International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-4 Issue-3, July 2015

Security Enhancement of Wireless Protocol WPA (WI-FI Protected Access)

D. J. Evanjaline, N. Kalpana, P. Raja Kumar

Abstract: ***A Wireless Local Area Network (WLAN) is a flexible data communication system implemented as an extension to or as an alternative for a wired Local Area Network (LAN). However, anyone can eavesdrop on information so that WLAN has the hidden security trouble such as leaking of electromagnetic wave or eavesdropping of data because WLAN adopts common electromagnetic wave as media to transmit data. Therefore, the security of WLAN is very important and outstanding. This paper discusses the security flaws in wireless security protocol WPA and to describe a solution to enhance the security WPA.***

Keywords: WLAN, WEP, Initialization Vector, TKIP, AES, WPA, WPA2, MIC.

I. INTRODUCTION

Wireless communications offer organizations and users many benefits such as portability and flexibility, in-creased productivity, and lower installation costs. How-ever, risks are inherent in any wireless technology. The loss of confidentiality and integrity and the threat of de-nial of service attacks are risks typically associated with wireless communications. WEP and WPA are designed to protect, but they still have weaknesses. Many solutions have been proposed for the remedy of the WEP and WPA encryption, key exchange and mutual authentication problems. WEP suffers security pitfalls due to weak key management of the shared secret key and initialization vector (IV) repetitions and inappropriate RC4 and CRC-32 algorithms. All WEP weaknesses come from four main conception flaws:

(i) The initialization vector is transmitted as clear text.
(ii) The key is rarely renewed.
(iii) The WEP has not planned a mechanism to ensure data source authentication.
(iv) CRCs allow attackers to forge their own messages, and send.

In order to overcome the flaws of WEP, Wi-Fi Protected Access (WPA) was introduced in 2003 by the Wi-Fi (Wireless Fidelity) alliance [4].WPA implements majority of the IEEE 802.11istandard, thus it is an intermediate solution. WPA was intended to address the WEP cryptographic problems without requiring new hardware.

Revised Manuscript Received on 30 July 2015.
* Correspondence Author
Dr. D. J. Evanjaline, Department of Computer Applications, Jayaram College of Engineering & Technology, Anna University,Trichy, India.
Ms. N. Kalpana, Department of Computer Applications, Jayaram College of Engineering & Technology, Anna University,Trichy, India.
Mr. P. Raja Kumar, Department of Computer Applications, Jayaram College of Engineering & Technology, Anna University,Trichy, India.

II. WI-FI PROTECTED ACCESS (WPA)

WPA is a security protocol designed to create secure wireless (Wi-Fi) networks. It is similar to the WEP protocol, but offers improvements in the way it handles security keys and the way users are authorized. For an encrypted data transfer to work, both systems on the beginning and end of a data transfer must use the same encryption/decryption key. While WEP provides each authorized system with the same key, WPA uses the temporal key integrity protocol (TKIP), which dynamically changes the key that the systems use. This prevents intruders from creating their own encryption key to match the one used by the secure network. WPA also implements something called the Extensible Authentication Protocol (EAP) for authorizing users. Instead of authorizing computers based soley on their MAC address, WPA can use several other methods to verify each computer's identity. This makes it more difficult for unauthorized systems to gain access to the wireless network.

A. WPA Encryption Process

WPA uses Temporal Key Integrity Protocol (TKIP) for encryption [4]. A new key is dynamically generated for every packet; 128 bit per packet key is used. Michael algorithm is used by TKIP to generate Message Integrity Code (MIC) which provides enhanced data integrity as compared to CRC-32 used in EP. Also, TKIP provides replay protection. MSDU is Medium Access Control Service Data Unit and MPDU is Medium Access Control Protocol Data Unit

B. WPA Authentication Mechanisms

The two authentication mechanisms provided by WPA are

1) WPA - Personal or WPA - PSK (Pre - Shared Key):

Pre-Shared Key is a static key shared between two parti es for initiating the communication. The key which is a Pairwise Master Key (PMK) in TKIP process must be in place before an association can be established. WPA-Personal is suitable for home and small office networks and an authentication server is not required. The wireless devices are authenticated with access point using 256 bit key. The key is never transmitted over air since station and access point already possess this key before initiating the communication. Also, 64 bit MIC key and 128 bit encryption key can be derived from pre shared key.

