International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 5

Comparative Analysis of Wireless Security Protocols and Issues

Farhaan Noor Hamdani
Student, Department of Computer Science and Engineering,
School of Engineering Sciences and Technology,
Jamia Hamdard, New Delhi, India

ABSTRACT

Almost every electronic device is connected to the internet today. We have different mechanisms of connecting the devices for feasible communication that maybe wired or wireless. Also, wirelesses LANs are most popular and frequently used because of their cost effectiveness, easy deployment and configuration. A lot of data is being generated and transferred every day, which includes sensitive information. Network security consists of various policies and practices which prevent and monitor proper safeguard of network systems against misuse, unauthorized access of the information. Though different security techniques are implemented to protect this kind of information, but the threat of hackers is always lurking there, to intercept or intrude the security by finding loopholes in the wireless communication. This paper focuses on the existing wireless security protocols such as Wired Equivalent Piracy(WEP), Wi-Fi Protected Access(WPA), Wi-Fi Protected Access 2(WPA2) and their security issues.

Keywords: *IEEE802.11; WEP; Wireless-security; Wireless-attacks; WPA; WPA2*

INTRODUCTION

Wi-Fi is technology developed for radio wireless local area networking of devices which are based on the IEEE 802.11 standards. Wi-Fi is a trademark of the Wi-Fi Alliance, which doesn't allow the use of the word Wi-Fi Certified to products that successfully complete interoperability certification procedures [1]. Wi-Fi is most used wireless networking technique that implements radio waves to produce wireless high-speed internet and network communication. It is based on IEEE 802.11 standard. Devices like personal computer, game-console, smartphone, etc. use Wi-Fi to connect to a network resource such as the internet with the help of a network access point. Wireless LANs are one of the dominant network topologies in the present world. With increase in the use of the technologies the non-wired network communication setup is preferable. Wireless LANs are used everywhere in college campuses, in office buildings, and in many public areas. There are different standards used by IEEE802.11 such as 802.11a, 802.11b, 802.11c, 820.11ac, 802.11n, 802.11ac, 802.11g etc. All operate as per different bandwidths and transfer limits. Security concern is always there while developing certain communication protocols, such as maintaining confidentiality, integrity and authentication. Wi-Fi security means preventing any kind of un-authorized access or breach in the network and protect network accessible resources from any damage. Some well-known wireless security methods are Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA). WEP is a weak security standard and is not recommended for practical use. WPA was developed as an alternative to improve security over WEP. WPA2 forms the current standard for Wi-Fi security, and is used widely over the former two standards. It uses an encryption that supports up to key size of 256-bit.

WIRELESS COMMUNICATION

Four major components of wireless communications are:

- **Distribution system-** used to forward frames to their respective destinations.
- **Access Points-** is a networking device which connects different Wi-Fi devices to a wired network.

- **Stations-** devices having Wi-Fi interface which enables them to communicate with other devices with same features via an Access point.
- **Wireless medium-** the medium in between the stations responsible for transferring data frames**.**

WIRELESS SECURITY PROTOCOLS:

Traffic flows via radio waves in wireless networks, so it is quite easy for hackers to monitor and attack without the need to connect to a network physically. Attackers can launch attacks over the internet anytime and can gain access to a network by being within the range of an unprotected wireless network. The best approach is to encrypt the information.

Various wireless Encryption techniques include:

- WEP
- WPA
- WPA2
- WPA2 Enterprise
- PSK (Pre-shared Key)
- TKIP (Temporal Key Integrity Protocol)
- AES (Advanced Encryption Standard)
- EAP (Extensible Authentication Protocol)
- RADIUS (Remote Authentication Dial-In User Service)
- VPN (Virtual Private Network)
- Other 3rd party encryption and authentication systems (Biometric system, Kerberos etc.)

