Journal of Theoretical and Applied Information Technology
15 June 2012. Vol. 40 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A REVIEW ON WEP WIRELESS SECURITY PROTOCOL

[1]MUHAMMAD JUWAINI, [2]RAED ALSAQOUR, [3]MAHA ABDELHAQ, [4]OLA ALSUKOUR

[1,2,3] School of Computer Science, Faculty of Information Science and Technology, University Kebangsaan Malaysia, 43600, Bangi, Selangor, Malaysia

[4]Department of Computer Engineering, Faculty of Engineering and Technology, The University of Jordan, 11942, Amman, Jordan

E-mail: [1]juwaini@gmail.com, [2]raed@ftsm.ukm.my, [3]maha@ftsm.ukm.my, [4]alsukour@gmail.com

ABSTRACT

WEP (Wired Equivalent Protocol) is a wireless security protocol ratified by IEEE (The Institute of Electrical and Electronics Engineers) in 1999. Since then, WEP is widely used in telecommunication field. In daily usage, it had been phased-out by IEEE since 2005 to be replaced by WPA/WPA2 (Wi-Fi Protected Access). WEP encryption algorithm can be easily cracked because of its widely documented weaknesses. Nevertheless, WEP is still has been used extensively as a research topic in the academic field. Certain enterprises still using WEP due to lack of security consciousness, economical constraint or because it is difficult to replace the legacy communication devices in which WEP is already bulged. In this paper, we give a review on WEP wireless security protocol in terms of its history, weaknesses, improvements, and current alternative approaches to overcome its weaknesses regarding the protocol in ICT (Information and Communication Technology) field. This research aims to address WEP protocol in its current versions and to give a spirit future direction research to enhance its security mechanism.

Keywords: *Rivest Cipher 4 (RC4), Wired Equivalent Protocol (WEP), Wireless Security*

1. INTRODUCTION

WEP (Wired Equivalent Protocol) [1] is a wireless security protocol introduced and ratified by IEEE according to 802.11 standards. For the purpose of data broadcast encryption by telecommunication devices, RC4 [2] (Rivest Cipher 4) stream cipher has been used as encryption engine in WEP protocol. RC4 is a stream cipher cryptographic engine used by WEP to encrypt wireless traffic. It was found by *Ron Rivest* of *RSA*[1] in 1987. The main reason for RC4's implementation in WEP is to increase its execution speed when using it in hardware..Also, its simplicity implementation over WEP makes it popular and widely used.

In WEP algorithm, a shared key used is 40-bit long with 24-bit long Initialization Vector (IV). For this initial phase, both are concatenated to produce a new 64-bit key. This new 64-bit key is used as a seed for Pseudo-Random Number Generator (PRNG). The key sequence generated by PRNG is used in the second phase, where plaintext that we want to broadcast is sent to integrity algorithm. The product of the integrity algorithm, Integrity Check Value (ICV), is compared with the previous plaintext. Afterward, key sequence generated by PRNG is sent to RC4 together with the ICV. The cipher text is generated by concatenating the IV with the product of RC4 encryption process. Figure 1 below explains the entire WEP algorithm.

In this paper, we give a review on WEP wireless security protocol development since its inception until now. Current WEP weaknesses, researches and improvements for WEP has also been discussed.

The rest of the paper organized as follows. In section 2, we take a glance into the history of WEP. In section 3, we discuss widely documented weaknesses in WEP as per stated in the abstract. Naturally, our next discussion in section 4 focuses on improvements to overcome

[1] **RSA** is an American computer and network security company. RSA was named after the initials of its co-founders, *Ron Rivest*, *Adi Shamir*, and *Len Adleman*, after whom the RSA public key cryptography algorithm was also named

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

all those weaknesses. To keep abreast with current trend, our final section 5 summarizes the alternatives for WEP suggested by either IEEE or another organization. Finally, section 6 is the summary for the entire article and a future work is also suggested.

