The Journal of
Mathematics and Computer Science

Available online at
http://www.TJMCS.com

The Journal of Mathematics and Computer Science Vol .5 No.4 (2012) 320 - 330

Security in Wireless Local Area Network (WLAN)

Kareshna Zamani*
IT Center, University of Mazandaran, Babolsar, Iran
kar_zamani@yahoo.com

Mehrnoosh Torabi
Department of IT, Shiraz University, Shiraz, Iran
mehrnoosh_torabi@yahoo.com

Hamidreza Moumeni
Department of Artificial Engineering, Shiraz University, Shiraz, Iran
momenir@yahoo.com

Received: February 2012, Revised: November 2012
Online Publication: December 2012

Abstract

Regarding increase of wireless network application, and fast development at these systems, security in such systems and networks has become a crucial matter. In this article, first different security methods of local wireless networks, as subsidiaries of wireless networks, are introduced and then the efficiency of so far introduced security methods such as WEP, WPA and WPAv2 are studied as well as their negative and positive aspects. The focus of this text is on IEEE security protocols including 802.1x and 802.11i, their functions and security levels. The privileges and shortcoming at the mentioned protocols would be discussed afterwards.

Keywords: Wireless LAN; Security; WEP; WAP; WAPv2

2010 Mathematics Subject Classification: Primary 54A40; Secondary 46S40.

1. Introduction.

In recent years wireless communication has significantly improved and wireless technology have found a particular position in business and computer industry local wireless networks have become important parts of networks architecture, having main impact on flexibility and mobility. In contrast to traditional wireless networks, clients can freely access the servers and wireless channels have been more accessible for both authorized clients and malicious internet attacks [21]. So this mobility and accessibility should be reliable and highly secure. The importance of a secure and reliable communication is often underestimated. The security threats in wireless networks is

* Corresponding Author

the equivalent of all security threats in wired networks, besides new introduced threats are the results of wireless system transmission capability. In general the structure at these networks is based on radio signals instead of wires and cables [7, 18].
By using this signals, in fact by having no border for network coverage, penetrators are capable of breaking the security barriers, which are not very strong, in order to access crucial information, attack the organization servers and destruct information and distort the network communication. They can produce misleading and unreal data and abuse the effective band width, thus nowadays strengthening these networks against the malicious attacks in one of the challenges of the network managers. In order to minimize these treats, organizations should take special security measures [16].

2. Wireless Networks

Wireless networks in their most simple type let hardware equipment connect each other without using physical backbones, such as cable and wire. These networks include a wide range of application and have a huge variety, but they are mostly divided into three categories based on their coverage range.

- Wireless Wide Area Network(WWLAN)
- Wireless Local Area Network(WLAN)
- Wireless Personal Area Network(WPAN) [5, 18]

In this article wireless local area networks are particularly focused and discussed.

3. Wireless Local Area Network (WLAN)

By wireless local area network we mean networks with limited coverage, which are used to cover a building or an organization, an area consisting of a hall and some rooms. In contrast to traditional local area networks which needed wire to connect the user's computers to the network, in this wireless network computers and all other equipment are connected to the network through access point. Access points generally cover up to 100 meters (300 foots) faraway. This coverage area in called a cell. Users are able to move freely through the cells by their laptops or other equipment without being discounted [9].

4. Three Security Generations in Wireless Local Area Network

Regarding the existing security problems in wireless networks, nowadays effective security measures are being taken. This is very important to know that the network manager is responsible for the security of wireless local area network, and he or she should be fully aware of the network's level of vulnerability and resolves and guarantees that the solutions are applicable all though the networks. As it is obvious for all the security system in order to have the best and the most optimum performance, hardware upgrading or service disconnection might be needed. If there were obligation to use the old systems, which lack compatibility with the new security systems, options should be very limited.

