order of which is known only to the sender and receiver. AES, being a block cipher divides the plaintext into number of blocks depending upon the key size for encryption. It is different from Blue-tooth stream cipher algorithm, cellular message encryption algorithm is completely safe and mathematically proven.

At first, AES algorithm encrypts Bluetooth data packet.

(1) The 128 bit AES key is used to encrypt the data to get the ciphertext C.

The second, RSA algorithm encrypts the key of AES algorithm:

(1) The pubic key of the receiver is first obtained from the server or respective sources.

(2) Then the 128-bit AES is encrypted using the public key of the receiver to form the ciphertext key (CK).

(3) Using the ciphertext C obtained from the AES encryption of the original message and the ciphertext key (CK) obtained from RSA encryption the complex ciphertext message CM is generated which is then transmitted. The entire hybrid encryption process is shown in Figure 2.

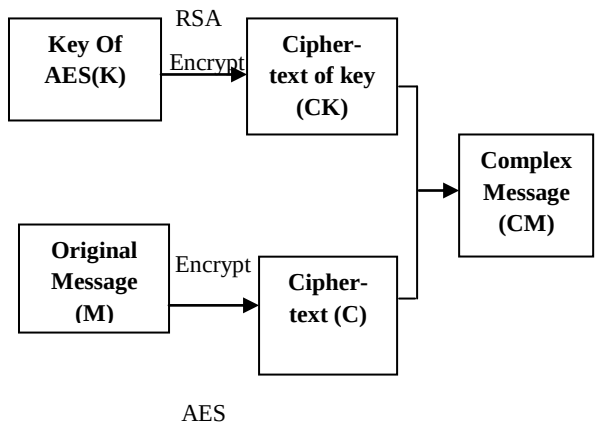

Figure 2: The Hybrid Encryption Process

4.2 Process of Decryption

During the decryption of hybrid encryption algorithm, the receiver B first divides the complex message (CM) into two parts AES encrypted ciphertext C and RSA encrypted AES session key CK. The receiver B uses its private key dB to decrypt the RSA encrypted AES session key CK to get the session key K. Using the AES key K it then decrypts the ciphertext C to generate the original message M. The entire hybrid decryption process is shown in Figure 3.

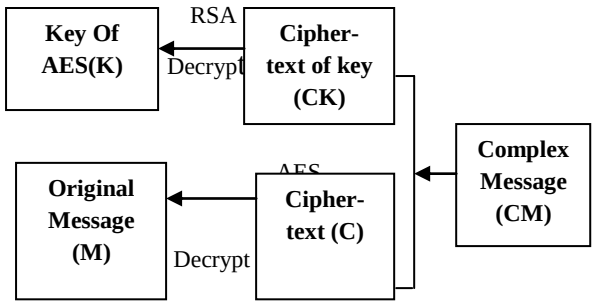

Figure 3: The Hybrid Decryption Process

4.3 Advantages of Hybrid Encryption Algorithm

(1) In AES communication, the AES key needs to be transferred before the communication. However, using the hybrid encryption algorithm the AES key need not be transferred before the communication as it is being sent in the encrypted form along with the transmitted data.

(2) As RSA algorithm is only used for key management, the speed of encryption and decryption process is the same as

AES which is faster than RSA.

(3) Key management in the hybrid encryption process is similar to that of RSA where the decryption key has to be kept secret.

(4) Another advantage of the hybrid process is that digital signatures can also be used for security due to the use of RSA.

4.4 Advantages of AES over other algorithms

As far as public key cryptography is concerned, RSA is very secure due to the factoring problem. However for private key cryptography there are many algorithms like DES, Triple DES, AES, Blowfish and many more [2][3].

(1) DES algorithm makes use of feistel network. It was developed in the 1970's and was very popular. However it is now considered insecure for many applications and has many weaknesses. This is mainly because its 56-bit key size is too small. Many attacks and methods that exploited the shortcomings of DES have rendered it an insecure block cipher.

(2) Triple DES which is an enhancement to DES was later proposed in which the original DES algorithm was applied thrice to increase the security. But it was found to be very slow.

