Encryption and Key Management Mechanisms in WLANs

Divya Amunugama
Department of Computer Systems Engineering
Faculty of Computing and Technology,
University of Kelaniya,
Kelaniya, Sri Lanka
damunugama8@gmail.com

Niromi C. Kotikambage
Department of Software Engineering
Faculty of Computing and Technology,
University of Kelaniya,
Kelaniya, Sri Lanka
niromi8@gmail.com

***Abstract* — Wireless technologies have been evolving rapidly for a considerably long time. As these wireless networks communicate through radio transmissions, they are vulnerable to attacks. Thus, to minimize these attacks a number of key management algorithms are introduced under 802.11 standards. In this paper, the authors will be discussing the cryptographic algorithms used in the cases of wireless networks.**

Keywords — WEP, WPA, Wireless networks, encryption, decryption, authentication

I. INTRODUCTION

With massive increase in the usage of technology, networks have become a very important and an underlying technology for all the technological development. Networks have been developed from the primitive wired networks which communicate through cables to wireless networks which communicate through radio waves.

The main principle that governs wireless networks is mobility. Communication in wireless networks happens between a transmitter and a receiver by using radio signals as the medium of transmission [3].

The benefits of WLANs are the mobility, scalability, flexibility, cost, ease of installation, reliability and reduced installation time.

The IEEE standard for wireless networks is 802.11. There are a number of IEEE standards introduced for wireless networks. These standards differ by their range, frequency, data rates and some characteristics. The currently used IEEE wireless network standards are mentioned in the Table 1 below.

Table 1. Wireless Network standards according to IEEE

Standard	Data Rate	Frequency	Range	
			Indoor	Outdoor
802.11a	5 GHz	54 Mbps	100 ft.	400 ft.
802.11b	2.4 GHz	11 Mbps	100 ft.	450 ft.
802.11g	2.4 GHz	54 Mbps	125 ft.	450 ft.
802.11n	2.4 GHz / 5 GHz	600 Mbps	225 ft.	825 ft.
802.11ac	5 GHz	1 Gbps	90ft	1000 ft

As the name implies, wireless technology requires no wires for the devices to be connected to the networks, thus, making this technology more convenient and easier to use. With all these efficient features of WLANs comes the need for a secure network, as the networks are wireless, they are more vulnerable to attacks. Thus, a proper set of security precautionary measures are required for a secure communication between devices connected through wireless networks.

Various cryptographic algorithms are used in order to secure the communication in WLANs. A cryptographic algorithm is a mathematical function used to encrypt or decrypt a message communicated within a network. The main component of a cryptographic algorithm is the key used for communication. The key should always be a secret.

There are different types of cryptosystems. Namely: Symmetric encryption, Asymmetric encryption, Physical encryption and Quantum encryption.

The types of ciphers are Substitution cipher, Transposition cipher, Steganographic cipher, Stream cipher and Block cipher.

A good cryptographic algorithm should not display patterns, should maintain One-way-ness and the algorithms should not be very complex but should be secure. This security means that the best attack on the weakest part of the cryptosystem should take a long enough time, usually expressed in terms of basic operations on a PC, in 2^n, where n is the security level. This unit is used to refer to the time that breaking a theoretically perfect symmetric cipher would need: with a key size of 128 bits, testing all the possible 2^{128} keys takes 2^{128} operations, where one operation is one tentative of decryption.

This review paper discusses about the set of security measure taken by WLANs in order to provide a secure communication without any tampering or attacks targeted towards the devices connected. The security measures are specifically the key management methods and the encryption and decryption methods of the communication happening through WLANs.

II. WIRED EQUIVALENT PRIVACY (WEP)

WEP has been the main security provision [1] as well one of the most common security protocols [2] introduced for 802.11 standard (Wi-Fi). As the name implies WEP was introduced to provide privacy equivalent to that of wired networks [1].

The goals of introducing the WEP protocol were as follows: Avoid eavesdropping, protect the privacy of information, prevent manipulation of data and detect tampering of data.

