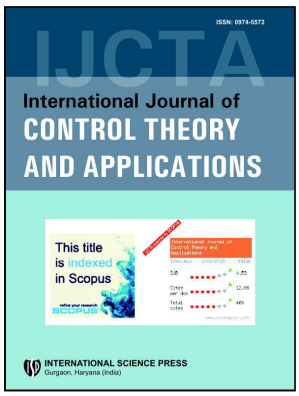

International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 13 • 2017

Wireless Security Issues and their Emerging Trends

Jaspreet Kaur[1]

[1] *Student of Department of Information Technology Indira Gandhi Delhi Technical University for Women, Delhi-110006 (IN), Email: jaspreetkaur9817@gmail.com*

Abstract: Now-a-days Wirelesses Local Area Networks (WLANs) have made more useful and valuable almost everywhere like colleges, cafes, metros, offices etc. as per the need. So, WLAN privacy is a very important factor for the user's data. These security issues occurs by either of the weakness in the security protocols or designs of WLAN and by many more ways. My mainly focus on these major types of important wireless security protocols: WEP, WPA, WPA2 and MSS. My aim to explore these security protocols and to present a brief description of their vulnerabilities by performing successful attacks against WEP and WPA protected WLANs and give comparative analysis with some new technologies such as WiMAX, WiGig with wireless networks (Wi-Fi).

Keywords: WLAN, WEP, WPA, WPA2, WiMAX, MSS, WiGig

1. INTRODUCTION

Wireless LAN is widely used today due to the mobile nature of devices. But in the WLAN all of the user's data are moving through the air medium which is easily captured by the attacker using monitor mode of the network. WLAN uses the various types of authentication protocols for the security of user data such as WEP, WPA, WPA2, MSS. Wired Equivalent Privacy (WEP) was the first IEEE 802.11 standard which came with a simplest authentication mechanism. WEP has some big vulnerabilities and was breached in 2001. An attacker may find out the authentication key of a network with a normal capacity laptop in an average of 1-2 hours. To remove the above vulnerability, a new protocol was developed in 2003, named Wi-Fi Protected Access (WPA). WPA used to remove the problems of WEP cryptography method. A year later, in 2004 came the second version, named WPA2, to replace normal WPA protocol. WPA2 developed an advanced encoding method for supporting the stronger security. WPA2 comes with several drawbacks. Then MSS (Multiple Slot System) authentication technique is used but it has also complex structure. So, there are various another approaches such as WiMax or WiGig are developed over the Wi-Fi for more security purpose.

In the following section I briefly described the WLAN network technology and their security issues. In the section 3 I analyze the Wireless protocols and its vulnerabilities. In the section 4 I discuss the new approaches over WLAN and their benefits in the network. Finally I conclude and give future scope for the WLAN.

2. WIRELESS NETWORK TECHNOLOGY

Wi-Fi is a short-distance wireless local area network technology. It supports only hundreds of feet access to the Internet related to a radio signal [1]. Wi-Fi transfers the data up to 54Mbps tramission rate, it also supports multimedia applications. Wireless uses the signal about to 100 m, without any actual infrastructure restriction, so is useful for internet users. Wi-Fi has defined these network nodes as:

1. A wireless client mainly made up of a PC or laptop or mobile phone with a wireless network card.
2. A wireless access point, its aim is to given a path between the wireless and wired network. when access point used in the network, then it called as infrastructure network otherwise the network called as the adhoc network.

Attacks on the Wi-Fi network can be occur on access control of resources, data confidentiality, integrity protection , wireless communication network design, deployment, and maintenance. But mainly wireless LAN have these security issue as:

1. Weaknesses in wireless security protocols.
2. wireless signal capture attack.
3. Wireless network eavesdropping.
4. Design of the Wi-Fi network.

For more details refer to [1]. There are various solutions available for these security issues as expand the signal strengths, network MAC addresses filtering, network protocol filtering, Port access control technologies, Improvement in wireless security protocols and many more. I am mainly focus on the security protocols improvement in this paper.

