International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 12, December - 2013

Comparative Analysis: Wi-Fi Security Protocols

Mayank Verma
M.Tech Scholar
JECRC University

Jitendra Yadav
Assistant Professor
JECRC University

Abstract: *In recent years, various wireless LAN technologies have gained rapid popularity and Wi-Fi can be cited as most prominent or proficient technology today. Wi-Fi stands for Wireless Fidelity and it operates in the unlicensed 2.4 GHz radio spectrum, support variable data rates and it is used to define the wireless technology in the IEEE 802.11b standard. Wireless network provides many advantages like mobility, cut costs but it is coupled with many security threats such as replay attack, eaves dropping, denial of services attack etc. The threats of intrusion into the wireless network have forced user to adopt a range of security.*

This paper presents an analysis of the three security protocols, from the WLANs security requirements point of view. In this paper, we discuss the wireless security protocols with details about the encryption & authentication mechanism used and their limitations.

Keywords: Advanced Encryption Standard (AES), Message Integrity Check (MIC), Rivest Cipher 4 (RC4), Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 2 (WPA 2), Temporal Key Integrity Protocol (TKIP)

I. INTRODUCTION

Wi-Fi can be defined as an arrangement of wirelessly connecting devices that use radio waves for communication, allowing for connection between devices without the outlay of unwieldy cables or without needing them to be facing one another. Wireless local area networks (WLANs) have achieved a tremendous amount of growth in recent years. Between various WLAN technologies, the IEEE 802.11b based wireless LAN technology, Wireless Fidelity (Wi-Fi), can be cited as most prominent technology today.

In a perfect world, without wires we could, "send a lot of data, very far, very fast, for many separate uses, and all at once". Unfortunately, we do not live in a perfect world; there are physical barriers that will not allow all of these goals to occur simultaneously [1]. When form front a wireless LAN, it is very important to set up secure methods for encryption and authentication so that the network can be used by those devices or individuals that are authorized. In past years several security protocols like Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and Wi-Fi Protected Access2 (WPA2) were emerged to add more authentication, confidentiality, message integrity in WLAN.

The objective of this paper is to present an analysis of the most efficient and used security protocols implemented to overcome the security problem of WLANs. This paper also discusses about vulnerabilities & weakness of wireless security protocols. Wired Equivalent Privacy (WEP) which was the first protocol for securing wireless network will be covered in Section 2, Wi-Fi Protected Access (WPA2) and Wi-Fi Protected Access 2 (WPA2) are discussed in Section 3 and 4 respectively. Section 5 presents a conclusion and comparative analysis between different wireless security protocols.

II. WIRED EQUIVALENT PRIVACY

Wired Equivalent Privacy (WEP) is the first encryption algorithm introduced for Wi-Fi to make the wireless network at least as secure as a wired LAN. It has no particular protection mechanism. WEP was used to define the wireless security in the IEEE 802.11 standard and it was ratified in September 1999. The objective of Wired Equivalent Privacy (WEP) is to provide security akin to that of wired networks. Rivest Cipher4 (RC4) stream cipher is used by WEP to secure wireless network in terms of confidentiality and CRC-32 for data integrity. The standard specified for WEP provides support for 40-bit key only but non standard extensions have been provided by various vendors which provide support for key length 128 and 256 bits as well[2]. Standard 64-bit WEP uses a 40-bit shared key which concatenated with 24-bit initialization vector (IV) to form the RC4 traffic key.

A. WEP Encryption/Decryption Process

WEP encryption process includes following steps:

1. 40-bit secret key is concatenated with 24-bit initialization vector (IV).
2. The resultant WEP traffic key act as seed to Pseudo Random Number Generator (PRNG).
3. Integrity Check Value (ICV) is generated by performing4 CRC-32 Integrity Algorithm on plain text.
4. The PRNG generates a key sequence (K) of pseudorandom octets equal in length to the number of data octets that are to be transmitted plus 4 (since the key sequence is used to protect the Integrity Check Value (ICV) as well as the data).
5. Afterwards, RC4 encryption process is applied on Plain text + ICV and Key generated by PRNG to generate cipher text.

