Global Journal of researches in engineering
Electrical and electronics engineering
Volume 12 Issue 5 Version 1.0 April 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 2249-4596 & Print ISSN: 0975-5861

Remodelling RC4 Algorithm for Secure Communication for WEP/WLAN Protocol

By Laxmi Mounika.Nannaka , Hepzybah.Singarapu & Ramadevi.Puli
Vignan's institute of management and technology for women

Abstract - Wireless Local Area (WLAN) has become a hot spot of application in the field oftelecommunication these years. To secure WLAN for data transmission, RC4 algorithm is able to provide the advantages of fast performance in the resource constrained environment. This paper analyzes the security of RC4 algorithm, presents a way to enhance the security of RC4 algorithm and analysis the affection of the enhanced algorithm by using MD5/hash function.

Keywords : *RC4, WEP, WLAN.*

GJRE- F Classification : *FOR Code: C.2.1,G.1*

Strictly as per the compliance and regulations of:

Remodelling RC4 Algorithm for Secure Communication for WEP/WLAN Protocol

Laxmi Mounika.Nannaka [α], Hepzybah.Singarapu [σ] & Ramadevi.Puli [ρ]

Abstract - **Wireless Local Area (WLAN) has become a hot spot of application in the field of telecommunication these years. To secure WLAN for data transmission, RC4 algorithm is able to provide the advantages of fast performance in the resource constrained environment. This paper analyzes the security of RC4 algorithm, presents a way to enhance the security of RC4 algorithm and analysis the affection of the enhanced algorithm by using MD5/hash function.**

Keywords : RC4, WEP, WLAN.

I. Introduction

Wireless Local Area Network (WLAN) is the network that utilizes radio frequency technology instead of traditional coaxial. WLAN is widely used in many conditions, especially when it's difficult to install traditional network. As the openness and sharing of wireless channel nature, the security of wireless data stream becomes particularly prominent [1].IEEE802.11 standard for WLAN defines two types of authentication open system authentication and shared key authentication, and uses RC4 stream encryption algorithm of the Wired Equivalent Protection (WEP) protocol to enhance its security. However, the facts show that the WEP protocol has not met the desired level of safety. On the contrary, WEP itself also has fatal security flaws, tampering with the data for a variety of active attacks and passive eavesdropping on the data provided to facilitate aggression. WEP uses the Initial Vector (IV) to avoid duplication of key stream. Beginning in 2001, several serious weaknesses were reported and they demonstrate that WEP protocol is vulnerable in a number of areas. In essence, the problem is not in RC4 itself but in the way to generate the key and in how to use the key for RC4 encryption. Many hackers and computer security experts have discovered the WEP design flaws, which indicate that IEEE802.11 standards can only provide limited support to confidentiality. WEP provides a 40-bit key, which may be sufficient to keep away a common hacker but incapable to ward off a professional hacker. Either a 40-bit key or a 128-bit key can be easily cracked within two or three hours. RC4 is probably the most widely used stream cipher nowadays due to its simplicity and high efficiency. This paper focuses on the research to enhance RC4 algorithm. The rest of the paper is organized as follows. RC4 algorithm is introduced in Section 2. In Section 3, we present the RC4 encryption and decryption. The weakness of RC4 is presented in Section 4. In Section 5, we provide analysis of the main attack. Section 6 introduces the improvement of RC4. Section 7 concludes this paper.

Author α : Vignan's institute of management and technology for women, Hyderabad. E-mail : monikachoudary1992@gmail.com
Author σ : Vignan's institute of management and technology for women, Hyderabad. E-mail : hepsi.singarapu@gmail.com
Author ρ : Vignan's institute of management and technology for women, Hyderabad. E-mail : puli.ramya31@gmail.com

II. Rc4 Algorithm

The principle of RC4 algorithm consists of two Components: key-scheduling algorithm (KSA) and pseudo-random number generation algorithm (PRGA). The key function of KSA is to complete initialization of RC4 Key, while the key function of PRGA is to produce pseudo-random number. The pseudo code for RC4 algorithm (KSA and PRGA) is shown below.

```
KSA
Begin
for i=0 to 255
Si=i; Ki=K[i mod n];
End
For k=0;for i=0 to 255
j=(j+Si+Ki) mod 256
swap(Si,Sj)
end for
end
PRGA
begin
i=0;j=0;
while(true)
i=(i+1) mod 256 j=(j+Si) mod 256;
swap(Si,Sj); t=(Si+Sj) mod 256
K=St;
end loop; end
```