WEP operation is a three-step procedure. The three steps are authentication, encryption and decryption. The following section provides a detailed explanation about the three steps.

A. WEP Authentication

The authentication process prevents any unauthorized access to the Wireless network. Authentication is maintained using the pre-shared WEP key. The authentication process is explained in figure 1.

ISSN 2756-9160 / November 2020.
International Conference on Advances in Computing and Technology (ICACT–2020) Proceedings

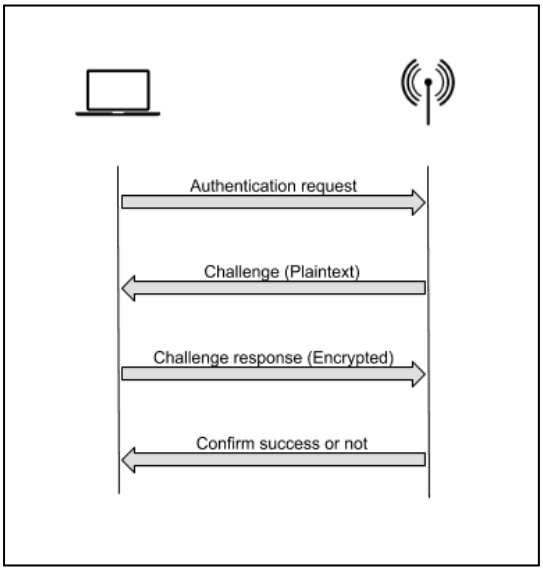

Fig. 1. WEP authentication mechanism

Step 01 - The client sends an authentication request to the access point to get connected to Wireless network.

Step 02 - Once the AP receives the request the AP sends a plaintext challenge to the client who sent the request.

Step 03 - The client encrypts the challenge by using the pre shared WEP key and sends the encrypted challenge response to the AP. The AP then decrypts the Challenge response using the Pre-Shared WEP key and matches it with the original plaintext challenge sent.

Step 04 - Once the matching is done, the AP sends a confirmation message, mentioning if it was successful or not.

This is the 04-way handshake of the WEP authentication process between the client and the Access point.

B. WEP Encryption

WEP uses Rivest Cipher 4 (RC4) algorithm for the encryption process. RC4 is a widely used stream cipher algorithm in software applications. Figure 2 illustrates the block diagram of the WEP encryption process.

The RC4 algorithm consists of two main operations

1. Pseudo Random Number Generation (PRNG)
2. Creating a key stream

Step 01 - The sender of the message does an integrity check to the plaintext to be sent and obtains an Integrity Check Value (ICV).

Step 02 - An Initialization Vector (IV) concatenated with the pre shared WEP key is sent into the RC4 algorithm. (IV = 24 bits and WEP key = 40 bits) RC4 creates a Pseudo Random number using the PRNG operation. This PGNR is used to generate the key stream.

Step 03 - The generated key stream is XOR ed with the plain text and the ICV.

Step 04 - The output of the XOR function provides the cipher text. This ciphertext / encrypted message is sent to the receiver together with the IV.

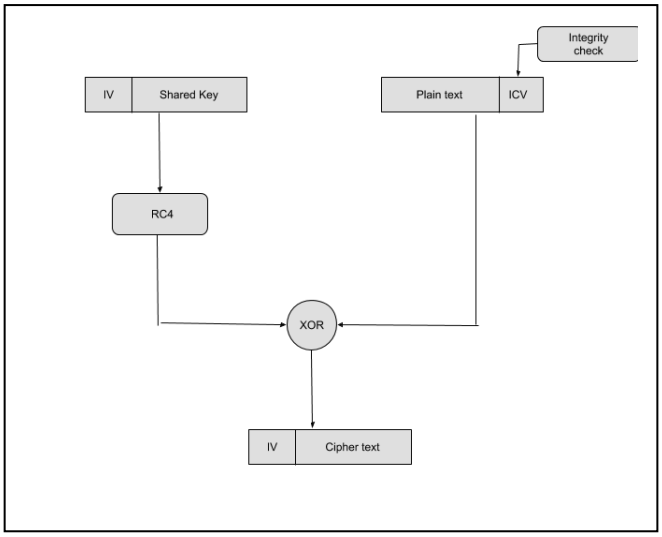

Fig. 2. WEP encryption mechanism

C. WEP Decryption

The decryption process is the same process as the encryption process, just reversed. Figure 3 illustrates the WEP decryption process.

