Technical report, IDE1013, April 2010

WLAN Security

Master's Thesis in Computer Network Engineering

Abdul Qudoos Memon, Ali Hasan Raza and Sadia Iqbal

School of Information Science, Computer and Electrical Engineering
Halmstad University

WLAN Security

Master's Thesis in Computer Network Engineering

School of Information Science, Computer and Electrical Engineering
Halmstad University
Box 823, S-301 18 Halmstad, Sweden

April 2010

Preface

By writing this report, it gave us the opportunity to understand the nature up to the bottom of wireless network from ideal and real life point of view especially in WLAN Security. It's a great opportunity for we people to work with the real hardware in the lab environment and allowed full access to all the hardware available. Therefore we want to say thank from core of heart to our supervisors Olga Torstensson & Yan Wang for their guidance and suggestions during all the time up till the completion of this thesis, both helped us a lot from the initial stage up to the final stage. So, it's a great opportunity for us to work with Olga Torstensson and Yan Wang.

In the end, warm thanks to our Parents for their endless efforts and motivations to get higher education, allowed and encourage us to study in another country away from them, this goal would be unachievable without their existence, also to our loving and sincere friends for their patience during this time and played an important role during our abroad studies.

Abdul Qudoos Memon, Ali Hasan Raza & Sadia Iqbal

Halmstad University, April 2010

Abstract

WLANs are become popular due to their different advantages. Beside all these advantages WLANs are also facing the major problem of the security, so that why lots of people are doing research on WLAN to improve the security because many companies want to transfer their sensible data over WLAN.

This report discusses the security issues of WLAN based on IEEE 802.11 standard, such type of networks are referred to as wifi network. WLAN is deployed as an extension of already existed wired LAN. Therefore it is necessary to provide the security of WLAN equals to Wired LAN.

We worked in a lab environment in order to configure the three different security solutions (WEP, WPA & WPA2 using IEEE 802.1X and RADIUS Server) on infrastructure mode for personnel and enterprise architecture of WLAN. For each security solution we used the backtrack as a security cracking tool, in order to break the WEP (64 and 128 bit long) security key of WLAN, make comparison between 64 and 128 bit long WEP key and also analyzed the different kind of attacks and some drawbacks of using WEP security in WLAN. In the same way configure the WPA and WPA2 (using IEEE 802.1X and RADIUS Server) security solution in infrastructure mode of WLAN and use the same security cracking tool backtrack in order to break the security of the WLAN and analyze the different attacks on the network in these architecture and drawbacks of using WPA and WPA2 Security solutions. By using IEEE 802.1X and RADIUS Server we can improve the security of the enterprise network.

In the end we come with many conclusions and suggestions that will help in order to provide better security while deploying Wireless LAN.

Contents

List of figures

List of tables

List of abbreviations

AAA	Authentication Authorization and Accounting
AP	Access Point
AC	Access Control
AES	Advanced Encryption Standard
ASCII	American Standard Code Information Interchange
ARP	Address Resolution Protocol
AAD	Additional Authentication Data
CAPWAP	Control and Provisioning of Wireless Access Points
CISCO	Computer Information System Company
CSMA/CA	Carrier Sense Multiple Access/ Collision Avoidance
CSMA/CD	Carrier Sense of Multiple access/ Collision Detection
CCK	Complementary Code Keying (RF modulation)
CCMP	Counter-Mode/CBC-Mac Protocol
CHOPCHOP	
CBC-MAC	Cipher Block Chaining-Message Authentication Code
CCM	Counter with CBC-MAC
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
DSSS	Direct Sequence Spread Spectrum
DDoS	Distributed Denial of Service
DNS	Domain Name Server
ESS	Extended Service Set
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol over LAN.
FHSS	Frequency Hopping Spread Spectrum
FIPS	Federal information processing standard
FMH	Fluhrer-Mantin_Shamir
IPS	Intrusion Prevention System
IDS	Intrusion Detection Systems
IPSec	Internet Protocol Security
IV	Initialization Vector
ICV	Integrity Check Value
IP	Internet Protocol
IEEE	Institute of Electrical and Electronics Engineers
IR	Infrared
IBSS	Independent Basic Service Set
ISM	Industrial Scientific Medical
IETF	Internet Engineering Task Force
MAC	Medium Access Control
MIC	Message Integrity Check
MHz	Megahertz
Mbps	Mega Bits Per Second
MIMO	Multiple Input Multiple Output
MPDU	Message Protocol Data Unit

NICs	Network Interface Cards
NAS	Network Access Server
OFDM	Orthogonal Frequency Division Multiplexing.
PSK	Pre Shared Key
PN	Packet Number
PAE	Port Access Entity
PRNG	Pseudo Random Number Generator
PBCC	Packet Binary Convolution Code
PTK	Pairwise Transient Key
RF	Radio Frequency
RADIUS	Remote Authentification Dial in User Service/Server (networking protocol)
RSN	Robust Security Network
SOHO	Small Office Home Office
SSL	Secure Socket Layer
SSID	Service Set Identifier
TMTO	Time Memory/Trade-Off
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TGi	particular task group
TSC	Temporal sequence counter
TKTA	Temporal Key Translator Address
UNII band	Unlicensed –National Information Infrastructure bandwidth
UDP	User Datagram Protocol
WFA	Wifi Alliance
WLAN	Wireless Local Area Network
LAN	Local Area Network
WEP	Wired Equivalent Privacy
WPA	Wifi Protected Access
WPA2	Wifi Protected Access Version 2.

1 Introduction

Now days WLANs are more and more famous due to their reduced price of components, easy to deploy at anytime and anywhere in the world. End clients are in a position to send big files through the communication medium that is air and free to move in the boundary of WLAN, able to access the internet and large bandwidth activities without the need of any cable or connectivity with a switch or a hub. Beside all of these advantages WLANs are facing the problem of security because many companies are transferring their sensible data across the WLANs. So lots of people are doing research on the WLAN security. WLANs are created for a sensible transfer of data. Initially the purpose of creating WLAN as an addition for the already installed wired LAN.

The most significant characteristic is to provide the security to the WLAN equivalent to wired LAN. In the starting, this target is seemed to be impossible but as year passed this target is achievable at some extent and fully now a days.

During the overall history of the WLANs it faces only single problem that is of Security. Still lot of research is going on that how to improve the security in order to make the network more secure and reliable then the Wired LAN. The breach in the security of WLAN will automatically harm the wired LAN as a result when RFs started moving in the air than there is a chance of hazard of special attacks which we will discuss in next chapters.

Our main goal of the study is to make our network more secure and reliable. There are five basic predefined goals for WLANs and there are different security solutions available which will help to provide the five basic goals. We are going to analyzed which security solution is fully providing the goals. When any security solution is ready to provide the above 5 goals, security is automatically achieved for the WLANs. We will also analyze that how many different attacks are possible and how to mitigate them as well described further in chapter3 & 4.

We are going to configure the different security solution like WEP, WPA/WPA2 & 802.1X using RADIUS Server on WLAN infrastructure mode in a lab environment. Divide the work load in three individual labs. For each lab we have different strategies which are described in the methodology portion & in chapter 5 in detail.

From three labs we are going to analyzed which security solution is best amongst all in order to provide the better security and which kind of general attacks are possible and how to mitigate all of them with their solutions in next chapters.

1.1 Background of the study

Before the starting of 21st century WLAN becomes famous and peoples want to use in home as well as for enterprise network due to its scalability, low cost and easy deployment. 802.11 WLAN technologies are introduced like 802.11b, a and g. The popularity of the WLAN is improved after the confirmation of IEEE 802.11b standard. Initially WLANs came with the WEP security [13], with the passage of time WLANs becomes more popular and the WEP security is failed to provide the security to the network. WLANs faced many drawbacks in the WEP security. The current study of WLAN provides knowledge to the administrator to improve the WLAN technology and approval of some important wireless security solutions like WPA & WPA 2 with AES. More threats and attacks are discovered for WEP security. To solve the problem of WEP, new security solution is introduced i.e. WPA [14] and then WPA2 [15]. To provide the security to any WLAN, three things are important to achieve Data confidentiality &

Integrity, Authentication & Access Control, Intrusion detection & Prevention [17]. Now a day's WPA & WPA2 security are integrated in the WLAN with the combination of 802.1x and RADIUS for providing authentication. Still security is considered to be a major task in the deployment of enterprise network. Joni Wexler's in his survey report ''State of the market report'' in year 2008 said round about 50% of the commercial customer still worried about the security issues in WLANs, but this is considered to be great achievement for the WLANs in comparison with the year 2006 & 2007 where 70% of the customers are worried for security in WLANs.

Current studies proved that WLANs can offer a high level of security even though it can beat the security provided by the wired LAN, until and unless it uses the security solution like WPA/ WPA2 with 802.1X & RADIUS. WLANS are already going through in the world of IT in majority of the enterprise, government bodies and also in public areas like hotels, cafes, hospitals, schools and airports. Scalability, mobility, flexibility, less cost, fast and easy installation is major benefits provided by the WLANs [11 & 12]. Even though some drawbacks are still available that can easily disturb the security of WLANs. Some possible holes are available in the network usually relates with the human mistakes which provide the cause to break the integrity of the WLAN like some stolen laptop, a computer effected by a virus or a give and take of username and password [18].

1.2 The WLAN security Problem

Problems that WLAN Security is facing due to the scalability, easy & large deployment of the network and these characteristics starts a numerous number of problems that need some solutions. If somebody compromise the security then network is useless.

Every AP available in the network is IP based, need some management, supervision and control. This action produces the extra load, creates difficulty for the wireless technologies during the implementation this is because every AP is having the same configuration this similarity between the APs will tend to some misconfiguration and inappropriate action of the WLAN and a big headache to distribute & maintain fast configuration for all APs available in the WLAN. It's very hard to provide the physical security to each AP in the network because there location is always outside from a server room or locked area. The stolen of that AP with its secrets, intruder can make use of those secret resources. To fix the above said problems, different vendors started work together in order to provide the solution by mixing the different network switching techniques, centralized, management and share wireless access in a new design. Hence mixed solution provides a benefit and friendly interface among the AP and a controller to fix all the problems seems undesirable. By use of ACs the threat of stolen IP is completely solved. The different WLANs using the devices for the control network access in order to offer packet delivery among the host to host for the different WLAN which also increased reliability. In order to provide the better security to the WLAN, the APs are installed at any place where there is a less physical security available, so CAPWAP design can decrease the importance of stolen AP. Let suppose all the high value secrets of AP are saved in the AC like the RADIUS shared secrets, after the stolen of AP will not produce any threat for the network. Hence AC is a device that can be place at a position where there is a physical security available.

1.3 Security requirement of the WLAN

To provide the security to WLAN, It requires five main security requirements to be achieved which are data integrity, confidentiality, authentication, access control & Non repudiation [5–9]. This section explains the purpose of each security requirement in terms of the security threats, means which security requirement is used to defend which security threat [5-9]. In general security threats are Eavesdropping and traffic analysis, Masquerade, Authorization violation, DoS & Modification of forgery of information [5-9]. So the below table best describes the purpose of each security requirement, means which security requirement is used to mitigate which threat in order to provide the better security to the wireless network.

Security requirements	**Security Threats**					
	Eavesdropping	Traffic Analysis	Masquerade	Authorization Violation	DoS	Modification
Confidentiality	Yes	Yes	Yes	Yes		
Authentication			Yes	Yes		Yes
Access Control			Yes	Yes		Yes
Integrity			Yes	Yes		Yes
Non repudiation			Yes	Yes		Yes

Table 1: Security goals w.r.t security threats.

Each security solution (WEP, WPA and WPA2) has to provide the above five security requirement to make a secure WLAN. Therefore to keep away from the different attacks in small or larger WLAN, the network administrator must use the specific security mechanism in the WLAN in order to make the network more and more consistent and scalable. Currently wireless internet is growing very fast, as a result there is a great need to make communication more secure else this fast speed of data flow becomes useless for everybody.

1.4 Goal of the study

Whenever the above five security requirements are achieved for WLAN, the security is automatically achieved. These WLAN security requirements are provided by different security solutions like WEP, WPA &WPA2. We are going to configure these security solutions in a lab environment and analyze which solution is able to provide the above five security requirements fully. In the end we will conclude which security solution is best amongst all from security point of view and we are also going to analyze which general attacks are possible for a different security solution also with their mitigation techniques and test some of the attacks in the lab environment.

1.5 Working Methods

There are different kinds of security attacks in WLAN network which can harm the network and can exploit it. This report explains the different general attacks with their mitigation techniques and some special attacks on security solutions. Mainly there are two general types of attacks, physical and logical attacks. Here are few attacks in WLAN and also there solutions how to secure from those attacks.

Logical Attacks with their mitigation techniques (Spoofing of MAC address, Denial of Service Attack, Man in the Middle Attack., Default Access Point Configuration, Reconnaissance Attacks, Conversation Sniffing, Dynamic Host Configuration Protocol Attack).

Physical Attacks with their mitigation techniques (Rogue Access Points, Physical placement of Access Points, Access Points Coverage, Spam Attack).

So firstly build simple Wireless Local Area Network (WLAN) in an infrastructure mode by using CISCO equipments. Initially no security to network means network is completely vulnerable to attacks means network is open for the intruder to access the information very easily. Practical work is divided into three experimental labs.

(1) For the 1st lab, designed a WLAN in infrastructure mode by using all the CISCO equipment. To provide initial security to the WLAN configure the WEP security solution from both AP and Client perspective in the lab environment although this WEP is comparatively good rather than WLAN having without security. After implementing WEP security, uses the cracking tool backtrack in order to break the WEP (64 and 128 bit) long security key and conclude that how WEP key is easy to break for WLAN and analyze that how WEP security is unreliable for secured network.

(2) For the 2nd lab use the same WLAN infrastructure network and configure the WPA and WPA 2 and try to break the WPA encryption key by dictionary attacks using the same cracking software backtrack3 and analyzed how much reliable this security solution with respect to WEP and conclude which one is more better.

(3) For the 3rd lab there is a need of the RADIUS server, connect RADIUS Server with the AP already build WLAN in infrastructure mode, configure the WPA2 using 802.1X security solution on the AP and try to break the security by using the same cracking software backtrack 3 to break the security of the network.

In the end compare all three labs and come up with a conclusions and suggestions, which one is the best security solution for the WLAN and drawbacks over each other.

1.6 Required Tools

In WLAN configuration many different types of tools are uses according to the requirements, in this project following tools are used to fulfill the task.

- Cisco Aeronet wireless adapter
- Cisco Aeronet desktop utility
- LinkSys wireless router
- LinkSys external wireless adapter (for cracking WEP and WPA)
- BackTrack

2 WLAN Basics

The WLAN is a wireless technology about which very limited number of people knows in the last few years. It grew rapidly in a small period of time just like a mobile communication and internet technology. This development is just because of the WLANs, which provide low cost, flexibility, scalability and ease of development. Yet this technology also brings lot of serious issues like security, low quality of service [25].

2.1 Overview of WLAN

This is the fact that after the invention of WLANs the networking becomes easy for the homes, business and in organizational environment because WLAN always used the electromagnetic waves (also known as radio waves) to carry the data signals from one end to another end in the network in order to get rid of from the use of cables in the network and it is implemented on the physical layer. During the earlier days, in wired networks the end nodes are connected through the wire by using the RJ-45 connectors. When WLANs are introduced end nodes are connected wirelessly with each other or through the telecommunication networks (on the other side these wireless nodes are connected through the internet or the backbone wired network). A wireless network is considered to be a type of computer network. Without interfering cabling the Wireless technology helped to make network simpler by enabling several computer users to share the resources in a business or in a home at the same time. These resources may consist of a network printer, broadband internet connection, data files, and even streaming video and audio [26].
WLAN Technologies are introduced in the end of year 1990, when the companies started to produce the products that usually operate on specific 900 MHz frequency band. These products are considered to be a non-company and proprietary standard that always helps to transfer the data at the rate of 1 Mbps not more than this, but in comparison to the wired network this data rate is considered to be 10 times less. The nonstandard proprietary architecture offers data rate of 1 (Mbps) but WLAN offers data rate up to 10 (Mbps) speed which is provided by a large number of wired LANs at the same period of time. In the beginning of 1992, different companies started to produce different products that usually works on 2.4 GHz ISM (Industrial, scientific and Medical) band. Even though these products provide maximum transfer rate of data as compare to 900 MHz band products because they were really costly and provide comparatively lower data rates with respect to WLAN products. In addition these 900 MHz band products also make some interference with other type of proprietary radio frequency technology.
IEEE group started work on IEEE 802.11 project in year 1990, in order to design a Medium Access Control (MAC) and Physical layer (PHY) which provides benefits to wireless connectivity to fixed stations, portable stations and moving station within the specific boundary of the network. In 1997, the IEEE approved the first international standard for WLAN which is interoperable between different vendors product. Wireless LAN has several benefit, some of them are described below [27].

2.1.1 Cost Stability

In contrast with the wired LAN WLANs are considered to be cheapest network, because whenever network administrator wants a device to connect, he needs cable to make a connection.

On the other hand if you have wireless network then you can connect as many devices as you can with the help of APs.

