International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 7, Issue 1, January - February 2018 ISSN 2278-6856

Wi-Fi Security protocols: A survey

Kritika Singh[1], Vishal Gupta[2]

[1] Ambedkar Institute of Advanced Communication Technologies and Research, Department of Computer Science & Engineering, New Delhi, India

[2]Ambedkar Institute of Advanced Communication Technologies and Research, Department of Computer Science & Engineering, New Delhi, India

Abstract

Over the years, the wireless technology has evolved significantly and therefore the need to protect the wireless network becomes equally substantial. The choice of the best security protocol has always been an issue for the IT security staff. This paper illustrates various types of security mechanisms of wireless LAN. These security protocols are (802.11 Wired Equivalent Privacy, 802.11i Wi-Fi Protected Access and Wi-Fi Protected Access-2). The paper gives an overview of the key concepts and the working of the wireless security protocols, their limitations and the countermeasures introduced. The three protocols are also compared on the basis of the common features so as to give a deeper insight.

Keywords: WLAN security, WEP, WPA, WPA2, 802.1X-based Authentication.

1. INTRODUCTION

Wireless networks offer a lot of benefits like scalability, flexibility, they are easy to install and also provide mobility to the devices. The data in the wireless networks is generally transmitted via radio waves which travel across the network through air, finally reaching the intended radio receiver. Since radio waves are not directional, some travel in all directions. Therefore, there arises a need to protect the data. Wireless technologies also include infrared devices like remote controls, cordless keyboards etc.

The wireless networks are classified as:

(i)Wireless Personal Area Network (WPAN)

This network requires low power transmission because it is a very small-scale network which covers only small local areas. Examples include mobile computing devices like PCs, wireless keyboard, mouse, PDAs [1]. The devices are usually needed to be placed in a close proximity to each other (within a several meters) for them to communicate with one another, with no infrastructure. WPAN works on the IEEE 802.15 standard. Some of the technologies used by WPAN are Bluetooth and Infrared data association [2].

(ii) Wireless Local Area Network (WLAN)

It is a wireless network that operates within a small geographic region, such as a campus, home or a building. One such type of wireless LAN is Wi-Fi, it generally uses 2.4GHz of frequency bands but 5GHz ISM band is also opted by users to provide additional bandwidth. Wi-Fi supports 802.11 standards.

(iii) Wireless Metropolitan Area Network (WMAN)

It is a network that provides connectivity to the users within a metropolitan area (generally a few kilometers). These networks are larger in size as compared to WLAN; therefore their functionalities also differ from each other. They establish a connection between the different buildings. Many WMANs also provides broadband access to the users in local areas [2].

(iv) Wireless Wide Area Network (WWAN)

This network can provide connectivity to the users and the devices across large geographic areas. They are mainly used for mobile and satellite communications. WWANs include technologies like Global System for Mobile Communications (GSM), UMTS, cellular, CDMA One/CDMA2000 and Wi-Max.

2. LITERATURE SURVEY

802.11 families were designed by IEEE to provide a high date rate to the applications and connectivity to the mobile and portable devices. The first IEEE standard: 802.11 which released it 1997 is obsolete now. It provided 1 Mbps or 2 Mbps of wireless data transmission. Wired Equivalent Privacy (WEP), a security protocol was also introduced in this standard with the intention to provide data integrity and confidentiality to the wireless network [3]. Many of the vulnerabilities [4], [5], [6], [7] were detected in WEP soon after its release; several of them are outlined in this paper. It was followed in 1999 by 802.11a. It supported 54 Mbps and operated on 5 GHz band. Also, in 1999 802.11b was released, supporting 11 Mbps of data rate and operating in the 2.4 – 2.48 GHz band [8]. In 2004, WPA ousted WEP by acting as stopgap to provide immediate solutions to the WEP vulnerabilities. Temporal Key Integrity Protocol was use in WPA to make it more secure [6]. It provided better integrity using Message Integrity Check (MIC) which was not included in WEP [9].

