Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 5; April-June, 2015 pp. 484-488
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/acsit.html

Analysis of Security Issues in Wired Equivalent Privacy (WEP)

Ashish Garg[1] and Rosy Verma[2]

[1]Department of Information Technology Centre for development of advanced Computing Noida (U.P.), India
[2]Department of IT Centre for development of advanced Computing Noida (U.P.), India
E-mail: [1]ashish.garg910@gmail.com, [2]rosyverma@cdac.in

Abstract—*In today's world, wireless networks are rapidly gaining popularity due to their excellent usability. For secure wireless data transmission there are various security protocols like Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) have been employed. WEP has a potential limitation that stems from its adaptation of RC4 stream cipher algorithm. This paper begins by introducing the concept of WLAN. The introductory section gives brief information on the WLAN components and its architecture. In order to examine the WLAN security threats, this paper .will look at the security of stream ciphers in detail. The paper will then explain the security & flaws of legacy IEEE802.11 WLAN standards. Finally, this paper ends with the conclusion of thorough analysis of three most popular researches done to enhance the security of WLAN.*

Keywords: *WLAN, WEP protocol, RC4, Security goal, cryptanalysis.*

1. INTRODUCTION

From starting of the wireless network, many solution to that have been introduced and many of them were replaced by better security standards these changes promoted the security field to be a permanent hot topic for research. Wireless network security is hybrid of wireless channel security and Network security [1].

For user perspective Wireless network is like a black box which user turns on and use without knowing what inside. Wireless network replace the wired network but the biggest issue is security for authorize user from unauthorized user (hacker). IEEE 802.11 standard offer some level of protection this protocol also known as wired equivalent privacy (WEP).

Starting with the introduction to security in wireless network .Section 2 describes briefly about Wireless network then Section 3 describes briefly about WEP. Section 4 introduces Stream Cipher encoding scheme with Ron's Code 4 (RC4) with its vulnerability. Section 5 introduces different variant of RC4. Finally in Section 6 summaries this paper.

2. WIRELESS NETWORK OVERVIEW

2.1 Wireless network

Due to Flexibility in nature and freedom which wired network doesn't have is the reason for success of wireless network [19].

Wireless LAN

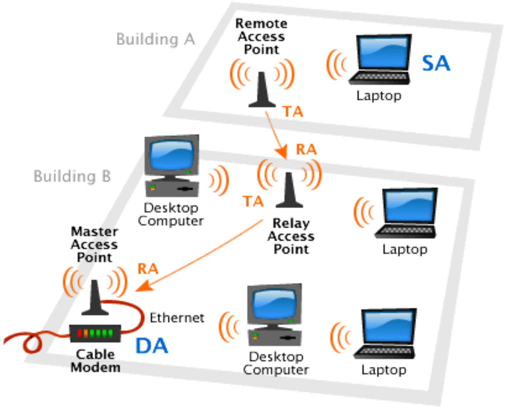


Fig. 1: Wireless LAN

Wireless Local Area Network (WLAN) tries to intimate the wired LAN. Two main entities in WLAN are end user device and Access point. End user device allow user to communicate with other user. Access points are act as a gateway between wireless device and wired device. Different type of Access points (AP) are:-

- Remote Access Point: - it is directly connected to sender which transmits the message to the office or master access point.
- Relay Access Point: - this only work to increase the range of remote access point. act as relay between remote and master access point
- Master Access point: - it is the final destination of message which connected to the wired network.

When relay access point receive frame, it knows destination on another side so it rewrite frame again turning itself into the TA and access point 3 into RA. Finally Frame arrives at master access point or to receiver [19].

2.2 Security in wireless networks

The main security goals in wireless network are [15]:

2.2.1 Authentication. Identity of receiver and sender should be verified before transmitting a message.

2.2.2 Secrecy or Confidentiality [8]. Authenticate user can interpret the message and prevent message from un-authorize user .This can be calculated via

- Entropy of message: - minimum number of bit required to encode all possible meaning of message.
- Uncertainty of message: - number of plain text bits that can be recovered from encrypted message.
- Equivocation- how much additional information is added to reduce uncertainty of message.

2.2.3 Integrity [5]. Integrity means that the content of the communicated data is assured to be free from any type of modification between the end points (sender and receiver).