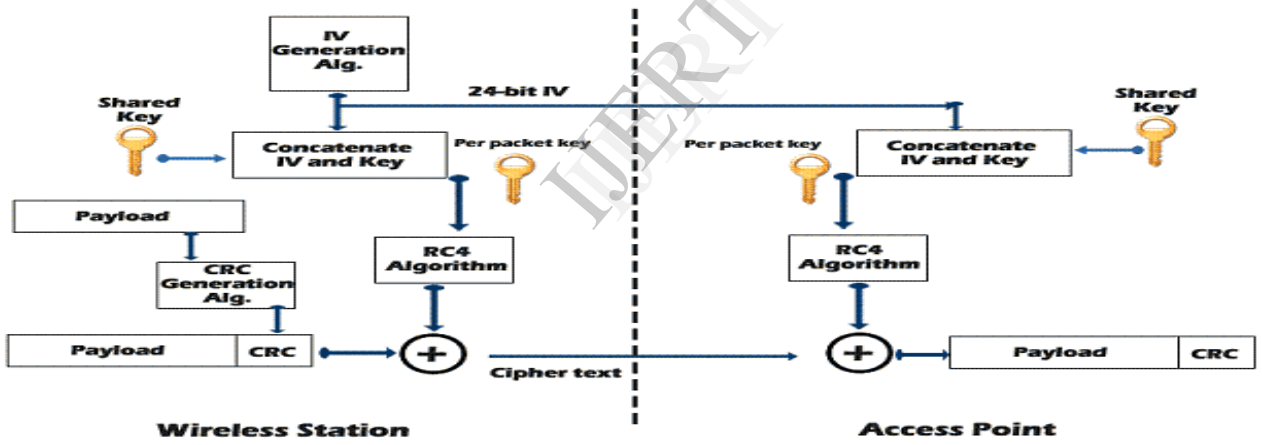

Figure 1: WEP Encryption Process [3, 3]

WEP Decryption process consists of following steps:

1. RC4 algorithm is applied to cipher text and key sequence to get plain text and ICV.
2. Plain text and original ICV is obtained.
3. To generate new ICV, plain text acts as seed value to Integrity Algorithm.
4. Finally, new ICV is compared with original ICV to verify the result.

B. WEP weaknesses

1. Authentication related issue, uses one way authentication.
2. Lack of Key Management, same keys is used for longer duration.
3. No session key is established during authentication.
4. No replay protection.
5. Attacker can easily crack the key and can manipulate the data.

6. The size of Initialization Vector (IV) is short and can be reused.
7. Flooding cause denial of service attack.
8. Easy forging of authentication message.

III. Wi-Fi PROTECTED ACCESS (WPA)

Wi-Fi Protected Access (WPA) is an enhanced version of wireless security which was introduced in 2003 by the Wi-Fi Alliance to overcome the flaws of WEP. As WEP was all broken, lot of cryptographic attacks were discovered like FMS attack, PTW attack etc. and basically what happen WEP was broken beyond repair. Then IEEE committee admitted that WEP cannot hold the required security concern and introduced WPA as an intermediate solution to WEP. IEEE committee recommended user to upgrade to WPA, which uses Temporal Key Integrity Protocol (TKIP) based on WEP for encryption. WPA runs on the same hardware that WEP does and requires only firmware update. While still utilizing RC4 encryption, TKIP utilizes a temporal encryption key that is regularly renewed, making it more difficult for a key to be stolen and then used to decipher a useful amount of information. In addition, data integrity was improved through the use of more robust hashing mechanism, the Michael Message Integrity Check (MMIC) [4]. It can also use AES for encryption but not all WPA hardware supports AES.

A. WPA Encryption Process

To improve data encryption, WPA makes practical and effective use of TKIP. TKIP dynamically changes keys for each packet as the system is used; 128-bit per packet key is used. Michael algorithm is used to provide a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP.