2.1.2 Easy to install

Hence it is proved that wireless APs/ Router are very easy in deployment or installing a networks. If somebody has the little knowledge then he can easily install the wireless devices at home or in SOHO (small office home office) without the need of some professionals, but on wired network some technicians are required whenever to install the network and also for RJ-45 connections and the cables that is installed in the ceil and floor.

2.1.3 Mobility

It becomes very simple with the help of WLANs to use real time information when interacting with customer. Hence it is proved that with the growth of the WLANs, someone can easily access the internet no matter where the user is. Consider the example of coffee shop and big malls that are usually provides the internet facility without any cost to their customers. The chances of errors in data interpretation are likely to be reduced with the help of WLAN. Besides, WLAN has proved to be quite effective in the launching of mobile applications. The students can also share the benefit of WLAN as it enables them to stay connected all the time with their lectures.

2.1.4 Short-Term Usage

WLAN is useful for short-term use and professionals like auditors can stay connected as long as they have to get their work done. This provides a significant working flexibility, facilitates, configuration to maintain an Adhoc working groups. Being so flexible WLAN provides a competitive advantage to the users.

2.1.5 Difficult Wiring Environment

Sometimes it is hard to install a wired network like in old buildings, similarly it is hard to install LAN at outdoor locations with respect to WLAN, like in parks and sporty arenas. Although there are some situations where WLAN is better to be installed as in the situations of disasters where its recovery is easy through WLAN. WLANs in the battlefield are quite obvious. On the other hand in some situations it is difficult rather impractical to install the wired network as in busy streets, from one building to another. Above are some of situations where the use of WLAN is more effective where there is no need of cabling like building to building connection of portable devices.

2.1.6 Scalability

To meet up the requirements of a particular applications and installations WLAN system can be configured in a variety of topologies and Configuration can easily be altered in the infrastructure mode where many portable users can accommodate in a single environment without the need of wired network and the network can easily be expanded by adding more APs in the network [25].

2.2 How WLAN works

Wireless Local Area Networks always use to broadcast information signal from one end to another without the need of cables by utilizing of radio waves, infrared waves, and microwave transmission. So WLAN suggest method to make a Local Area Network with no cables.

Basically every WLAN is connected to wire network like internet. In WLANs the AP works like the Switch in wired networks. WLAN works on unlicensed bands of radio frequency (RF). WLAN usually apply Carrier Sense Multiple Access/ Collision Avoidance (CSMA/CA) instead of Carrier Sense of Multiple access/ Collision Detection (CSMA/CD). A Wireless LAN can be constructed by the combination of end nodes and access points. The purpose of using of an Access point is to transmit and receives the data signals of the nodes or between the nodes of another network. Following are the three basic technologies of WLANs [31].

- FHSS (Frequency Hopping Spread Spectrum)
- DSSS (Direct Sequence Spread Spectrum)
- IR (Infrared).

2.2.1 Frequency Hopping Spread Spectrum

The purpose of using the Frequency Hopping Spread Spectrum (FHSS) is to make some changes in the frequency sample of the data signal with the permission of transmitter and receiver. It is well synchronized, the goal of FHSS is to continue the communication on a single logical channel. For an unplanned receiver, FHSS works as a short- duration impulse noise [31].

2.2.2 Direct Sequence Spread Spectrum

The purpose of using the Direct Sequence Spread spectrum (DSSS) is to produce an extra redundant bit pattern for each and every bit that is to be transmitted. This type of bit pattern is also known as a chipping code or chip. If the chip is longer in size, it means chip has bigger chance in order to recover the actual information and for that additional bandwidth is needed. The main purpose of using the Statistical technique method is to recover the original information without requiring the retransmission, whenever one or more than one bit in the chip damaged during the period of transmission. For an unplanned receiver, DSSS appears as a low-power wideband noise which helps to avoid the most narrowband receivers [31].

2.2.3 Infrared Technology

To transmit data by using Infrared (IR) waves, the systems use extremely high set of frequencies, just less than detectable light in the electromagnetic field. In comparison with the light, Infrared waves are unable to clear the solid objects, rather then it works on directed (Line-of-sight) or disperses technology. Low-priced directed systems provide specific range of 3ft and are rarely used in permanent WLAN application. High performance directed IR waves are always used in the fixed sub networks and unreasonable for the mobile users. If the WLAN is using the disperse IR waves, then there is no need of line of sight, but in this techniques the area of cells are fixed in a specific room [31].

2.3 Types of WLAN

WLAN operates in two modes, which are given below.

- Ad Hoc Mode.
- Infrastructure Mode.

2.3.1 Ad Hoc Mode

Ad hoc mode is also known as peer to peer or IBSS (Independent Basic Service Set). It is a type of LAN in which the network is created only by the wireless devices without the need of any centralized controller or AP. In this architecture the wireless network is comparatively easy to create and each and every device can communicate with each other equipment in the network with help of NICs. This type of network is very useful for small organization where computers

are not interested to see the information of other computers. In ad hoc mode there is no need of Access Point because all of the workstation and computers are connected with a wireless NIC card which can communicate with one and other via Radio waves. The Ad hoc mode is suitable for rapidly setting up a wireless network in a hotel conference centre, meeting room or anyplace else where enough wired infrastructure mode do not exist.

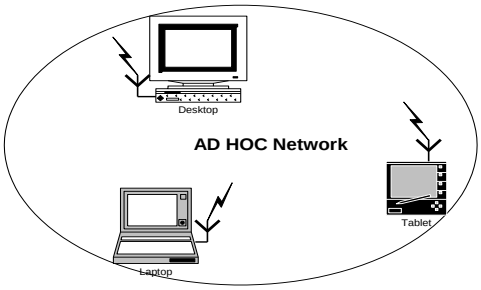


Figure 1 Adhoc Mode Architecture

2.3.2 Infrastructure mode

The purpose of using the infrastructure architecture in WLAN is to expand the wired network by using the wireless equipment i.e. base station also known as access point (AP). AP is perform as a bridge between wireless and wired network and also performs like a centralized controller in a wireless network for all wireless clients. The AP is responsible for manage the transmission and reception of several wireless equipments within a limited boundary of the network. Different vendor's product can support the different ranges and number of wireless equipment based on the wireless standard. Network administrator can use the several APs in the infrastructure mode in order to increase the size of the network. This project relates with the infrastructure mode, all the work done in this architecture [28].

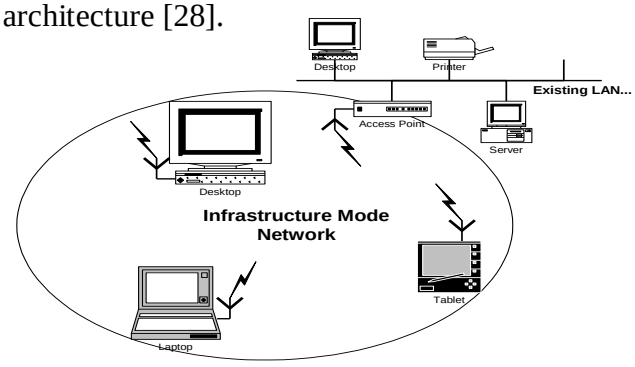


Figure 2 Infrastructure Mode Architecture

2.4 IEEE 802.11 Standards for WLAN

2.4.1 IEEE 802.11b

In 1997 the IEEE 802.11 standard planned and it was a signpost for WLANs. But after two years, the IEEE 802.11 standard was formally revised on 16th September 1999.The new standard called 802.11b, still working on the 2.4 GHz frequency band and offers speed of data at

a rate of 11 Mbps data, which is equivalent to a current wired network. The IEEE 802.11b is considered to be a new robust system and has a capacity to compensate the same 802.11 protocols. Furthermore, this modified version provides the interoperability between different vendor's product and compatibility with legacy 802.11 products. This guarantee not only boosted the manufacturing of 802.11b products but also motivated the competition between WLAN Vendors. Hence it is proved that IEEE 802.11b products successfully controls the WLAN Market, but the major problem occur that is the interference of the 802.11b products with the ISM band, specially not only with the Bluetooth devices but also with the medical devices and the household appliances (microwave ovens and Cordless phones) that all are using the 2.4 GHz band of frequency. For all of above said reasons IEEE 802.11 is introduced to overcome the problems of 802.11b [29].

2.4.2 IEEE 802.11a

In September 1999, the IEEE 802.11a standard was officially announced in which all the devices are operated at 5 GHz frequency band. This is completely defined by the band that 802.11 a and b are not compatible to each other in any case, because 802.11 a works on a new coding scheme that is Orthogonal frequency division multiplexing (OFDM) that offers a high data rates up to 6, 12, 24, 54 Mbps and sometimes beyond this speed in comparison to 802.11 b. It is proved that IEEE 802.11a supports high data rate at any level w.r.to 802.11 b. Two main obstructions occur during the process of IEEE 802.11a. First is the compatibility issue of the 802.11a products with 8011b products and the second is the 5 GHz band is not available free of cost for all the countries in the world. That's the reason that IEEE starts planning to introduce a new band known as IEEE 802.11 g. [29].

2.4.2 IEEE 802.11g

In November 2001, IEEE suggests the new standard 802.11g over 802.11a in order to improve the 2.4 GHz 80211b technology. IEEE 802.11g introduced the two different modulation techniques that support the different data rates. First modulation technique is known as Packet binary convolution code (PBCC), this modulation technique offers speed of data at a rate of 22 and 33Mbps for its pay load. Second modulation technique is known as orthogonal frequency division multiplexing (OFDM), this modulation technique offers speed of data at a rat of 54Mbps for its pay load. Compatibility issue also resolved in 802.11g products with 802.11b products. IEEE finalized the 802.11g standard on 13 june 2003 [29].

2.4.3 IEEE 802.11n

The main purpose of initiating the 802.11n is to increase the range and the speed of data for the WLANs at a speed of 300Mbps. IEEE 802.11n perform work on two different WLAN bands one is 2.4 GHz ISM band and other is 5 GHz UNII band and has the characteristic of backward compatibility with 802.11b, 802.11a and 802.11g. by using the 802.11n standard the throughput of the products are improved as compare to the previous standard products with the help of large bandwidth channels and multiple antennas are connected with the devices to get the better reception of the RF signals. By using the 802.11n products Network administrator can simply increase the range of WLAN that is almost double [27].

2.4.4 IEEE 802.11i

IEEE 802.11i is introduces in order to solve the weakness that is available in WEP and TKIP security solutions, so for that reasons IEEE suggest a new individual standard that offers an improved level of security in the WLAN products i.e. access points (APs)and wireless network interface cards (NICs) and also supports the backward compatibility with previous standards. The main target is to improve the security in the MAC layer. This standard is finalized in july 2004. The particular task group (TGi) is responsible of designing and updating the IEEE 802.11i, the group tried its best in order to complete all the necessary security goals like authentication, confidentiality and integrity. This section is further described in the chapter 4 [30].

2.5 Summary of IEEE 802.11 WLAN Standards

All the standards are best summarized in the below table with main functions [29 & 30].

IEEE Standard	Explanation	Main Function And Other comments	Availability
802.11	Uses 2.4 GHz (ISM) RF band. Maximum data rate is 2Mbps.	Legacy technology that is used minimally.	
802.11a	It works up to 5 GHz (UNII) radio frequency band. 8 available radio channels and sometimes 12 channels, in few countries. Maximum data rate is 54 Mbps. Uses OFDM, usual range is 50-100m.	It provides a higher performance. The big advantage is fast maximum speed; it means that no signal interference as it operates in licensed frequency.	In 1999, this standard was completed and products are available now.
802.11b	2.4 GHz (ISM) RF band. Maximum data rate is 11 Mbps. Uses DSSS/CCK, typical range is 50-100m.	Performance enhancements. The main advantage is minimum cost; good range of signals that are not easy to obstruct.	Completed in 1999. Since 2001, big range of products is available.
802.11g	2.4GHz (ISM) Radio frequency band. Maximum data rate is 54 Mbps. Uses OFDM/PBCC.	Higher performance with IEEE 802.11b Backward compatibility. Provides speeds similar to IEEE 802.11a.	Completed in 2003 and now products are available.
802.11n	Future business standard that will extensively recover network throughput. 2.4 GHz (ISM) and 5 GHz (UNII) RF band. Maximum data rate is 300Mbps. Uses (MIMO) technology.	Increased data throughput. Backward compatible with IEEE 802.11a/b/g. Greatest maximum speed and most excellent signal range; additional resistant to signal interference.	Completed in Oct 2009.
802.11i	Design for wireless networks security mechanisms. It is based on the AES (Advanced Encryption Standard) and can encrypt communication that run on 802.11a, 802.11b and 802.11g technologies.	Improved security	Completed in 2004 and now products are available.

Table 2 Summary of IEEE 802.11 WLAN Standards

3 Attacks on WLAN

This chapter attempts to describe the prospective of security issues faced during the transfer of data between the WLAN users. The current study is provided to identify the impact of security problems in WLAN. Currently WLAN faces several security threats and attacks due to its nature because the information is broadcast into the air through which one can break the security of WLANs having little understandings about the network.

3.1 Different kind of Attacks on WLAN

Different types of attacks and threats are categorized in to two main parts. These type of attacks are considered to be general in context for every WLANs and will described further in detail with their drawbacks and solutions.

1. Logical Attack
2. Physical Attack

3.2 Logical Attacks with their mitigation techniques

A logical attack always relates with the software, system and the sensitive data flowing in the network. In this type of attack the target of the intruder is to find the code and software or any drawback in the network which will help the intruder to access the network and altered the sensitive data easily. The main target of this attack is to find the sensitive data flowing in the network. If the attacker is successful, then this attack will produce lot of problems for the network as well as for all the networks that is in connection with. Some logical attacks are defined below with their mitigation techniques.

- Spoofing of MAC address.
- Denial of Service Attack.
- Man in the Middle Attack
- Default Access Point Configuration.
- Reconnaissance Attacks.
- Conversation Sniffing.
- Dynamic Host Configuration Protocol Attack.

3.2.1 Spoofing of MAC Address

MAC addresses are sent over the medium when communication has to start between the node and the AP. When any node tries to establish a connection with AP (access point) it must be authenticated through its MAC address of Wireless NICs to make the connection more secure. In the normal process of authentication the MAC addresses are forwarded in the clear text form and any attacker can pick the address of any authenticated user while using different tools like kismet. It will create a data base of legal wireless nodes and also their MAC addresses. The intruder can simply spoof the MAC address of any node and use that MAC address to gain access to WLAN. This stealing of nodes with MAC addresses that are authenticated via AP is also possible. It can create a main security violation. To eliminate this condition the network engineer must be notified of any stolen user or lost node to remove the MAC addresses of those from the list which are allowed to access the AP in the WLAN [19, 20].

3.2.2 Denial of Service (DoS) and Distributed Denial of Service (DDoS)

The availability of a network is significant for crucial services. In the WLAN network, the transfer of a data must be guaranteed with a high success rate while providing prompt first-response services. DoS and DDoS are used to lose the availability of different services of a network.

DoS attacks are considered to be a most common type of security attacks, very complex in nature and difficult to mitigate fully, but it can be controlled up to some extent. The target of the DoS attacks is to restrict the legal client from accessing the network. DoS attack makes the services ineffective for the legal client. DoS attacks can be implemented by using Flood attack, SYN attack and Ping of death attack.

Distributed DoS is considered to be a common category of DoS. The target of the Distributed DoS is to attack on the Server by sending lot of irrelevant request to the network Server and network Server becomes slow after sometime and unable t provide the services to the legal user.

The most important way to protect from DoS and DDoS attack is to locate the source of the attack and then block that traffic from that source. There are three common mitigation techniques for DoS and DDoS.

- Anti-spoof feature.
- Anti-DoS feature.
- Traffic rate limiting.

The DDoS attacks are a series of DoS attacks which are more harmful than DoS in the network. WLAN allows these intruders to begin easily inside WLAN network. Therefore, WLAN network has to face many challenges and has to discover different kinds of tools to protect it from these attacks. This type of attacks can be blocked through authentication, authorization, and accounting server (AAA) [21, 23].

3.2.3 Man-in-the-Middle Attack

A man in the middle attack is used to get the secret information or to modify the data packets, therefore violating the reliability of a session. This is a form of active eavesdropping, in which the attacker makes independent connections with the different users. These users are sending and receiving data to each other, making them believe that they are connected each other over a private connection but in fact the entire transmission is controlled by the attacker. The main target of this type of attack is to read and alter the data whenever intruder wants during the communication session without knowing the hosts. This type of attack is also known as session hijacking attack. There are different issues created by man-in-the-middle attack in WLAN.

- To capture the information
- To introduce new information into network sessions
- To compromise confidentiality, integrity and availability
- To corrupt the transmitted data
- The rogue proxy issue can lead both the source user and end user to be deceived when they transfer data.
- It can collect enormously secret information, e.g. pin numbers of credit cards, password of OS (operating system), and also other types of personal information.

This type of attack can be reduced through the use cryptographic encryption and authentication known as secure socket layer (SSL) [21].

3.2.4 Default Access Point Configuration

All new bought APs are not configured with security. Sometime it is better for ordinary users because if they are configured with security then difficult for new users to operate. Now a day the ambition of manufacturers is to deliver data on high data rate and also provide some kind of security for the device. The network engineers must configure the AP according to the security required for the company because few companies require more security like banks. In new APs there is no security configured which is not good for any company whose data is very crucial.