2.2.4 Service Reliability and Availability. Since secure systems usually get attacked by intruders, which may affect their availability and type of service to their users. Such systems should provide a way to grant their users the quality of service they expect

3. WIRED EQUIVALENT PRIVACY

This section illustrate about Wired Equivalent privacy (WEP) which is an important security protocol in wireless network.

3.1 Introduction to WEP

WEP used to secure communication between AP and user to provide secure authentication and encryption of data Based on algorithm called Ron's Code 4(RC4).

Design objective of WEP according to IEEE 802.11 states are as follow [5]:

- Reasonably strong: WEP allow changing of key and initialization vector.
- Self Synchronizing: Self synchronization for each message.
- Efficient: implemented either on hardware and software.

3.2 Encryption and Decryption

In WLAN, both station and AP have same shared secret key to communicate. Length of key is 40 bit.

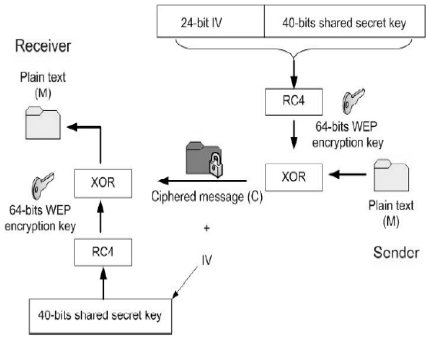

24-bit IV
40-bits shared secret key
Receiver
Plain text (M)
RC4
64-bits WEP encryption key
XOR
Ciphered message (C)
+
IV
XOR
Plain text (M)
64-bits WEP encryption key
RC4
Sender
40-bits shared secret key

Fig. 2: WEP Encryption and Decryption

Encryption key generated from 40 bit shared key and 24 bit Initialization vector (IV) form 64 bits key. Cipher text generated from simple XOR operation between key and plain text.WEP also provide integrity to assured that message is error free and algorithm use for integrity is called as Integrity check Value(ICV)[10].

4. STREAM CIPHER

Stream cipher process plain text in small blocks usually one bit.

$$\sigma_{t+1} = f(\sigma_t, p_t, k)$$
$$c_t = g(\sigma_t, p_t, k)$$

Fig. 3: Stream Cipher Equations

Here f is next state function and g is output function [4].

This section describe RC4 algorithm which is a stream cipher encoding used in WEP

4.1 RC4

IEEE 802.11 standard uses RC4 encryption algorithm to enhance security of wireless network. RC4 is widely used stream cipher because of simple, efficient and fast. This section organized as follow; Encryption and Decryption mechanism of RC4 with their vulnerability and different type of attack.

4.1.1 Encryption and Decryption

Encryption: WEP uses RC4 stream cipher to encrypt message.

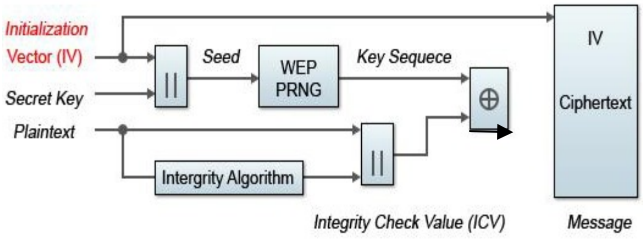


Fig. 4 RC4 Encryption

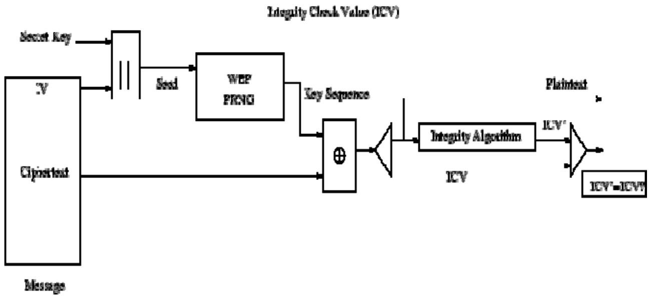


Fig. 5: RC4 Decryption

In RC4, key and IV insert into Key scheduling algorithm (KSA) and output of which is known as seed act as input to Pseudo Random number generator (PRNG) which produce key sequence to perform XOR with plain text to generates cipher text. This Cipher text along with IV as plain text sends to receiver. At sender side for data integrity it uses integrity check value with the use of CRC algorithm [6] [9].

Decryption:

a) Cipher text message received by receiver.

b) XOR secret key with cipher text.

c) Again ICV is checked against message obtains.

d) For calculating ICV same algorithm applied as at the time of encryption.

e) If previous ICV is equal to new ICV then message is accepted [6] [9].

