MEE08:39

Wireless Local Area Network (WLAN): Security Risk Assessment and Countermeasures

Nwabude Arinze Sunday

This thesis is presented as part of Degree of
Master of Science in Electrical Engineering

Blekinge Institute of Technology
August 2008

Blekinge Institute of Technology
School of Engineering
Department of Telecommunications
Supervisor: Fredrik Erlandsson
Examiner: Fredrik Erlandsson

ABSTRACT

Wireless LANs popularity has been on the rise since the ratification of the IEEE 802.11b standard in 1999. In recent years, wireless LANs are widely deployed in places such as business organizations, government bodies, hospitals, schools and even home environment. Mobility, flexibility, scalability, cost-effectiveness and rapid deployment are some of the factors driving the proliferation of this technology. However, the architecture of this technology made it insecure as WLANs broadcast radio-frequency (RF) data for the client stations to hear. This presents new challenges for network administrators and information security administrators.

This study was undertaken to find out if wireless networks are inherently insecure thereby limiting enterprise deployment. If yes, what are the known holes, and can they be fixed? The security mechanisms of wireless LANs were not within the scope of this work. The author tried to answer these questions through comprehensive and broad literature study.

The study shows that wireless LANs are prone to many different kinds of attacks – ranging from passive to active, and that wireless security initiative has come a long way, from weak WEP to a more robust WPA2. It also show that optimal security solution for Wireless LANs involves a combination of security technologies, and that vulnerability assessment and risk analysis are essential for development of effective security policy and determination of appropriate security measures for risk mitigation.

Keywords:
Wireless LANs, IEE 802.11, Attacks, Security, Access Point (AP).

ACKNOWLEDGEMENT

I am grateful to God Almighty for his grace and strength that sustained me through out the duration of this work, thereby making it a success.

Special thanks go to my supervisor, Fredrik Erlandsson, for his support and guidance.

I, also, wish to express my profound gratitude to Mikael Åsman, program manager, Master in Electrical Engineering, BTH; Lena Magnusson, Student Administrator, Master in Electrical Engineering, BTH; and May Gulis, Student Nurse, BTH, for their relentless efforts and assistance in getting this thesis work approved.

Finally, I wish to thank my mom, siblings and all my friends in BTH and at home for their prayers all through the period of this work. Thank you all.

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

LIST OF FIGURES

LIST OF TABLES

CHAPTER ONE

1.0 INTRODUCTION

Wireless communication has broken the constraint users used to have with wired technology. The liberty to gain access to corporate network without being bonded, mobility while accessing the Internet, increased reliability and flexibility are some of the factors driving the wireless local area network technology. Other factors that contribute to tremendous growth of Wireless Local Area Networks (WLANs) are reduced installation time, long-term cost savings, and installation in difficult-to-wire areas. Today, Wireless Local Area Network (WLAN) is a choice to reckon in various sectors, including business, education, government, public and individual. IEEE 802.11 dominates the wireless networking technology. This can be attributed to the low cost of the hardware and high data rates that support current applications (from 1 to 54 Mbps) as well as promising future extensions (possibly exceeding 100 Mbps with 802.11n). Increasingly, portable devices (Laptops, PDAs, and Tablet PCs) are being sold with wireless LAN as a standard feature.

However, this technology brings with it important limitations in the field of security. The communication medium of wireless LAN is radio wave, thus it's more susceptible to eavesdropping than wired networks, and as the wireless market grows, the security issues grow along with it. There have been several works on WLAN security since it was discovered that the 802.11 security architecture is weak. However, most of these works were on the security mechanism enhancement.

For an organization to best protect its information there is need for security risk assessment. This will help to determine the threats its information is prone to, and then develop appropriate security measures to counter it.

This thesis assesses the security risks associated with WLANs that limits its deployment in enterprise environment and proffers countermeasures that should be put in place for secure implementation as integral part of LAN.

1.1 PROBLEM STATEMENT

Information is a valuable asset of an organisation and thus need to be protected against threats, to give the confidence that the business can proceed continuously. The result is reduction in possible losses of business and increase in the rate of return on investment and business opportunities.

It is therefore of uttermost importance to assess the security risks associated with the deployment of WLAN in an enterprise environment and evaluate countermeasures to mitigate these risks for information security: Confidentiality, Integrity and Availability.

1.2 PREVIOUS STUDIES

Several works have affirmed the weakness of Wired Equivalent Privacy (WEP) security algorithm in the original IEEE 802.11 standard and suggested how the security mechanism of WLAN can be enhanced - the paper by Borisov, Goldberg, and D. Wagner, for example, demonstrated the weakness of WEP. There are also few works on how external security apparatus can be used to strengthen the WLAN inbuilt security mechanism – James Burrell and others. This study therefore is undertaken in order to add something new to existing knowledge in the globalised and ever-changing world of technology.