Stream ciphers and block ciphers are two classes of encryption algorithms. Stream ciphers encrypt a one-bit plaintext at a time, using a timedependent encryption transformation. Block ciphers encrypt groups of plaintext characters using a fixed encryption transformation. Stream Ciphers and block ciphers have their respective characteristics, but stream ciphers are almost always faster and use far less code than block ciphers do. RC4 is a variable key-size stream

cipher based on a 256-byte secret internal state and two one-byte indexes. The data is encrypted by XORing data with the key stream which is generated by RC4 from a base key. For a given base key, KSA generates an initial permutation state denoted by S0. PRGA is a repeated loop procedure and each loop generates a one-byte pseudo-random output as the stream key. At each loop, a one-byte stream key is generated and it is XORed with one-byte of the plaintext, in the meantime a new 256-byte permutation state S as well as two one-byte indices i and j are updated, which defined by (Sk+1, ik+1, jk+1) = PRGA(Sk, ik, jk) where ik+1and jk+1 are the indices and Sk+1 is the state updated from ik, jk, and Sk by applying one loop of PRGA.

III. Rc4 Encryption and Decryption

The encryption process of WEP is shown in Figure1, WEP uses 40-bit or 104-bit encryption key connected with 24-bit IV to generate 64-bit or 128-bit seed key, and then send the seed key to a random generator PRNG, encrypt the plaintext with pseudo-random sequence [2]. System uses CRC32 (32-bit cyclic checksum) for integrity verifying to ensure that the message will not be modified during transmission that sends IV, plaintext and integrity check value (ICV) to the other [3]. The decryption process of WEP is shown in Figure 1. The decryption key sequence is generated in the same way that generates encryption key, XORed with cipher text to get the plaintext. Compare ICV with integrity check value

ICV ' calculated by CRC32, if the encryption key is the same as decryption key, and ICV '= ICV, then the receiver gets the original plaintext data. Many encryption algorithms are widely available in wired networks. They can be categorized into a symmetric key encryption. In symmetric key encryption and secret key encryption, only one key is used to encrypt and decrypt data and the key should be distributed before transmission between entities. It is also very efficient since the key size can be small, while the functions used for encryption are hardware operations, and the encryption time can be very short. However, in large communication networks, key distribution can be a significant problem. Asymmetric key encryption or public key encryption is used to solve the key distribution problem. This uses two keys, one for encryption and another for decryption, and there is no need for distributing them prior to transmission. Public key encryption is based on mathematical functions, computationally intensive and not very efficient for small wireless devices.

Generally, most encryptions used in wireless devices are based on symmetric key encryption, such as RC4. RC4 is a stream cipher designed by Ron Rivest in 1987 and it is widely used in many applications today and in wireless networks such as IEEE 802.11 WEP and CDPD. With a unique key, a stream of pseudo-random numbers is generated, and then the encryption of data XORs the pseudo-random numbers from the stream with the data. RC4 is known to be fast and efficient, for it can be written using only a few lines of codes and requires only 256 bytes of random access memory (RAM). Hence, it is one of the best encryption schemes during the past decade. RC4 is standardized to provide security services in WLAN using the WEP protocol. However, Fluhrer and many researchers have discovered several vulnerabilities in the RC4 algorithm. The weaknesses in RC4 and loopholes in the WEP protocol have resulted in a new standard for security in WLAN (IEEE 802.11i) proposing a new protocol based on the advanced encryption standard (AES). AES is a block cipher designed by Joan Daemen and Vincent Rijmen that has a variable key length of 128, 192, or 256 bits to encrypt data blocks of 128, 192, or 256 bits long. Both block and key length are extensible to multiples of 32 bits. AES encryption is fast and flexible, and it can be implemented on various platforms especially in small devices and smart cards. Also, AES has been rigorously tested for security loopholes for a few years before it was standardized by NIST.Figure 1 shows the process of encryption and the reverse of this is decryption.

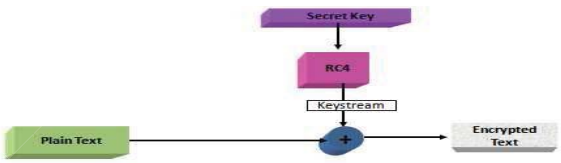


Figure 1 : WEP Encryption

IV. Rc4 Weakness

The algorithm loopholes and key management loopholes are the weaknesses of RC4 algorithm.

a) Algorithm Loopholes

WEP uses RC4 algorithm to enhance the security, but there are still some problems. First of all, RC4 is a stream encryption algorithm. If one bit lost, the entire data packet must be discarded, and the sender need to retransmit the lost data packet until the receiver accept the data packet, and WEP algorithm must reinitialize IV after sending each data packet.

