International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.22 (SJIF-2017), e-ISSN: 2455-2585
Volume 4, Issue 6, June-2018

Wireless Security Mechanisms For Home and Enterprise Clients

[1] Aarti Chugh, [2] Charu Jain
[1,2] Assistant Professor, Department of Computer Science, Amity University Haryana

Abstract

The introduction and evolution of security standards for wireless networking is not an easy task. Flaws in the initial security standard resulted in quick-fix solutions and interoperability issues. This paper discusses the progress of wireless security protocols and its effect on home and enterprise users. Wireless networking was initially marketed towards home consumers and specialized applications, but was limited by low throughput speeds. Popular encryption and authentication protocols used in wireless networks such as WEP, WPA, and WPA2 implementation are analyzed. Possible problems and attacks for these protocols discussed in this paper. Each protocol is being analyzed for the security for home users and enterprise. The main impact of this paper is to bring awareness to the Society about the capabilities that a WLAN attacker may obtain.

Keywords: WLANs, security, attacks, WEP, WPA, WPA2

1. Introduction

Wireless networking is being popular day by day due to its flexibility of providing mobility in the home, work place and community to connect to the internet without wires. By deploying WLANs, organizations have sacrificed security for mobility. Although Internet Security problems with WLANs continue to emerge through time, the deployment of WLANs has not decreased. "By 2008, research firm Gartner expects 99 million WiFi users and 89,000 public WiFi access points around the world." This proves the need and desire for a safer and a better WLAN environment. With the benefits of Wi-Fi there are also some risks which users should be aware of. Without any security implemented, unauthorized users may steal data or load malicious code onto the network with the intention of creating havoc. Wireless networks security standards are providing security for these networks has proven to be a challenge due to the problems inherent with the way information is transmitted. The majority of wireless networks use the IEEE 802.11 standard for communication. Initially the IEEE 802.11b was the de-facto security standard for wireless networking technology for small businesses and home users, with all Wireless Access Points equipped with Wired Equivalency Protocol (WEP)[3]. Flaws in WEP were soon discovered and in response to this, the 802.11 task group was developed to address the major problems with WEP. They addressed three main security areas: authentication, key management and data transfer privacy. Then Wi-Fi Protected Access (WPA) as a Wi-Fi standard is developed by Wi-Fi alliances, which accelerated the introduction of stronger security. Flaws in WPA [4] are removed by the WPA2 by using strong AES encryption method. This paper is exploring three popular standards for security and authentication, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and Extensible Authentication Protocol (EAP). Each of these protocols is being explained, analyzed, and vulnerabilities are being identified and discussed. The impact of this paper will hopefully bring awareness to the community about the capabilities that a WLAN attacker may obtain. The paper seeks to allow readers to perceive how attackers may undertake the attacks, and then analyzes each attack. The defense solution offered against some of the WLAN attacks will provide a more secure Internet accessing environment

The reminder of paper is structured as follows. In section 2, I give an introduction of possible security vulnerabilities in WLAN. Following that I points out strengths and weakness existing secure algorithm in section 3. In section 4 I discuss the comparison among all algorithms. Finally I closed with a conclusion of our findings and suggested future work.

2. Possible security Vulnerabilities

Like wired networks, wireless networks are subject to malicious attacks. Following are the few possible security vulnerabilities for wireless networks:

2.1. DoS Attack: [5] Exploits unauthenticated nature of 802.11 management frames. Due to deficiency of well-built authentication, a wireless customer can take-off de-authenticates messages, thus disturbing network services. Since an access point [AP] must associate with a wireless client first before traffic can be transmitted, an attacker can effectively keep one or more stations from transmitting by repeatedly sending disassociate frames. It requires well-built authentication of management and control frames for prevention of such attacks.

2.2 Authentication Attacks: [6] Exploits authentication methods to gain network access. Flawed mutual authentication mechanism, based on a challenge-response protocol. During the shared-key authentication process, each party responds to a challenge with an encrypted message proving its knowledge of the key. An attacker can simply XOR the challenge and response message and determine a portion of the key stream to generate a successful authentication response in the future.

2.3. MAC Address Spoofing: [6] Sniffing can detect valid MAC addresses that can be used with certain 802.11 card drivers to spoof a MAC address and gain network access.