To organize the options, we can look at WLAN security solutions in three generations:

Pre-Security: Wired Equipment Privacy (WEP), years 1997-2002

Short term security improvement(accepted technique): Wi-Fi Protected Access(WPA), years 2003

Recommended Security Solutions (Best Practice): 802.11i, WPAv2, since 2004 [9, 16]

5. WEP Protocol

WEP is a security protocol which increases the level of security in wireless networks and encrypts the data transformed to wireless local area networks. Unfortunately the security provided by WEP is easily threatened by free softwares that sniff the network traffic for duration of time in order to access the WEP key [1, 14]. (See Figure 1)

Figure 1. WEP protocol

In IEEE 802.11b network sniff is encrypted by WEP algorithm. This algorithm is a symmetrical algorithm that uses the shared keys. These shared encryption keys, pointed as WEP key, should be identical on both client and access point. If the access point used WEP and the client didn't have the right WEP key there would be no connection to access point and no access to the network consequently (see Figure 2). Since WEP has its own shortcoming and defects, its static keys wouldn't suffice. These keys are potentially vulnerable. According to manufacturer and the network, they might need replacing every 10 minutes, which is impossible, thus it's firmly suggested to use dynamic WEP keys.

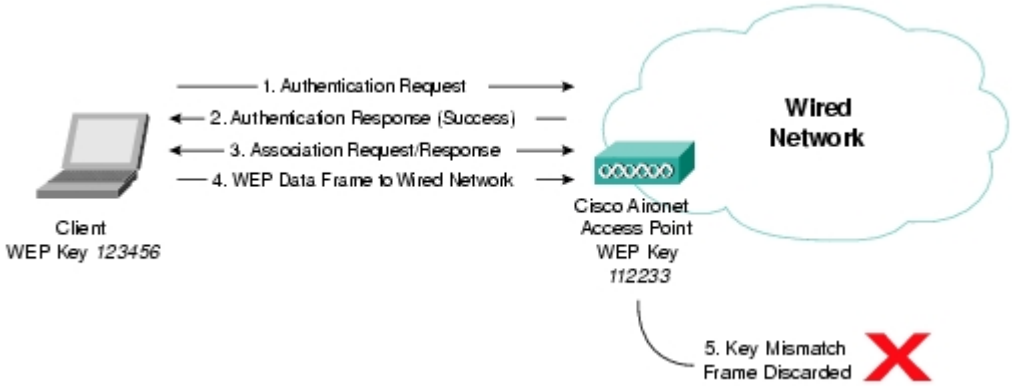

Figure 2. Key mismatch in WEP protocol

Before going through the negative aspects and shortcoming of WEP security we prefer to discuss the WEP function [2, 15].

WEP provides three security specifications:

1- RC-4 based encryption using a static 40 or 104 bit key

2- Shared key authentication based on WEP encryption

3- MAC address filtering [16]

A. RC-4 based encryption using a static 40 or 104 bit key

WEP encryption uses RC-4 (Rivest Cipher-4) algorithm to generate key stream which must XOR with the main message and finally create the encrypted text. To make sure not to have identified encryption for the same text, one extra datum is added to the WEP key in order to change the RC-4 algorithm basis, this amount, which is called salt in cryptography literature is named Initiation Vector or IV and is transferred in encrypted WEP packet. The length of IV is 24 bits, thus it

increases the length of WEP shared keys to 64 bits. The problem is that this length wouldn't seem to be sufficient for security supply. Most of the manufacturers have implemented a 128-bit WEP key and it has been emphasized to be used for WLAN.
It should be pointed that a 128-bit key consists of a 104-bit useful length and a 24-bit length that is related to IV. However a 104-bit key is not considered safe enough and based on this reason dynamic WEP keys are recommended. Since they can be replaced for several times which is one of their main specifications. [2, 3, 9, 16, 20].

B. Shared key authentication based on WEP encryptography

802.11 protocol determines an authentication process in order to connect to the network. In authentication access point's shared keys respond to an Authentication frame from a client by sending a 128-bit text message. User's device encrypts the Challenge text by its own WEP and sends it back to the AP. If the AP decipher the Challenge Text (client and AP both use the same WEP key) the user has been authenticated. In fact authentication is based on WEP static key. So if the hacker obtains WEP key, he could eavesdrop all the data sent to wireless local networks as well, and pass the authentication in the network (see Figure 3). As it was mentioned before WEP key is a 128-bit or 46-bit key but, it consists of a 24-bit IV so the real length is 40 to 104 bits [16].