WIRED EQUIVALENT PIRACY (WEP):

It was developed as the first-generation security standard for the IEEE 802.11 Wireless communication. However, its use is not recommended, as it has been cracked already. WEP was the only encryption protocol convenient to 802.11a and 802.11b devices built before the WPA standard, which was applicable only for 802.11g devices. However, some 802.11b devices were later provided with firmware or software updates to enable WPA, and later devices had it built in. [2]. WEP was appended as the privacy component of the original IEEE 802.11 standard approved in 1997 [3][4]. WEP uses the stream cipher (Rivest Cipher 4) RC4 for confidentiality [5], and the (cyclic redundancy check) CRC-32 checksum for integrity. Its use was disapproved in 2004 and is registered in the current standard [6].

WEP ENCRYPTION:

WEP is an encryption algorithm. The security between two end users of a WLAN is an aim of WEP algorithm over radio signals. RC4 algorithm is used for encryption in WEP and uses two key sizes: 40 bit and 104-bit, to which we add a 24-bit initialization vector (IV) which is directly transmitted. The plain text is XOR'ed with the key at the transmitter side, generated after (key-scheduling algorithm) KSA and (Pseudo Random Generation Algorithm)PRGA process of RC4 and cipher text is obtained. WEP uses CRC-32 algorithm for data integrity [7]. Input or plain-text is provided which along with the integrity check (CRC-32). Which calculates the IC value, this value is later used as cross reference for data validation. Initialization vector (random number) is calculated and merged along with the shared key respectively. Here IV is sent as a plain text. Shared key and IV are first passed through RC4 encryption (which is a shared key stream cipher algorithm). It is based on symmetric key encryption. The values from plain-text, IC value and IV, shared key is then XOR'ed to from cipher-text. WEP uses 24-bit IV in both 40 and 104-bit operation.

WEP DECRYPTION:

At destination the other user receives preshared IV along with cipher text. Two modes of operations are applied to the received message for decryption. First it is passed through RC4 algorithm mechanism, and then XOR'ed with the received IV, cipher text. The result yields the plain-text, whose integrity is then checked via CRC32 and the IC value. If the values are matching the message is unaltered.

ATTACKING A WEP NETWORK:

Flaws present in the WEP made it vulnerable to many attacks. The encrypted packet along with IV is sent as plain text. Thus, the information which is out in the air-ware can be easily cracked by anyone and can hack the secret key. During few iterations KSA and PRGA leak information of their algorithm. With the help of XOR which a simple process is used to deduce unknown value if the other two values are known. The format is (B+3, 255, x) where B is the byte of the secret key being cracked. It needs lot of patience to crack the WEP key by simply listening of the network traffic and saving them. The process injection is used to speed up the process. Injection involves resending operations repeatedly very rapidly. Thus, in a short period of time we can capture many IVs, after determining the IVs we use this IVs to determine the WEP key [8]. Another drawback is that IV is sent in with clear-text, making it easier for the attacker to recover the actual key based on the rotating 24-bit IV.

After certain number of frames, the IVs are revised (interesting IV's). It makes cracking WEP key network easy [9]. Keys are static, no replay protection and the WEP checksum is linear and predictable Thus, WEP is considered cryptographically a weak algorithm.

Wi-Fi PROTECTED ACCESS (WPA):

WPA came into existence due to the limitations found in WEP. It is the part of the IEEE's 802.11i/D3.0 wireless security specification and overcomes the weaknesses of WEP. Many changes were made in this security technique such as use of Temporal Key Integrity Protocol (TKIP), also increasing the size of IV and use of mix functions. For authentication it uses EAP and 802.1x. The Temporal Key Integrity Protocol (TKIP) was developed and practiced for WPA. WEP uses a 64-bit or 128-bit encryption key that is manually entered on wireless access points and devices and remains same throughout the process. TKIP employs a per-packet key, meaning that it dynamically generates a new 128-bit key for each packet and thus prevents the types of attacks that compromised WEP [10]. However, TKIP itself is no longer considered as a strong security protocol, and its use was discontinued in the 2012 revision of the 802.11 standard.