2. WEP HISTORY

WEP was ratified by IEEE in September 1999. Since its inception, WEP has been used by organizations or individuals as wireless security protocol[2] [4] [5]. In 2005, a group of FBI personnel gave a demonstration on how they can use easily accessible tools to crack WEP encrypted system in less than 3 minutes [6]. This demonstration is one of the most popular references to confirm the weakness of WEP. Subsequently, IEEE declared that WEP was obsolete and it was superseded by WPA. Nearly all of the wireless communication devices in the market after 2003 which were sold with WEP feature

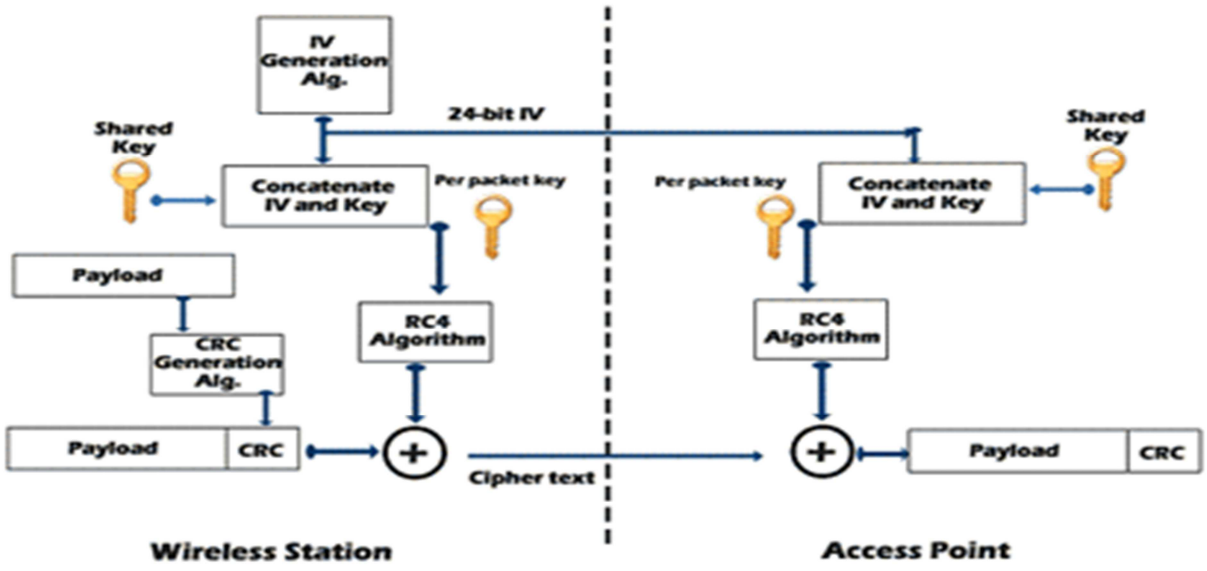

Figure 1: WEP Encryption Process[3]

were disabled. However, for certain devices, there are options to allow WEP feature, mainly for academic and research purposes. Whenever WEP is enabled, a warning message would be displayed to prompt the user about the vulnerability of WEP to be used in practical.

3. WEP WEAKNESSES

Researches in [2] [5] [7] show that WEP can be cracked easily in a few minutes by using software/tools available on the Internet. As aforementioned, FBI employees used widely available tools from internet to crack WEP encrypted network.

Among the biggest weaknesses of WEP is its inability to prevent fake data packets [4]. Anybody can broadcast forged packets of data and then the communication devices have no way to determine whether the packet is coming from a valid source or not. Phishing websites exploit this weakness to prey for their victims. Lastly, improper use of RC4 can also bring the problem in term of security to the user.

WEP is unable to avoid replays attack [2]. It has the tendency to repeat the same key after a few thousand bits. By observing the pattern of data recorded, anyone can record, compare and crack WEP key.

Lashkari et al., [8] has shed light on the WEP weaknesses within the following points:

1. The *Size of IV is short and reused:*
   Regardless of the key size, 24-bit key length of WEP's IV can only provide 16,777,216 different RC4 cipher streams for a given WEP key. On a loaded network, this number can be achieved in a few hours and reuse the same IV then becomes unavoidable.