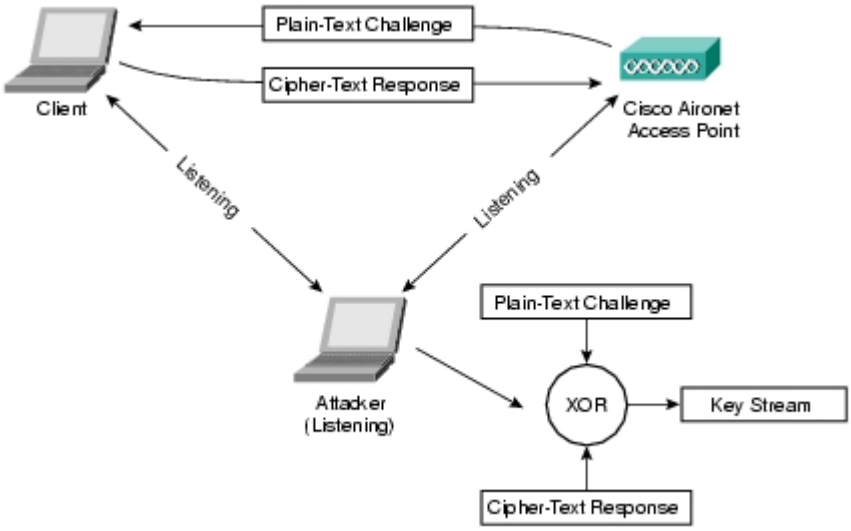

Figure 3. Shared key authentication based on WEP encryptography

C. MAC Address filtering

With this possibility the network manager can enter a list of MAC address on AP, since MAC address is an exclusive address, only authorized addresses could connect the network. This filter can be used to exclude or exempt unauthorized stations (see Figure 4). Here raises a problem, header fields of wireless local area networks are sent without encryption so hackers would easily discover authorized MAC and abuse or change their addresses to it. As a result this security layer like other security layers is not impenetrable, but success probability of such attack is very low, especially if these would be a combination of different security methods. The other problems are the necessity of entering MAC address list in each AP and list updating as soon as a new user is added to the network [9, 16, 21].

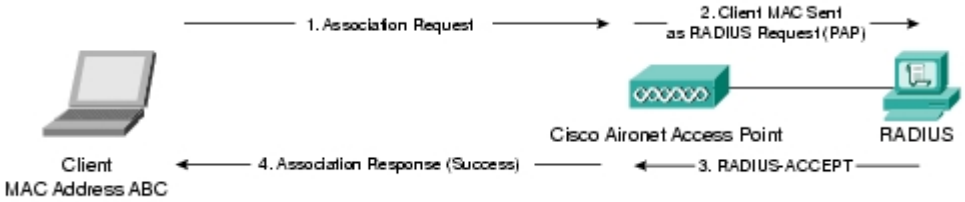

Figure 4. MAC Address filtering

6. WEP security weaknesses

In WEP, privacy is based on identical fixed keys and it can be simply recognized that these keys are vulnerable against the attacks such as brute force [16]. One of the general attacks against WEP is abusing the weakness in RC-4 which happens while IV main data is used. One of these attacks is FMS attack which has been described by Shamir, Mantin, and Fluhrer. They have discovered that extract of WEP key from stream key produced by algorithm RC-4 is possible due to RC-4 implementation methods and 24-bit IV and static encryption key [15]. Since 24-bit length is easily broken, and by breaking IV the hacker can access the whole WEP key and decrypts and reads all data. This threat is very dangerous because it is a passive attack and as soon as attackers access the traffic they can analyze it offline [15]. In fact in order to break WEP many IVs should be reached, but new available softwares such as Air-Snort and WEP Crack, have solved this problem for hackers. [8, 9, 10, 11, 12, 14].

The second type of attack is called inductive key derivation attacks, in this method the key is inducted by data force from wireless local network. This is an active attack. This is a fact in this kind of attack: with the XOR function in the end of the process, if there were two determined amount, another amount would be easily determined as well. For example if we have the main text and know the encrypted text, we can easily calculate the key stream, which is in fact RC-4 algorithm output. Due to the above mentioned function of algorithm, when the main text of the sent packet is determined or easily guessed, a few techniques have been developed for clients or end devices deception. Another subject is wireless station eavesdrop, leading to reach the encrypted packet which can be calculated through key stream [9, 15].

- Repeat in key stream which allows easy decryption of data for a moderately sophisticated adversary (Short IV).
- RC-4 algorithm weak implementation, causes the key be revealed.
- Brute force attack probability as the result of short key.
- Shared key and lack of management (weak management) threatens the keys
- It is possible for the message to be changed
- There is no user authentication
- Organizations doubt to deploy wireless 802.11 due to its weak security [4].