SSID is a security check which is assigned to WLAN and it is announced by AP. For security purpose SSID is important and it works like initial security check in any WLAN. Sometime in many APs the SSID is disabled by default the users can access the AP without any authentication of SSID. In many cases AP don't disable SSID request, the SSID is active but the actual name of SSID is broadcasted in the air that makes the network vulnerable. In a secure network SSID must be enabled and SSID name must not be broadcasted in the network so that users first have to prove the knowledge of SSID and then can join the AP. The other problem is through DHCP server every user will get IP address automatically and can run any application. So it is responsibility of the network engineer to disable DHCP which is on and put this DHCP value under security so that only authentic users can access the network.

If the AP is in the reach of the attacker, then simply attacker can reset the AP and AP will come in its default settings and attacker can get the benefit from that default settings. So it is the duty of network security administrator to change the default configurations of the AP in order to enhance the security of the APs [20].

3.2.5 Reconnaissance Attacks

This attack is used to gather information and provide base for DoS attacks. In the start, Reconnaissance attacks try to get the information of live addresses, ping sweep is used. From this the intruder gets information about the active ports on the live addresses. While using this information, the attacker sends the query to operating system and applications running on the desired node. The reconnaissance attack consists on the following four processes.

- Ping Sweep.
- Port Scan.
- Packet Sniffer.
- Internet Information Queries.

The ping sweep is a network scanning method which determines the range of IP addresses assigned to live computers. The ping sweep is a collection of echo requests that are sent to multiple nodes. If any address which is in the list is live, then it will respond back. This method is old and slow to scan a network. Many requests are sent to an array of addresses to discover which computers can be captured for vulnerabilities.

The purpose of port scanning is to break into the system to get access which services are running in the network. Every service is associated with a distinct port number. It can also be an automated scan of TCP or UDP ports on a computer to obtain listening services. Port scanning is a preferred method to attack on a network that provides the weak points of a network. In port scanning the message is sent to all the ports but one port at a time. If any port reply, it means it is an active port and can be used a weak spot.

The packet sniffer is a software application that uses a network card in the special mode known as promiscuous to get network packets which are sent across the network. The packet sniffer always works in the same field area as the network being attacked. The promiscuous mode is a

type of mode in which network adapter card sends all data and voice packets to a software application for processing. The data which is in plaintext form is not encrypted, although few network applications distribute packets in plaintext. When the packets are not in the encrypted form, these can be processed and can be understood by any application.
Asking some question to the internet for collecting some useful information regarding the website or any organization is known as IIQ and DNS query is considered as one kind of IIQ. To get information, DNS queries are used, such as which addresses are assigned to which domain and also who owns this domain. The DNS queries helps ping sweeps to find live computers in a particular area. After creating such a list, the port scanning tools can be deployed to know all the services which are running on the computers that the ping sweep discovered. The intruders always take the notice of the properties of all the applications that are running on the computers. To eliminate reconnaissance attack, IPS & IDS are used [22].

3.2.6 Conversation Sniffing

Conversation sniffing is a process of catching and understanding network information that is flowing in the medium. In the networked environment all the information is passing from the NICs across a communication medium and centralized device is responsible for broadcasting the information to the clients. Whenever attacker wants to perform the conversation sniffing, attacker simply re-configure the NIC in a promiscuous mode, means in the same mode from where the centralized device broadcast the data in the network. Attackers can make use of conversation sniffing with the help of sniffers freely available on the internet to steal the secret data and to eavesdrop on the network data like collecting user login credentials, IP address of the client, Mac address of the NICs, emails and everything that is moving in the medium [24].
The confidentiality is an important factor in the transmission of data and voice. WLAN traffic can be sniffed if signalling and media traffic are not properly secured. Confidentiality and integrity are two key points in WLAN. The confidentiality means to ensure the privacy of information which is exchanged amongst all users. The integrity refers that the information which is exchanged is not tampered during the transmission. There are many techniques exists that can be used to guarantee the integrity and confidentiality of WLAN network. IPSec can be used, either in transport or tunnel mode for an authentication [21].

3.2.7 Dynamic Host Configuration Protocol Attack

Many requests are sent to DHCP server through DHCP attack. This attack forces the server to issue address against each request. The aim of this attack is to spoof DHCP replies. After getting the addresses from DHCP server the intruders have more points to attack DHCP server and then DHCP server will not be able to respond against the user requests. This type of attack is like DoS and man in the middle is created. To avoid from this type of attack it is recommended to use static IP addressing in WLAN network [22].

3.3 Physical Attack with their mitigation techniques

A Physical attack always relates with the hardware and the design of the network. In this type of attack the target of the intruder is to interrupt or decrease the network performance rather than searching for a sensitive data and then make some changes with the data. This type of attack can produce fewer problems for any organization for the hardware rather than the secret information is stolen. It should be noted that this type attack will always makes the way clear for the logical attack. Some Physical attacks are defined below with their mitigation techniques.

- Rogue Access Points.
- Physical placement of Access Points.
- Access Points Coverage.
- Spam Attack.
-

3.3.1 Rogue Access Points

The main purpose of this type of attack is to get access of others people's resources. Once attacker is successful to get access of resources then attacker can easily add any service applications to make the data rate successfully. In order to get rid off from this type of attack, the network administrators use a simple technique known as lock down mechanism. By installing this application the network administrator will get the logs whenever attacker tries to add some application. The transfer of data will rejected when any users gains illegal access of network. The attacker is automatically blocked when more than three attempts are made [22].

3.3.2 Physical placement of APs

The installation place for the AP is an important factor, if keeping AP improperly it will expose to its physical attacks. The AP can be easily being shut down by attackers and after this action whole configuration will be lost and again AP will come into default configuration which is completely insecure. As a result it is important for network security engineer to carefully select the location to place the APs [20].

3.3.3 AP's area coverage

The major difference between wired LAN and WLAN is that WLAN depend on the RF signals. The signals are propagated from AP to outside the building where the AP is placed permitting the users which are not physically in the building to access the network. To find a WLAN the attackers use different tools and even can communicate while driving. In RF there is no boundary fixed for the signal to travel. The attackers which are outside can launch attacks on the WLAN. This type of attack is known as war driving. Hobbyists also chalk buildings to show that signals are broadcasted from the AP and the WLAN in it can easily be accessed. Sometime the access of public WLAN is preferred which is called hot spots. When hot spot is implemented it is the origin of many security issues. It is significant to know that if breaking the security of hot spot then it is easy to break the security of wired LAN which is connected to that hot spot [19].

3.3.4 Spam Attack

Spam messages create problems in WLAN, like spam emails which consumes bandwidth. If spam exists in the WLAN network, delay is increased at the time of authentication of users and also data transmission. The purpose of spam is to flood messages over the whole network like traditional emails. The spam attack consumes bandwidth, which is not scalable for the WLAN network. To eliminate spam messages, it is recommended to use anti-spam software [22].

4 Security in WLAN

This chapter describes the different security solutions for IEEE 802.11 standard like WEP, WPA, WPA2 using 802.1X and RADIUS Server with their architecture, drawback and explanation of different attacks on these security solutions in detail and how they overcome each other and which one is considered to be best in which environment.

4.1 WEP

WEP is a first security technique that is used in IEEE 802.11 standards. The main purpose of using the WEP is to provide the security to WLAN like the wired LAN. WEP helps to make the communication secure and provide the secret authentication scheme between AP and the end user which is going to access the WLAN. Basically WEP implemented on initial Wifi networks so that the user can not access the network without the correct key. WEP uses symmetric key encryption that ranges from 64 to 128 bit long encryption key. Usually, the same encrypted key is used for all the nodes in the network and manually forwarded to each node means WEP is unable to provide the key management function [32&33]. WEP is using the shared key authentication method in which the user needs two things in order to access the WLAN, one is SSID and second is WEP key generated by the AP. The IEEE 802.11 standard defines the three different parameters for the WEP i.e. access control, data privacy and data integrity [32].

4.1.1 WEP Architecture

The IEEE 802.11 standard uses the RC4 encryption algorithm for WEP in order to provide the privacy to Wifi Network because it is easy to implement in software as well as hardware and very cheap in comparison with other encryption algorithm. RC4 is considered to be an initial and reasonable encryption algorithm, but now a day it is not in action [33]. The basic and standard way to make the integrity safe is to add the some message authentication code to each part of data before transmitting it towards the wireless medium. The WEP uses the 32 bit cyclic redundancy code (CRC-32) as an integrity algorithm that is generated at the transmitting side. It is generated for each frame of data that is to be transmitted by performing some polynomials calculation, and after that checksum is added with each data frame. At the recipient side similar polynomial calculations are performed on the data frames, if the checksum calculated at the both side is same, than it assumes that data is safe otherwise it is assumed as altered data. CRC-32 is considered to be a fundamental approach and very easy to implement [33]. WEP used to encrypt the information at transmitting side and decrypt the data at receiving side.

(a) Encryption of information at sender side.

There are four steps helps to define how WEP Works in order to encrypt the information before transmitting into the communication medium that is air.

(1) The secret PSK that is 40 bit long is hashed with Initialization Vector that is 24 bit long.
(2) A PRNG is generated from the result of mixed IV and pre shared key to form a new sequential key.
(3) The plaintext and the ICV are hashed in the mixer, when a copy of plain text is transferred to integrity Algorithm the ICV is created.
(4) The sequential key and the result of hashed plaintext and ICV is transferred to RC4 algorithm, where RC4 algorithm performs the XOR operation to give the encrypted result.

In the end encrypted message can be obtained by first adding the IV in front of Cipher text. Hence the encrypted message is ready to send across the air. The whole process is clearly shown in the figure below [34].

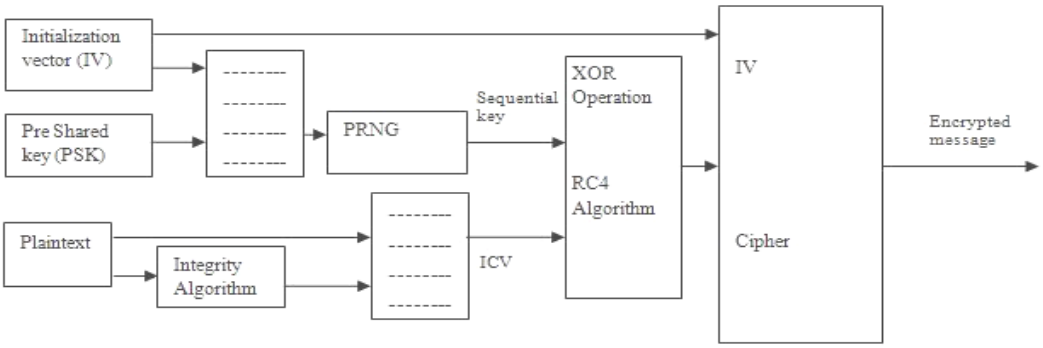


Figure 3 Encryption process of information at sender side by using WEP technique.

(b) Decryption of information at receiving side.

There are five steps helps to define how WEP works in order to decrypt the information or separate the IV and Cipher text from each other at the receiving side.

(1) The pre shared key that is 40 bit long is hashed with IV that is 24 bit long and available in the encrypted information to generate a PRNG to form a sequential key.
(2) The cipher text that available in encrypted message and the Sequential key that is already generated are transferred into RC4 algorithm, which performs the XOR operation on both of them to form a plain text.
(3) The ICV is separated from the Plain text.
(4) Plain text is transferred to integrity algorithm to form a new ICV.
(5) The new ICV is compared with the original ICV, if the both ICV matched then the data becomes safe otherwise it is altered.

Hence the message is successfully decrypted and the original message is available at the recipient side. The whole process is clearly defined in the figure 2 below [34].

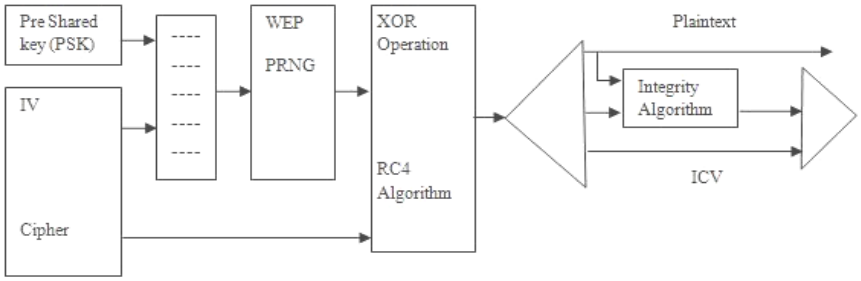


Figure 4 Decryption of process at the recipient side by using the WEP technique

4.1.2 Flaws in WEP

WEP is considered to be a weak security technique for WLAN now a day. Below are some major reasons due to WEP is unable to provide the security to WLAN, hence each component of WEP is very weak.

- It uses the RC4 stream cipher algorithm for authentication and privacy point of view. The problem is not available with the RC4 algorithm even though it's a good encryption algorithm but unfortunately it was not applied correctly for the WEP technique. At every stage of RC4 it is clearly defined not to use the same key material for more than one time, it is not specify that whatever the payload is. RC4 simply performs the XOR operation for the data.

- It uses the 24 bit long Initialization Vector (IV) that is clearly added with the packet that is ready to transmitted across the air. There are two solutions available in order to get rid from this drawback i.e. the use of longer IVs and some secure mixing algorithm in place of CRC-32 for integrity.
- Another problem with the RC4 algorithm is that its adding the IV with the WEP pre shared key. If there is lot of traffic available in the wireless networks, there is chance for many packets to drop in between the communication that will require resending. So in WEP for every resend of packet the IV is changed, which only has 2^{24} key spaces.
- Well adding the IV with the WEP key is the major drawback in the design. If WEP is using 40 bit long key then it will need more protection from attacks as compared to 128 bit long WEP key. Hence, both are very weak and unable to provide the security to Wifi Networks.
- It uses weak authentication algorithm.
- It uses weak data encapsulation method.
- Size of IV is very small that is 24 bit long.
- The use of improper integrity algorithm i.e. CRC-32.
- Unable to prevent from replay protection.
- Lack of mutual authentication and key management.

From the previous studies and the current research it is proved that the WEP is failed to provide security to WLANs [32&33].

4.1.3 Attacks on WEP

WEP is a kind of security protocol that is based on encryption algorithm called "RC4". Its purpose is to provide security to WLAN similar to the security which is provided in the wired LAN. There are few drawbacks in WEP like small RC4 encryption key and also utilization of small IV. Another drawback is to use XOR procedure for cipher key with plain text to create cipher text. Both MAC address and the IV are sent in the simple clear text form. Secret keys are shared between nodes which are the major security concerns. Data which is encrypted through WEP can easily accessible to attacker through different tools e.g AirSnort and WEPCrack [50].

There are so many problems with the WEP security solutions, it also affected by the poor key management in the network, in result the keys stored in the device remained unchanged during the whole session of the communication. During this period if some of hardware is stolen or lost, the intruder can make use of that stored keys in the lost hardware and not only affect that hardware but also the hardware that is sharing the same keys. In order to mitigate this problem the Dynamic key management solution will help a lot, by doing this WEP keys will not go into the wrong hands and this process will also increase the complexity of the network [54].

WEP is suffering from vulnerabilities since it is developed and faced lot of attacks in early age but all attack seems very impractical, so for that reasons vendors decided not to invest on new security solution and planed to provide the mitigation solution for those problems at that time, but due to the passage of time attacks developed gradually and proves to be more serious to the WEP. This section describes some attacks on WEP and how vendors provide solution[50].

1. Brute force attack.
2. Attack against key stream re-uses.
3. Weak IV attacks.
4. Modern attacks.

1 Brute force Attack

The bruit force attack considered to be most foolish attack which tries all possible keys manually in order to find the accurate key. A single modern machine will help to find the key within the time period of less than a month by a continuous search, particularly when the work is divided (to find a key is not impossible through bruit force attack on 40 bit WEP key). Some of the tools have the ability to change the human readable pass-phrase into WEP keys [50&51]. New tools have an option to change the pass-phrase into hexadecimal keys with the help of ASCII codes of the alphanumeric characters. This type of non standard methods minimized the lot of difficulties for the bruit force attack. Possibly, a standardized algorithm would help to get rid from the easy bruit force attack by mixing the pass-phrase into a WEP key. Different vendors introduced 104 bit WEP key which is considered to be more impressive for bruit force attacks [50].

2 Attack against key stream re-uses

Security to Algorithms is totally independent from its key, defined by the Cryptanalysis on WEP entropy [52]. In initial time it seems useless to extend the size of key in order to get better WEPs security. If an attacker successfully recovers the key stream, then surely he will decrypt the data which is connected to that key stream. The most sensible mechanism is discovered which is based on shared key authentication to be enabled, the main purpose of this mechanism is to restrict the unauthorized access into the network. In this process, first authenticator sends a clear text challenge to the supplicant also known as authentication peer. The supplicant is authenticated and replies with the encrypted message of the challenge. If the attacker successfully snoop this communication, then simply he can do XOR of the cipher text and plain text pair in order to get the key stream.

This attack is recognized by the IEEE 802.11 standard and they discourage the clients not to repeat the same IVs in the communication process. After this attack authentication schemes are discourage and SSID cloaking and MAC address filter mechanisms are introduced. Hence association request and MAC address mechanisms are both have drawback but contains little importance over authentication scheme [50].