Afterwards, WPA2 came with the improvements which made it even more efficient and resistant to attack. Many researchers have detected vulnerabilities in this protocol. Hwang et al. [13] proposed a wireless Man in the Middle (MITM) framework proving that a MITM attack is possible during the authentication mechanism of WPA2. Denial of Service attack [19], jamming and replay attack [20] are the most common attacks that are performed on WPA. There are many controls that have been proposed by different researchers, which make it less vulnerable to attacks. Temporal Safe Tunnels method is used to establish a more secure connection between the client and the AP [18]. Eien et al. proposed a method in which deadlocks can be

detected before they can cause much harm [19]. Secure Control Packets provides protection against the NAV jamming attacks, as shown in [18]. Several other controls have also been presented in the later section of this paper.

802.11w standard was introduced in 2009. This standard was designed to increase the security in the management frames. The wireless network remains vulnerable to jamming attacks and other vulnerabilities are present due to hardware limitations [15, 17, 18]. Xiong et al. [20] proposed a SecureArray which provides against most the vulnerabilities mentioned above.

The rest of the paper is organized as follows: section 3 briefly discusses the key concepts of the Wi-Fi security protocols, their vulnerabilities, strengths and the comparison is also outlined. The section 4 presents several other vulnerabilities and controls scrutinized by various researchers. These vulnerabilities and controls mainly focus on the authentication mechanism of the security protocols. Finally, the paper concludes with highlighting all the important aspects of this study.

2.1 WIRELESS SECURITY PROTOCOLS OVERVIEW

2.1.1 Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) was introduced in 1997 with the intention to provide security to the wireless network through encryption and checksum. WEP uses the traditional stream cipher RC4 as shown in the Figure 1 [3]. The purpose of using RC4 for WEP encryption was to provide data confidentiality and integrity with less CPU utilization and complexity [7] (refer Figure 1).

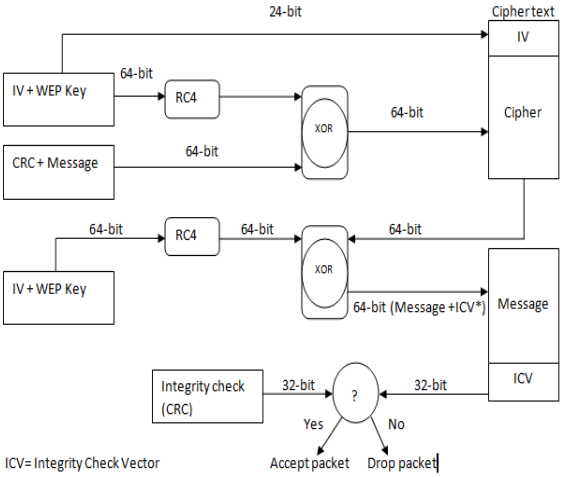

Figure 1 WEP working [3]

At the time of encryption, a 40-bit master key combines with a 24-bit Initialization vector to form a 64-bit seed; it goes though the RC4 algorithm. The output of the RC4 algorithm is the random key sequences. The second input is the actual message along with its checksum, after passing both the inputs through XOR function the cipher text is generated. On the receiver's side the master key and the IV is used to decrypt the message and its checksum and calculates the checksum again.

Vulnerabilities of WEP

Although WEP was intended to be efficient, there were many flaws in technique that made it easily crackable. The problems in the RC4 algorithm are presented by Fluhrer, Mantin and Shamir in [4]. They described that WEP can be attacked through a cipher-text only attacked against the KSA of RC4. Some information about the individual key bytes can be leaked by the first byte generated by RC4 which means that if enough WEP-encrypted packets were analyzed, there could be possibility of reconstructing the key in WEP. Demonstration of this attack was later shown by Stubble-field et al. [5].