WPA can be implemented as:

- ➢ WPA PSK (Pre-shared Mode)
- ➢ WPA Enterprise
- ➢ WPS (Wi-Fi Protected Setup)

WPA ENCRYPTION:

WPA requires following values to encrypt a wireless data frame [11]:

- ➢ Initialization vector (IV)
- ➢ Data encryption key
- ➢ Source and destination addresses (SA, DA)
- ➢ Priority field value
- ➢ Data integrity key

It uses the existing WEP hardware and runs as s WEP sub-component. It uses RC4 and TKIP as encryption algorithm with IV size of 48-bit. The encrypted key length is 128-bit, followed by integrity check mechanism of Michael algorithm plus CRC-32. This procedure never uses the same key twice, after some data transfer the key keeps on changing based on TKIP. At input key mixing (TKIP, transmit address, IV, Extended Initialization Vector) which is then combined with clients MAC address to create a key stream. The result is then used to encrypt data via the RC4. MAC service Data unit (MSDU) and message integrity check) are merged via Michael algorithm. Which is then combined with the CRC32 checksum. The RC4, key stream and Mac service data unit (MPDU), Integrity Check Value (ICV) are XOR'ed to form the Cipher text. The final packet to be transmitted contains Mac header, IV, KID, EIV, Cipher text. Temporal keys are entitled during the four-way handshake phase. It is used in both WPA and WPA2.

WPA DECRYPTION:

The WPA decryption process can be described as follows: The IV is extracted from the IV and extended IV fields. The IV, DA and the Data encryption key are used as the input for the key mixing function to produce the per-packet key. IV and per packet key are used as the input for RC4 PRNG (pseudo random number generator) function to generate key stream of the same size as the encrypted data, MIC and ICV. The key stream is then XORed with the encrypted data, MIC and ICV to produce unencrypted ICV, MIC and the data.ICV is calculated and compared with the value of unencrypted ICV [11] [12]. The message(data) is thereby validated.

Wi-Fi PROTECTED ACCESS 2(WPA2):

Current IEEE 802.11/D9.0 standard security mechanism used world -wide. Developed by Wi-Fi Alliance, with strong security features and better encryption technique. But it requires hardware upgrade to support WPA2. Like WPA, it also has two modes of operation WPA2 PSK and WPA2 Enterprise. WPA2 protects the network better because its layer 2 based. But WPA2 alone can't provide Enterprise security. Most security concerns can be eliminated by combining WPA2 with IEEE 802.1X (port-based authentication protocol for access control). WPA2 uses a new encryption method called Counter mode with CBC mac protocol(CCMP) which is based on Advanced Encryption Standard (AES). A stronger algorithm than RC4. WPA2 personal generates a 256-bit key from a plain text passphrase which is called pre-shared key. The PSK in conjunction with service set identifier and SSID length form the mathematical basis for the pair wise master key(PMK), that is used to initiate the four-way handshake protocol to generate session key between client and the access point. It uses an AES type symmetric encryption which works on blocks of data instead of stream. Also, it operates on 128,192,256 bits key lengths. The encryption mechanisms take place in many rounds depending upon key length. CCMP (CCM mode Protocol) is an encryption protocol adopted for Wireless LAN devices that involves the standards of the IEEE 802.11i rules to the original IEEE 802.11 standard. CCMP is better data cryptographic encapsulation mechanism developed for data confidentiality and based upon the Counter Mode with CBC-MAC (CCM) of the AES standard. It was created to address the vulnerabilities showed by WEP, a dated, insecure protocol [13].

ADD (additional authentication data, temporal key and nonce along with CCMP are used for data encryption. Also, an aligned 48-bit packet number (PN) is used to build nonce. Cipher Block Chaining Message Authentication Code (CBCMAC) is used for integrity (instead of Michael's algorithm).CCM = CTR + CBC-MAC for confidentiality and integrity [14]. IV size used here is 48-bit and CBC-MAC for integrity check mechanisms. The WPA2 mac frame consists of MAC header, CCMP header, encrypted data and encrypted MIC. Overall, WPA/WPA2 enables protection against forgery and replay attacks.