2.4. Man-in-the-Middle (MitM): An attacker has ability to capture/decrypt frames during the association process to provide critical information. With this information, an attacker can setup a rogue AP to force a wireless client to re-associate with a bogus AP. This allows the attacker to access all data transmitted back and forth between a wireless client and a server. Note: the wireless client and server believe they are connected directly to each other, and not a bogus AP or MitM.

2.5. Traffic Injection: After recovering one key stream, an attacker has the capability to inject packets by reusing the same IVs.

2.6. Replay Attack: [6] derived from recovering key streams from a WEP key, an attacker can grow the key stream by using the same IV/WEP key pair as the observed frame. Reuse or replay of this IV/WEP key pair can generate a key stream large enough to subvert a network.

2.7. Dictionary Attacks: [6] an attacker can collect challenge and response exchanges from password-based protocols, with the capability to determine the login name - password combination. Use of open source tools based on a dictionary of hundreds of thousands of words/phrases, and an offline computer to cycle through every possible name - password combination, login information can be compromised. Once compromised, an attacker has WLAN access with the rights and privileges of that user.

2.8. Brute force attack*:* A brute force attack is the systematic testing of different letters, numbers and symbols until the correct password or key is guessed. There are a number of software programmes available on the Internet that can be used to recover encryption keys on wireless LANs, these include AirSnort and WEPCrack. AirSnort requires approximately 5-10 million encrypted packets to be gathered. Once enough packets have been collected, AirSnort can guess the encryption password in under a second. WEP can easily be cracked because the Initialization Vector is sent as plaintext within the encrypted packet. This means that if anyone intercepts the data using a sniffer package, they will be able to decipher the secret key [6].

2.9 Attacks thought Internet:

In these days' information available on internet increases rapidly in a business or organization, there are a number of security risks that may occur when computers are connected to the Internet. These risks include the unauthorized viewing of sensitive information by intruders or legitimate users. The deletion, modification or disclosure of information by internal or external users may occur on an unsecured network. The unauthorized connection of a personal Wi-Fi access point to a company's network could put the whole network at risk if the security options are not properly set up. Security breaches may be caused by either internal or external events.

3. **Wireless security standards**

To prevent attacks on wireless networks, there are many security standards is supported by IEEE802.11. In this section, security standards and analysis of its strengths and problems are discussed.

3.1 Wireless Equivalent Privacy (WEP)

In 1997, WEP was developed by the 802.11b task force with the introduction of wireless technology, and was the first encryption protocol to be deployed with wireless networks. WEP is a protocol that utilizes RC4 encryption and a 24 bit IV. It began with a 40 bit key that was later expanded to 104 bits. The keys it uses are called Preshared Keys (PSK). The keys are manually entered. WEP adds a checksum of 32 bits called the Integrity Check Value (ICV) to the end of a packet. The authentication method is weak and even helps attackers decipher the key [3]. another problem with WEP is that you have to manually configure the key for each wireless device used. This can be problematic if a key is compromised in a large network relying on that key because every device on the network must have their keys changed which creates a logistical in a university or enterprise setting. This discourages organizations from implementing WEP. It also discourages organizations using WEP from ever changing keys. Characteristics of WEP are given table 1 on the basis of above analysis.

Table 1. Characteristics of WEP

Encryption method	RC4
Hash method	ICV
Key distribution	Manual
Key size	40 bits
802.11x authentication	optional

After some year implementing of WEP, many flaws were include in it. Next subsection analyzes the problems related to WEP.

3.1.1 Problems include in WEP

(a) ICV is insecure [7] which opens up a number of potential attacks due to the fact that a forged packet can be made to appear valid. ICVs are based on the CRC32 error checking algorithm which works well for detecting errors in transmission but is not well-suited for a cryptographic hash. The ICV can be modified to match the contents of a message.

(b) IV Key reuses attack: which is made possible by the small size of the IV [7]. This enables ciphertext attacks using replayed IVs. This is possible because the IV is sent as plaintext in RC4 encryption.

(c) Known plaintext attack: which is possible because of the large amount of known plaintext present in TCP/IP traffic? [5]

- It is possible to send pings from the internet to the attacker that travel through the access point.
- A key string of length N can be recovered for a given IV.
- Packets of size N can be forged using the IV. [3] The insecure ISV also makes this possible.

(d) Partial Known Plaintext attack: where only a portion of the message is known. for example the IP header.