Regarding the above explanation WEP is a defeated way but in case of having no choice except implementation there are solutions to increase security. For example: higher layers could be encrypted (SSL, TLS, etc) or techniques such as VPN/VLAN can be used as well [9, 22, 23].

A. VPN/VLAN implementation

The main idea of VPN/VLAN configuration is that separate virtual LANs are implemented for all network APs. by default, all WLAN clients will become part of that VLAN when they associate with any of those access points. Before WLAN clients access virtual LAN, they should be authenticated and a secure tunnel connection should be made between the wireless client and the firewall. Authentication prevents any unauthorized accessibilities and the secure tunnel encryption ensures

privacy within data transmission. Instead of partial security in WEP, VPN usually uses IPsec that provides session-based keys and 168-bit 3DEC encryption [16].

7. WEP development and WPA (Wi-Fi Protected Access) substitute

Wi-Fi Alliance has introduced WPA as substituent of WEP. WPA presents a medium security condition and increases security specifications significantly. The most important advantage of WAP is that it is implemented through softwares upgrade instead of hardwares upgrade. WAP can be implemented by using a pre-shared key, which is entered to the system manually or by 802.1x authentication, which provides key distribution based on session [8, 6]. In order to overcome the already mentioned negative aspects, using dynamic keys, which change within a very short duration of time, is highly recommended.

The exact time depends on the number of clients and the type of traffic, but approximately 10 minutes would be logical. A 10-minute-time can cause scaling, but by using Temporal Key Integrity Protocol (TKIP), this would be a better timing without security threat; however an authentication based on EAP is required.

Two other developments are recommended by IEEE 80.11i WG (Working Group) which are not standard yet, but some of the vendors such as Cisco have performed them in pre-standard form. These two methods are IEEE 802.1x infrastructure for authentication and TKIP function used to develop WPA security. TKIP the same as WEP use RC-4 encryption so there is no need to promote or upgrade any hardwares [9, 13]. Two specifications in TKIP which increases WPA security are as follows:

- Per Packet Key Hashing
- Message Integrity Check (MIC)

A. Per packet key hashing

The first specification means that each packet uses individual origin to enter RC-4 algorithm [15]. In other world code key differ for each packet. So there might be same key among millions of packets. As a result gathering enough packets with same key is impossible. In addition when the key on each packet is exchanged, hackers won't be able to copy or repeat the same packets [8]. This subject means that by using the existing attacks inducting something about the main WEP would be very difficult [15].

B. Message Integrity Check (MIC)

Using MIC guarantees the integrity of each encrypted packet [15] that helps the receiver make sure that each packet hasn't been changed at all [8]. It also includes a sequence number which protects the packets from any change and being replay. When the access point checks the MIC amount of each packet, it slowly throws the damaged packets out. The amount of MIC is calculated before encryption and it is added to the packets before encryption as well [15].

C. Advantages of using WPA

- Improved cryptography (68-bit IV)
- Strong Network access control
- Support of 802.1x, EAP, EAP-TLS, Radius and Pre-Placed keys
- Key management
- Protection against replaying the information
- Information integrity provision (using Michael algorithm to produce accurate message code)
- Having key specifications such as using TKIP for data encryption and user authentication by using PPK and 802.1x EAP

- Ability to adapt the 802.00i standard after approval [4]

D. WPA Cracking tools

Regarding the above-mentioned security preparation, inefficiency of WPA cryptography was approved in the year 2009. The researcher, who reported the security defect of SSL in 2008, has performed a project in which the password of the wireless networks was obtained by using a calculation service based on cloud. In Moxie Marlinspike project a 400-CPU cluster was used to separate the packets obtained by wireless network, which all have been protected under WPA encryption. As it was mentioned before the packets can be collected the same as Wireshark through sniff softwares. The obtained information is uploaded in the service's website and finally the password would be revealed.