The flaws in WEP can be summarised as follows [6]:

- The forgery of packets cannot be prevented in WEP.
- Replay attacks are not prevented.
- RC4 was easily crackable.
- Weak keys could be cracked by brute force attack which only took minutes to hours on standard computers.
- The IV was being sent to receiver in the clear text which was not secure.
- CRC-32 checksum was weak and did not provide adequate security.
- 24-bits IV was relatively small which provided only limited initialization vectors, after that they were just being reused [7].
- The message can be modified without knowing the encryption key.
- Key management is not included.

2.1.2 Wi-Fi Protected Access (WPA)

WEP weakness is patched up to some extent through WPA. It implements Temporary Key integrity Protocol (TKIP), which allowed better mixing of the key with the IV. WPA was designed so that it could work with the existing hardware that was enabled with WEP. WPA included improvements that added more security features in the WEP.

The strengths of WPA can be summarised as follows [6]:

- It uses Temporal Key Integrity Protocol (TKIP) that is quick fix to the security problems of WEP without any requirement of hardware upgrade. Hashing algorithm is used to ensure the integrity of the key.
- The size of the IV is increased to 48 bits. It mixes the key well with the IV unlike in WEP.
- The sequence counter was used to prevent the replay attacks.
- Extensible Authentication Protocol (EAP) is used to provide a much stronger authentication.
- The integrity of the data is maintained through a Message Integrity Code (MIC) [9].

Vulnerabilities of WPA

In 2004, two tools were released to perform the brute-force attack on WPA-PSK to determine the passphrase. First tool was "WPA Cracker", it was released by Takehiro

Takahashi and another tool known as "cowpatty" was released by Josh Wright [10], [6].

The flaws of WPA are as follows:

- WPA retains the old stream cipher RC4 which was already proved to be weak even in WEP.
- Brute force attacks are possible if weak passphrase is used [6].
- Denial of Service attacks is possible in WPA as shown in [19].
- WPA has greater performance overhead unlike WEP.
- WPA-enterprise requires a complicated setup.

2.1.3 Wi-Fi Protected Access-2 (WPA2)

802.11i uses the Counter Mode with CBC-MAC Protocol (CCMP) and Advanced Encryption Standard (AES). CCMP along with AES provides WPA2 a stronger security as compared to WPA [11]. A stronger authentication is provided by 4-way handshake [12]. The comparison of all three protocols based on the common features has been shown in Table 1.

Table 1: Comparison of WEP, WPA and WPA2

	WEP	WPA	WPA2
Purpose	As good a s no security	Overcomes the weakness of WEP with hardware up gradation	Provides strong security as it implements 802.11i std.
Encryption	RC4 (vulnerable)	Temporal Key Integrity Protocol (TKIP)	CCMP and AES
Authentication	Open and shared	WPA-PSK, WPA-Enterprise	WPA2-Personal, WPA2-Enterprise
Key per packet	Concatenated	Mixed	Not required
Integrity for header	No	MIC	CCM
Initialization vector	24-bits	48-bits	48-bits
Integrity	CRC-32	Message Integrity Code (MIC) generated by Michael	CCM
Key management	No	802.11x	802.11x
Security against replay attack	No	Sequence counter is used	48-bit packet number
Hardware upgrade	Compatible with existing hardware.	Works with existing hardware but requires firmware NIC upgrades.	Supports Wi-Fi certified devices since 2006, older NIC is not supported.

The authentication process in WPA2 works in two modes:"personal mode" and "enterprise mode". Access points and clients are all needed to be manually configured. The "enterprise mode" authentication is based on 802.1X, the EAP authentication which includes RADIUS server, it is one of several EAP types (like EAP-TLS, which provides an even stronger authentication), and secure key distribution [16]. 802.11X authentication framework provide a stronger authentication process to the clients that want to connect to a LAN or WLAN. 802.1X Authentication process is shown in Figure 2.