- It is possible to recover M octets of the key stream where M<N. It is then possible through extended probing to extend the known key stream from M to N.
- It is also possible to flip bits in real-time while adjusting the CRC32, allowing packets to be diverted to the attacker. This is a direct result of ICV being a poor cryptographic hash.

(e) Authentication forging: it is possible because once a key stream is recovered for a given IV; the IV can be easily reused because the client specifies the IV to be used [7].

(f) Dictionary attacks: theses are possible where the key is derived from a vulnerable password.

(g) Real-time decryption: it is possible when a dictionary of IVs and key streams are obtained through probing and IV reuse. This is possible due to the small size of the IV. 1500 octets of each key stream are needed. With only 2^24 possibilities, the dictionary can be stored in 24GB of space [7]. On the basis of above analysis we can say that what is good for home user and business in WEP. Finally conclusion of this security method is given in table 2.

Table. 2 Summery of WEP

Advantages	Disadvantages
• First encryption protocol used so it is present in older devices. • Mature protocol. • Better than plaintext.	• Weak encryption • Small IV size • ICV is insecure • Lots of known attacks • Key management

WEP2 sought to eliminate some of the shortcomings of WEP by implementing a 128 bit IV and using Kerberos authentication. However, the only attack completely eliminated is the ability to perform real-time decryption. Using Kerberos, also introduced other vulnerabilities such as dictionary attacks. By Using a combination of statistical techniques focusing on unique IVs captured and brute-force dictionary attacks to break 128-bit WEP keys. A report conducted in 2005 by Webtorials found 40% of the users surveyed still used WEP for securing their wireless network and only 22% deployed WPA2/802.11i security [17]. finally WEP includes alots of problem which possess to user to move other secure standard so next section points out on Wi-Fi protected Access.

3.2 Wi-Fi Protected Access (WPA)

WPA was created by the Wi-Fi Alliance once the flaws associated with WEP were discovered, and used as an intermediate standard until the IEEE 802.11 working group developed a more secure protocol. WPA was based on the WEP protocol, but utilizes the stronger encryption technology used in TKIP [8], which offers pre-packet key mixing and a message integrity check. WPA works to address the shortcomings of WEP.

It uses many of the same protocols employed by WEP. This makes it possible for WEP devices to be upgraded to WPA. WPA still uses RC4 as its encryption method on the message body and still employs ICV. However, in addition to ICV, a Message Integrity Code (MIC) is added to each frame. This process is called Michael which uses authentication. The MIC is 8 bits and is placed between the data portion of the packet and the ICV. The size of the IV is increased to 48 bits. 802.1 x authentications can be required and Temporal Key Integral Protocol (TKIP) is used. 802.1.x authentication is optional under WEP. TKIP allows keys to be changed automatically (frame to frame) and synchronizes keys between access points and clients. TKIP sets a unique starting key for each authenticated client that is using a pre-shared key. As a result, WPA [4] has stronger authentication and a better key management system.

Table. 3 Characteristics of WPA

Encryption method	RC4, TKIP
Hash method	ICV, Michael
Key distribution	TKIP
Key size	128
802.11x authentication	Can be required

3.2.1 Problems include in WPA

3.2.1.1 Michael Vulnerabilities

- **Birthday attack** – An attacker gets a D,M pair: D_1 = MIC(M_1). Look at other pairs D_i = MIC(M_i). When D_i = D_1 (where I != 1) attack is successful. The probability for success is after 2^32 attempts. If D_1 and D_i were created using different keys, then a forgery would be garbage[6].
- **Differential cryptanalytic attack -** Michael results have special characteristic differences where a difference in input has a high probability of producing a corresponding difference in output. The formula for this is: ΔM = Mi XOR Mj and ΔD = Di XOR Dj. Optimal attack is when inputs are the same length. There are n! possible comparisons for n pairs of inputs. After obtaining characteristic differentials, it is possible to start attacking the MIC to learn parts of the key. This attack has probability of success after 2^30 attempts. This is not a trivial attack, it is both computationally and storage intensive. An optimal attack has O(2^29) complexity but requires that the messages differ only in the last byte. These messages are very difficult to acquire because in TKIP both M and D are encrypted. Both of these attacks can be thwarted by re-keying. The new key is involved with both data sets and cancels itself out in the differential [6].