3. WIRELESS PROTOCOLS SERVICES AND ITS VULNERABILTIES

There are mainly these wireless protocol used in WLAN such as WEP, WPA, WPA2, MSS. These wireless protocols operates on the data link layer and physical layer of the network protocol stack. These protocols used for 802.11 or 802.11i or for many more versions of wireless networks and it gives the these services:

1. Diffusion: Transfer Frame to the particular or all destinations .
2. Combination: Allow connectivity from IEEE to another WLAN networks.
3. Connection: Recognize clients connect with an AP.
4. Re-connection:The transition between different APs when connection is lost.
5. Termination: Terminate an existing association or connection.
6. Validation: Only authorized users can access the networks.
7. De-authentication: removal of a valid user.
8. Secrecy: No one another can see another's private data.
9. MSDU: MAC Service Data frames responsible for getting data from client to its final destination.

For more information about the services refer to [2, 10].

3.1. WEP (Wired Equivalency Privacy)

This is an authentication protocol for wireless local area networks to provide security of the data same as in wired local area network. This protocol comes under the 802.11 wireless standards. WEP uses an RC4 cryptographic algorithm to encode and decode packets. WEP was developed to provide Confidentiality, Integrity, and Authentication of frames. Confidentiality is provided from the encoding (RC4 algo.) of the packets. Integrity is given through the cyclic redundancy check (CRC) and Authentication is given by the use of shared key that is only known by valid

users on the network. The aim of WEP algorithm was to provide the security between end users of a Wireless local area network over radio signals. RC4 algorithm uses two key sizes: 40 bit and 104 bit, add a 24- bit initialization vector (IV), directly (in plain text) transmitted which makes total of 64 and 128 bit key.

WEP Weaknesses:

1. The Size of IV is short and reused.
2. Vulnerability in the RC4 encryption itself.
   -RC4 algorithm itself vulnerable from weak keys. Frames which were encoded with these weak keys is a simple to break. Since the first three bytes of the keys are taken from the IV that is sent unencrypted (plain) in each packet,
   this vulnerability can be misused easily by a passive attack. For capturing a 104-bit WEP key, it needs to take between 2,000 and 4,000 real packets [3]. On a normal loaded network, the packets are captured in a very short range of time.
3. WEP does not stop fraud of frames.
4. WEP does not stop replay attacks.

WEP2 (Wired Equivalency Privacy version 2)

It increases up to the 128 bits values of both the IV and the keys. It was used to minimize the replicate IV problem as well as prevent brute force key attacks.

WEP Plus

WEP+ is a general extension to WEP given by Agree Systems that increases WEP security by reducing the problems of "weak IVs".

Dynamic WEP

In dynamic WEP keys changed dynamically for not easily captured by the attackers.