2. *Problem in the RC4 algorithm itself:*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

RC4 implementation has been considered to have weak keys. Determination of which packets were encrypted with weak keys is an easy task. Since the first three bytes of the key are taken from the IV that is sent unencrypted in each packet, this weakness can be exploited easily by a passive attack. Out of the 16 million IV values available, about 9,000 are used. To determine a 104-bit WEP key, it needs to capture between 2,000 and 4,000 interesting packets. On a fairly loaded network, the capture of the interesting 5,000 average packets might not pose any difficulty and can be achieved in a short period of time [9].

3. *Easy forging of authentication messages:* Turning on authentication with WEP reduces the overall security of the network and make it easier to guess WEP key by attackers. Shared key authentication involves demonstrating the knowledge of the shared WEP key by encrypting a challenge. Any monitoring attacker can observe the challenge and the encrypted response and as a result, determines the RC4 stream used to encrypt the response. Also, the attackers can use that stream to encrypt any challenge it would receive in the future. However, by monitoring a successful authentication, the attacker can later forge an authentication.

4. IMPROVEMENTS OVER WEP

Even though WEP has its own weaknesses, it is still relevant in our daily life. In the academic world, WEP has been studied extensively in information security, cryptology and telecommunication fields. Certain small and medium enterprises find it difficult to stop using WEP because the process of replacing their current WEP-compatible telecommunication devices to WPA/WPA2-compatible telecommunication devices is too expensive and cumbersome.

A research by Sato et al., [10] presented means of strategies to make an improved version of WEP algorithm without having to replace the hardware. The 'new' WEP is using less power and faster compared to its predecessor. Another research by Gupta et al., [11] used Linear Feedback Shift Register (LFSR) and dynamic keys. LFSR is a stream cipher used by the authors to replace RC4. It is proven by Diehard Test [11], a suite of study to assess the strength and randomness of stream cipher, as shown in Table 1, LFSR is the best stream cipher security-wise compared to RC4.

Table 1: Diehard Test Result

Test Name	LFSR	RC4
Birthday spacing	Pass	Fail
GCD	N/A	Fail
Overlapping Permutations	Pass	Fail
Ranking of 31x31 and 32x32 matrices	Fail	Fail
Ranks of 6x8 matrices	Pass	Fail
Monkey Tests on 20-bit words	N/A	N/A
Monkey Tests OPSO, OQSO, DNA	N/A	Fail
Count the 1's in a stream of bytes	Pass	Fail
Parking Lot Test	Pass	Fail
Minimum Distance Test	Pass	Fail
Random Spheres Test	Pass	Fail
The Squeeze Test	Pass	Fail
Overlapping Sums Test	Pass	Fail
Runs Up and Down Test	Pass	Pass
The Craps Test	Pass	Pass

Out of eighteen tests in Diehard Test, LFSR only failed in one test compared to twelve failed tests by RC4. That is more than 70% of all available tests for RC4 indicate that RC4 as a whole is not a strong encryption algorithm.

Temporal Key Integrity Protocol (TKIP) [12] is an improvement to WEP which fixes all the security problems and does not require new hardware. Like WEP, TKIP uses the RC4 stream cipher as the encryption and decryption processes and all involved parties must share the same secret key. This secret key must be 128-bit and is called the Temporal Key (TK). TKIP also uses IV of 48-bit and uses it as a counter. Even if the TK is shared, all involved parties generate a different RC4 key stream. Since the communication participants perform a 2-phase generation of a unique Per-Packet Key (PPK) that is used as the key for the RC4 key stream [8]. TKIP adds four new algorithms to WEP:

- A cryptographic Message Integrity Code (MIC) called Michael, to defeat forgeries.
- A new IV sequencing discipline, to remove replay attacks from the attacker's arsenal.
- A per-packet key mixing function, to de-correlate the public IVs from weak keys; and
- A re-keying mechanism, to provide fresh encryption and integrity keys, undoing the threat of attacks stemming from key reuse.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5. WEP ALTERNATIVES

Some alternatives had been suggested to overcome security weaknesses in WEP. For example, WEP2 [2] is a temporary measure implemented by prolonging the IV and key values to 128-bit. However, as this paper suggested in the previous section, making IV and key values longer is not enough to compensate for the inadequate security in WEP. In fact, longer key length can make a larger data sample to be recorded. As a result, WEP2 had been dropped as well.