3 Weak IV attacks

The current studies proved that the key can be re-calculated by the attacker [53]. This type of attack requires collecting approximately 1,000,000, in which some of packets used weak IVs [32&33]. In fact these properties are already defined in the RC4 algorithm four years before introducing the WEP [54]. Simply unskilled attacker can give and take information with a network, by collecting the huge number of weak IVs, one can easily calculate the accurate key. Only one single weak IV will help to find out the correct key byte 5% of the time. Hence it is proved that weak IVs are considered to be important threat to WEP Solution. In spite of that, this attack can be mitigated only in particular situations after collecting a larger number of weak IVs, which could take several days to found the accurate WEP key [50].

4 Modern Attacks

The above attacks faced two major hitches in past. First is how to reduce the time in order to calculate the accurate key in Weak IV attack and second is how to achieve the key stream reliably in the attacks against key stream re uses. Both problems are solved now. For the first problem it is proved from the current studies that one can easily recover the one byte of key stream after catching the maximum 256 packets [50,55&56]. For the second problem it is also proved, to reduce the time period in weak IV attack, if any packet obtains a answer is replayed, after that traffic is automatically produce on the network and the attacker will not wait for the data to capture manually, attacker can actively root the data traffic which is using the weak IV.

At this stage, it is proved that WEP is completely failed to provide the security. An attacker can break the security of the network within minutes by using these vulnerabilities [50].

4.1.4 WEP SUMMARY

Originally IEEE 802.11 faces some serious problem that is of wireless vulnerabilities. The IEEE 802.11 standards properly recognize that wireless communications are susceptible to eavesdropping, message alteration and different type of attacks in comparison with the wired LANs. On the other hand the motive of using WEP is to provide the security and authentication like wired LANs, which is an undefined goal. Large numbers of problems are available with the WEP. When the FMS breaks WEP [60] security for the first time, it was a big shock for Wi-Fi network. Hence, the selection of encryption and integrity algorithms are not suitable for WEP technique and as well as communication of packets in 802.11 networks. If we are comparing the 64 bit WEP encryption to 128 bit WEP encryption, the 128 is better because it produce a big WEP encryption key as compared to 64 bit but both are weak. There are many dull weaknesses available in WEP that provides the insufficient security to the networks that handles the very sensitive data. Hence all the components of WEP technique are very weak and unable to provide the security to Wifi networks [32&36].

4.2 WPA

Wifi Alliance (WFA) provides a new technique in year 2002 for wireless security that is WPA in order to solve the problems that is available in initial security solution WEP. WPA has several advantages over WEP that are depicted below.

- Overcome with a strong, interoperable and replacement of security flaws of WEP.
- Improved data encryption, because WEP has very weak data encryption method.
- Strong user authentication, which is also not available in WEP.
- There are many of attack relates to static key, so WPA minimize shared secret key in accordance with the frame transmission.
- WPA uses a secured and complex encryption hashing function for the ICV algorithm that works in a passion that it shared the secret key between user and AP.
- Use the RC4 algorithm in a proper way and provide fast transfer of the data before someone can decrypt the data.
- WPA avoids the repetitions by using of larger IVs.

WPA is an intelligent security solution then the WEP and work in a passion that it transfers the WEP key by using the TKIP encryption mechanism as fast as possible before somebody decrypts the key. When this technique is correctly configured then the automatically data confidentiality is available to all the authorized users that are connected to the wifi network. On the other hand all the components used in WPA are considered to be subset of 802.11i extension and all the components of WPA is backward compatible with 802.11i devices. Two modes of the WPA are.

- Enterprise/commercial WPA
- Personal/WPA-PSK (pre shared key) WPA

In enterprise WPA the centralized component is used that is known as RADIUS server, which is the responsible for authentication, authorization and accountability of users with AP.

In Personal WPA network there is no any concepts of RADIUS, it works on pre shred key in which the users need two things in order to access the network that is the SSID of the network and the WPA key generated by the access point [33&49].

4.2.1 Temporal Key Integrity Protocol

A new data encryption and integrity methods are developed by the 802.11i i.e. TKIP and CCMP because the WEP has many flaws. TKIP has the two basic goals first to get rid from the problems that are available with WEP and secondly it also performs as legacy hardware this is because of why almost all the encryption algorithm of the WEP is implemented on hardware point of view. So from that point it is observed that TKIP will be connected with basic structure of WEP, by knowing the Initialization Vector, RC4 encryption and integrity check vector and some stronger encryption schemes are also included in TKIP so that the huge number of old Network interface card (NICs) and Access points (APs) that are used in the network will not be absolute. Basically the TKIP is cipher suite and known as a secure encryption algorithm in comparison with the WEP encryption algorithm, it combines the mixing algorithm a packet counter and performs functioning in a way so that it can provide the protection to the cryptographic keys. The TKIP is using the Michael as integrity algorithm also known as Message integrity check (MIC) algorithm. The TKIP will work together with the MIC and packet counter in order to prevent the packet replay and alteration of message in between the medium. The TKIP and Michael will work together in any type of network without requiring the changes in the hardware components. TKIP provide the best solution and suggest to use the different base WEP key for the every packet in order to solve the Problem available in the WEP encryption i.e. the reuse of RC4 key more than one time and usage of some weak RC4 keys. Mainly TKIP consists of three basic protocols.

- A cryptographic message integrity algorithm i.e. Michael or also known as MIC.
- A key mixing algorithm
- Extension of initialization vector according to size

TKIP cryptographic algorithm is avoiding the problem that is available in WEP i.e. to generate the separate key for each packet rather than only one key for all packets in WEP technique. The hashing algorithm is avoiding the alteration of packets in the medium. TKIP also solve the drawback available in IVs by increasing the size of IV which will help in order to solve the problems by using a longer packet counter and avoid the replay protection. The purpose of using the packet counter is tried not to use the weak RC4 keys. By doing all this TKIP is able to solve the problems available in WEP at some extent [35].

4.2.2 WPA Architecture

The new security technique created after WEP that is WPA, the main goal of WPA is to provide the more complex encryption method and authentication by using the TKIP with the help of MIC. The purpose of MIC is to prevent from the attacks of bit flipping also known as the alteration of message that can be easily performed in the WEP hashing technique.

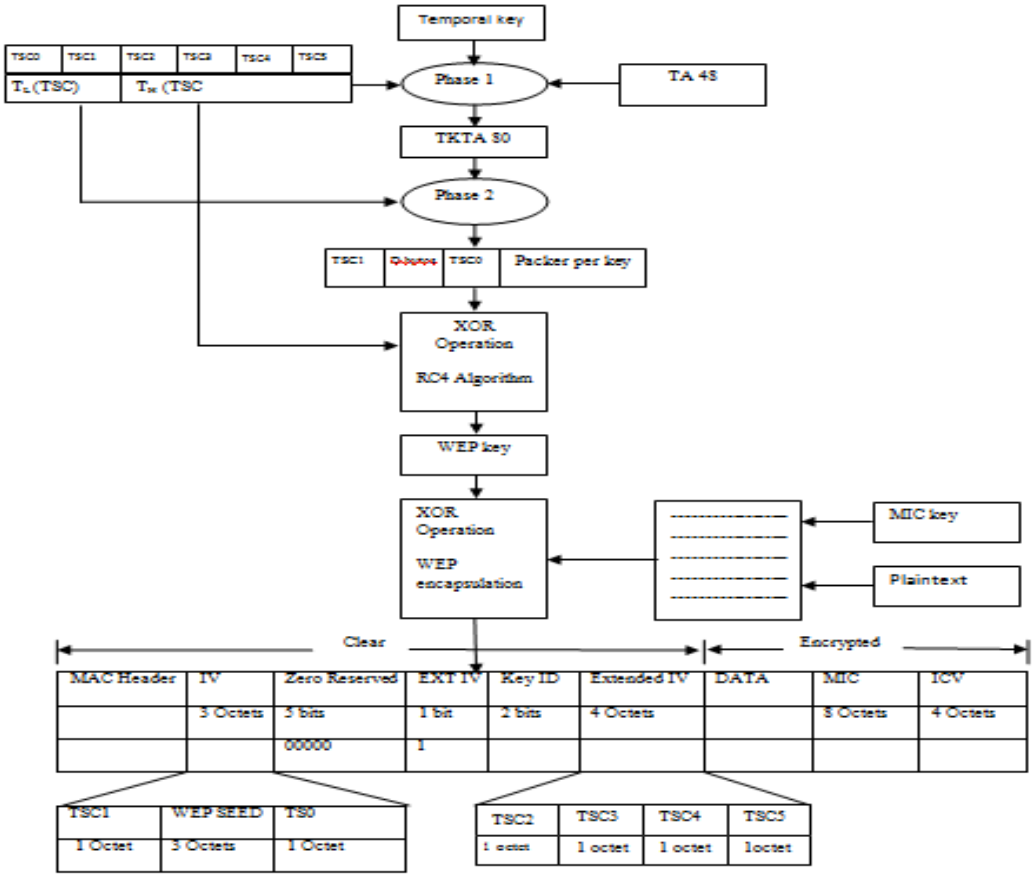


Figure 5 Encryption process of WPA using TKIP and MIC

There are five basic steps helps to define that how WPA is working in order to encrypt the data by using the TKIP encryption algorithm with the help of MIC integrity method.

1. Three things are to be combined in the first phase to generate the TKTA at the transmitter side of TKIP i.e. IV, temporal key and Mac address of the NIC. To get rid from the replay attacks, first TKIP transmitter uses TSC that is 48 bit long and also serves as an IV, TSC is combination of two fields i.e. T_H and T_L , indicates that TSC0 and TSC1 belongs to T_L and TSC2, TSC3, TSC4 and TSC5 belongs to T_H. Second, TKIP also uses temporal key that is 128 bit long and is distributed between the AP and the user. Third, TKIP uses the translator address of the network interface card that is 48 bit long.
2. The generated temporal key for translator address (TKTA) that is 80 bit long and T_L are transferred to phase2 in order to generate a separate packet key for each packet that is 128 bit long. The purpose if using the T_L here is to avoid from the selection of weak keys.
3. XOR operation is performed on Packet per key and full TSC by RC4 algorithm to generate the WEP key.
4. Message integrity check (MIC) code that is 64 bit long is combined with the plaintext. TKIP introduce the new cryptographic message integrity code (MIC). The TKIP transmitter always

uses to add this MIC before the ICV. The transmitter and receiver only know this MIC keyed, at the receiving side the receiver check the MIC after decrypting the data.

5. In WEP encapsulation process the XOR operation is performed on WEP key generated earlier and the combined result of the MIC and Plaintext to generate the encrypted message. The whole process of encryption and the TKIP packet format is shown in the figure above [36]

4.2.3 Flaws in WPA

WPA provides the drawback with the use of Pre-shared Keys (PSKs) that is considered to be a substitute authentication device for small business and home client that do not need to use the individual authentication server and entire 802.1 x key architecture. Anybody is having little understanding of the PSK can conclude some PTK in the ESS during passive sniffing of the wireless network, by eavesdrop for all those necessary key that exchange data frames.

WPA tools are using handshake process for interchanging the data encryption keys for the wireless session between the access point and the end user, attacker who do not know the PSK can make a guess that is known as dictionary attack or bruit force attack. If a small passphrase or weak passphrase is used, by using the offline dictionary attack one can easily make a guess of the PSK having dictionary of 2giga byte or more than this. Given that the ordinary practice will be an only one PSK for the ESS, once this is identify by the intruder then the intruder is considered to be a member of an ESS and the whole ESS is accessed by the intruder.

PSK is supplied in the standard to make simpler deployments in small and less hazard networks. The hazard of using the PSK against internal attacks is comparatively as worst as WEP and hazard of using the passphrase based PSKs against external attacks is greater than WEP [48].

4.2.4 Attack on WPA

It is necessary for every attacker to first capture the data traffic of the network until and unless attacker founds the encrypted ARP request [57] or response. In some cases these types of packets can easily be recognized by the attacker depends upon the length of characteristic. On the other hand WEP and TKIP are unable to protect the source and destination addresses and always sent these addresses to broadcast address of the network. In this case the hacker knows overall of the plaintext excluding the last eight bits of source and destination IP address, 64 bits of the MIC code known as MICHAEL and 32 bits of ICV. The last portion of the plaintext is the combination of MIC and ICV that is 12 bytes long [60]. Now hacker introduce an enhanced version of CHOPCHOP attack [58-60] in order to decrypt the unidentified plaintext that is moving in the communication medium. Basically WPA suggests two solutions to prevent the network from CHOPCHOP Attack.

- Firstly, if the end user received the packet having invalid ICV, network assumes that mistake as a transmission error and in result that packet is rejected. Secondly, if the MIC code is incorrect then network think it as an attack, no matter ICV value is correct and the AP is informed by exchanging MIC failure report frame from the client side. The communication is automatically shutdown if the network received more than two MIC failure reports within the time period of 60 seconds. After a fine of 60 seconds again keys are re settled and communication start begins.
- If a packet is successfully received at the end user side, a Temporal sequence counter (TSC) is checked if the TSC number is lower than the current counter received (the received packet is assumes as out of order and simply it is rejected).

In spite of all that CHOPCHOP attack is still achievable. Simply attacker tries to focus on special QoS channels [30] on which the packet is originally received. Frequently network consists of many channels having no or low data is flowing where the TSC number is still lower than the current counter. Two possibilities are there, if the attacker fails to guess the last byte during the CHOPCHOP attack, that packets is discarded. If the attacker successfully guesses the last byte, simply end users send a MIC failure report frame, but in this case TSC number is not updated. For safety precautions attacker will have to wait for at least 60 seconds otherwise end user will start work on countermeasures and block the communication. Within the time period of maximum 12 minutes the attacker can recognize the last 12 bytes of plaintext that contains MIC code and ICV. For the rest of bytes like exact source and destination addresses attacker can simply make a guess for that addresses based on decrypted ICV. Once the MIC code and plaintext is identified, the next step for the attacker to find the MIC key that is used to protect the packets at the sending side (Access point to end user) by simply reversing the MICHAEL algorithm [29, 30]. After finding the MIC and key stream at the sending side to client, attacker is in position to send the packets towards the end user on those QoS channels where the TSC number is lower than the counter of the captured data. When the attack is completely implemented, attacker can simply identified the further key stream within the time period of 6-7 minutes because attacker have to only know the 4 byte ICV using CHOCHOP. The other information like source and destination IP address are easily guess and the MIC key can be easily identified. In order to mitigate this type of attack vendors suggest using very short rekeying let suppose 130 seconds or more less. The practical suggestion to get rid off from this attack is to simply replace the TKIP with the CCMP (AES) [60].

4.2.5 WPA Summary

In IEEE 802.11 standard introduced Wi-Fi Protected access (WPA) in year 2002 to overcome all the vulnerabilities available in the less secure 40 or 104 bit WEP encryption technique. WPA also comes up with a solution of the user authentication that is not available in WEP. Basically WPA is an intermediate step between WEP and IEEE 802.11i specification and considered as a subset of IEEE 802.11i. WPA provides a secure and future version of IEEE 802.11 components.

WPA is considered to be a substitute of WEP in terms of new and strong encryption algorithm known as temporal key integrity Protocol (TKIP) with the help of Message integrity Check (MIC). WPA also supports the new facility that is the mutual authentication between the end user and the access point (AP) by using with one of three technologies i.e. IEEE 802.1X, Extensible Authentication Protocol (EAP) authentication or Pre-shared key (PSK) technology.

Initially the purpose of introducing the WPA is to implement the network immediately with WPA technique, more easily and inexpensive by changing less amount of hardware and software in the networks without reducing the performance of the network. The current and future research shows that WPA is able to provide the high level of assurance to personal and Enterprise networks, data between these networks must be protected from unauthorized access and only legal users can access the networks easily The major drawback of WPA is of the dictionary and bruit force attacks [37].

4.3 WPA2

IEEE 802.11i is an additional standard that is finalized in fall of 2004 in order to improve the authentication and encryption. WPA2 introduced a new concept of RSN by using a large number of IEEE 802.11 MAC layer protocols which helps to provide further key management and authentication to the networks. The IEEE 802.11i improved the three basic areas in order to provide the security to IEEE 802.11b for which WEP is unable to provide the security.

- Authentication
- Key management
- Data transfer

The architecture of WPA 2 is totally different from the WPA and WEP, because of WPA 2 uses a single component for key management and message integrity that is CCMP based on advanced encryption security (AES). There are two purposes of CCMP

- The Counter mode is used for providing data protection from unauthorized access.
- The CBC-MAC is used to provide the message integrity to the network.

802.1X and EAP are considered to be authentication schemes for the network in IEEE 802.11i standard; these are the improved security features of WPA 2 which are using the dynamic key distribution and new encryption scheme as compared to WEP and WPA. In WPA 2 the RADIUS is known as AAA protocol that performs as a user authentication in EAP transport mechanism. The main purpose of using the EAP and RADIUS for the new packet security methods of key distribution, this facility is not available in WEP algorithm.

In WPA 2 the novel key is generated for all encrypted data packets that are ready to send over the air, with its own encryption key, by using this technique the complexity of decoding the packet in the network is increases and it's very difficult for decrypting the key for an unauthorized user. These new techniques are more scalable and secure specially for the larger networks but very much complex as compared to current wireless security mechanisms. WPA 2 provides some benefits over the WEP and WPA techniques [36].