4.1.2 Vulnerability [5]

a) IV is used to ensure that key are not repeated but in actual after certain number of combination it repeats.

b) IV sent as plain text to receiver but during collision attacker determine key stream.

c) p1 and p2 are plain text, k is key stream which produce cipher text c1 and c2. if attacker knows one plain text and two cipher text then attacker can obtain another plain text such as:

c1 XOR c2=p1 XOR p2

4.4.3 Cryptanalysis of Stream cipher. There are number of attack on stream cipher such as Brute Force attack, Divide and conquer and Resynchronization attack.

a) Brute Force Attack: - In this all the possible Combination is checked one by one and in worst case it needs to search whole space search. When password is short guessing help to easily recognize key but for longer word there is another called Dictionary attack is used [9].

b) Divide And Conquer: - in this type attacker Search for initial seed through all the possible combination or attacker can guess the initial seed in LFSR. Then observe pattern of LFSR to obtain key.

c) Resynchronization attack: - In this a correlation between cipher text and plain text is obtain in form of equation to obtain key which use to encrypt plain text to cipher text.

5. ADOPTABILITY IN RC4

5.1 Enhancing RC4 algorithm for WLAN WEP protocol:

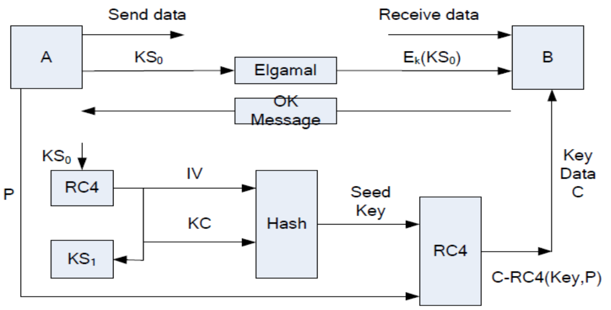


Fig. 6: Enhance RC4

In this paper [9] author describe Elgamel encryption which is used in asymmetric encryption algorithm for public key cryptography. It consist three parts: key generator, Encryption algorithm and Decryption algorithm. Elgamal state that plain text can be encrypted to many possible cipher texts.

Conclusion

11 (Mbps) network which transmit 917 packet per second where each packet has 1500 byte have 2^{24} Initialization Vector so 2^{24} /917=5.1h

So IV repeats after 5.1 hour.

But according to this paper author take 32 bit IV which is repeated after 54 days on same environment.

5.2 PC-RC4 Algorithm: An enhancement over standard RC4 algorithm

According to this paper [20], KSA uses j index location pointer to provide randomness at the index which is not present in standard RC4 algorithm. Here it use temp[j] and s[j] in the statement j=(j+s[i]+s[j]+temp[i]+temp[j])% 256. This statement adds some strength in generation of j index. It also provides more randomness to the j index location pointer.

In PRGA also increase the randomness on generating j value by using the statement s[j] in j=j+s[i]+s[j] % 256.j is random index location indicator after first loop of execution because starting pointer of j initialize by 1.