WPA2 ENCRYPTION:

- Encrypt starting 128-bit block with data integrity key and AES, derived from a passphrase of 8 to 63 ASCII characters.
- In the next step, XOR Result1 with next 128-bit block to render XResult1.
- Encrypt XResult1 with AES and data integrity key.
- XOR Result2 and the next 128-bit block of data [15].

WPA2 DECRYPTION:

Decryption process can be formulated in these 4 steps:

- Find the value of the starting counter from values in 802.11 header and MAC header.
- The starting counter value and the encrypted portion of the 802.11 payload are used as an input for the AES counter mode decryption algorithm with the data encryption key.
- The result is the decrypted data and MIC. To yield the decrypted data block, AES counter mode XORs the encrypted counter value with the encrypted data block.
- The starting block, 802.11 MAC header, CCMP header, data length, and padding fields are used as an input for the AES CBC-MAC algorithm with the data integrity key to calculate a MIC. To discover if the data is valid, compare the unencrypted MIC with the calculated value of MIC. If the values do not match, WPA2 discards data [15].

WPA/WPA2 Enterprise implements RADIUS or EAP (Extensible Authentication Protocol) for centralized client authentication via other authentication schemes, like Kerberos, token cards, authentication certificates etc. Users are given login credentials which is later required to connect the network. It provides extra layer of authentication security as compared to the WPA personal mode.

Various Security Issues in WPA/WPA2:

Brute Force method: Weak passwords are generally vulnerable to these types of attacks. Various tools like Air-crack, Airgeddon etc. intercepts the secure session, by sending re-authentication packets. The captured data is then tested for cracking methods via some dictionary. This attack generally takes some time.

Packet spoofing and decryption: Mathy Vanhoef and Frank Piessens improved on the WPA-TKIP attacks of Erik Tews and Martin Beck. They showed how to inject an arbitrary number of packets, with each packet containing at most 112 bytes of payload. This was determined by using a port scanner, which can be executed against any client using WPA-TKIP. Moreover, they showed how to decrypt arbitrary packets sent to a client. They specified that this can be used to hijack a TCP connection, enabling an attacker to inject malicious JavaScript when the victim visits a website. In contrast, the Beck-Tews attack could only decrypt short packets with mostly known content, such as ARP messages, and only enabled injection of 3 to 7 packets of at most 28 bytes. The Beck-Tews attack also needed Quality of Service (as defined in 802.11e) to be implemented, while the Vanhoef-Piessens attack doesn't require as such. Not either attackslead to recovery of the shared session key between the client and Access Point. The authors say using a short rekeying interval can restrain some attacks but not all, and strongly advised switching from TKIP to AES-based CCMP [16] [17] [18].

WPS Pin: A more concerning security flaw was revealed in December 2011 by Stefan Viehböck that influences wireless routers with the Wi-Fi Protected Setup (WPS) feature, regardless of which encryption method they use. Most models (modems) have this feature and enable it by default. Many Wi-Fi device manufacturers had taken steps to eradicate the potential of weak passphrase choices by providing other methods of automatically generating and distributing strong keys when users cast a new wireless adapter or product to a network. These techniques incorporate pushing a button on the devices or entering an 8-digit PIN. The Wi-Fi Alliance standardized these methods as Wi-Fi Protected Setup. While the PIN feature as extensively implemented, received a considerable new security loophole. This flaw facilitates remote attacker to recover the WPS PIN and, with it, the router's WPA/WPA2 password in a few hours [19] [20]. Its recommended to disable this feature on network access devices.

Key Re-installation Attack (KRACK) Attack: Found recently by Mathy Vanhoef and Frank Piessens. It compromises the most famous four-way handshake protocol by re-installing the key that is already being used. In a key reinstallation attack, the attacker conspires against a victim into reinstalling an already-in-use key. This is accomplished by manipulating and replaying cryptographic handshake messages**.** When the victim reinstalls the key, co-related parameters such as the incremental transmit packet number (i.e. nonce) and receive packet number (i.e. replay counter) are reset to their initial values. Substantially, to guarantee security, a key should only be established and used once. Unfortunately, this is not affirmed by the WPA2 protocol. By manipulating cryptographic handshakes, its vulnerability can be manipulated [21].All the leading manufactures circulated a patch for their devices against this attack, but a large section of devices still remain affected. Wi-Fi Alliance recently announced WPA3 with some important security fixes over WPA2.