- Providing more excellent security by using advanced encryption security (AES)
- Using stronger key management
- Protecting against the man-in-the-middle attacks by using two way authentication process.
- Providing improved message integrity performance by using CBC-MAC.

4.3.1 Counter Mode- Cipher Block Chaining MAC Protocol

The CCMP is an encryption algorithm of IEEE 802.11i. CCMP performs in a particular mode of operation that is AES. In other words the mode of operation is known as the algorithm, whose purpose is to change the cipher text to plaintext and vice versa. The main purpose of using the encryption technique is to provide the confidentiality to data and hence it is proved that previous encryption technique is failed to provide the data integrity. In order to provide the integrity to data, a new message authentication code is appended with the original message. The message authentication code is useful for keyed cryptographic function in order to generate the integrity value (ICV).

In IEEE 802.11i standard is divided the CCMP in to two parts.

- *Counter mode ''CTR-Mode'.* The counter mode is used in AES to encrypt the data.
- *Cipher block chaining- MAC mode ''CBC-MAC Mode''.* CBC-MAC mode is used to create a MIC code that provides integrity to data.

Same Temporal key is used by both modes that are 128 bit or 16 byte long that is generated during the 802.1x authentication for encryption and MIC calculation. CCMP uses the newly obtained temporal key for every session. It also uses the specific nonce value for separate frame and provides protection by using the temporal key so because of this reason CCMP contains 48 bit long Packet number (PN). The security guarantees failed when the same temporal key is try to reuse the Packet number (PN) [38&39]

4.3.2 WPA2 architecture

The payload of the plaintext message protocol data unit (MPDU) is encrypted by the CCMP and also performs the operation of encapsulation on the cipher text. The encryption process of CCMP in 802.11i is further described in the following points [38&39].

- For each MPDU a new PN is required, which can be obtained by incrementing the previous PN, because same temporal key uses the different PN, means PN may not be used more than one time with the same temporal key. For each MPDU the PN is incremented.
- AAD for CCM is constructed from the fields that are available in MPDU header, the fields that are available in AAD is also provided integrity by the CCM algorithm.
- CCMP nonce is constructed from three things that are packet number (PN), Priority field of the MPDU and A2 is considered as an address of MPDU. The zero is set to be the reserved value for the priority field.
- The CCMP header is constructed by the combination of key identifier and the new packet number; the length of the CCMP header is 64 bit long.
- The cipher text and the MIC are generated by the combination of the temporal key, AAD, nonce and MPDU data. This step of combination is also known as CCM originator processing.
- The encrypted data and MIC are concatenated with the original CCMP header and MPDU header that are already constructed to form an encrypted MPDU.

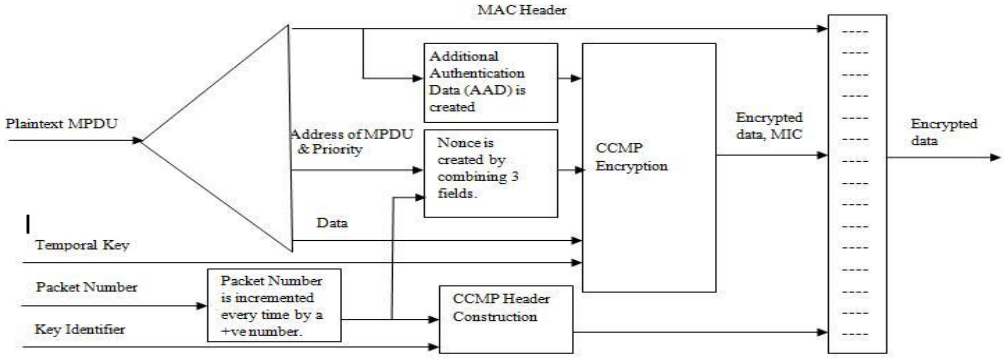


Figure 6 Encryption process of data by using CCMP in 802.11i

The de capsulation process of plaintext MPDU and decryption of cipher text MPDU by using CCMP in 802.11i is described below [38&39].

- AAD and nonce value is reconstructed from the encrypted MPDU.
- The AAD is reconstructed from the MPDU header of the encrypted MPDU.
- The nonce value is reconstructed from three things, A2 that is known as address of MPDU, Packet number (PN) and the priority field of the MPDU.

- Using the CCM integrity checking the MIC is obtained from PN, plaintext and temporal key.
- The MPDU plain text can be formed by combining the AAD, nonce, temporal key, MIC, and MPDU cipher text at the CCM decryption side, I n this process the integrity of the plaintext and AAD is also checked.
- The decrypted MPDU plaintext and the original MAC header of MPDU are combined to generate a plaintext MPDU.
- MPDUs are prevented from the replay by comparing the PN in the MPDU is higher than the actual counter that is already assigned before the decryption process.

The whole process of de capsulation of plaintext and decryption of cipher text is described below in the figure.

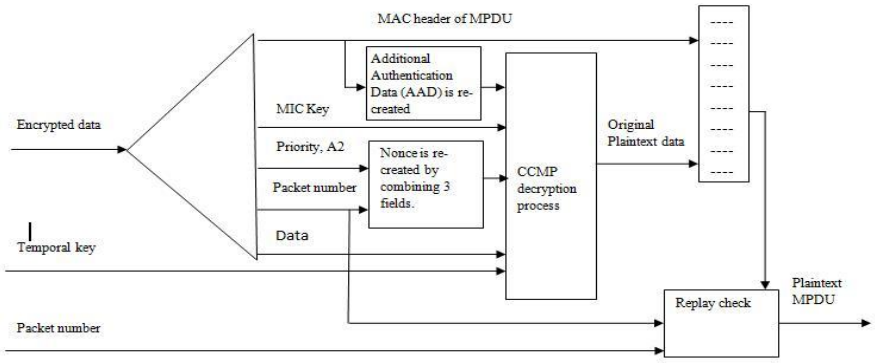


Figure 7 Decryption process of data by using CCMP in 802.11i

4.3.3 Flaws in WPA2

WPA2 has limited drawbacks available in comparison to initial security solution WEP and substitute security solution WPA [36].

- WPA 2 technique is very much costly for the already deployed networks due to the new encryption CCMP and AES needs to change the overall hardware for the network.
- Sometimes the network is vulnerable to security risks because WPA 2 is completely trust on secrecy session keys.
- WPA 2 requires more hardware due to the two way authentication between user and AP
- More difficult and complicated to understand as compared to current networks.
- Personal version of WPA 2 faces lot of threats like MAC Spoofing, adhoc connection, missconfiguration and rogues.

4.3.4 Attack on WPA2

This attack is only possible if the initial counter value [40] of AES CCMP is significantly knowable otherwise this attack has no any importance. The current studies prove that if the attacker has sufficient knowledge then he can easily guess the initial counter value that is used in AES CCMP of 802.11 WLANs and Nonce [40] value can easily be re calculated, Nonce is the combination of three things priority field, Address of the MAC (Header) and Packet number field. The intruder only wants to know about the initial counter value and the payload size [40]. The payload size can easily be identified from the priority information [40]. Current studies proved that wireless communication is sensitive in nature, if intruder has compatible devices then he can easily sniff the MPDUs. It is clear from the figure 6 that the CCMP header and MAC

header is transmitted with plaintext and their location is already fixed in the MPDUs. If intruder want to verify the already calculated Nonce value then he can, by extracting A2 and priority from MAC header and PN field from the CCMP header [40]. In order to find the counter block value, it is necessary to find the size of the payload and the size of the IEEE 802.11MPDUs are already defined that is 2312 Bytes containing 2296 bytes for data and 8 bytes for MIC code and 8 bytes for CCMP header. Once intruder finds the size of payload then he can easily compute the Initial counter value (128 bit long) by simply combining the Flags field, Nonce field and size of payload size [40]. This initial counter value is providing base for the time memory/trade-off attack.

The TMTO pre-computation attacks are only used to find the comprehensive key search and always work on cipher data. This type of attack is only possible if the attacker have a huge database in order to attack on any secret keys. In between the attack stage the attacker can make use of that huge database and have a capability to attack on lot of different secret keys at a time. The benefit of this type of attack is that during the attack there is no need of the plaintext. This attack is famous where there is unreliability in the plaintext during the attack and network is using multiple secret keys [40]. The large number of data available in the network plays an important role in a success of TMTO attack and attacker plan about how to attack is also an important. The initial counter and the counter mode encryption are continuously incremented in the identical session. It is noted that the size of the MPDU in CCMP is 2296 bytes and there is no any upper limit is fixed for the MPDUs in a session. Hence this amount of data is feasible in order to attack on any network by using TMTO attack. It is clearly defined in [62] that counter mode faces threat from the TMTO pre-computation attack until and unless it is guessed by the attacker. If the initial counter and update counter both are in reach of attacker then TMTO attack is achievable. TMTO attack uses a formula 2n/3 which will help to calculate the effective key size of the network where n is a size of cipher key that is 128 bit long in AES counter mode [32&38]. Hence TMTO effective key size can be given as 2 x 128/ 3 = approx: 85 bits. In order to mitigate the TMTO pre-computation attack there are three basic suggestions to follow [40&63].

- The size of the key should be greater than the 128 bits.
- Used at least 64 bits in initial counter that are unidentified by the attacker and included as a part of AES counter mode key.
- OR make use of some identifiable but identically allocate the component in the initial counter.

4.3.4 WPA2 Summary

The WPA 2 is not introduced to overcome the problems of WPA. Indeed the WPA has several same characteristics as compared to WPA2. The main difference between WPA and WPA2 is of Advanced Encryption Standard (AES) using the CCMP algorithm for the complex encryption of data, while WPA uses temporal key integrity Algorithm (TKIP) for encryption. The AES offers sufficient security to meet the requirements of the Federal information processing standard (FIPS). The only one drawback of using AES which require new or additional equipments for the current deployed WLANs and must require specific chip for controlling encryption and decryption.

For a long time the security is considered to be a major task in order to provide the privacy to each WLANs. The WPA 2 supports two types like WPA, enterprise and home also known as personal version. The personal version works on a Pre shared key for authentication and the

enterprise mode works with the help of 802.1x and RADIUS server. WPA2 devices are backward compatible with the devices that supports WPA, previous WPA devices can be upgrade to WPA2 only if the support AES. It is clear from the current studies that WPA 2 personal version is unable to protect the full security and faces many threats from misconfiguration, rogues, adhoc connections, MAC spoofing and DOS attacks. Hence WPA 2 is finalize version of IEEE 802.11i and considered to be a complex and secure way for the wireless networks from security point of view especially for the enterprise network [47].

4.4 IEEE 802.1X using RADIUS Server

A wireless network provides a major security challenge during the last decade. This section describe the basics of how IEEE 802.1x is using the RADIUS Server and how both are providing the security to the WiFi networks. First presents the overview of IEEE 802.1x, RADIUS Server and combined functionality of both. IEEE 802.1X is initially created to provide the access control to the wired LAN. Previously in 802.1X, if the user successfully connected to the live network port, user can get the entrance to the network and it is designed to provide the control access to the network. A lot of companies are spending time and money in AAA technology to manage their client's network access, so 802.1 x forces to install the AAA servers, a RADIUS server to supply these utilities to fresh 802.1x users [46].

4.4.1 IEEE 802.1X architecture

The main purpose of using the IEEE 802.1X standard is to provide the port based network access control by using well suited A&A methods and the data transmission for the components that are connected with each other through different 802.11 LAN. By enabling the public key authentication and encryption among the AP and end user, the IEEE 802.11 is able to provide the distributed secret keys for the network. The concept of the port in 802.1X is shared among the AP and end user. The 802.1X considered being a future stage of IEEE WLAN requirements and protocols which will help to improve the security and management in 802.11b. The problem with the 802.1x protocol is that, it avoids the single authentication procedure over a new process. So that's the reason that RADIUS is suggested to use with 802.1x in order to provide the authentication process over each other in WLANs based [10-12]. The 802.1X authentication system works on three major components in the network they are supplicant, authenticator and authentication server [41&42].

The authentication method in 802.1x uses PAE that control protocols and algorithms between supplicant and authenticator as shown in the figure below. In the authentication process the authorized or unauthorized condition of the ports are controlled by the authenticator PAE. The authenticator PAE utilize the uncontrolled port to make a communication with the supplicant PAE prior to supplicant is authenticated. The 802.1x authenticator will deny all kind of information except 802.1x messages until and unless the supplicant is authenticated. The EAP messages are encapsulated between the supplicant and authenticator by EAPOL is defined by the 802.1x. The authenticator PAE is intermediate device and responsible to transfer the encapsulated EAP messages between the supplicant and authentication server. Before transmitting the encapsulated EAP messages to the RADIUS server the authenticator PAE converts that encapsulated PAE messages into the RADIUS packet format and then transferred that RADIUS packet to authentication server, that conversion process is known as RADIUS encapsulation. Once the supplicant is authenticated by the authentication server, the controlled

port is activated at the authenticator side and supplicant can access the network services easily through controlled port [42].

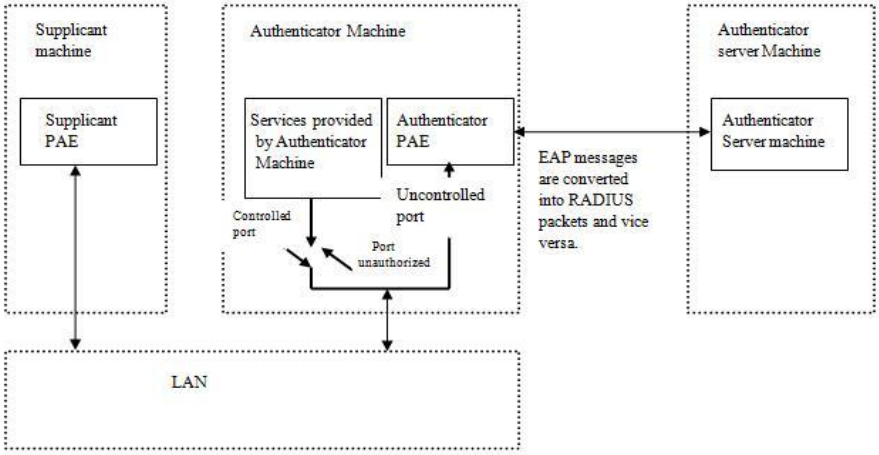


Figure 8 IEEE 802.1x Structure

4.4.2 RADIUS Server architecture

The Remote Authentication Dial-In User Service (RADIUS) is the most commonly used AAA server, it is proposed by the IETF, developed by the Lucent Remote Access and best suitable for providing the security between the client and Server. RADIUS Server is responsible for saving all the information of the user profile to a central site. RADIUS is used to authenticate the user and operate in a way so that RADIUS client is known supplicant makes a communication with the RADIUS server known as authentication server through the authenticator (AP). The authentication server i.e. RADIUS SERVER reply to the RADIUS client i.e. supplicant through the authenticator (AP) that what the authenticated user is authorized to do. In other words RADIUS is also known as network protocol so that the communication can occur easily among the client and server. Consider the big and heavy network in which the information is dispersed at every host of the network so security is major problem for that network. Hence RADIUS provides a security to such type of network and collects all the information and saved at a centralized location in order to reduce the risk regarding the security and no need to configure the switch ports, which is time consuming and effort. The working functionality of RADIUS is divided into three main sections that are authentication, authorization and accountability [44].

RADIUS Authentication & Authorization.

There are six steps which are best described in below figure in order to provide the authentication and authorization services to client by the RADIUS Server [44].

- Whenever client wants to connect to the network through the intermediate device network access server (NAS) ask the end user for the username. NAS also performs like gateway.
- The end user supplies the correct username to NAS.
- Intermediate device NAS ask the end user for the password.
- End user supplies the valid password.
- Once all the data is provided to the NAS i.e. user name and password, NAS transferred that piece of information to authentication server that is RADIUS Server with the help of access request data gram which will add all the data in attribute value known as AV pairs. This is the piece of information that is encrypted by the RADIUS.

- AV pair is matched with the information available in the data base of RADIUS, if the information is correct than Access is accepted and data gram message is forwarded to client appending additional information in AV like IP address etc. the authentication server will reject the access and the NAS end its connection with the end user if the information is mismatched.