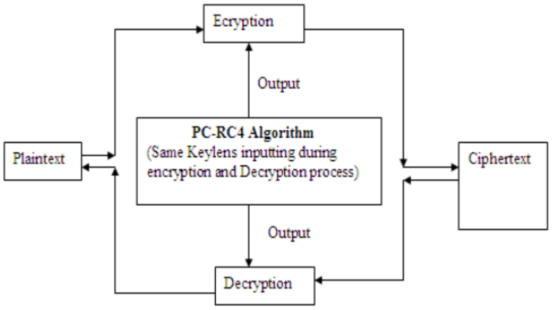


Fig. 7: PC-RC4 Encryption and Decryption

Conclusion

Based on Execution time-

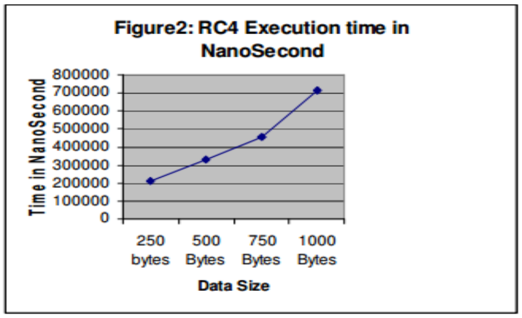


Figure 2: RC4 Execution time

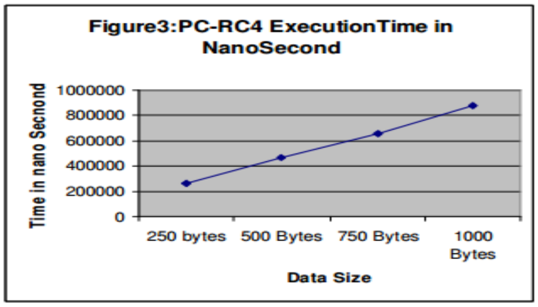


Fig. 8: Comparison of PC-RC4 with RC4

Based on memory utilization

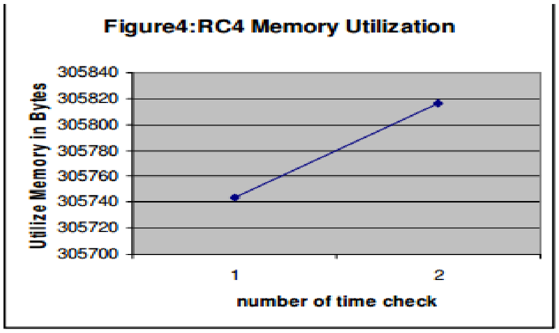


Figure 4: RC4 Memory Utilization

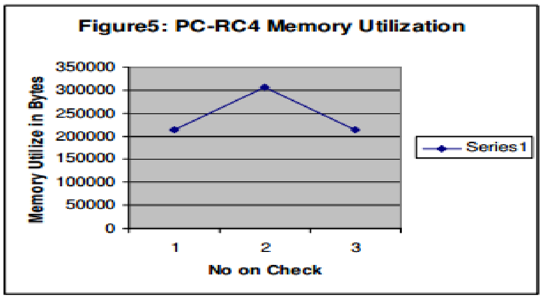
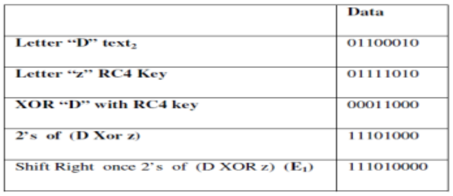


Fig. 9: Comparison of PC-RC4 with RC4

5.3 RC4c: A Secured Way to View Data Transmission in Wireless Communication Networks

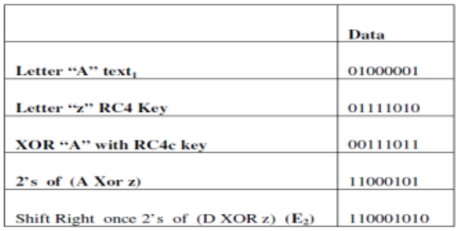
Author illustrates in this paper [21] that RC4c algorithm work on 4 phases: Initialization, Operation, De-exclusive Level 1 and De-exclusive Level 2 stage. Output of starting two stage is same as the original RC4 algorithm but in third stage output of second stage which generate key stream is find 2's compliment of given stream and in final stage right shift is perform on output of third stage.

Example



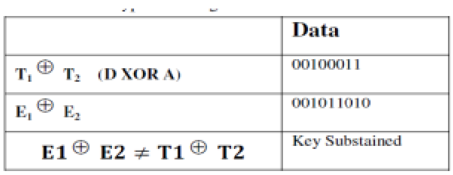
	Data
Letter "D" text$_2$	01100010
Letter "z" RC4 Key	01111010
XOR "D" with RC4 key	00011000
2's of (D Xor z)	11101000
Shift Right once 2's of (D XOR z) (E$_1$)	111010000

Fig. 10 Encryption "D" in RC4c technique



	Data
Letter "A" text$_1$	01000001
Letter "z" RC4 Key	01111010
XOR "A" with RC4c key	00111011
2's of (A Xor z)	11000101
Shift Right once 2's of (D XOR z) (E$_2$)	110001010

Fig. 11: Encryption "A" in RC4c technique



	Data
$T_1 \oplus T_2$ (D XOR A)	00100011
$E_1 \oplus E_2$	001011010
$E1 \oplus E2 \neq T1 \oplus T2$	Key Substained

Fig. 12: Key sustained

Conclusion

C1 XOR C2 = P1 XOR P2.

But in this more hardware support is needed to maintain shift register.