CONCLUSION

Nowadays every device has access to the internet, huge chunks of data is being carried over the network. The data mostly include user generated data, texts, private secret information etc. Wireless security is bit difficult to maintain as compared to wired. With the advancement and modernization in technology, security challenges to maintain confidentiality, integrity, and availability of computational systems and their components are increasing abruptly. Open availability of certain cracking tools are present there, which possess security threats that are overwhelming. Though the security encryption features like WPA/WPA2, AES, TKIP, VPN etc. are highly practicable, there is a need for creating public awareness for the importance of security. The four-way handshake, one of the dominant security procedure for many years, until recently its flaw was found in WPA/WPA2.Not everything is fully secure over the internet, but with the right security practices we can minimize the threat/attack. Knowing about the attacks and their prevention, is of no use until applied practically i.e. Keeping the devices up to date(patching), configuring network devices properly as per strong policies, following the new trends in technologies, software and hardware protection (Anti-viruses).

REFERENCES

1. "What is Wi-Fi (IEEE 802.11x). A Webopedia Definition". Webopedia.com. Archived from the original on 2012-03-08.
2. "Solution Base: 802.11g vs. 802.11b". techrepublic.com.
3. RC4" Harwood, Mike (29 June 2009). "Securing Wireless Networks". Pearson IT.WEP is an IEEE standard introduced in 1997, designed to secure 802.11 networks.
4. Walker, Jesse. "A History of 802.11 Security". Rutgers WINLAB. Intel Corporation. Archived from the original on 9 July 2016. Retrieved 9 July 2016. IEEE Std 802.11-1997(802.11a) defined Wired Equivalent Privacy (WEP).
5. "WPA Part 2: Weak IV's". Informit.com. Retrieved 2008-03-16.
6. IEEE 802.11i-2004: Medium Access Control (MAC) Security Enhancements. 2004.
7. Alexander Gutahr "wired Equivalent Piracy (WEOP) Functionality, weak points, Attacks".
8. Scott Fluhrer, Itsik Mantin, Adi Shamir "Weaknesses in the Key Scheduling Algorithm of RC4" Lecture Notes in Computer Science.
9. Adam Stubblefield, John Ioannidis, Aviel D. Rubin "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP", 2001
10. Meyers, Mike (2004). Managing and Troubleshooting Networks. Network+. McGraw Hill.
11. J. Edney and W. A. Arbaugh, Real 802.11 Security: Wi-Fi Protected Access and 802.11i. Addison Wesley, 2004

12. A. A. Vladimirov, K. V. Gavrilenko, and A. A. Mikhailovsky, Real 802.11 Security Wi-Fi Protected Access and 802.11i. Addison Wesley

13. Cole, Terry (12 June 2007). "IEEE Std 802.11-2007" New York, New York: The Institute of Electrical and Electronics Engineers, Inc. Retrieved 11 April 2011.

14. J. Edney and W. A. Arbaugh, "Real 802.11 Security: Wi-Fi Protected Access and 802.11i," Addison Wesley, 2004, 481 pp., ISBN:0321156209

15. Eng. Wi Fi Security A Literature Review of Security in Wireless Network Ruchir Bhatnagar".

16. Vanhoef, Mathy; Piessens, Frank (May 2013). "Practical Verification of WPA-TKIP Vulnerabilities". Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security. ASIA CCS '13: 427–436

17. "Practical Attacks against WEP and WPA" (PDF). Retrieved2010-11-15.

18. "Enhanced TKIP Michael Attacks" (PDF). Retrieved2010-11-15.

19. Viehböck, Stefan (26 December 2011). "Brute forcing Wi-Fi Protected Setup"

20. "Practical Attacks against WEP and WPA" (PDF). Retrieved2010-11-15.

21. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2 by Vanhoef, Piessens. (https://papers.mathyvanhoef.com/ccs2017.pdf)