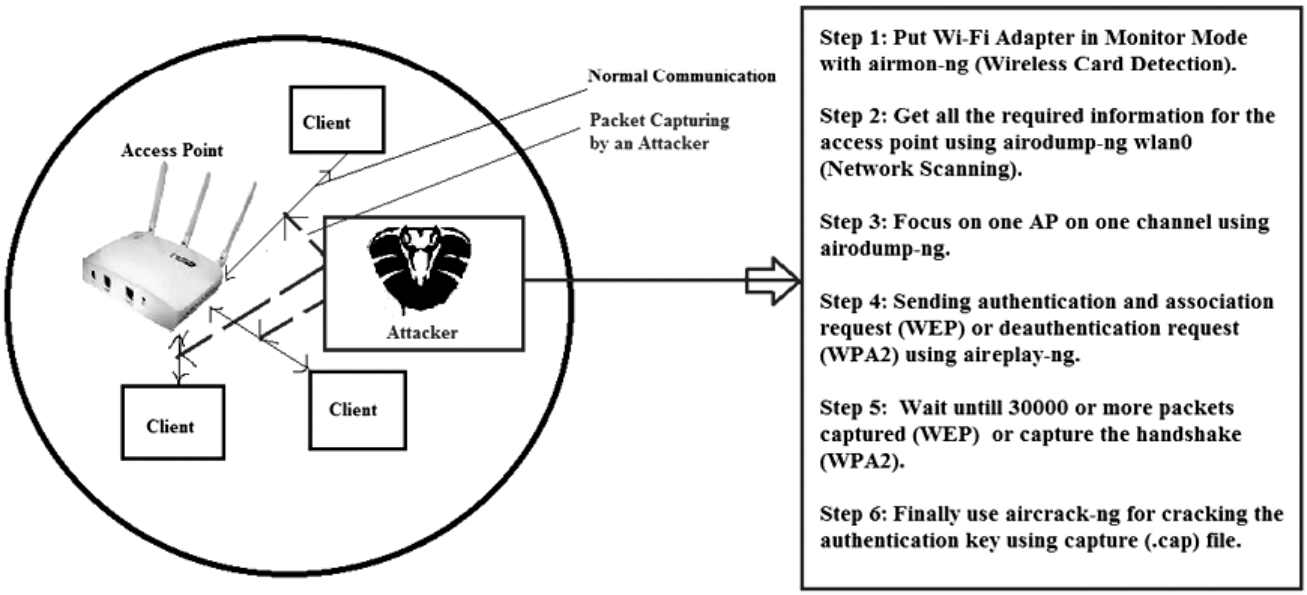

Figure 1: Setup and Steps for Wireless Protocols Cracking

3.2. WPA Personal OR Enterprise

WPA came for solving the problems in the WEP cryptography method, without changing the network resources. The standard WPA used two method same as the previous one (WEP) as:

WPA Personal or WPA-PSK (Pre-Shared Key)

It used for small range of networks such as in colleges, hotels etc. The authentication key can used up to 256 bits. Unlike WEP, this can be any alphanumeric pattern and is used only for the negotiation of the first session along with the AP. This key is pre-shared between the clients and the access point for mutual authentication of both and never send over the air.

WPA Enterprise or Commercial

For authentication (802.1X+EAP), authentication server such as RADIUS (Remote Authentication Dial-In User Service) server is used. It replaces WEP with the more valuable TKIP encryption. WPA allows a very strong data encryption algorithm such as TKIP (Temporal Key Integrity Protocol) and followed by MIC (Message Integrity Check) for integrity purpose.

WPA Improvements:

1. For reducing frauds it used the a message integrity code (MIC), called Michael.
2. For reducing replay attacks from the intruders a new IV sequencing method is used.
3. For strengthen the public IVs from weak keys a per-packet key mixing function is used.
4. For providing the actual encryption a rekeying mechanism is used.

WPA Weakness

There is a weakness in Passphrase Choice. The passphrase can be easily taken by the attacker by performing a dictionary attack and capturing the four-way authentication handshake. This weakness was based on the pairwise master key for the verification of this key normal traffic should be broadcasted that can be easily obtainable by the attacker.

3.3. WPA2 Personal or Enterprise

WPA2 is the upgrading version of WPA. It obtained encryption using AES algorithm, authentication using EAP-TLS protocol and data integrity using CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol). Same as previous one it has two security modes as:

WPA2 personal

A pre-shared authentication key is used, same as previous protocols. Access points and clients both are having the same secret key up to 64 ASCII characters, such as My password is secure. This secret key is manually configured at both side and 256-bit key is produced randomly for encryption.

WPA2 corporate

The enterprise security is based on 802.1X (RADIUS server) which includes the EAP authentication framework.

Vulnerabilities of WPA as a pairwise key is improved by these 1. The pairwise key suite, used to encrypt point-to-point traffic. 2. The group key suite, used to encrypt point-to-multipoint and broadcast data frames. 3. The use of either a pre-shared key or RADIUS server authentication [4-6].

WPA2 Weakness

In WPA2 there is two types of keys are to be used such as PTK (Pairwise Key) for the protection of unicast data frames, for group addressed data frames protection GTK (Group Key) is used. This Group addresses of frames are always given by an access point and never assigned by a Wi-Fi client. But any attacker sends forged GTK to all clients on the behalf of access point. This is called as the insider attack and WPA2 is vulnerable from it [6].