6. SUMMARY

This paper reviewed about security in wireless network with possible attack in protocol used in network but if corrected policy and standard are used then possible attack can be avoided. IEEE 802.11 protocol WEP is used widely to secure network. Other technology is available but still WEP is used widely. After many evolution in RC4 still it remains as hot topic for research to increase security of wireless LAN. Finally reaches to the RC4 algorithm with encryption and decryption mechanism along with their weakness.

REFERENCES

[1] Steve F. Russell "Wireless Network Security for Users ", Information Technology: Coding and Computing, 2001. Proceedings, International Conference on, pp 172-177, 2001 IEEE

[2] Ankush Karnik, Katia Passerini "Wireless network security - A discussion from a business perspective ", Wireless Telecommunications Symposium, 2005, pp 261-267, April 28-30, 2005 IEEE

[3] Hai Cheng, Qun Ding "Overview of the Block Cipher "second conference on Instrumentation , Measurement , Computer , Communication and control second conference , pp 1628-1631 , IEEE 2012.

[4] C .S Lamba "Design and Analysis of Stream Cipher for Network Security", second conference on Communication software and Network, PP 562-567, IEEE 2010.

[5] Shivaputrappa Vibhuti "IEEE 802.11 WEP (Wired Equivalent Privacy) Concepts and Vulnerability ", CS265 Spring 2005

[6] ARASH HABIBI LASHKARI FCSIT, FARNAZ TOWHIDI, RAHELEH SADAT HOSSEINI “Wired Equivalent Privacy (WEP) “, Future Computer and Communication, 2009. ICFCC 2009. International Conference on, pp 492-495, 3-5 April 2009 IEEE

[7] Songhe Zhao and Charles A. Shoniregun “Critical Review of Unsecured WEP “, pp 368-374, 9-13 July 2007 IEEE

[8] T.D.B Weerasinghe “An Effective RC4 Stream Cipher “8th International Conference on Industrial and Information Systems, Aug. 18-20, IEEE 2013.

[9] Yao Yao, jiang Chang, Wang Xingwei “Enhancing RC4 algorithm for WLAN WEP Protocol” Control and Decision Conference, pp 2623-2637, 26-28 may 2010.

[10] Ahmad M. Al Naamany, Ali Al Shidhani, hadj Bourdoucen” IEEE 802.11 Wireless LAN Security Overview”, IJCSNS, VOL. 6 NO. 5B, May 2006.

[11] Christophe De Canniere, Alex Biryukov, Bart Prennel “An Introduction to Block Cipher Cryptanalysis”, Proceeding of IEEE, VOL. 94, NO. 2, February 2006.

[12] Tang Songsheng, Ma Xianzhen “Research of Typical Block Cipher Algorithm”, International conference on Computer, Mechatronic, Control and Electronic Engineering (CMCE), 2010 IEEE

[13] Nidhi gupta , G.P biswas “WEP Implementation using Linear Feedback Shift Register(LFSR) and Dynamic key”, International Conference on Computer and CommunicationICCCT), 2011 IEEE.

[14] Andreas Klein ”Stream Cipher” , Springer 2013.

[15] Aaron E. Earle "Wireless Security Handbook,". Auerbach Publications 2005.

[16] “Data Confidentiality”,Microsoft[Online], December 2005, http://msdn.microsoft.com/en-us/library/ff650720.aspx.

[17] ”Linear feedback shift register”, Wikipedia,[online], http://en.wikipedia.org/wiki/Linear_feedback_shift_register, ,(Accessed: march 2015)

[18] “WEP Shared Key Authentication”, NETGEAR, Inc.,[online],http://documentation.netgear.com/reference/sve/wireless/WirelessNetworkingBasics-3-09.html,(Accessed: 15 march 2015)

[19] Glenn,Fleishman, ” Back to the Future: New Wi-Fi Bridges Use 1999 Standard”, (O’Reilly Wireless DevCenter), [online]08/28/2003,http://archive.oreilly.com/pub/a/wireless/2003/08/28/wireless_bridging.html, (Accessed: 4 march 2015).

[20] Pardeep, Pushpendra Kumar Pateriya,” PC-RC4 Algorithm: An Enhancement Over Standard RC4 Algorithm”, Volume 1, Issue 3, June 2012, International Journal of Computer Science and Network (IJCSN).

[21] O. O Olakanmi “RC4c: A Secured Way to View Data Transmission in Wireless Communication Networks” Vol.4, No.2, March 2012, International Journal of Computer Networks & Communications (IJCNC).