2) WPA-Enterprise:

This is designed for enterprise /networks. IEEE 802.1x and Extensible Authentication Protocol (EAP) provide stronger authentication. In this mode, Remote Authentication Dial In User Service (RADIUS) server is required which provides excellent security for wireless network traffic.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The various EAP methods are EAP-Lightweight Extensible Authentication Protocol (EAP-LEAP),EAP-Flexible Authentication via Secure Tunneled (EAP FAST), EAP-Message Digest 5 (EAP-MD5), EAP-Transport Layer Security (EAP-TLS), EAP-Tunneled Transport Layer Security (EAP-TTLS), EAP Subscriber Identity Module of Global System for Mobile Communications (EAP-SIM). There are 3 components for EAP infrastructure: EAP - Peer: access client, attempting to access the network, EAP - Authenticator: access point that requires authentication before granting access to network, Authentication server: RADIUS server, validates credentials of EAP -Peer and authorizes network access

C. WPA Shortcomings

i) WPA uses old cryptography algorithm RC4 instead of superior Advanced Encryption Standard (AES).
ii) WPA is vulnerable to brute force attacks in case of weak passphrase for pre shared key mode.
iii) Prone to threats during Hash collisions due to use of hash functions for TKIP key mixing.
iv) Also, WPA remains vulnerable to availability attacks like Denial of Service.
v) WPA has greater performance overhead unlike WEP.
vi) Complicated setup is required for WPA – enterprise

I. PROPOSED SOLUTION: WPA IMPROVEMENT

WPA uses old cryptography algorithm RC4 instead of superior Advanced Encryption Standard (AES). This proposed scheme implemented in the application layer, and it is executed before entering in the WPA to protect information from eavesdropping and other types of attacks. The algorithm randomizes the data and prevents access from unauthorized users by adding some standard randomness to it.

Random Addressing Mechanism (RAM)

This RAM implemented in the application layer, and it is executed before entering in the WPA to protect information from eavesdropping and other types of attacks. The RAM shuffles the plain text based on the random addresses. The output produced by the RAM is taken as an input for WPA protocol.[5]

Encryption Algorithm: RAM -I(Block Shuffling)

Input: Binary form of Plain Text.

Output: Shuffled bit pattern of plain text.

Step 1: Divide the source file into number of blocks (n bits/block)

Step 2: Number the blocks from 1ton

Step 3: Generate the random block from the random numbers S_{12} sub-key generation algorithm. Consider as key r.

Step 4: The secret key r is, then XORed with different blocks of the source file.

$Sb = b_1 \oplus r, b_2 \oplus r, b_3 \oplus r \ldots\ldots b_n \oplus r$

Step 5: Generate random numbers controlled from 0.. n using the S_{12} key generation algorithm.

Step 6: Shuffle the blocks based on the random numbers.

Encryption Algorithm: RAM-II(Bits Shuffling)

Input: Output of RAM-I

Output: Shuffled Text

Step 1: Select any number of random numbers from as key r, where $0 \le r \le 7$.

Step 2: Each round takes one number from the key to specify the bit location called 'rbit' in each byte of RC4 sub-key k_2.

Step 3: A shuffle key is constructed by listing the numbers of bytes in the shuffle key with the value of bit number rbit equal to zero, followed by the numbers of bytes with the value of bit number rbit equal to one in the sub-key.

Step 4: The bits in the blocks are shuffled based on shuffled key.

Step 6: Rotate the blocks based on sum of shuffle keys.