WEP+ [2] is a proprietary enhancement to WEP by Agree Systems which enhances WEP security by avoiding 'weak' IVs. This protocol only selects 'good' IVs. However, because of the nature of WEP+ as proprietary protocol, it is difficult to enforce everywhere except for telecommunication devices produced by Agree Systems.

Another research by Gupta et al., [11] proposed a WEP equivalent method to encrypt the traffic. In this method, RC4 encryption is replaced by LFSR. Based on the previous section, we should agree that LFSR is much better encryption engine compared to RC4.

In the current standard, WPA/WPA2 has been used as de-facto wireless security protocol standard to replace WEP. Until now , there is no attack to crack WPA/WPA2 except brute force method. However, brute-force method is infeasible especially with the enough long key.

6. CONCLUSION AND FUTURE WORK

In a nutshell, this paper gives a review about the development of WEP since its inception until now. Current researches and improvements for WEP had also been discussed. This paper limits its scope to WEP protocol and does not review the other wireless security protocols. As a future work, we aim to study in deep other wireless security protocols and discuss their weaknesses and improvements. In addition, we aim to find an enhancement for WEP to be used in non-compatible WPA/WPA2 communication devices.

ACKNOWLEDGEMENT

This research was supported in part by the Centre for Research and Instrumentation Management (CRIM), University Kebangsaan Malaysia, Malaysia. Grant: UKM-GUP-2011-252.

REFERENCES:

[1] Goutam, P., and Subhamoy, M. (2011). "RC4 Stream Cipher and Its Variant", *CRC Press*. Kolkata. India.

[2] Arash, H. L., Mir, M.S.D., and B, S. (2009). "A Survey on Wireless Security Protocols (WEP, WPA and WPA2/802.11i)", *2nd IEEE International Conference on Computer Science and Information Technology* (ICCSIT), pp. 48-52.

[3] Abdel-Karim, R. A., Security in Wireless Data Networks: A Survey Paper. Retrieved from: http://www.cse.wustl.edu/~jain/cse574-06/ftp/wireless_security/index.html

[4] Rehman, S.U., Ullah, S., and Ali, S. (2010). "On Enhancing the WEP Security Against Brute-Force and Compromised Keys", *International Conference on Computer Information Systems and Industrial Management Applications* (CISIM), pp. 250-254.

[5] Reddy, S.V., Sai Ramani, K., Rijutha, K., Ali, S.M., and Reddy, C.P. (2010). "Wireless Hacking - A Wifi Hack By Cracking WEP", *2nd International Conference on Education Technology and Computer* (ICETC), pp. V1-189 – V1-193.

[6] SmallNetBuilder, 2005, The Feds can own your WLAN too. Retrieved from: http://www.smallnetbuilder.com/wireless/wireless-features/24251-thefedscanownyourwlantoo. 15/4/2012.

[7] Mavridis, I.P., Androulakis, A.-I.E., Halkias, A.B., and Mylonas, P. (2011). "Real-life paradigms of wireless network security attack", *15th Panhellenic Conference on Informatics* (PCI), pp. 112-116.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[8] Lashkari, A.H., Towhidi, F., and Hosseini, R.S. (2009). "Wired Equivalent Privacy (WEP)", *International Conference on Future Computer and Communication* (ICFCC), pp. 492-495.

[9] Hytnen, R., and Garcia, M. (2006), "An analysis of wireless security", *Journal of Computing Sciences in Colleges*, Vol 21, Issue 4, pp. 210-216.

[10] Sato, T., Moungnoul, P., and Fukase, M.-A. (2011). "Compatible WEP Algorithm for Improved Cipher Strength and High-Speed Processing", *The 8th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology* (ECTI-CON), pp. 401-404.

[11] Gupta, N., and Biswas, G.P. (2011). "WEP Implementation Using Linear Feedback Shift Register (LFSR) and Dynamic Key", *2nd International Conference on Computer and Communication Technology* (ICCCT), pp. 422-427.

[12] Park, J.S., and Dicoi, D. (2003), "WLAN security: current and future", *IEEE Internet Computing*, Vol 7, pp. 60-65.