Step 01 - The initialization vector is obtained from the header of the packer received from the sender.

Step 02 - The IV is concatenated with the PSK of WEP and sent through the RC4 algorithm function.

Step 03 - The key stream output of the RC4 algorithm is XOR ed with the ciphertext sent by the sender.

Step 04 - The output of XOR is the plaintext.

Step 05 - Further this plaintext is sent through an integrity check and the value received is matched with the original ICV.

Step 06 - If the values are matched the receiver receives the message [2] [7].

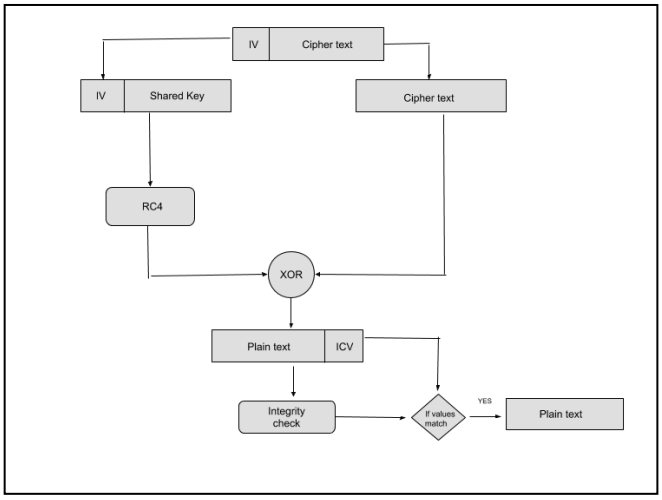

Fig. 3. WEP decryption mechanism

III. WI-FI PROTECTED ACCESS (WPA)

WPA is a solution to the limitations of WEP that was discussed in the section above. WPA has 2 operation modes. The operation modes are as follows: [2][7]

a. Personal mode - This mode has no authentication server and the secret key is shared between the client and the access point. It is also known as WPA-PSK [7].

b. Enterprise mode - This mode uses an authentication server that has security controls to avoid unauthorized access [7].

Similar to WEP, WPA also contains 03 steps as follows: authentication, encryption and decryption [4].

A. *WPA Authentication*

WPA uses 802.1x and EAP for authentication of users.

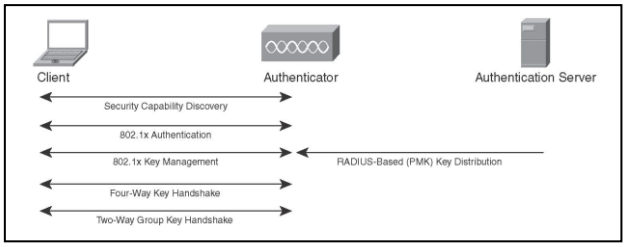

Fig 4 - WPA enterprise mode authentication

B. *WPA Encryption*

The weaknesses of WEP are avoided by using Temporal Key Integrity Protocol (TKIP) as the encryption algorithm. [6] The use of TKIP assures that data will remain protected. In WPA, the key is changed for every frame and change is communicated between the AP and the client [5] [2].

Unlike in WEP, the key is automatically distributed and there are dynamic session keys.

The encryption process consists of the following parameters: Initialization Vector, Data encryption key, Source Address, Destination Address, Priority field value, Data integrity key.