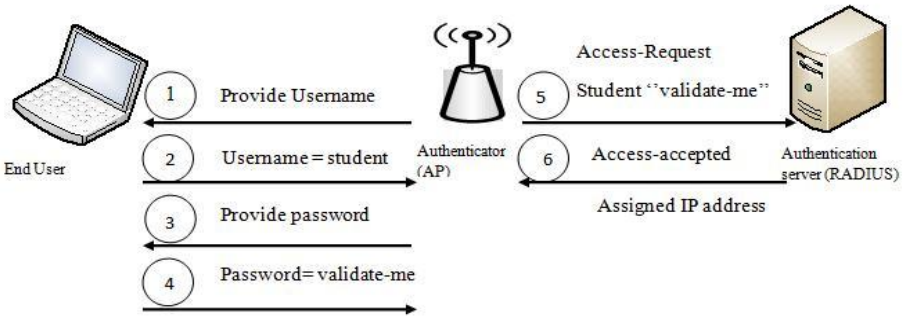


Figure 9 RADIUS Authentication and Authorization

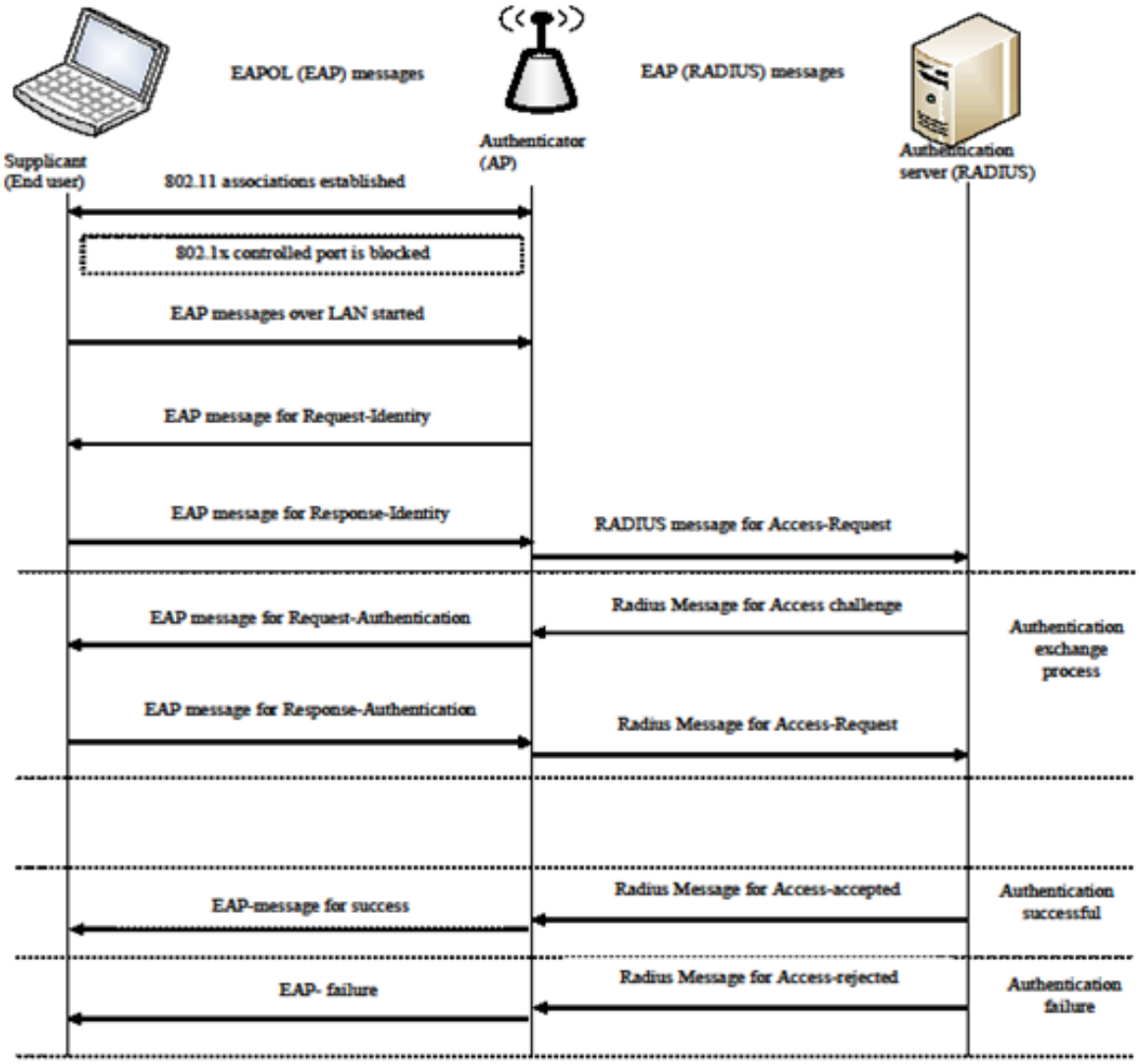
4.4.3 802.1X WORK TOGETHER WITH RADIUS SERVER

Figure below describes the working functionality of 802.1x with the RADIUS by using the supplicant PAE and authenticator PAE [41&42].

- The 802.11 Association process occurs between the supplicant and authenticator through their PAE state machine.
- Before the authentication starts the port is blocked and unauthorized only the 802.1x messages can be shared.
- The supplicant transferred the EAPOL towards the authenticator the authentication process will start by sending this message. After receiving the EAPOL message by the authenticator from the supplicant, the authenticator sends the special message that is EAP-Request/identity and asks for the secret information in order to make a connection to the network.
- When the end user receives the EAP-Request/identity message it will change it states and replied authenticator with a new message EAP-Response/identity message that contains secret information about the end user. After receiving EAP-Response/identity message from the supplicant successfully, the authenticator will change it state to authenticating state, in which the authenticator PAE encapsulate that message into RADIUS access request and transferred to authentication server that is known as EAP message attribute.
- The RADIUS server sends the RADIUS-access challenge towards the AP, AP will convert that message into EAP-Request authentication and transferred to supplicant.
- After receiving the EAP-Request/ authentication message the supplicant will change its state to authenticating state and replies the authenticator by EAP-response/authentication message to authenticator. After that authenticator will encapsulate that message into RADIUS access-request and transferred to RADIUS server.
- Now RADIUS server will take action against all information available, whether the supplicant is permitted or rejected. If the information provided is correct, the RADIUS server sends RADIUS access accepts to the authenticator. Authenticator converts that message into EAP success message and informs the authentication. The controlled port is now activated after authentication process is completed.

- If the information provided by the supplicant is incorrect, then the RADIUS server sends a special message to the end user through authenticator for rejection that is RADIUS-Access-Rejected.

Figure 10 IEEE 802.1x message exchange using RADIUS Server.



4.4.4 Summary

When IEEE 802.1X and RADIUS Server is configured for any network then the Network administrator can easily guard the network from the illegal clients in order to access the network, both these techniques help to reduce in the security break including DoS attacks within their network architecture. Even though by configuring the IEEE802.1X and RADIUS Server combined will increase the security for the wireless network. It is necessary for the administrator to plan and implement both these technologies based on their prerequisite [45].

5 WLAN Test and Experiments

Previous chapter 3 describe the attacks on WLAN security in this chapter we implement some of them in lab environment. This chapter shows the attacks on WEP, WPA/WPA2 and finally shows the best security technique using 802.1X. First lab WEP shows that how attacker can attack on WLAN network and gain access to the network after getting the encryption key. 2nd lab shows the attack on WPA/WPA2 pre-shared key using the dictionary attack. 3rd lab shows the best way to secure the wireless network using the 802.1x authentication.

5.1 Attacking on WEP

Objective

This lab shows that how network is vulnerable if it uses the WEP key. WEP uses the 24-bit or 48-bit long vector key called IV. This experiment shows the attack on IVs and once enough IVs collected then decrypt collected IVs and generate the WEP key.

Scenario

To crack the WEP key large collections of IVs are required. This lab shows that how attacker can crack the WEP key using the Backtrack 3 by applying the series of commands. In initial step run the command airmon-ng to check the connectivity of connected devices. After establishing the connection to the AP run the command airodump-ng to grab the packets and collect the IVs. For the slow network use the tool airplay-ng to inject the additional packets to connected AP. Once 20,000 to 40,000 packets of data collected apply the cracking tool i.e., aircrack-ng tool to crack the WEP key.

5.1.1 Hardware Requirement

Device	Description
Linksys WAP54G	Wireless access point
D-Link DWL-G650	External wireless card
Laptop Sony Vaio VGN-fs990	Acting as a host

Table 3 Hardware used to connect WEP network

5.1.2 Software Requirement

Software	Description
Cisco aironet desktop utility	Client configuration and management
Backtrack 3	Cracking WEP tool
Cisco aironet 1300 utility	To configure 1300 AP/Bridge

Table 4 Software used to configure WEP network

5.1.3 Assumptions for WEP

Before applying following steps it's assumed that:

- Wireless card should be compatible with the Backtrack (See appendix A for compatible list)
- User should be close enough to AP to transmit the packets remember that wireless card adapter strength is less as compare AP.
- Aircrack-ng version should be v0.9.1 or above

5.1.4 Steps involve in cracking of WEP

STEP 1 wireless card detection
As described above, wireless card should be in monitor mode to capture the network traffic without any association with an access point. To do this in backtrack environment open terminal window and login as root then type iwconfig to search all access points interfaces and their status.
Bt~# Airmon-ng it will return the compatible wireless card here in this case its D-link rausb0 card for cracking the wep security.

Figure 11 Detection of wireless card.

Following given are some additional commands which may be uses during the cracking process e.g., view available networks, start or stop network interface card.

Command	Description
Ifconfig	View available networks interfaces
ifconfig rausb0 down	Stop the specified network card
ifconfig rausb0 hw ether 00:55:44:33:22:11	Change the MAC address of NIC
iwconfig rausb0 mode monitor	Set network card in monitor mode
ifconfig rausb0 up	Start network card

Table 5 additional command list

Step 2 Network scanning
Once wireless card set into the monitor mode next step is to finding available wireless networks and choose the target network under Backtrack command prompt type
Bt~# Airodump-ng rausb0
Above command watch all channels and shows the available access points and connected clients within the range. It is good to choose the target access point with strong signal (PWR column).

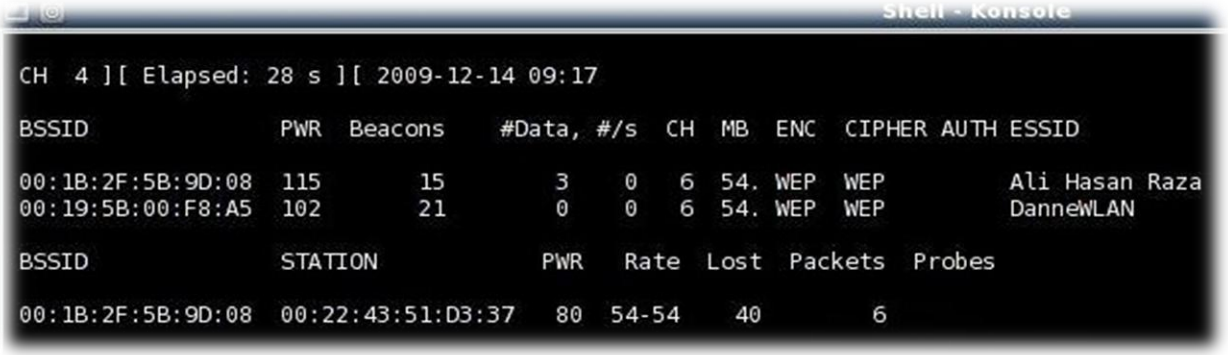


Figure 12 Detection of wireless network

Step 3 Data capturing
To store data in file airodump-ng command is uses with some more parameters to target a specific AP and channel. In this whole process wireless card should be restrict to single channel to speed up data collection, in this scenario wireless card is rausb0 and capturing packets on channel 6 into text file called data. Type the following command on Backtrack command prompt
Bt~# Airodump-ng –C 6 bssid 00:1B:2F:5B:9D:08 –W data rausb0

Parameter	description
-c 6	Represent number of channel is 6
bssid	Represent the MAC address of target AP
-W	shows that captured packets store into a file
rausb0	wireless network adapter
data	Stored file name

Table 6 Airodump-ng command parameters and descriptions

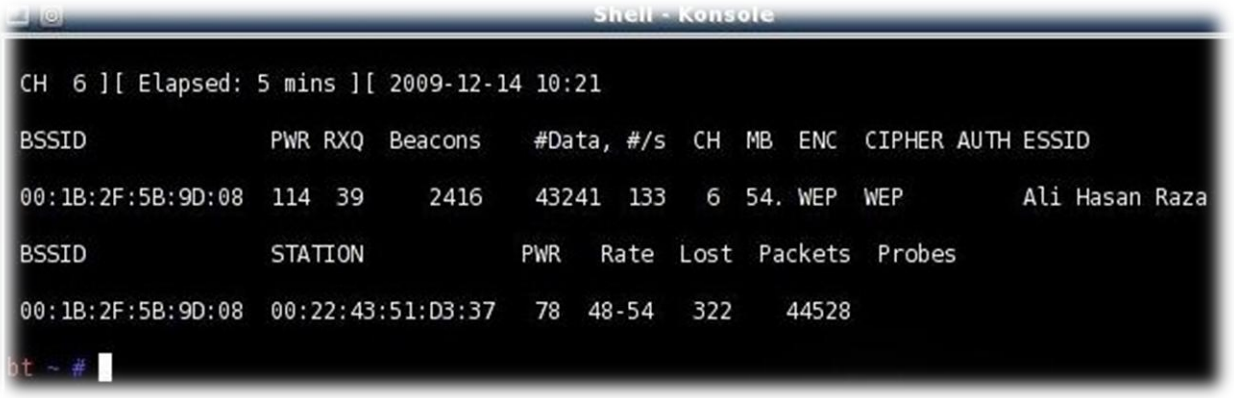


Figure 13 Packet capturing.

Normally data packets between 20,000 and 40,000 need to successfully recover the WEP key. In a network where traffic streaming is fast it can be break in minutes but in slow network it may take hours to penetrate in the network.

Step 4 Increase traffic (optional step)
If the network traffic is slow then this additional step can be use, in this step additional data injected to increase traffic on the wireless network. The aireplay-ng command should be run in the separate window to inject the packets in the network. Type the following command on Backtrack command prompt.
Bt~# aireplay-ng -3 -b 00:1B:2F:5B:9D:08 -h 00:14:A5:2F:A7:DE -x 50 rausb0

Parameter	Description
-3	specifies the type of attack, in our case ARP-request replay
-b	MAC address of access point
-h	MAC address of associated client from airodump
-x 50	limit to sending 50 packets per second
rausb0	wireless network interface card

Table 7 aireplay-ng command and parameter description

STEP 5 WEP cracking

WEP cracking process involves collection of enough data, extraction of key and connection to the network. Aircrack-ng re-attempt cracking the key every 5000 packets.

To recover the WEP key, in new separate window type

Bt~# Aircrack-ng data*.cap

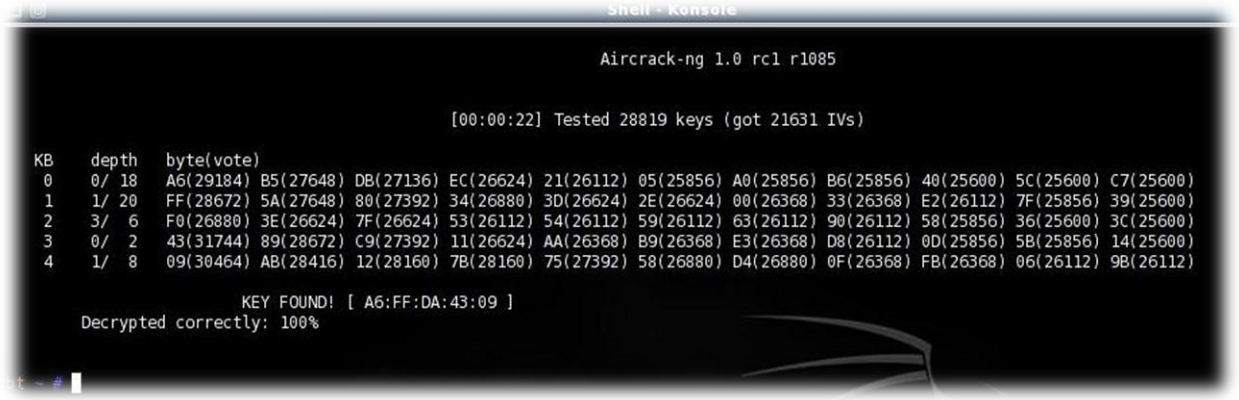


Figure 14 Crack WEP key using aircrack-ng

Here in this scenario captured file called “data” and it’s located in the same directory. Aircrack-ng cracked the key successfully, retrieved key is in hexadecimal and can be use to connect to network.

5.1.5 Summary

As demonstrated above, WEP cracking has become increasingly easier over the years, in past it may required hundreds, thousands packets or days of capturing data to crack the WEP but now a days it can be accomplished within few minutes approximately 20k data packets. WEP attack can be minimize or harder by using longer IVs size like 48 bit long IVs rather than 24-bit long IVs.

5.2 Attacking on WPA and WPA 2

Objective

The purpose of this experiment is to capturing the handshake of WPA/WPA2 and after successful handshake it performs the aircrack-ng to crack the pre-shared key. This type of attack can be done by active attack or passive attack. In active attack de-authentication perform manually to get the handshake with AP. This experiment shows the active way to attack on the network.

Scenario

In WPA/WPA2 attacker usually perform dictionary attack using the captured data and handshake between the AP and an associated client which may or may not work. The Main drawback of

WPA/WPA2 pre-shared key is that it comes with passphrase and it can be 8-63 character long and any weak passphrase may be vulnerable to dictionary attacks. To perform the successful attack on the WPA/WPA2 put the wireless card in monitor mode and connect to the specific channel of the AP then apply the aireplay-ng command that uses for de-authentication of client and provide the handshake once handshake done, apply the airodump-ng command which collect the authenticated handshake data. Finally run the aircrack-ng command to perform the dictionary attack on given data.