1.3 OBJECTIVES OF THE STUDY

1.3.0 To find out the known security holes that limit enterprise deployments of a WLAN

1.3.1 To find out if these known security holes can be fixed.

1.4 RESEARCH QUESTIONS

In accordance with the objective of the study, the following research questions are posed to guide this research.

1.4.0 Research question I

Are there known inherent insecurities that limit enterprise deployments of a WLAN?

1.4.1 Research question II

Are there countermeasures that can be put in place to fix these known security holes for secure enterprise deployment of wireless networks?

1.5 METHOD

This thesis is descriptive in nature as the problem is well structured and understood. The approach adopted in this research paper is deductive as it looks at the bigger picture (WLAN) and narrows down to security (vulnerabilities and countermeasures). The data is collected from literature and Internet. The subjects of the literature are mainly wireless communications, network security and WLAN security. Most of the literature is published not later than 2002, and the main part of the collected data consists of published articles and papers that were found on Internet. Care was taken to ensure the information from the articles and papers from internet are true and have been published.

1.6 SIGNIFICANCE OF THE STUDY

There is a mindset prevailing that wireless networks are inherently insecure. Can this be actually true, a fact or fabrication? This study is important because it tries to access wireless security issues that limit enterprise deployment of wireless network. It encourages companies to carry out security risk assessment so as to know the threats their network is facing and, then, determine the appropriate security policy to adopt for their network for reduction and/or possibly elimination of the threats.

1.7 ORGANISATION OF THE STUDY

This work is organised in five chapters.

The first chapter is the introduction to this work. It basically deals with problem statement, research questions, method, objective and significance of the study.

The second chapter is the literature review. Here a brief overview of wireless local area network technology is presented.

The third chapter is on WLAN standards. This chapter gives a description of all the available IEEE 802.11 family of standards.

The fourth chapter is wireless LAN vulnerabilities, threats and countermeasures. It describes in details all known wireless LAN attacks, and explains how to mitigate them through vulnerability assessment.

The fifth chapter gives the conclusion, summary and areas of future research.

CHAPTER TWO

2 A BRIEF REVIEW OF WIRELESS LOCAL AREA NETWORK (WLAN)

2.0 INTRODUCTION

Wireless local area networks (WLANs) are the same as the traditional LAN but they have a wireless interface, thereby providing location-independent network access. It enables a local network of computers to exchange data or other information by radio waves and without the use of cables. It can either replace or, more usually, extend a wired LAN. Today, wireless LANs have occupied a significant segment in the local area network market. Increasingly, organizations have found that wireless LANs are indispensable attachment to traditional wired LANs, to satisfy the requirements for mobility, relocation, ad hoc networking, and coverage of locations difficult to wire.

This chapter provides a brief survey of wireless LANs. The following subtopics were covered: basic WLAN components, WLAN transmission technology, WLAN spectrum allocation, WLAN topologies and WLAN applications.

2.1 BASIC WLAN COMPONENTS

For one to set up a wireless local area network, two basic components must be available: wireless network cards and wireless access point(s). The third basic component, wireless bridge, is used to link two or more buildings together.

The wireless network cards are attached to mobile computing devices, and they connect to an access point. An access point is essentially a hub that gives wireless clients the ability to attach to the wired LAN backbone. To maintain a coverage area, more than one access points are used as in cell structures, which are used by cell phone providers to maintain a coverage area. Wireless bridges, on the other hand, enable high-speed long-range outdoor links between buildings. Based on line-of-sight, wireless bridges are not affected by obstacles such as freeways, railroads, and bodies of water, which typically pose a problem for copper and fibre-optic cable.

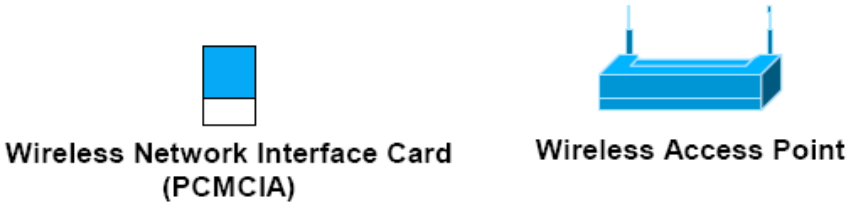


Figure 1 Basic components of WLAN
Source: J. Burrell [8]

2.2 WLAN TRANSMISSION TECHNOLOGIES

Wireless LANs are generally categorized according to the transmission technique in use. All available wireless LAN products fall into one of the categories below:

- **Infrared (IR) LANs:** Infrared light does not penetrate opaque walls; as a result, an individual cell of an IR LAN is limited to a single room. No licensing is required.
- **Spread Spectrum LANs:** Here, spread spectrum transmission technology is used, and in most cases, the LANs operate in ISM (Industrial, Scientific, and Medical) bands so as to avoid licensing requirement as in the United States for example.
- **Narrowband Microwave:** This category of LANs operates at microwave frequencies. Some operate at frequencies that require FCC licensing, others operate at the unlicensed ISM bands, but they do not use spread spectrum.