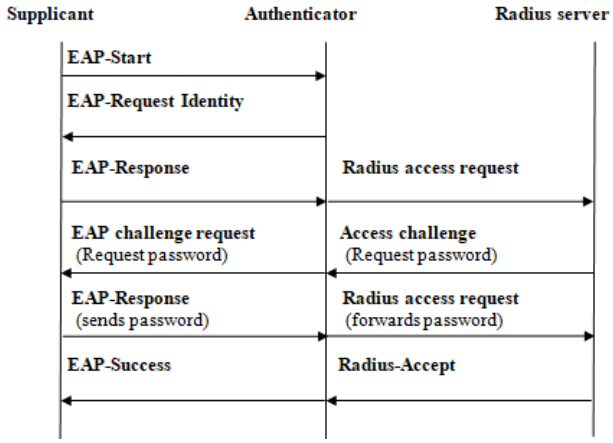

Figure 2 802.1X Authentication process [10], [16]

Once the client is authenticated by the server it sends out a "Radius-Accept" message to the authenticator and finally the authenticator replies with an "EAP-Success" message to the supplicant [14], [13]. Over the years, several vulnerabilities have been detected in the authentication framework of 802.11 which is based on 802.1X authentication.

3. FURTHER DEVELOPMENTS

Hwang et al. [13] proposed a wireless Man in the Middle (MITM) framework proving that a MITM attack is possible during the authentication mechanism if the attacker intrudes between the client and the AP. The procedure is shown in the Figure 3.

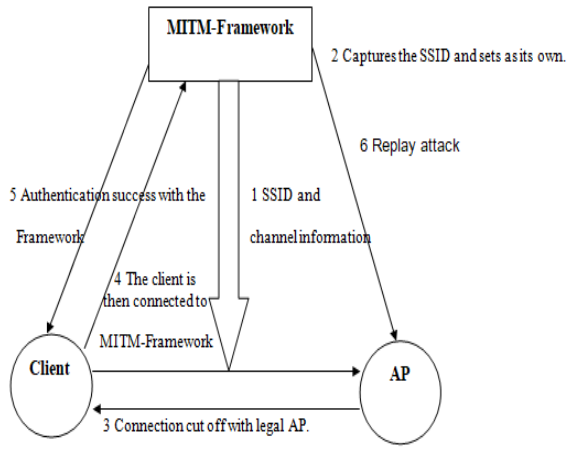

Figure 3 MITM-Framework [13]

First the attacker captures the SSID and the channel information of the AP by listening to the communication between the client and the AP. The attacker then sets up the captured SSIS as his own and disconnects the client from the legal AP. When the client scans the network to reconnect through the MITM-Framework, it connects with the rogue AP of the attacker.

Even the 802.11w that was introduced to provide security to the management frames are vulnerable and can be exploited. The management frames can be forged in 802.11w and studies also shows that it is also vulnerable to Denial of Service attacks.. This standard was intended to prevent masquerading, detection of replay attack, forgery detection and prevention, despite all the added security features it still remains vulnerable. Some of these vulnerabilities are highlighted in Table 2 and the controls for some of these vulnerabilities are presented in Table 3.

Table 2: Vulnerabilities in 802.11i and 802.11w

Vulnerability	Description
Radio frequency (RF) in 802.11w	No protection against malicious radio frequency in 802.11w. The wireless network remains vulnerable to jamming attacks and other vulnerabilities are present due to hardware limitations [15], [17, [18].
4-way handshake in 802.11w	• Does not prevent the forge message sent to the client. • 802.11w does not provide security to any frames before the Pair-wise Transient Key in generated.
Denial of Service attack in 802.11i	In 2011, Eian et al. discovered denial of service vulnerabilities in 802.11i He proposed a model that discovers a denial-of-service vulnerability in authentication mechanism [19].
Jamming and replay attacks	The attacker can use two directional antennas to initiate these attacks [20].