WPA CRACKER provides two services for the network password applicants. The first service costs 17$ and would return the password within 40 seconds, and the second service costs 34$ and presented the result within 30 minutes. Marlinspike claimed that his system would perform better than the two existing Rainbow tables and could obtain the WPA password within 20 minutes. Rainbow tables have been made up through common SSIDs combinations (for example default or Linksys) with hundreds of thousands indefinite words. Information packets should occurred with obtained hashes, in case of accordance the password can be found out. WPA hackers provided a service which can hack network's PSK (pre-shared key) by using ESSID (of course by using a dictionary which is big in size). The introduced WPA CRACKER has been presented as a useful tool for security managers and penetration testers who want to know whether they could penetrate special WPA network or not. In the service presented by this researcher, the tester registers a small "handshake" file including a back-and-forth primary connection between WPA router and PC. According to this information, WPA CRACKER can declare whether this network is vulnerable against this kind of attack or not. Since long time ago hackers have known that WPA-PSK networks are vulnerable against the attacks which are called dictionary attack. In this attack the hacker tries thousands of common passwords until eventually one of them works, but such an attack takes a long time due to WPA designation method. As far as each WPA password should be hashed for thousands of times, a normal computer can only guess 300 passwords per second, whereas other password crackers can process, hundreds of thousand passwords per second. This means that a WPA CRACKER's work, guessing 135 million choices takes 20 minutes while it takes 5 days on a dual core computer. This attack will perform if only the network password is chosen from a 135 million phrase Marlinspike dictionary, but if the network password were strong or accidentally made, it wouldn't probably be broken. This service can save a lot of time for the network security inspectors [8].

8. WPAv2, 802.11i

IEEE has presented a more comprehensive solution for wireless local area network encryption, which is called 802.11i. Wi-Fi Alliance recalls it as WPAv2. WPAv2 uses standard protocol widely in all layers [2]. In comparison with WPA [2], the first development was that AES-CCMP had been included in it as one of the necessary specification [4]. This choice uses a stronger encryption based on AES (Advanced Encryption Standard), which is one of the safest and fastest symmetric encryption methods. (See Figure 5)

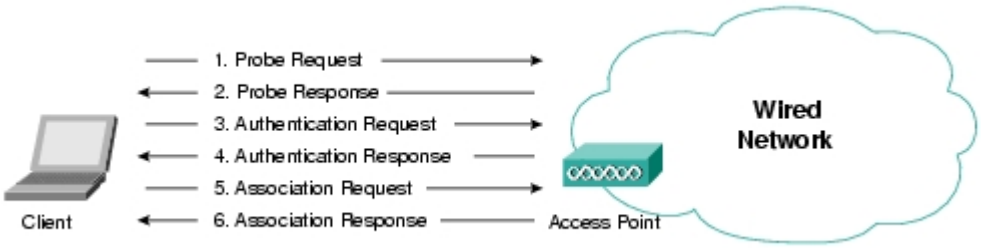

Figure 5. WPAv2, 802.11i

AES is a symmetric block encryption which is applied for file and text encryption, etc. This is a very safe and fast algorithm which is uses one key or code for coding and decoding. The function of this algorithm is the same as a similar famous algorithm called DES (Data Encryption Standard). DES has an easier and faster implementation, but is not safe [24]. AES needs different hardwares from WEP and WPA that means, 802.11i performance includes replacement of NICs and access points and similar to WPA and 802.11 can be implemented by the pre-shared keys, which are entered to the system manually or with 802.1x authentication provide a session basis key distribution [8]. Whereas WPAv2 is based on known standards, there is a big chance to become sure that the security services particularly authentication, verification, non-repudiation and privacy are confident [2, 13].

A. 802.11i positive aspects

- Strong cryptography
- Old equipment support
- Strong control on network accessibility
- RADIUS, EAP-TLS, EAP, 802.1x support and pre-placed key support
- Key management
- Data and header integrity
- Protection against information resending
- Having key specifications such as using TKIP for data encryption and user authentication using PPK and EAP 802.1x
- Roaming support [4]

802.11i needs hardware upgrading for EAS processing. Of course some of the implementations only need firmware upgrading. The problem which raises here is that most users don't tend to use 802.11i since they still trust and rely on WPA [4].

B. WPAv2, 802.11i implementation problems

The biggest 802.11i implementation problem is that the old access points and NICs are not able to use this algorithm. To supply a suitable efficiency, data cryptography is usually done in hardware instead of software. Each access point or client with NIC need a chip to perform AES cryptography, but any way since early 2006 Wi-Fi Alliance has supplied all wireless system having 802.11i support capability [8].