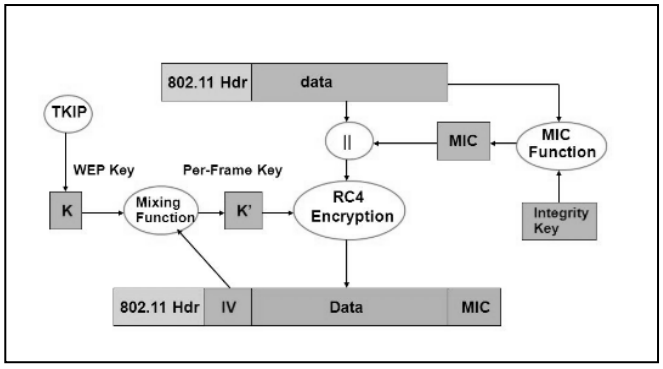

Fig 5 - WPA encryption mechanism [8]

WPA should: allow only authorized users to access the network and protects data, should be interoperable in all IEEE wireless standards and use dynamic session keys [7].

An alternative to TKIP (which was introduced as a temporary protocol in IEEE 802.11) a protocol has been introduced with higher security features. This protocol is Counter Mode Cipher Block Chaining Message Authentication Code Protocol (Counter Mode CBC-MAC Protocol - CCMP) [9]. CCMP is the latest and the standard protocol used to maintain both integrity and data confidentiality in WPA – II. It provides data confidentiality, authentication and access control. This is because CCMP is a block cipher of a key size of 128 bits [9].

IV. Conclusion

In this paper, the author has discussed the encryption and authentication mechanisms used in the key management of wireless networks. These discussed topics of this area are some of the common protocols used. This review paper will be useful for future researches planning to conduct research or build new algorithms related to the wireless networks' domain.

In conclusion, WEP can be identified as a depreciated protocol due to the usage of short keys and using WPA-II is the best solution for security of a WLAN due to the large key size of at least 128 bits.

References

[1] D. Gritzalis and T. Karygiannis, "Editorial - "Wireless Network Security"", *Computers & Security*, vol. 28, no. 8, pp. 729-730, 2009. Available: 10.1016/j.cose.2009.10.004.

[2] V. Poddar and H. Choudhary, "A Comparitive Analysis of Wireless Security Protocols (WEP And WPA2)", *International Journal on AdHoc Networking Systems*, vol. 4, no. 3, pp. 1-7, 2014. Available: 10.5121/ijans.2014.4301.

[3] U. Wadhwa, "Wireless network security: Tough times", *Conference: 2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*,2015. Available: 10.1109/ICGCIoT.2015.7380613

[4] R.Bhatnagar and V. Kumar, "Wi-Fi security: A Literature review of security in wireless network" *IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET)*, vol. 3, Issue 5, May 2015, 23-30

[5] E. Lorente, C. Meijer and R. Verdult, "Scrutinizing WPA2 Password Generating Algorithms in Wireless Routers", *Usenix.org*, 2020. [Online]. Available: https://www.usenix.org/conference/woot15/workshop-program/presentation/lorente. [Accessed: 05- Oct- 2020].

[6] Ismail Mansour, Gérard Chalhoub, Pascal Lafourcade. "Key Management inWireless Sensor Networks", *Journal of sensor and actuator networks*, MDPI, 2015, 4 (3), pp.251 - 273. ff10.3390/jsan4030251ff. ffhal-01593134f

[7] Y. Zou, J. Zhu, X. Wang and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends", *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727-1765, 2016. Available: 10.1109/jproc.2016.2558521.

[8] "Hacking Wireless Networks (Part II – WEP & WPA) - ppt video online download", *Slideplayer.com*, 2020. [Online]. Available: http://slideplayer.com/slide/8774040/. [Accessed: 05- Oct- 2020].

[9] What is the difference between TKIP and CCMP? – Computer Technology Pass. Comtechpass.com. (2020). Retrieved 6 November 2020, from http://www.comtechpass.com/what-is-the-difference-between-tkip-and-ccmp/.