Secondly, RC4 algorithm has the following characteristics: assuming CT1, CT2 as the cipher text, PT1, PT2 as the plaintext, we get the relationship that CT1=PT1 XOR RC4 (key), CT2=PT2 XOR RC4(key), CT1 XOR CT2=PT1 XOR PT2. As RC4 uses the same key, if we know PT1, and then we can *3624 2010 Chinese Control and Decision Conference* get PT2. If there is enough plaintext, through "dictionary" we will decrypt almost all the data [4]. 802.11 uses 24-bit IV to ensure that each data packet uses a different key, but if the standard 802.11 runs in 11Mbps network in a single

base station, the whole key space will exhaust in less than an hour, and in a larger network with multiple base stations the time to exhaust the key space will be much shorter. The phenomenon of the IV re-emergence results in the degradation of RC4 algorithm performance, and the WEP becomes much more vulnerable to be attacked.

At present, most of the 802.11 WLANs are used as a datalink layer in TCP / IP networks, and each packet contains a transmission that contains a large number of known plaintext information which will allow hackers to restore transmission frames for each part of the key stream. Hackers can get enough information to use RC4 encryption algorithm to calculate the seed of the original information.

b) Key Management Loopholes

In the WEP mechanism for key generation and distribution, there is no provision for key management. The use of the key is not clearly defined, and the key is used rather confused.

The data encryption keys are mainly two kinds default key and key-mapping key. Default key is to configure the default settings. Key-mapping key is for different senders and the receivers to send and receive data packet by using key encryption to deal with the key. In order to get this key, each systemust maintain a key table to keep the communication used for their key-mapping keys record. In each communication, receiver finds in the table to get whether it is shared by users themselves and the communication key used for information encryption and decryption. Otherwise, we use the default key with the selected key ID,and encrypt key-mapping keys for the selection of superior to any other keys. The use of keymapping keys can enhance the security, but in fact people rarely use this key. As the network expands, the space will be used to store the key growing; on the other hand this key needs to use other methods to send which is much more difficult to achieve. For the users' man-made factors, in fact people use mainly the key ID for the 0 default key. From the above analysis we can see that most users use the key ID for the 0 default key. In this way, it increases the possibility of key reuse between sites, while the mechanism of the WEP key reuse has no restriction, and once the second key is manually loaded, it rarely updates. As the use of WEP mechanism devices is to store the key, so if the device is lost, it is possible for hackers to use.

V. Attack

As RC4 is probably the most widely used stream cipher nowadays due to its simplicity and high efficiency, the attack on RC4 is also a hot research topic. The attack can be mainly divided into two types, force attack, key stream distinguisher.

a) Force Attack

Brute Force Attacks, a brute force attack on encrypted messages, otherwise known as a "known plaintext attack", consists of decrypting an intercepted message with every possible key and comparing the result to the "known" plaintext. The "known" text is essentially guessed, but is easily deduced from the fact that communication sessions often begin with the same sequence of bytes. For an attack of this kind to be successful, only a small number of "known" bytes are necessary, making the guessing process significantly easier.

b) Key Stream Distinguisher

The key stream generator can not be really random, so that we can distinguish the key stream generated and true random key sequence, which is a theoretical attack model. Distinguisher is an effective algorithm to distinguish the really random sequence from the generated key stream. The distinguisher between what we call key stream generated by RC4 and really random key stream is to provide some basis and method to confirm the RC4 key stream generated in which specific key word is not random, and find the non-random key stream in order to attack. Golic [5] found the weakness of RC4 linear changes, and Fluhrer and McGrew [6] moved on with the result. Maintin and Shimir[7] give the attack method on this point.

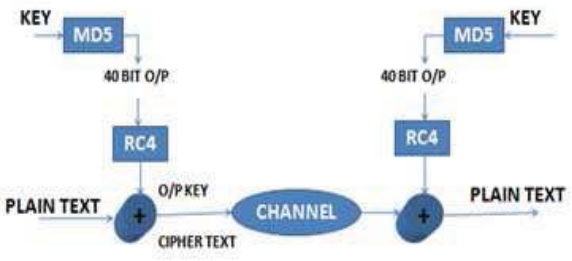
VI. Improvement

Modern cryptographic technique is divided into two types, symmetric encryption system and public key encryption system. Symmetric encryption system communicating parts need a safe way to ensure key sharing; public key encryption system communicating parts have their own pair of keys.