5.2.1 Assumptions for WPA/WPA2

Before applying following steps it's assumed that:

- Wireless card should be compatible with the Backtrack (See appendix A for compatible list)
- User should be close enough to AP to transmit the packets remember that wireless card adapter strength is less as compare AP.
- Aircrack-ng version should be v0.9.1 or above

5.2.2 Hardware Requirement

Device	Description
Linksys WAP54G	Wireless access point
D-Link DWL-G650	External wireless card
Laptop Sony Vaio VGN-fs990	Acting as a host

Table 8 Hardware used to connect WPA/WPA2 network

5.2.3 Software Requirement

Software	Description
Cisco aironet desktop utility	Client configuration and management
Backtrack 3	Cracking WEP tool
Cisco aironet 1300 utility	To configure 1300 AP/Bridge

Table 9 Software used to configure WPA/WPA2 network

5.2.4 Steps involve in cracking of WPA/WPA2

Step 1 Card detection and network scanning

First step that requires to attack on WPA/WPA2 is capturing initial handshake. WPA/WPA2 hashes the network key with the help of AP's SSID.

- Repeat the above WEP step 1-3 for wireless card detection and network scanning using airomon-ng and airodump-ng commands on Backtrack 3 command-line prompt.

Step 2 Active attack

In some cases it may require to de-authenticate the connected client and again connect to AP to get a handshake. Type the following command on Backtrack command prompt

aireplay-ng deauth 3 -a MAC_AP -c MAC_Client

BT~# aireplay-ng deauth 3 –a 00:1b:2f:5b:9d:08 -c 00:22:43:51:D3:37

Parameter	description
Deauth 3	De-authentication AP
MAC_AP	MAC address of the access point
MAC_Client	MAC address of an associated client
-c	Channel
-a	Authenticate Access point

Table 10 aireplay-ng command and parameters description

Figure 15 WPA handshake

Above mention is the hard part to do once four-way handshake achieved remaining part only requires a large/relevant dictionary file with common passphrases. See related links in Appendix B.

Step 3 WPA/WPA2 Cracking
This step involves cracking the WPA/WPA2 pre-shred key using the dictionary and aircrack-ng suite on command prompt of Backtrack 3 type the following commands to crack the key
Bt~#aircrack-ng data.cap
After running above command it will show the message that it requires the dictionary file to crack the key
Aircrack-ng of Backtrack it self contained the "password.lst" file but that file is very small and have low probability to crack the key but for high probability it requires the large file to crack see Appendix B for large file source. Now run the final command to crack the key
Bt~# aircrack-ng –w password.lst data.cap

Parameter	Description
-w	shows that captured packets store into a file
Password.lst	Dictionary file
Data.cap	Captured data file

Table 11 aircrack-ng command and parameter description

Above command only works if the both files i.e., dictionary and captured data file are in the same directory.

Figure 16 Aircrack-ng crack WPA/WPA

After entering command aircrack-ng start attempting to find the key it all depend upon the processing of the CPU and the size of the dictionary file.

5.2.5 Summary

Above section shows that using the WPA/WPA2 pre-shared key is not fully secure. Although this attack does not work 100% but if end user uses the common world phrase it can be easily break. Encryption of WPA/WPA2-PSK is more secure and strong if it uses the long phrases. On the other hand weak passphrases are vulnerable to dictionary attacks.

5.3 Recommended solution for security using 802.1x

Objective

802.1X provides the port base security it provides the better way to control the access to network. The most common way for authentication in wireless communication is EAP. In general practice two types of modes can be set using WPA/WPA2

- Enterprise mode
- Personal mode

This experiment implements the Enterprise mode using WPA2.

Scenario

This experiment implies the following three main features:

- Supplicant connectivity with the AP.
- Authenticator which provide the access.
- Usage of authenticator server for authentication.

Above given are the three major configurations which will be implemented on the coming steps. 802.1X EAP provide the mutual authentication which will be shows in implementation part. 802.1X also provides the protection against the dictionary attack. 802.1X perform the following steps for configuration.

- Configure server manager
- Configure security manager

- Configure the SSID Manager
- configuring local RADIUS server
- create users list

5.3.1 Hardware Requirement

Device	Description
Linksys WAP54G	Wireless access point
D-Link DWL-G650	External wireless card
Laptop Sony Vaio VGN-fs990	Acting as a host

Table 12 Hardware used to connect network using 802.1x

5.3.2 Software Requirement

Software	Description
Cisco aironet desktop utility	Client configuration and management
Cisco aironet 1300 utility	To configure 1300 AP/Bridge
Windows XP	To configure client
Windows server 2003	For external RADIUS server

Table 13 Software used to configure network using 802.1x

5.3.3 802.1x implementation

Step 1 Configure server manager

Open the GUI utility software to configure the AP, under this configure the AP that act as local RADIUS server and running LEAP authentication protocol. Under the security option choose the server Manager to configure the IP address, ports and shared secret of the RADIUS server, In this case AP using the local RADIUS server that's why it will use the port 1813. EAP authentication priority is 192.168.1.1

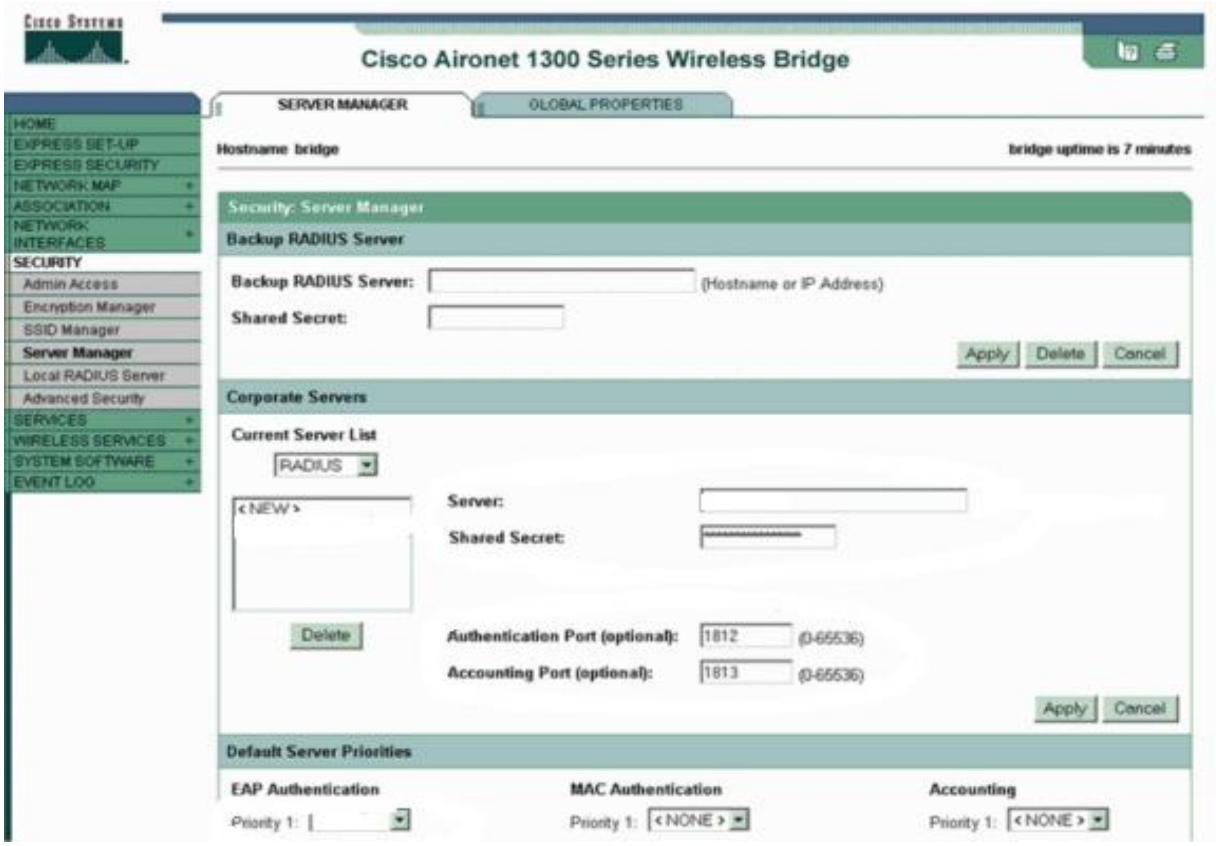


Figure 17 Configure server manager

Step 2 Configure security manager

This step involves the configuration of encryption method here in this case under the cipher menu select the AES CCMP for the encryption purposes.

Figure 18 Configure security manager

Step 3 Configure the SSID Manager

For the configuration of the Service Set Identifier (SSID) Click on the check box of network as EAP which enable the authentication type of WPA2.

Figure 19 Configure SSID manger

Step 4 configuring local RADIUS server

Change the main tab to general setup option on the top of window then select the LEAP box and click on apply button, after that define the IP address and shared secret key of the radius server here in this case radius address will be the same as AP address because it is working as local radius server.

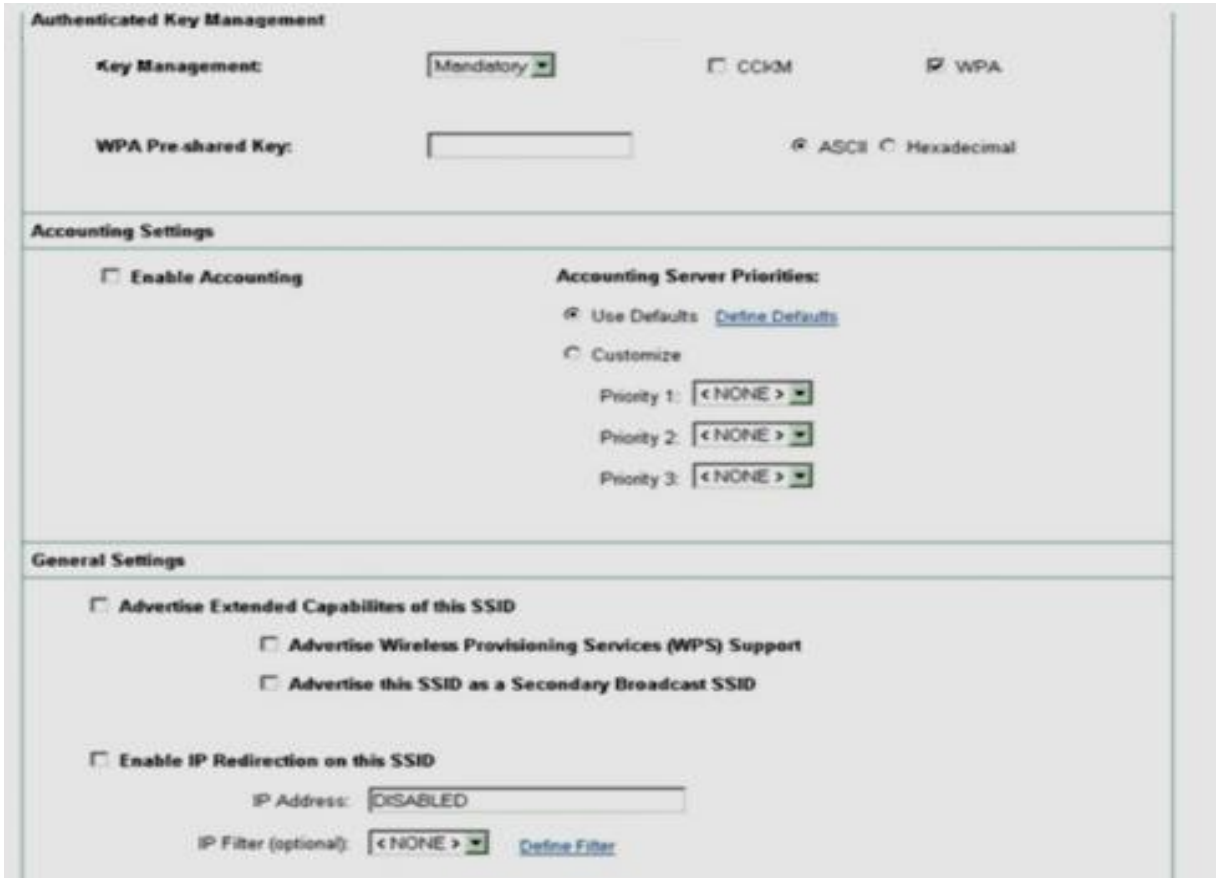


Figure 20 Configure local RADIUS sever

Step 5 create users list
In final step under the general setup create the users and there passwords.
5.3.4 AP configuration
For detail configurations of AP check Appendix C

5.3.5 Configure client

Using the desktop utility of the aironet adapter complete the following steps to configure the client side configuration.

Step 1 Profile Management
Open the aironet desktop utility and click on new button to create the new profile under the general tab type the name of new profile and SSID of the client network adapter, here in this scenario profile name and SSID is "WPA2"

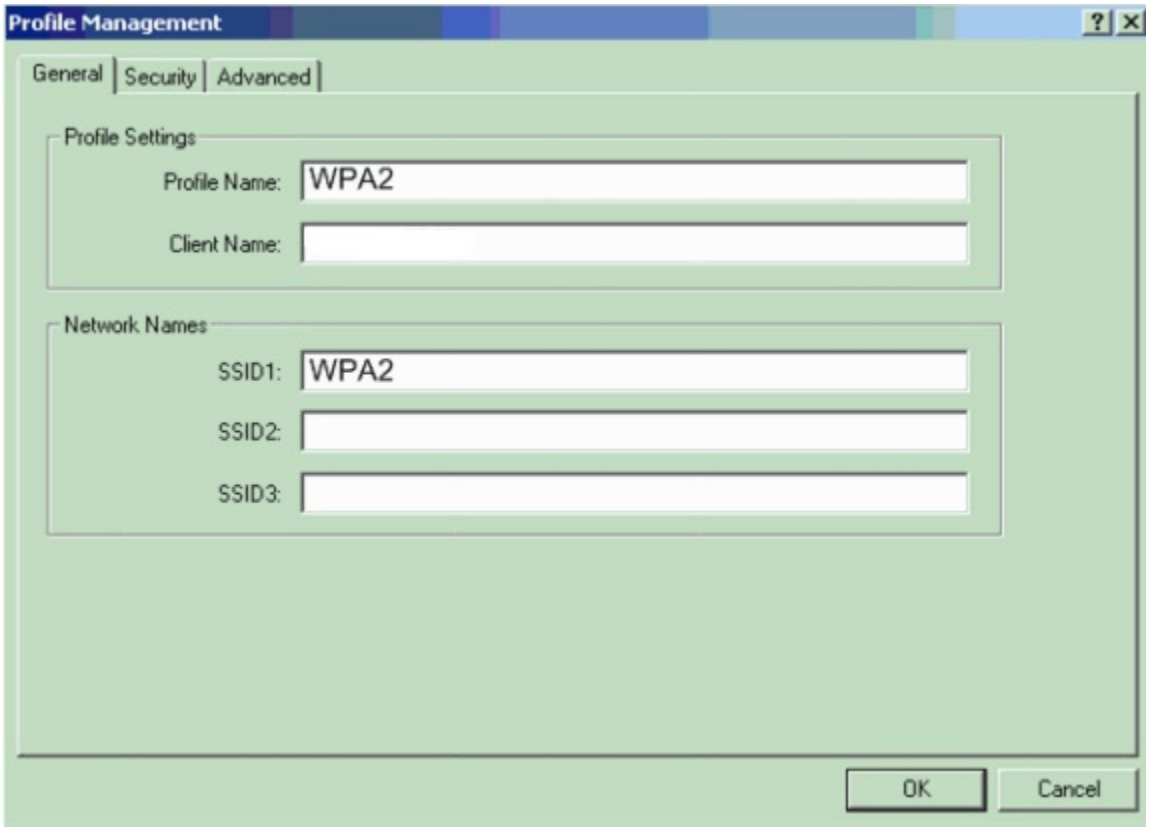


Figure 21 Configure client Profile management

Step 2 configure security

On the top of window select the security tab and choose WPA/WPA2/CCKM and select LEAP under its menu. This step active the security option whichever enabled on the AP.

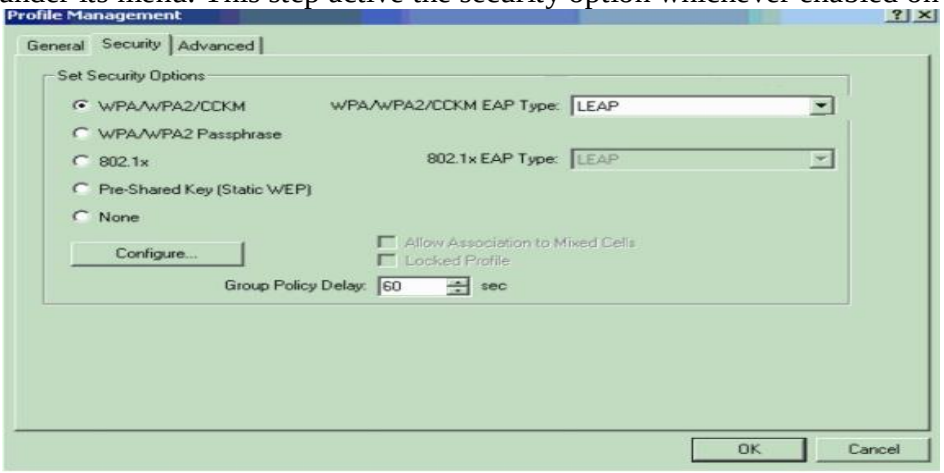


Figure 22 Configure security policy on client

Step 3 LEAP settings

Choose the option of configure to define the LEAP settings under LEAP give the desire username and password here in this case username is Ali and password is Hasan after giving this information click on the box where it ask the option of automatically prompt for username and password.