Compression and Decompression

The cipher text is re-shuffled with the random numbers to get the source bits get back in its original form. The receiver will generate the plain text by XOR ing the random block with every other block. This decryption restores the original plain text without loss of integrity. The main idea of this algorithm is to split the input data into two data where the first data will contain original nonzero byte and the second data will contain bit value explaining position of nonzero and zero bytes. Both data then can be compress separately with other data compression algorithm to achieve maximum ompression ratio. Step-by-step of the compression process can be describe as below:

1.Read input per byte, can be all types of file.
2.Determine read byte as non zero or zero byte.
3.Write non zero byte into data I and write bit '1' into temporary byte data, or only write bit '0' into temporary byte data for zero input byte.
4.Repeat step 1-3 until temporary byte data filled with 8 bits of data.
5.If temporary byte data filled with 8 bit then write the byte value of temporary byte data into data II.
6.Clear temporary byte data.
7.Repeat step 1-6 until end of file is reach.
8.Write combined output data
  a) Write original input length.
  b)Write data I.
  c) Write data II.
9.If followed by another compression algorithm, data I and data II can be compress separately before combined (optional).

As for step-by-step of the decompression process can be describe below:

1. Read original input length.
2. If was compressed separately, decompress data I and data II (optional).
3. Read data II per bit.
4. Determine whether read bit is '0' or '1

Decryption

The decryption operation is similar to the encryption, but with the inverse of shuffle and rotate operations. First the receiver calculates the random numbers using the sub-key generation algorithm. Next the decryption of RAM-II performed. Last n^{th} iteration with nth key is executed first; then $n\text{-}1^{th}$ iteration executed and so on. Finally, the inverse of rotation is performed. After that, the decryption process of the RAM –I performed.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Experimental Results

For the proposed algorithm implementation, laptop Intel core I3 with 1.86 GHz CPU used, in which performance data is collected. In the experiments, the laptop encrypts a different file size ranges from 350 KB to 7.139MB. 140MB for text data, from 350 KB to 8090 KB for audio data, and from 4015 KB to 5073 KB for video files. Several performance metrics are collected for the different size files. The encryption time is considered the time that an encryption algorithm takes to produce a cipher text from a plaintext. Encryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption.

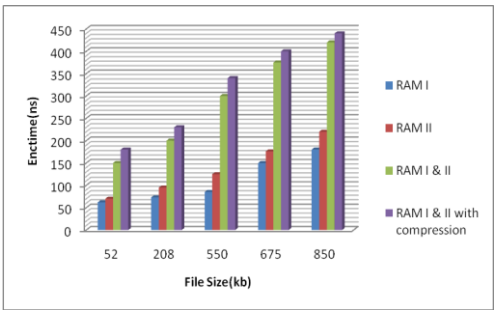

Figure 1. Encryptions of different size of text files

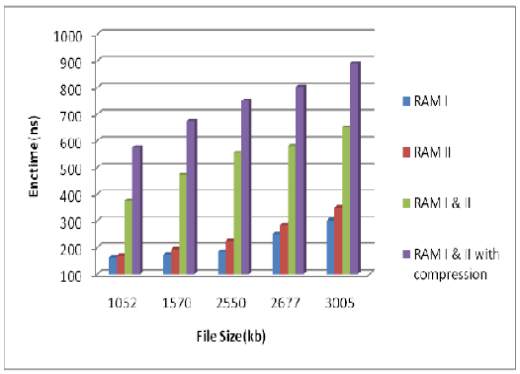

Figure 2. Encryptions of different size of video files

Experimental results of the proposed algorithm for video files compared to RC4 algorithm shown in Figure 2 at encryption stage. When combining RAM-I & II algorithms and compression takes more time for encryption similarly for text files. RAM encryption of image files shown in Figure 3

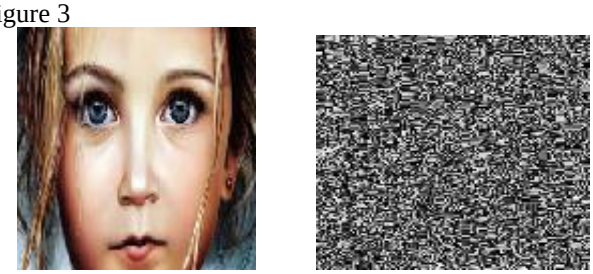

Figure 3. RAM Encryptions and Compression of image file

Figure 4 shows the performance comparison point of RAM and RAM with compression. It always shows that when combining encryption and compression increased the encryption time also increased.