B. WPA Authentication Mechanism

WPA can be enabled in two authentication versions:

1. **WPA-Personal:** This is mostly suitable for small offices or home computers. WPA-Personal is also known as WPA-PSK (Pre-Shared Key). For initiating the communication this static key is shared between two communicating parties. The key which is a Pairwise Master Key (PMK) in TKIP process must be in place before an association can be established [2, 23]. With WPA-PSK we shape each WLAN node and the wireless devices are authenticated with access point using 256-bit key.

2. **WPA-Enterprise:** This is designed for large corporation, business or enterprise networks. WPA-enterprise set up 802.1x authentication by means of a Remote Authentication Dial In User Service (RADIUS) and Extensible Authentication Protocol (EAP) to provide stronger authentication. The Enterprise mode gives dynamic encryption keys distributed securely after a user logins with their username and password or provides a valid digital certificate. Users never see the actual encryption keys and they aren't stored on the device. WPA-Enterprises provide excellent security to the wireless network traffic. 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).

C. WPA Weaknesses

1. WPA uses weak encryption algorithm RC4 instead of Advanced Encryption Standard (AES).
2. Open source utility called Reaver can bypass WPA password if Wi-Fi Protected Setup (WPS) is enabled.
3. WPA is vulnerable to dictionary attack in case of weak passphrase.
4. It is vulnerable to Denial of Service (DOS) attack.
5. Increased data packet size leading to longer transmission
6. Complex setup is required for WPA-enterprise.
7. Incompatibility issues with legacy hardware.
8. Larger performance overhead.

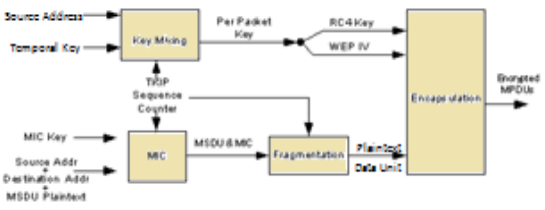

Figure 2: TKIP encryption process

IV.Wi-Fi PROTECTED ACCESS 2 (WPA2)

Wi-Fi Protected Access 2 (WPA2) is used to define the wireless technology in the IEEE 802.11i standard. WPA 2 draft standard was authenticated on 24th June, 2004 and established in September, 2004. WPA 2 is an enhanced version which uses AES instead of TKIP to overcome the flaws of WPA. In particular, the Michael Algorithm (MIC) is replaced by a message authentication code, CCMP, that is considered fully secure, and RC4 is replaced by AES (Advanced Encryption Standard) [5]. Similar to WPA, WPA 2 also includes two modes of authentication i.e. WPA2-Personal and WPA2-Enterprise.

A. WPA 2 Encryption/Decryption Process

CCMP encryption consists of following steps:

1. For every Medium Access Control Protocol Data Unit (MPDU), packet number (PN) is incremented by a positive number and is unconnected for MPDU's sharing an identical temporal key.
2. Additional Authentication Data (AAD) is constructed and integrity protection for the fields is included in the AAD which is provided by CCM algorithm.
3. CCM Nonce block is constructed using PN, MPDU address 2 and the priority field (PF). PF value is set to zero.
4. 8-octet CCMP header is constructed using new PN and key identifier.
5. To form cipher text and MIC, the temporal key, AAD, MIC, MPDU data are used.
6. As a result the encrypted MPDU is formed by integrating the encrypted data, MIC, original MPDU header and the CCMP header.

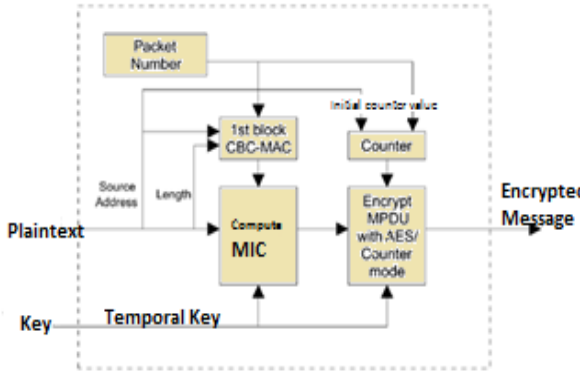

Figure 3: CCMP encryption process

And, the decryption process is done in reverse order to obtain plaintext MPDU. It is done by concatenating the received MPDU header and the MPDU plaintext data from CCMP processing.