9. IEEE 802.1x authentication process

In today's distribution systems authentication is necessary for entity authorize and confidence level depends on process output. Ideally authentication should be done very clearly without any pause. The correct performance of this process can prevent unauthorized penetrations [17]. There are two suggest solutions for WLAN authentication which is done in at either layer 2 or layer 3 of the 7 layer ISO stack. Layer 3 schemes is based on IP addresses and the most common example of such

schemes on VPN technology would be similar to IPsec, which is usually in public networks and extranets, but they are rarely uses in intranets due to complexity and high expenses [9, 15].
For setting access point, it is used three different authentication ways:
Open authentication: where anyone can join AP and enter the network. This one usually is not suggested, except in public hot spot where a secondary authentication is used.
Shared authentication: is used where WEP keys are pre-shared and for client authentication by AP. This is not a safe way due to WEP security weaknesses. In fact it means that the key should be changed for several times which is impossible in large networks. Also if a client is robbed, all shared keys would be threatened and would need to be replaced.
EAP Network: one of the best suggestions is to use any of EAP authentication methods as described below. While establishing layer-2 authentication, it is firmly suggested to use a structure based on various EAP algorithms performed in IEEE 802.1x framework. Cisco systems performed a version of EAP called LEAP for the first time in the year 2000 [9, 15].
WPA and 802.1x cause privacy and eavesdrop prohibition. Authentication and authorization are other important factors in security. 802.1x does the above mentioned tasks by port based authentication. Generally, using such an authentication process causes to increase network security. IEEE 802.1x authentication ensures a mutual authentication. Through using an authentication server a RADIUS server is usually used as an authentication server and EAP protocol is used to send messages. 802.1 x authentications consists of three parts:
Connection applicant (which is usually a software in the receiver's computer), authenticators (in Ethernet networks are switches and in wireless local networks are APs) and the authentication servers (are the radius server). When the connection applicants send their connection requests to AP, AP sends this request to RADIUS server and authentication is performed in this server. While authentication is being done the connection applicant and RADIUS server are connected through AP. Since RADIUS server is located in AP local network, penetrator is not able to penetrate in it, thus this method can guarantee a high security. This mutual authentication method is very efficient to prevent the man-in-the-middle attacks especially when a Rouge AP perm client to be connected to the network through it and distribute data legally in the network. In two-way authentication, it is necessary for a Rogue AP to check the threats to connection with RADIUS server. Since the system is wireless, particular technologies must be used to strengthen this area. The second advantage of using such structure is that WEP dynamic keys can be implemented. With these keys, WEP keys can be automatically distributed in pre-determined times, which increases the security of WLAN [15].

10. Extensible Authentication Protocol (EAP) in 802.1 xs

There are many derived algorithms of EAP, such as EAP-MD5, EAP-Transport Layer Security (TLS), EAP-Tunneled TLS (TTLS), EAP- protected EAP (PEAP), EAP-Cisco wireless (LEAP). There would be more over time.

A. Some points regarding different models of authentication:

- Although EAP-MD5 supports username and password authentication, but cannot provide a two-way authentication and cannot support WEP dynamic keys.
- EAP-TLS (IETF RFC 2716) supports two-way authentication, but it's very expensive. Each user must have a certificate. In addition EAP-TLS can only be supported in Microsoft windows XP.
- Cisco LEAP supports all recommended security specifications such as username, password, two-way authentication and dynamic WEP. In addition there are available drivers for all operation systems as follows: Windows 2000, Windows 98, Windows 95, Windows CE, Windows XP, Windows ME, Linux and Apple Max OS 9-x.

In addition there are available drives for all operation systems as follows: Windows 2000, Windows 98, Windows 95, Windows CE, Windows XP, Windows ME, Linux, Max os9