3.2.1.2 Temporal Key Vulnerabilities [10]

- **Lost RC4 keys** – If an attacker is able to get multiple RC4 keys, they will be able to discover the temporal key and MIC [6]. Then they are able to construct both previous keys and future keys allowing them to both read and forge messages. However, this is not a practical attack with a complexity of O(2^105). Even if the attack as a whole is not practical, itshows that parts of WPA are susceptible to attack.

- **DOS** The authentication in WPA exposes the hardware to a unique DOS attack [8]. WPA will shut down a device for 60 seconds if there it receives 2 packets of unauthorized data or "forgeries" within a 1 second interval because it assumes it is under attack. This allows an adversary to disable any access point within range, sending very little network traffic.

3.2.1.3 PSK vulnerabilities

If a PSK is used for authentication instead of 802.11x, the PTK can be found through passive listening by an internal attacker [9]. To generate a PTK, a device needs 2 MAC addresses and nonces which are available at the initial handshake. This vulnerability exists because most WLANS use only one PSK for an Extended Service Sets (ESS) which consists of multiple access points. An attacker can readily use an offline dictionary attack if a weak passphrase is used for PSK. After gaining knowledge of the PSK, they are able to obtain the temporal key.

Advantages	Disadvantages
• Strong encryption, especially in WPA2 • Document forgery much more difficult • Can require 802.11x authentication • WEP hardware can often be upgraded to WPA • Key management synchronizes keys	• Susceptible to unique DOS attack • Michael is vulnerable • PSK mode susceptible to dictionary attack • PSK vulnerable • It can be complicated to setup which makes it unsuitable for home users.

Table.4 Summery of WPA

Problem due to RC4 encryption method here some encryption flaws in WPA which is removed by using WPA2 discuss in next subsection.

3.3. Wi-Fi Protected Access 2 (WPA2)

The current standard for wireless security, Wi-Fi Protected Access 2 (WPA2), was introduced in September 2004. The IEEE 802.11i standard WPA2, addresses three main security areas: authentication, key management, and data transfer privacy. WPA2 uses the Advanced Encryption Standard (AES) for data encryption and is backward compatible with WPA. Like WPA, WPA2 is also available in Personal and Enterprise modes. WPA2 allows an easy transition from WPA mode by using WPA/WPA2 mixed mode, so networked computers can use either WPA or WPA2. However, although WPA2 implements the full standard, it will not work with some older network cards. The encryption algorithm used in the 802.11i security protocol is AES-Counter Mode CBC-MAC Protocol (AES-CCMP). It uses the AES block cipher but restricts the key length to 128 bits. AES-CCMP incorporates two sophisticated cryptographic techniques (counter mode and CBCMAC). The counter mode uses an arbitrary number that changes with each block of text, making it difficult for an eavesdropper to spot a pattern. The CBC-MAC protocol (Cipher Block Chaining- Message Authentication Code) is a message integrity method, which ensures that none of the plaintext bits that were used in the encryption were changed. It is similar to WPA in that it still utilizes the 802.1x and EAP for authentication.. WPA2 does not address any flaws with WPA, but provides an advantage to corporations and government entities since it provides a security solution (AES) that meets the FIPS (Federal Information Processing Standards) 140-2 compliance requirements. WPA2 certified products are backward compatible with WPA. Upgrading to WPA2 may require new hardware requirements due to AES, and not be available for firmware (software) upgrade.

3.3.1 Problem includes in WPA2

3.3.1.1 DOS this attack is still working in WPA2 as the WPA standard.

3.3.1.2 EAP-TLS authentication method is vulnerable due to one way authentication in which access point authenticates the clients while clients don't authenticate the access point so fake access point is still possible.

3.3.1.3 Encryption overhead WPA2 use AES as the encryption method which most secure method but execution complexity is so poor which affect the throughputs of the whole network as well as power consumptions.

3.3.1.4 Backward compatibility it not support the existing hardware equipment it means we will be changed the hardware devices.

3.3.1.5 Poor Authentication here is EAP-TLS authentication method which is one way authentication method i.e. AP authenticates to clients while clients don't authenticate the AP so possibilities of fake access points and Man in Middle attack are still working.