2.2.0 INFRARED (IR) LANs

There are three types of infrared transmission: directed beam, ominidirectional, and diffused.

- **Directed Beam Infrared:** Directed beam infrared transmission provides the highest transmission speed. Here the receiver is aligned with the sender unit to create a point-to-point link. The range depends on the degree of focusing and the emitted power. The light source used in infrared transmission depends on the environment. Light emitting diode (LED) is used in indoor areas, while lasers are used in outdoor areas.

- **Ominidirectional:** In ominidirectional configuration, a single base station is within the line of sight of all other stations in the LAN, and this station is typically mounted on the ceiling. This station then acts as a multiport repeater.

The ceiling station broadcasts ominidirectional signals which are received by all the other IR transceivers in the area, and these transceivers in turn transmit a directional beam aimed at the ceiling base station.

- **Diffused:** The infrared light transmitted by the sender unit fills the area (e.g. office). Therefore the receiver unit located anywhere in that area can receive the signal.

2.2.1 SPREAD SPECTRUM LANs

In exclusion of very small offices, a spread spectrum wireless LAN makes use of a multiple-cell arrangement. Each of the adjacent cells in the configuration is assigned a different centre frequency within the same band to avoid interference.

With this transmission technology, there are two methods used by wireless LAN products: frequency hopping and direct sequence modulation.

- **Frequency Hopping**: Here, the signal jumps from one frequency to another within a given frequency range. The transmitter device "listens" to a channel, if it detects an idle time (i.e. no signal is transmitted), it transmits the data using the full channel bandwidth. If the channel is full, it "hops" to another channel and repeats the process. The transmitter and the receiver "jump" in the same manner.

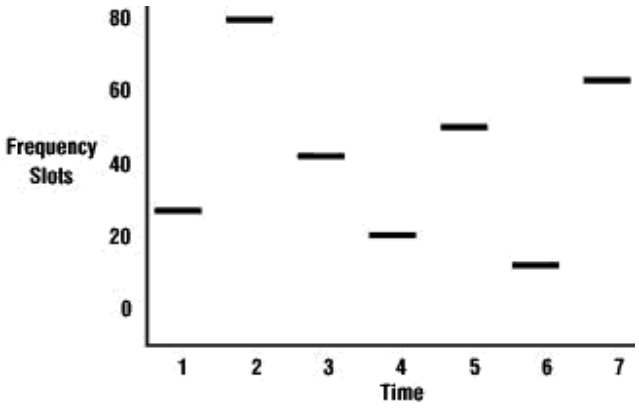


Figure 2 Frequency hopping
Source: WLANA [65]

- **Direct Sequence Modulation:** This method uses a wide frequency band together with Code Division Multiple Access (CDMA). Signals from different units are transmitted at a given frequency range, and at a very low power. A code is transmitted with each signal so that the receiver can identify the appropriate signal

transmitted by the sender unit. The frequency at which such signals are transmitted is called the ISM (industrial, scientific and medical) band. This frequency band is reserved for ISM devices. The ISM band has three frequency ranges: 902-928, 2400-2483.5 and 5725-5850 MHz.

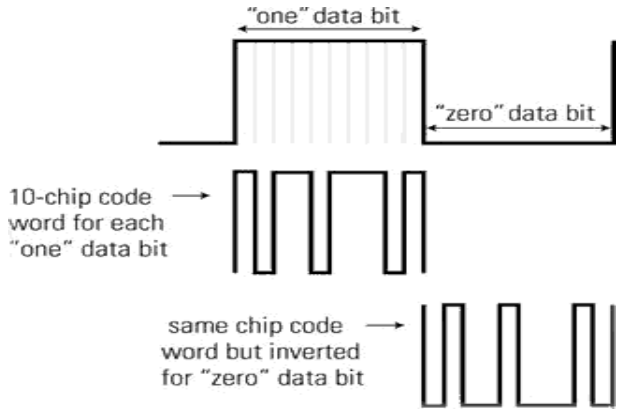


Figure 3 DSSS with CDMA
Source: WLANA [65]

2.2.2 NARROWBAND MICROWAVE LANs

This involves the use of relatively narrow bandwidth microwave radio frequency band to transmit signals. Most of the available narrowband microwave LAN products operate at frequencies that require FCC licensing - uses the 18.82 to 19.205GHz of the radio spectrum. It has two bandwidth, they are:

- **Licensed Narrowband RF:** A typical narrowband scheme makes use of cell configuration in which adjacent cells use nonoverlapping frequency bands within the overall 18 GHz band. One advantage of licensed narrowband LAN is that it guarantees interference-free communication. Also, all communications are encrypted to avoid eavesdropping.