3.4. MSS (Multiple Slot System)

MSS consider four cryptography algorithms as Blowfish, RC4, RSA and AES. This method uses 256 sections from which one of the four algorithms is selected randomly. It used 2-bit binary code for selecting one of the four algorithms rather than real name of the algorithms. For each algorithm it uses a key table corresponding to that algorithm. So, that it has 4^256 different possible combination of algorithm and key as well for encrypting each message. It means any hacker needs to go through 4^256 computations just to finding out the exact formation of the slots. It provides authentication using EAP protocol and works on the application layer [7].

MSS Weakness

It is hard to implement on the existing hardware and it's reduces the chance of attack rather than eliminating of it.

4. NEW APPROCHES ON WLAN

Wi-Fi have several drawbacks when comes into the security point of view. So, there are new technologies come over the Wi-Fi as:

4.1. WiMAX

It has the full name as Worldwide Interoperability for Microwave Access. This Wireless technology mainly used for large networks as MAN. It is a scalable wireless platform used for the delivery of IP related services over a large area and able to be managed in both authorized and unauthorized range [8].

4.2. WiGig

It has the full name as Wireless Gigabit Alliance. This new technology allows to communicate wirelessly at multi-gigabit speeds for network nodes. It gives very high efficiency for wireless data, video and audio usage. It Widely used advanced security and power management for WiGig devices [9].

Table 1
Comparison of Wi-Fi over New Technologies

Feature	*Wi-Fi (802.11b)*	*WiMAX (802.16a)*	*WiGig (802.11ad)*
Primary Application	Wireless LAN	Broadband Wireless Access	Wireless Alliance
Frequency Band	2.4 GHz	2G to 11GHz	60 GHz
Half/Full Duplex	Half	Full	Full
Speed	upto 11Mbps	upto 2Mbps	upto 7Gbps
Security	Data Levels	Data Level	Data and Content Level

5. CONCLUSION AND FUTURE WORK

As I see there exist various security and non-security issues in Wi-Fi network. I also discuss the authentication protocols, their vulnerabilities and their improvements in the network security. There are new technologies as WiMAX or WiGig which are more useful than Wi-Fi and adopted by our network environment more easily. For the future work I shall also study these new technologies vulnerabilities.

REFERENCES

[1] Haishen P., "WIFI network information security analysis research", Chongqing College of Electronic Engineering, Chongqing, China, IEEE, 2012.

[2] Hong, Jumnit, and Riad L., "WEP protocol Weaknesses and Vulnerabilities", Oregon State University, 2003.

[3] Muhammad Juwaini, Raed A., "Review on wep wireless security protocol", University Kebangsaan Malaysia, The University of Jordan, Journal of Theoretical and Applied Information Technology, IJANS, Vol.40, No.1, June 2012.

[4] Vipin P., "Comparative analysis of wireless security protocol (WEP and WPA2)", International Journal on AdHoc Networking Systems (IJANS), Vol.4, No. 3, July 2014.

[5] Arash Habibi L., "Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA)", Computer Science Dept. of FCSIT, University of Malaya, International Conference on Signal Processing Systems, 2009.

[6] Ahmad, Md S., "Wpa too!", DEFCON 18, 2010.

[7] Prof. Dr. Gamal S., "New protocol design for wireless network security", International Conference on Advanced Communication Technology, 2006.

[8] Tutorialspoint, WiMAX-What is WiMAX? https://www.tutorialspoint.com/wimax/what is wimax.htm. Accessed 29 Nov 2016.

[9] Computerweekly, Goodbye Wi-Fi, hello WiGig. http://www.computerweekly.com/feature/Goodbye-Wi-Fi-hello-WiGig. Accessed 26 Nov 2016.

[10] informIT, Overview of the IEEE 802.11 Standard. http://www.informit.com/articles/article.aspx?p=24411& seqNum=7. Accessed 27 Nov 2016.