Table 3: Controls for mitigating the vulnerabilities in 802.11i and 802.11w

Controls	Description
Temporary Safe Tunnels (TST)	A TST is established between the client and the AP and a new Temporary Safe Tunnel Entity is created which is used in the actual authentication phase [18].
Deadlock and Denial of Service detection	Eian et al. modeled a method which allowed detecting the deadlocks before they could be too much problem [19]. He also uncovered denial of service vulnerabilities in 802.11i. He proposed a model to discover an authentication related denial-of-service vulnerability in [23].
Secure Control Packets (SCP)	Protection against NAV jamming attacks can be obtained by using the Secure Control Packets. A one-way hash of the shared key between nodes is created by the Encryption key Derivation algorithm [18].
STROBE	STROBE stands for Simultaneous Transmission with Orthogonally Blinded Eavesdroppers. In this approach a multi-antenna is designed that supports 802.11 standards. A beam is sent toward a user and "blinds" the potential eavesdroppers. It sends the "orthogonally blinding" signals everywhere except the intended receiver [21].
SecureArray	Xiong et al. proposed a SecureArray so as to provide defense against active attacks. This technique includes a multi antenna AP that which monitors the direction in which the client's signal is coming. This angle of Arrival (AoA) information generates the sensitive signatures, which is used to start a challenge response by the AP and the client in case of suspicious transmission [20].

In the four-way handshake mechanism when the ANonce is sent to the client by the AP, the client constructs the PTK+MIC. This construction process requires some time providing an opportunity to the intruder to send out malicious frames before the client replies with Snonce and MIC [18]. Also, no security is provided to prevent the attacker from eavesdropping the four-way handshake whatsoever [19].

In another vulnerability related to four-way handshake the attacker can send fake deauthentication request after receiving third message of four-way handshake process because after the client receives the Message 1 of the four-way handshake, a delay is caused by the generation of the PTKSA [18, 22]. The amendment 802.11w does not mitigate this vulnerability because the attack takes places during the EAPOL four-way handshake.

In 802.11w standard, CCMP from 802.11i is used to provide confidentiality, and the broadcast management frames are protected by the Broadcast Integrity Protocol (BIP). Protection is only provided for de-authentication and dissociation management frame subtype action [20].

4.CONCLUSION AND FUTURE WORK

In this paper we presented the brief overview of the Wi-Fi security protocols: WEP, WPA and WPA2. Despite all the security features added to these protocols, they still remain vulnerable to certain attacks. The aim of this paper was to highlight the vulnerabilities and controls associated with these protocols. The paper briefly discussed about the vulnerabilities present in the 802.1X based Authentication mechanism of 802.11i. Finally, we presented some techniques to control these vulnerabilities proposed by various researchers.