B. WPA 2 Weakness:

1. Unencrypted management and control frames lead to DOS attack.
2. Deauthentication lead to MAC address spoofing.
3. Brute Force Attack due to use of weak passphrase in WPA2-Personal.
4. WPA 2 is expensive as it needs change in existing hardware.
5. Management frames that are used to report network topology are not encrypted thus enabling attacker to analyze the network layout [6].
6. WPA2-Enterprise which is based on port-based 802.1x access control protocol is prone to Hole196 vulnerability [7].
7. Jamming and Flooding of large size packets.
8. WPA 2 not supports legacy hardware.

V. CONCLUSION

In this paper, we present different protocols for securing Wireless LAN. As wireless LAN gaining rapid popularity it is necessary to utilize some of the security protocol which ensure that the data communication is secure. Besides all wireless LAN technologies, Wi-Fi is most popular and uses air as a medium for communication. And the communication through air is not secure enough. The IEEE committee decided to form front some security protocols namely WEP, WPA and WPA 2. WEP was the first security protocol but it was unable to provide security against various attacks. Then, WPA was introduced as a subset of IEEE 802.11i standard and it was considered as a quick patch over the flaws of WEP. But, it is still vulnerable to various attacks due to loopholes in the TKIP algorithm. Thus, an enhanced version WPA 2 was introduced by Wi-Fi Alliance. WPA 2 protocol uses Advanced Encryption Standard (AES) to provide stronger encryption with CCMP algorithm. But it is still prone to various threats due to sharing of Group Transient Key and Management Frames in unencrypted form. After analyzing the three

wireless security or encryption protocols and enumerating their weaknesses, we clear that WPA 2 is sufficiently great improvement over WEP and WPA. And it is also anticipated that in the continuing paper, we will present the suggestion or solution addressing WPA 2 weaknesses.

Table 1: Comparison of security protocols

	WEP	**WPA**	**WPA 2**
Encryption	RC4	TKIP based on RC4	AES-CCMP
Key Length	40bits and non standard extension (128 and 256 bits)	128-bits	128-bits or more depend on rounds
Data Integrity	CRC-32	Michael algorithm	CBC-MAC
Replay Protection	NO	YES	YES
Authentication	NO (open or shared not secured)	IEEE 802.1x or PSK	IEEE 802.11X
Network Performance	High	Less than WEP and Higher than WPA 2	Lesser

REFERENCES

[1] Leeper, David G, "A Long Term View of Short Range Wireless", Computer, IEEE Computer Society, June 2001.
[2] Swati Sukhija, Shilpi Gupta, "Wireless Network Security Protocols A Comparative Study", *International Journal of Emerging Technology and Advanced Engineering*, 2(1), 2012.
[3] Muhammad Juwaini, Raed Alsaquor, Maha Abdelhaq, Ola Alsukour, "A Review on WEP Wireless Security Protocol", *Journal of Theoretical and Applied Information Technology*, 40(1), 2012.
[4] Siemens Enterprise Communications Whitepaper, "WLAN Security Today: Wireless more Secure than Wired", 2008.
[5] Vandana Wekhande, "Wi-Fi Technology: Security Issues", *Rivier Academic Journal*, 2(2), 2006.
[6] Paul Arana, "Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2)", INFS 612, 2006.
[7] Shadi R. Masadeh and Nidal Turab, "A Formal Evaluation of the Security Schemes for Wireless Networks", *Research Journal of Applied Sciences, Engineering and Technology*, 3(9), 2011.
[8] Min-kyu Choi1, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim, "Wireless Network Security: Vulnerabilities, Threats and Countermeasures", *International Journal of Multimedia and Ubiquitous Engineering*, 3(3), 2008.
[9] Frank H. Katz Armstrong, Atlantic State University, "WPA vs. WPA2: Is WPA2 Really an Improvement on WPA".
[10] Nidal Turab, Florica Moldoveanu, "A Comparison Between Wireless LAN Security Protocols", U.P.B. Scientific Bulletin, 71(1), 2009.