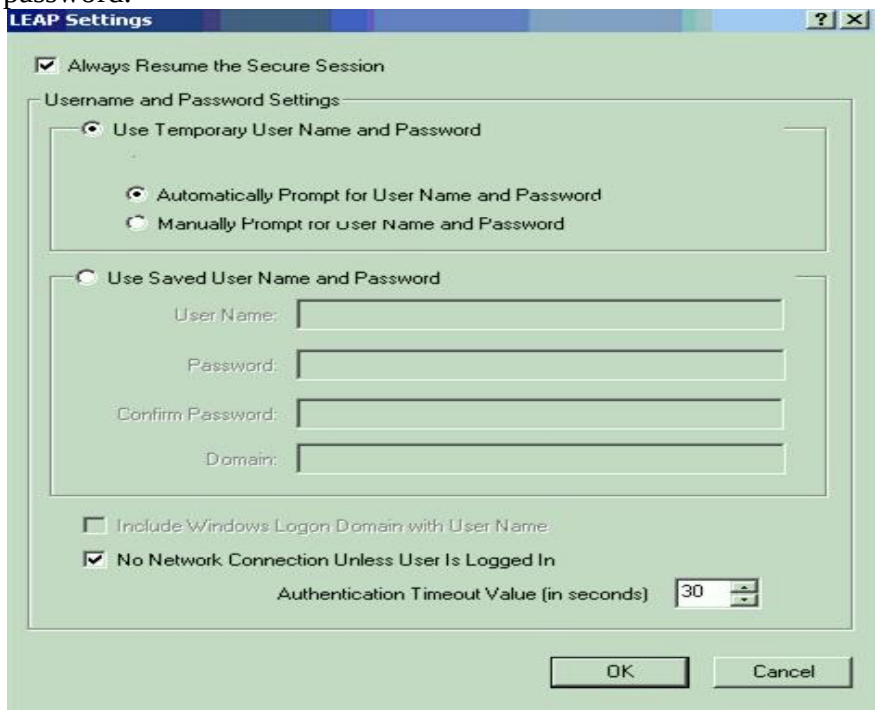


Figure 23 Configure LEAP settings

Step 4 Activation of profile

In final step exit from the profile management and click on the option of activate profile. To verify the all step try to connect the network and give the credential i.e., username and password after that it will show the LEAP authentication status window which will shows the success status of current connection.

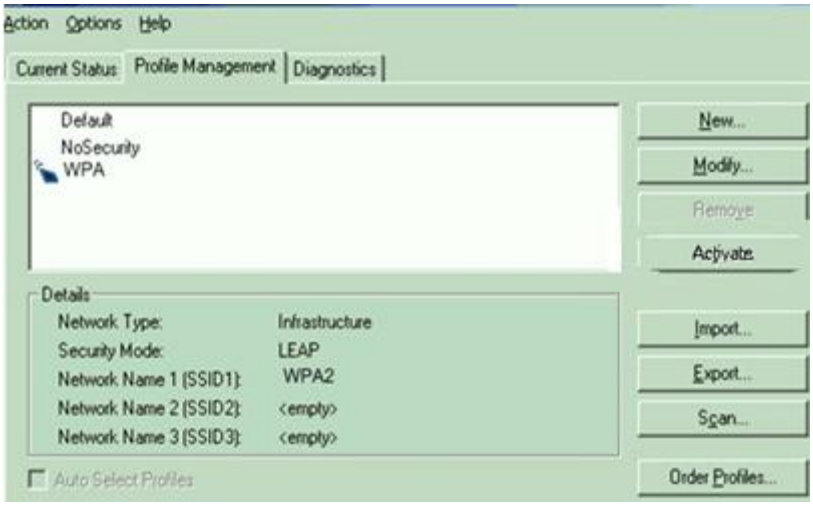


Figure 24 Active user profile

5.3.6 Summary

Using the 802.1x EAP provides the mutual authentication which leads to transfer the key to right entity and it also provides the per-packet authentication. TLS server provides a certificate as prove of private key as a whole 802.1x is one of the best security technique to secure the enterprise network.

6 Conclusions and Suggestions

The main goal of this thesis was to show the attacks on WLAN and test the few of attack in lab environment and finally implement the best solution in lab environment. This thesis implemented the three major security techniques WEP, WPA/WPA2 and WPA2 using 802.1X authentication.

First lab implemented the WEP security technique and this lab clearly showed that how much network is vulnerable if it uses the WEP static key regardless of the size of IVs, by using the cracking tool aircrack under Backtrack 3 environment.
Second lab implemented the WPA/WPA2 pre-shared key; this lab showed that the dictionary attack and showed that how network is unsecure if it uses the common phrase key. This lab successfully cracked the 8-63 character long key.
Third lab implemented the recommended solution for the WLAN security by implementing WPA2 using the 802.1x authentication technique and due to port based security it is impossible to crack the key.

Although, it is quite tough to secure wireless network due to RF signals on the air but by using the proper security technique these attacks can be minimized. This thesis recommended the WPA2 security using 802.1X authentication

7 References

[1] http://www.usr.com/download/whitepapers/lan-security-wp.pdf
[2] http://paper.ijcsns.org/07_book/200605/200605C01.pdf
[3] http://documents.iss.net/whitepapers/wireless_LAN_security.pdf
[4] (RFC standard 3990)
[5] Prasad, A. R., WLANs: Protocols, Security and Deployment, Ph.D. Thesis, Delft University Press (DUP), Delft, The Netherlands, December 2003.
[6] Prasad, N. R., Adaptive Security in Heterogeneous Networks, Ph.D. Thesis, University of Roma "Tor Vergata," Rome, Italy, April 2004.
[7] Prasad, N. R., and A. R. Prasad (eds.), WLAN Systems and Wireless IP for Next Generation Communications, Norwood, MA: Artech House, January 2002.
[8] Black, U., Internet Security Protocols: Protecting IP Traffic, Upper Saddle River, NJ: Prentice Hall, 2000.
[9] Stallings, W., Cryptography and Network Security: Principles and Practice, Upper Saddle River, NJ: Prentice Hall, July 1998.
[10] Anand R. Prasad & Neel R. Prasad. 2005. 802.11 WLANs and IP Networking Security, QoS and Mobolity. Artech house Universal personal communication Series.
[11] AvHarold F. Tipton & Micki Krause. 2009. Information security management handbook. Auerbach Publications.
[12] Arinze Nwabude. 2008. Wireless local area network (WLAN): security risk and counter measures. Blekinge Institute of Technology.
[13] O Hara & A. Petrick. 1999. IEEE 802.11 Handbook, A designer companions. IEEE Presss.
[14] Wi-Fi Protected Access: Strong, Standard based, interoperable security for today's Wi-Fi networks. Retrieved june 28 2005. Online available http://www.wifialliance.com/opensection/pdf/whitepaper_Wi-Fi_Security4-29-03.pdf
[15] Wi-Fi Protected access 2. Retrieved june, 28 2005. Online available: http://www.wi-fi.org/opensection/protected_access.asp
[16] Sebastin Bohn & Stephan Grob. 2006. An automated system interoperability test bed for WPA and WPA2. IEEE Xplore
[17] White paper. July 2008. WLAN Security Today: Wireless more secure than wired. Siemens Enterprise Communications.
[18] White paper. July 2008. WLAN Security Today: Wireless more secure than wired. Siemens Enterprise Communications.
[19] Ahmed M. Al Naamany, Ali Al Shidhani & Hadj Bourdoucen. 2006. IEEE 802.11 Wireless LAN Security Overview. Department of Electrical and Computer Engineering, Sultan Qaboos University. Oman.
[20] ISS Technical Paper Internet Security System, Wireless LAN Security 802.11b and Corporate Network. Barfiled Road, Atlanta.
[21] F. Cao & S. Malik, 2005. Security Analysis and Solutions for Deploying IP Telephony in the Critical Infrastructure, Critical Infrastructure Assurance Group Cisco Systems, Inc.
[22] Patrick C.K & M. Vargas. 2006. Security Issues in VOIP Applications. Hung University of Ontario Institute of Technology Oshawa, Canada.
[23] Joon S.Park & Derrick Dicoi. 2003. WLAN Security: Current and Future 'Wireless LAN deployment improves users' mobility, but it also brings a range of security issues that affect emerging standards and related technologies. IEEE computer society.
[24] Nguyen The Anh & Rajee Shorey. 2005. Network sniffing tool for WLANs: Merits and Limitations. IEEE Computer Society

References

[25] Anand R. Prasad & Neeli R. Prasad. 2005. 802.11 WLANs and IP networking: security, QoS and mobility. Artech House.

[26] Andrea Goldsmith. 2005. Wireless Communication. Cambridge University Press, New York.

[27] Karen Scarfone, Derrick Dicoi, Matthew Sexton & Cyrus Tibbs. July 2008. Guide to Securing Legacy IEEE 802.11 Wireless Networks. NIST Special Publication 800-48 Revision 1.

[28] U.S Robotics. 2009. Wireless LAN Networking White Paper. IEEE Computer Society.

[29] Jui-Hung Yeh, Jyh-Cheng &Chen and Chi-Chen Lee.2010.WLAN Standards in particular 802.11 family. IEEE computer Society, ©RUBBERBALL PRODUCTIONS, ©DIGITALVISION, ©DOVER PUBLICATIONS, INC./COMPOSITE: MKC

[30] Nwabude Arinze Sunday. 2008. Wireless Local Area Network (WLAN): Security Risk Assessment and Countermeasures. Blekinge Institute of Technology School of Engineering Department of Telecommunications.

[31] Tran Nghi & Mikko Valle. 12 April 2000. How does WLAN Works. Published on URL URL: http://www.netlab.tkk.fi/opetus//s38118/s00/tyot/25/page2.shtml

[32] Hardjono, Thomas & Dondeti, Lakshminath R. 2005. Security in Wireless LANs and MANs. Artech House, Incorporated.

[33] Benny Bing & TK tin. 2003. The worldwide wifi technological trends and business strategies. John Wiley & Sons, Hoboken New Jersey.

[34] Arash Habibi Lashkari, Masood Mansoor & Aamir Syed Danish. 2009. Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA). International conference on Signal Processing Systems, Singapur.

[35] Krishna Sankar, Sri Sundaralingam, Andrew Balinsky & Darrin Miller. 2004. Cisco Wireless LAN Security. Cisco Press.

[36] Mohammad Ilyas and Syed Ahson. 2005. Hand Book of Wireless Local Area Networks Applications, Technology, Security, and Standard (internet and communicatins). CRC Press.

[37] Wi-Fi Alliance. March 2005. Deploying Wi-Fi Protected Access (WPA™) and WPA2™ in the Enterprise. Wi-Fi® is a registered trademark of the Wi-Fi Alliance.

[38] IEEE. IEEE standard 802.11i-2004. Local and Metropolitan Area Networks- Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancement. IEEE Inc, Three park Avenue, New York.

[39] Mansoor Ahmad Khan, Ahmad Raza Cheema and Aamir Hasan. 2008. Improved Nonce Construction Scheme for AES CCMP to evade initial counter Prediction. IEEE Computer Society, Washington DC USA.

[40] M junaid, Dr Muid Mufti and Myhammad Ummar Ilyas. 2006. Vulnerabilities of IEEE 802.11i Wireless LAN CCMP protocol. World Informatika Society.

[41] Neal Leavitt. 2008. Industry trends Will IEEE 802.1X Finally Take Off in 2008. IEEE Computer Society.

[42] Jyh-Cheng Chen, Ming-Chia Jiang & Yi-Wen Liu. 2005. Migration towards 4G Wireless Communications Wireless LAN Security & IEEE 802.11i. IEEE Computer Society, National Tsing Hua University.

[43] Matija Sorman, Tomislav Kovac, Damir Maurovic**.** 2004. Implementing Improved WLAN Security. 46th International Symposium Electronics in Marine, Zadar Croatia**.**

[44] Cisco Online material of secure and Optimized converged networks

[45] Anthon James. 2002. Using IEEE 802.1x to Enhance Network Security. Foundary Networks.

[46] Interlink Networks. 2006-2007. RADIUS Server vs. VPN - Link Layer and Network Layer Security for Wireless Networks. Interlink Networks, USA.

[47] Eric Griffith. September 2, 2004. A warm welcome to WPA2. Article, http://www.wi-fiplanet.com/news/article.php/3402971.

[48] Robert Moskowitz. November 4 2003. Weakness in Passphrase Choice in WPA Interface. ICSA Labs, a division of TruSecure Corp.

References

[49] Paramjit S. Kahai & Simran K. Kahai. Deployment Issues and Security Concerns With Wireless Local Area Networks: The Deployment Experience At A University. Journal of Applied Business Research, Volume 20, Number 4.

[50] Andrea Bittau, Mark Handley &Joshua Lackey. 2006. The Final Nail in WEP's Coffin. IEEE Symposium on Security and Privacy, IEEE Computer society.

[51] Tim Newsham. Cracking WEP Keys Applying known techniques to WEP Keys, 2001. http://www.lava.net/ ~newsham/wlan/WEP password cracker.pdf.

[52] J. R.Walker. Unsafe at any key size; an analysis of the WEP encapsulation, 2000, D. Simon and B. Aboba and T. Moore. IEEE 802.11 security and 802.1X, 2000

[53] S. Fluhrer, I. Mantin, and A. Shamir. Weaknesses in the Key Scheduling Algorithm of RC4. Lecture Notes in Computer Science, 2259:1–24, 2001

[54] D. Wagner. Weak Keys in RC4, 1995. http //www.cs.berkeley.edu/~daw/my-posts/my-rc4-weak-keys.

[55] KoreK. chopchop (Experimental WEP attacks) , 2004. http://www.netstumbler.org/showthread.php?t=12489

[56] W. A. Arbaugh. An Inductive Chosen Plaintext Attack Against WEP and WEP2, 2001.

[57] D. C. Plummer. RFC 826: Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware, November 1982.

[58] KoreK. chopchop (experimental WEP attacks). http://www.netstumbler.org/showthread.phpt=124892004

[59] Erik Tews. Attacks on the wep protocol. Cryptology ePrint Archive, Report 2007/471, 2007. http://eprint.iacr.org/

[60] Martin Beck. 8 November2008. Practical attacks against WEP and WPA. IEEE computer Society.

[61] IEEE-SA Standards Board. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifcations. Communications Magazine, IEEE, 2007

[62] Jin Hong & Palash Sarkar. 2005. "Rediscovery of Time Memory Tradeoffs". [Online] Available: http://cr.yp.to/2005-590/hong.pdf

[63] David A. McGrew. November2002. "Counter Mode Security: Analysis and Recommendations", Cisco Systems.

8 Appendix A

- http://madwifi-project.org/wiki/Compatibility
- http://linux-wless.passys.nl/
- http://atheros.rapla.net/
- http://www.linux-wlan.org/docs/wlan_adapters.html.gz
- http://customerproducts.atheros.com/customerproducts/
- http://www.seattlewireless.net/index.cgi/HardwareComparison
- http://backtrack.offensive-security.com/index.php?title=HCL:Wireless
- http://acx100.sourceforge.net/matrix.html

9 Appendix B

- http://www.openwall.com/mirrors/
- http://gdataonline.com/downloads/GDict/
- http://www.theargon.com/achilles/wordlists/
- http://theargon.com/achilles/wordlists/theargonlists/
- http://www.outpost9.com/files/WordLists.html
- http://www.securinfos.info/wordlists_dictionnaires.php
- http://www.vulnerabilityassessment.co.uk/passwords.htm
- http://packetstormsecurity.org/Crackers/wordlists/
- http://www.ai.uga.edu/ftplib/natural-language/moby/
- http://www.insidepro.com/eng/download.shtml
- http://www.word-list.com/
- http://www.cotse.com/tools/wordlists1.htm
- http://www.cotse.com/tools/wordlists2.htm
- http://wordlist.sourceforge.net/

10 Appendix C

AP Configurations

```
#show running-config
Building configuration...
aaa new-model
aaa group server radius rad_eap
 server 192.168.1.1auth-port 1812 acct-port 1813
aaa authentication login eap_methods group rad_eap
bridge irb
interface Dot11Radio0
 no ip address
 no ip route-cache
 encryption vlan 10 key 1 size 128bit
encryption vlan 10 mode wep mandatory
broadcast-key vlan 10 change 300
ssid cisco vlan 10
authentication open eap eap_methods
authentication network-eap eap_methods
 speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
 rts threshold 2312
 channel 2437
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
interface FastEthernet0
 no ip address
```

```
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
interface BVI1
 ip address 192.168.1.1 255.255.255.0
no ip route-cache
ip default-gateway 72.10.155.294
ip http server
ip radius source-interface BVI1
snmp-server community cable RO
snmp-server enable traps tty
radius-server local
nas 192.168.1.1key shared_secret
group testuser
user Ali nthash Hasan group testuser
user Abdul nthash Qudoos group testuser
radius-server host 192.168.1.1 auth-port 1812 acct-port
1813 key shared_secret
radius-server retransmit 1
radius-server attribute 32 include-in-access-req format %h
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
bridge 1 route ip
line con 0
line vty 5 15
end
```