References

[1] Menal, “Evolution of Wireless LAN in Wireless Networks.” International Journal on Computer Science and Engineering (IJCSE), March 2017.
[2] S. Gopalakrishnan, "A survey of wireless network security." International Journal of Computer Science and Mobile Computing 3.1: 53-68, 2014.
[3] T. Mekhaznia, A. Zidani. "Wi-Fi Security Analysis." Procedia Computer Science 73: 172-178, 2015.
[4] S. Fluhrer, I. Mantin, A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4" In Selected areas in cryptography, vol. 2259, pp. 1-24, 2001.
[5] A. Stubble, J. Ioannidis, A.D. Rubin, “A Key Recovery Attack on the 802.11b Wired Equivalent Privacy Protocol (WEP)”, ACM Transactions on Information and System Security, Volume 7 Issue 2, pp. 319-332, May 2004.
[6] A.H. Lashkari, M.M.S. Danesh, and B. Samadi. "A Survey on Wireless Security Protocols (WEP, WPA and WPA2/802.11 i)." Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on. IEEE, 2009.
[7] A.M.A. Naamany, A.A. Shidhani, H. Bourdoucen, IEEE “802.11 Wireless LAN Security Overview.” In IJCSNS (Vol. 6, No. 5B, p. 138), May 2006.
[8] V. Gandhi, “A Study on Wireless LAN Fundamentals, Architecture, Benefits and Its Security Risks” (September 1, 2014). Indian Streams Research Journal, Volume-4, Issue-8, Sept-2014. Available at SSRN: https://ssrn.com/abstract=2503782.
[9] R. Housley, D. Whiting. "Temporal Key Hash." IEEE 802.11 doc 01- 550r1 (2001).
[10] Bhagyavati, W.C. Summers, A. DeJoie, ”Wireless Security Techniques: An Overview”; InfoSec Conference, September 2004.
[11] H.I. Bulbul, I. Batmaz, M. Ozel, “Wireless Network Security: Comparison of WEP (Wired Equivalent Privacy) Mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) Security Protocols.” In Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop (p. 9). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), January 2008.
[12] H. Altunbasak, H. Owen, “Alternative Pair-wise Key Exchange Protocols for Robust Security Networks (IEEE 802.11i) in Wireless LANs.” Southeast Con, 2004. Proceedings. IEEE, 26-29 Mar 2004 Page(s):77. 83, 2004.
[13] H. Hwang, et al. "A Study on MITM (Man in the Middle) Vulnerability in Wireless Network Using 802.1 X and EAP." Information Science and Security, 2008. ICISS. International Conference on. IEEE, 2008.
[14] C. Rigney, S. Willens, A. Rubens, W. Simpson. “Remote Authentication Dial in User Service (RADIUS).” No. RFC 2865. 2000.
[15] C. He and J.C. Mitchell, “Analysis of the 802.11i 4-way handshake.” In Proceedings of the 3rd ACM workshop on Wireless security (WiSe '04). ACM, New York, NY, USA, 43-50, 2004.
[16] Y. Zou, et al. "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends." Proceedings of the IEEE 104.9 (2016): 1727-1765.
[17] A. Mishra, N.L. Petroni, Jr., W.A. Arbaugh, T. Fraser. 2004. “Security Issues in IEEE 802.11 Wireless Local Area Networks: A survey: “Research Articles. Wirel. Commun. Mob. Comput. 4, 8 (December 2004), 821-833.
[18] B. Bertka, "802.11w Security: DoS Attacks and Vulnerability Controls." In Proc. of Infocom. 2012.
[19] M. Eian, S.F. Mjølsnes, "The Modeling and Comparison of Wireless Network Denial of Service Attacks." Proceedings of the 3rd ACM SOSP workshop on networking, systems, and applications on mobile handhelds. ACM, 2011.
[20] J. Xiong, K. Jamieson. "Securearray: Improving Wi-Fi Security with Fine-Grained Physical-Layer Information." Proceedings of the 19th annual international conference on Mobile computing & networking. ACM, 2013.

[21] N. Anand, S.J. Lee, E.W. Knightly, "Strobe: Actively Securing Wireless Communications using Zero-Forcing Beamforming." INFOCOM, 2012 Proceedings IEEE. IEEE, 2012.
[22] M. Eian, S.F. Mjølsnes. "A Formal Analysis of IEEE 802.11w Deadlock Vulnerabilities." INFOCOM, 2012 Proceedings IEEE. IEEE, 2012.
[23] M. Eian. "Fragility of the Robust Security Network: 802.11 Denial of Service." In Proceedings of the 7th International Conference on Applied Cryptography and Network Security (ACNS '09), Michel Abdalla, David Pointcheval, Pierre-Alain Fouque, and Damien Vergnaud (Eds.). Springer-Verlag, Berlin, Heidelberg, 400-416, 2009.

AUTHOR

Kritika Singh is currently pursuing M Tech Information Security in the Department of Computer Science and Engineering from GGSIPU, New Delhi, India. She received her B Tech degree in Information Technology from GGSIPU, New Delhi, India. Her research interests include Network Security and Steganography.

Dr. Vishal Gupta is an Assistant Professor (Pre-Revised) in CSE Department at AIACT&R, New Delhi, India. He has more than 16 years of experience in teaching. His areas of specialization include Computer Networks, Database Management Systems, Operating Systems, Compiler construction and Information Security.