(3) Blowfish algorithm being in the public domain is used only for software applications. It suffers from weak key problems.

(4) The most preferred algorithm is AES. It is considered to be the best encryption standard. Brute force attack is the only known possible attack against AES algorithm.

(5) RC4 is of 128- bits. RC4 is a fast cipher and is always subjected to many types of attacks.

Considering the weaknesses of other algorithms, AES is found to be the best encryption standard and is given priority over other standards. Studies have shown that when processing time is considered, blowfish is found to be the fastest but where security is a concern, AES algorithm is considered to be the best. Thus AES algorithm along with the use of RSA algorithm for key management will provide an efficient technique to ensure the security of transmitted data using Bluetooth.

4.5 Security Analysis Of Hybrid Encryption Algorithm

Due to the use of AES and RSA algorithms, security of data transmission using hybrid encryption algorithm depends on the security of AES and RSA algorithm and its operating efficiency depends on the speed and high efficiency of encryption and decryption by AES algorithm. Security of data transmission in Bluetooth Technology is improved by the security strength of the proposed hybrid encryption scheme. Data remains secured due to the special design and strength of all key lengths of the AES algorithm (128,192,256). Side-channel attacks are the only known successful attacks against AES. Thus the security strength of data transfer using bluetooth technology is improved using AES encryption.

Presently, RSA is the only popular algorithm used for public key cryptography. Its security mainly depends on the difficulty of factoring large numbers in reasonable amount of time.

Presently, RSA is the only popular algorithm used for public key cryptography. Its security mainly depends on the difficulty of factoring large numbers in reasonable amount of time.

The original message remains safe as long as the encryption key that is being used remains secret. Even if the data sent using the hybrid encryption algorithm is tracked, the complex message is organized in such a way that the tracker will not understand which part of the complex message contains the AES encrypted key and the ciphertext. Also, the private key of the receiver will not be known and hence the AES key cannot be decrypted ensuring the data in transit remains safe. So the transmitted data remains secure due the security of hybrid encryption algorithm using AES and RSA.

5. CONCLUSIONS

Bluetooth technology is widely used for transmission of data over short range distances. Bluetooth being a wireless technology is more susceptible to attacks as compared to other fixed networks. So it is important to consider the security of data during transmission. E0 stream cipher algorithm which is currently used in Bluetooth for encryption has many shortcomings and can be easily broken down. AES algorithm is highly secure with very few published attacks against it. Also the difficulty of factoring large integers ensures the security of RSA algorithm. Thus the proposed Hybrid Encryption Algorithm using AES and RSA provides a more secure and convenient technique for secure data trans-mission among bluetooth devices as compared to the E0 algorithm.

6. REFERENCES

[1] Gustavo Padovan, "Bluetooth Security", July 4, 2011

[2] MR. GURJEEVAN SINGH; MR. ASHWANI SINGLA; MR. K S SANDHA, "CRYPTOGRAPHY ALGO-RITHM COMPARISON FOR SECURITY ENHANCE-MENT IN WIRELESS INTRUSION DETECTION SYSTEM", International Journal of Multidisciplinary Research, Vol.1 Issue 4, August 2011.

[3] Sudhir Nagwanshi, Akhilesh A.Waoo, P. S. Patheja, San-jay Sharma, "Performance Analysis of Triple DES-Tiger-RSA Vs DES-RSA algorithms for Bluetooth Security Systems", IOSR Journal of Engineering, July 2012.

[4] Wuling Ren and Zhiqian Miao, "A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication", Second International Conference on Modelling, Simulation and Visualization Methods, 2010.

[5] Ma Chui and Cao Pitying, "Research of Bluetooth Security Manager", Dec 14, 2003.

[6] Cryptanalysis of Bluetooth key stream Generator two-level E0. Yale and Serge Vaudenay

[7] WUxing-Hui ZHOU Yu-Ping."Analysis of data encryption algorithm based on WEB"

[8] Cracking the Bluetooth PIN, Yaniv Shaked and Avishai Wool

[9] Man Young Rhee. Network Security Encryption Principle, algorithm and Protocol [M]. Peking: Tsinghua University Pres, 2007.