In general, data processing efficiency of public key encryption system is not as high as symmetric encryption system, but the key is easier to manage. Therefore, we use public key encryption system for both parts to consult and then consult the key, use symmetric cryptography for data encryption and decryption. This maximizes the advantage of two types of cryptography. Key of variable or constant length is given to MD5 and the output of MD5 is 128 bits. Among those 128 bits only 40 bits are taken(any 40 bits) and given as input to RC4. The input and output of RC4 is 40 bit.

In RC4, the key is generated and it is XORed with plain text. This project uses the concept of stream cipher, where the data is encrypted bit by bit(encryption is fast when compared with block cipher). Stream cipher is used because this algorithm is used in Wi-Fi where continuous transmission is desired.

Elgamal, as a typical public key encryption system, is widely used, and we use Elgamal for key agreement to resolve the RC4 key management issues. Elgamal encryption is an asymmetric key encryption algorithm for public-key cryptography. Elgamal encryption consists of three components: the key generator, the encryption algorithm, and the decryption algorithm. The RC4 algorithm encryption improved data processing is shown in Figure 2.



Assault for different lengths IV has different analysis lengths. If the IV length is 4 byte, the probability that each IV can be used for the first byte correlation analysis is only 4.32×10-5, and the number of weak IV that needs to analyze a byte KC in the key is l .33×106. In order to improve the RC4 security, we use a 256-bit key.

In the analysis of 8 byte RC4 pseudo-random streams, we get the result that the first output bit has 36% probability to equal with the approximate; the second bit has 35.9% probability, and so on.

The 48th bit has 0.4% probability. Therefore, in order to ensure the difficulty of cryptanalysis, in the improved RC4 method, we don't use the first 48 bit pseudo-random stream to avoid the attack by using the bias of the first few bits in output stream. In the 11Mbps network, the transmission of 1500 byte data packets will come up with the situation that different packets use the same IV in about 5 hours: 11(Mbps)/ (1500Byte/packet*8bit/Byte) = 917 packet/s 2_{24} = 1677216

1677216/917 = 5.1 h

Using the improved RC4 in the 11 Mb/s networks, the time that different packets use the same time IV in the transmission of 1500 Byte data packets is about 54 days.

2_{32} = 4294967296

4294967296/917 = 1301 h = 54 d

VII. Conclusions

WLAN has some security weakness due to RC4 weakness, linear weakness and IV weakness. The improved RC4 can raise the security level of RC4, so does the WLAN, and it can be used as temporary method as it's easy to update. The new block encryption algorithm, such as RC5, will be used as the security solution for its high encryption level in future.

References Références Referencias

1. BORSE M, SHINDE H, Wireless Security & Privacy [J]. Personal Wireless Communications, ICPWC 2005.
2. Yukio Mitsuyama, Motoki Kimura, Takao Onoye, Isao Shirakawa, Architecture of IEEE802.11i Cipher Algorithm for Embedded Systems. IEICE Trans. on Fundamentals, vol. E88-A, no.4, 2005, pp. 899-905.
3. Jun-Dian Lee, Chih-Peng Fan, Efficient lowlatency RC4 architecture designs for IEEE 802.11i WEP/TKIP. Intelligent Signal Processing and Communication Systems, Nov. 28, 2007, pp.:56-59.
4. Maocai Wang, Guangming Dai, Hanping Hu, Security Analysis for IEEE802.11. Wireless Communications, Networking and Mobile Computing, 2008.
5. Jovan Dj.Golic, Linear statistical weakness of alleged RC4 keystream generator. Advances in Cryptography EUROCRYPT'97, Lecture Notes in Compur, vol.1233, Springer, Berlin, 1997, pp.226-238.
6. Scott R.Flunhrer and David A.McGrew, Statistical analysis of the alleged RC4 keystream genenrator, Fast Software Encryption 2000, Lecture Notes in Comput.Sci., Vol.1978, Springer Berlin, 2000, pp.19-30.
7. Itsik Mantin and Adi Shamir, A practical attack on broadcast RC4, Fast Software Encryption 2001, Lecture Notes in Comput.Sci., vol.2355, Springer, Berlin, 2001, pp.152-164.