11. Conclusion

Security supply WLANs is one of the barriers in expansion of wireless networks. First they must be correctly installed and configured. A right authentication framework is very necessary and in fact it includes an important part of security supply in WLANs. Although cryptography and authentication for 802.11i standard in wireless networks are developing, they have their own short comings and defects. Key distribution is the major problem of cryptographic techniques, but a few solutions have been presented for this problem. Despite WEP cryptography specification doesn't supply enough security and it easily gets attacked by the hackers due to its own short comings, but it's better than nothing. For more security, WPA is used as improved WEP for IEEE 802.11i standard in wireless networks. As it was mentioned in the article each WPA key has 48-bits IV which consists of 500 trillion combinations and has a stronger encryption than WEP. Security level is higher than WEP encryption as a result of having many combinations and less reputation in key cryptography. WPA doesn't directly use the main encryption keys and easily control to all messages. It uses TKIP algorithm for data cryptography. Key hashing per packet and message integrity check in TKIP, are two specifications which increase WPA security. However even WPA is threatened by the hackers. So in order to improve network security, WPA has been replaced by WPAv2, which has improved cryptographic methods. The most important advantage of WPAv2 in comparison with WPA is that it contains AES-CCMP algorithm. This method uses stronger encryption basis on AES that is one of the safest and fastest symmetrical cryptography methods. Regarding authentication, since WPAv2 is based on known standards, there is an opportunity to become sure that the security services particularly authentication, verification, non-repudiation and privacy are confident. Using a strong authentication process increases network security, thus one of the EAP authentication, is highly recommended. In addition, while layer-2 authentication is being established it is firmly suggested to use a structure based on various EAP algorithms, performing in IEEE 802.1x frameworks. This important task requires RADIUS 802.1x authentication server which is now able to provide the best level of security and authentication right now. High complexity can be considered as the only negative aspect of using RADIUS 802.1x, but any way, the key distribution problem has been solved by using this server [19].

References:

[1] A. Louw and William A.Yarberry, Jr., Wireless security :here we go again , Information Strategy, (2002)

[2] A.S. Tanenbaum, Computer Networks, Foutrh Edition, (2008)

[3] B. Issac, L. A. Mohammed, War driving and WLAN security issues-attacks-security design and remedies , Information Systems Management, 24(2007)

[4] B. R. Miller, and B. A. Hamilton, Issues in wireless wecurity (WEP, WPA & 802.11i), 18th Annual Computer Security Applications Conference, (2002)

[5] B. V. Solms and E. Marais, From secure wired networks to secure wireless networks e what are the extra risks?, Computers & Security,23 (2004), 633-637

[6] C. Ellison, Wireless security:WPA step by step ,Pc Magazine, Special wireless issues,(2003), 47-51

[7] D. L. Evans and Phillip J. Bond and Arden L. Bement, Wireless network security—802.11, bluetooth and handheld devices, National Institute of Standards and Technology, USA, (2002)

[8] Elsevier, WPA cracking tool launched, Network Security, Published by Elsevier Ltd, 12(2009), 1-2

[9] Internet Security Systems (ISS) group, Wireless LAN security 802.11b and corporate networks, http://documents.iss.net/whitepapers/wireless_LAN_security.pdf, (2001)

[10] J. Chen and M. Jiang and Y. Liu, Wireless LAN Security and IEEE802.11i, IEEE Wireless Communications, 12 (2005), 27–36

[11] J. Edney and W. Arbaugh, Real 802.11 Security, Addison Wesley, Reading, Massachusetts, (2004)

[12] J. Kindervag and CISSP and CCNA and ICE, The five myths of wireless security, Telecomminucation and Network Security, (2006), 7-16

[13] J. Lei and X. Fu and D. Hogrefe and J. Tan, Comparative studies on authentication and key exchange methods for 802.11 wireless LAN, Computers & Security, Volume 26, Issue 5, (2007), 401-409

[14] K. Dunham, Wireless worries and wisdom, Information Systems Security, Auerbach Pubication, (2005)

[15] K. Regan, Wireless LAN security: things you should know about WLAN security, Network Security, (2002), 7-9

[16] M. F. Finneran, Voice over WLANs: the complete guide book , By Elsevier Inc, (2008)

[17] M. Rahman and H.Imai, Security in wireless communication, Kluwer Academic Publishers, Wireless Personal Communications 22(2002), 213–228

[18] N. Baghaei and R.Hunt, Security performance of loaded IEEE 802.11b wireless networks, Computer Communications 27 (2004), 1746–1756

[19] Proxim, Wireless network security, ORiNOCO ,(2003)
http://www.proxim.com/learn/library/whitepapers/wireless_security.pdf

[20] S. Jason, Security in a wireless world , Macworld, 07418647, 20 (2003)

[21] S. Madhavi, An Intrusion detectionsystem in mobile adhoc networks, International Conference on Information Security and Assurance,(2008)

[22] S. Phan, 802.11b update: stepping up your WLAN security , Network Maganize, (2001)

[23] Wikipedia, http://en.wikipedia.org/wiki/Wireless_security

[24] Wikipedia, http://en.wikipedia.org/wiki/Advanced_Encryption_Standard