4. Comparison among security standards for securing a wireless networks

For securing a wireless network, users should follow any security procedure to prevent the network from being penetrated. From the above discussion about attacks and security standards user and business can choose appropriates methods and setting up the wireless device.. Although WPA and WPA2 are securer encryption protocols then WEP, and WEP is well renowned for its weaknesses, if the access point only supports WEP it is worthwhile enabling it. This will prevent neighboring Wi-Fi users without the knowledge or intention to hack from sharing bandwidth. If someone has the ability and intention to hack then WEP is not very protective. When using WPA or WPA2 encryption in consumer mode, the password should contain a minimum of 20 randomly selected letters. WPA2 is best secure method but its poor backwards software and hardware capabilities problem for home user because they would be changed hardware such as access point which support WPA2. this is expensive procedure so then home user still use WEP with taking some risks. finally the user or business use table 5 which gives the strength of WEP,WPA and WPA2 choose the best security options.

Table.5 Comparisons among WEP,WPA and WPA2.

	WEP	WPA	WPA2
Cipher type	stream	block	block
Cipher Algorithm	RC4	RC4 (TKIP)	Rijndael (AES-CCMP)
Encryption Key	40-bit	128-bit (TKIP)	128-bit (CCMP)
Initialization Vector	24-bit	48-bit (TKIP)	48-bit (CCMP)
Authentication Key	None	64-bit (TKIP)	128-bit (CCMP)
Integrity Check	CRC-32	Michael (TKIP)	CCM
Key Distribution	Manual	802.1x (EAP)	802.1x (EAP)
Key Unique to:	Network	Packet, Session, User	Packet, Session, User
Key Hierarchy	No	Derived from 802.1x	Derived from 802.1x
Cipher Negotiation	No	Yes	Yes
Time attack	2^{104} permutation	2^{128} permutation	2^{128} permutation
Ad-hoc (P2P) Security	No	No	Yes (IBSS)
Pre-Authentication (Wired LAN)	No	No	Using 802.1x (EAPOL)
Execution time	less	more	most
Complexity & Power consumption	Less	more	poor
Overall	Not secure	Moderate security	High level

5. Conclusion

In this paper, the security strength of standard security protocols used in WLANs and their overhead as the performance concern were analyzed. We use the strength of standard security protocols for IEEE 802.11 WLANs to determine the answer to the issue -which is good for home and business. Moreover, while there is an immediate advantage in moving from all versions of WEP to WPA, WPAv2 may be an good choices with latest wireless devices and high speed processor for business users because of the crypto mechanisms used in this protocol. This paper improves the WLAN Internet accessing environment by pointing out security flaws and suggesting solutions to them. This paper provides another layer of protection to those data, impacting on the economy as a whole.

6. REFERENCES

[1] J. Best, "100,000 Wi-Fi hotspots by the end of 2005", ZDNet, 2005. Sourced: 16 November 2005 http://news.zdnet.co.uk/communications/wireless/0,39020348 39222683, 00.htm

[2] Department of Trade and Industry (DTI), "Information Security Breaches Survey 2004"Technical Paper URN04/617, PricewaterhouseCoopers, UK, 2004. Sourced: 9 January 2006. http://www.security-survey.gov.uk/

[3] Scott R. Fluhrer, Itsik Mantin, Adi Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", Selected Areas in Cryptography, Springer- Verlang, London, 2001, ppl-24.

[4] Wi-Fi Alliance. Wi-Fi Protected Access, October 2002. URL: http://www.wi-fi.org/OpenSection/ pdf/Wi-Fi Protected Access Overview.pdf

[5] Bellardo, J. and Savage, S. (August 2003). 802.11 Denials-of-Service Attacks: Real Vulnerabilities and Practical Solutions. Unpublished talk from University of California at San Diego.

[6] Cryptography and Network Security principals and practices by William Stallings 3rd addition 2005

[7] C. Peikari, and S. Fogie, "Cracking WEP", Airscanner, 2003. Sourced: 15 November 2005 http://www.airscanner.com/pubs/wep.pdf

[8][Walk2002] _ -802.11 Security Series Part II: The Temporal Key Integrity Protocol (TKIP**)**, Jesse Walker, Intel Corporation, 2002

[9] J. Wright, "CoWPAtty - Offline WPA PSK Dictionary Attack Tool", 2005 Sourced: 9 January2006. http://www.securiteam.com/tools/6L00F0ABPC.html

[10] S. Fogie, "Cracking Wi-Fi Protected Access (WPA), Part 2", 2005. Sourced: 21 November 2005 http://www.ciscopress.com/articles/

.