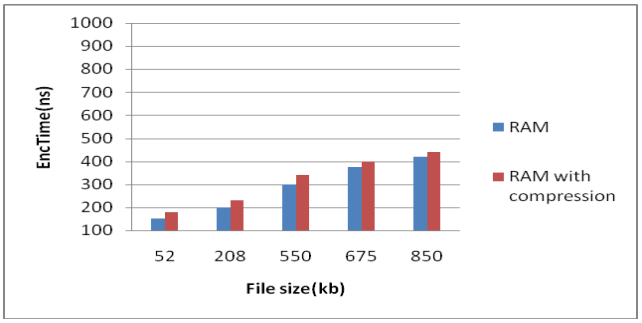

Figure 4. RAM Encryption with Compression

II. ADVANTAGES

The proposed modification to the existing WPA protocol makes it more secure and robust in terms of Message Privacy. If one or more bits in the key are changed, a different shuffle bit is chosen, and the substitution is changed. There is K x 2^b different possible shuffle vectors for an input of size b bytes encrypted in k iterations. So the brute force attack is impossible. When different keys were used with the same plain text, they produced different cipher texts. The fact that in the proposed mechanism frequently change the shared secret keys through the random numbers make any kind of cryptanalytic attack futile. The proposed system works well with the existing hardware and gives an edge over the present WEP protocol.

III. CONCLUSION

This paper describes how the proposed algorithms are achieved the security goal of WEP. The strength of the proposed algorithms is compared with WEP protocol. It proved that the time to the ability of enduring attack, break or crack the cipher text is increased. Furthermore, the proposed algorithms efficiently withstand the IV reuse attacks. This makes the brute force attack futile. In the nutshell when implementing all the three proposed algorithms in different layers of WLAN thwarts all kind of cryptanalytic attacks.

REFERENCES

1. Mohamed Juwaini, Raed Alsaqour, Maha Abdelhaq , “A Review On WEP Wireless Security Protocol,” Journal of Theoretical and Applied Information Technology, ISSN: 1992-8645, E-ISSN: 1817-3195 Vol. 40 No.1, 15 June 2012.
2. Dr.R.N. Rajotiya, Pridhi Arora, “Enhancing Security of WI-FI Network”, International Journal of Computer Applications, ISSN: 2250 – 1797, Issue 2, Vol 3, June 2012.
3. Arash Habibi Lashkari,Farnaz Towhidi,Raheleh Sadat Hosseini.Wired Equivalent Privacy (WEP). International Conference on Future Computer and Communication, IEEE, 2009.
4. Lashkari, A.H.; Mansoor, M.; Danesh, A.S.; Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA). International Conference on Signal Processing System. IEEE, 2009
5. DR.D.J.Evanjaline,P.Rajakumar,N.Kalpana; Two Tier Security Enhancement of Wireless Protocol WEP(Wired Equivalent Privacy). International Journal of Soft Computing and Engineering.ISSN: 2231-2307, Volume-5, Issue-I, March 2015.
6. Lashkari, A.H., A survey on wireless security Protocols (WEP, WPA and WPA2/802.11i), Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on 8-11 Aug 2009, E-ISBN: 978-1- 4244-3878-5
7. Sandirigama, M, Security weaknesses of WEP Protocol IEEE 802.11b and enhancing the Security with dynamic keys, Science and Technology for Humanity (TIC- STH), 2009, IEEE Toronto International Conference

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)