- **Unlicensed Narrowband RF:** Operating at ISM spectrum, unlicensed narrowband RF can be used for narrowband transmission at lower power 0.5 watts or less.

In table 1 shown in the next page, the WLAN transmission technologies are compared relative to range limitation, susceptibility to signal interception, interference, jamming and license requirement.

Table 1 Comparison of WLAN Transmission Technologies. [8]

Transmission Technology	Range Limitation Low High	Signal Interception Susceptibility Low High	Susceptibility To Interference/Jamming Low High	Licence Required
Infrared	**********	****	**********	No
Spread Spectrum	****	****	****	No
Narrowband Microwave	****	**********	**********	Yes unless ISM

2.3 WLAN SPECTRUM ALLOCATION

The infrared and spread spectrum wireless LAN technologies operate in ISM (Industrial, Scientific, and Medical) bands. This radio spectrum is unlicensed. The table below shows the ISM frequency bands.

Table 2 Showing 900 MHz, 2.4 GHz and 5 GHz ISM Bands.

ISM FREQUENCY BANDS				
Frequency (Lower Limit)	**Frequency (Upper Limit)**	**Total Bandwidth**	**Max Power**	**Max EIRP**
902 MHz	928 MHz	26 MHz	1 Watt	4 Watt (+36 dBm)
2400 MHz	2483.5 MHz	83.5 MHz	1 Watt	4 Watt (+36 dBm) for multi-point, 200 W (+53 dBm) for point-to-point
5.725GHz	5.850 GHz	125 MHz	1 Watt (+30 dBm)	200 W (+53 dBm)

2.4 WLAN TOPOLOGIES

The IEEE 802.11 standard defines three basic topologies to be supported by the MAC layer implementation. These are:

- Independent Basic Service Set (IBSS)
- Basic Service Set (BSS)
- Extended Service Set (ESS)

The 802.11 standard further defines the following two modes:

- Ad hoc
- Infrastructure

2.4.0 AD HOC MODE

This consists of a group of 802.11 stations that communicate directly with one another within a limited range. It is essentially a simple peer-to-peer WLAN, and it is sometimes referred to as IBSS topology. Here, there is no need for access point and the networks do not require any pre-planning or site survey. So, the network is usually a small one and only last long enough for the communication of whatever information that needs to be shared.

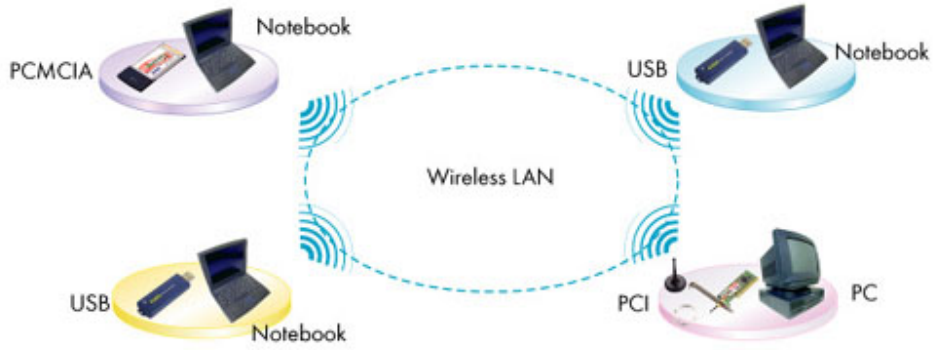


Figure 4 WLAN Ad Hoc Mode
Source: EUSSO [64]

2.4.1 INFRASTRUCTURE MODE

An infrastructure mode consists of a group of 802.11 devices communicating with each other through a specialized station known as the access point (AP). The client stations do not communicate directly with each other, rather they do with the access point which forwards the frames to the designated station. The access point (also often referred to as a base station) is connected to the wired network infrastructure. If only one access point is involved, then we have a basic configuration referred to as a BSS topology in the 802.11 standard. Communication between wireless nodes, wireless computers and the wired network will be via the AP.
For communication of data to take place, wireless clients and AP's must establish a relationship, or an association. It is only after an association is established can the two wireless stations exchange data.

APs transmit a beacon management frame at fixed intervals. To associate with an access point and join a BSS, a client listens for beacon messages to identify the access points within its range. The client selection of which BSS to join is carried out in a vendor independent manner. A client may also send a probe request management frame to find an access point associated with the desired SSID (service set identifier).

Multiple infrastructure BSSs can be combined via their uplink interfaces to form a single sub network referred to as an ESS topology. It is thus possible to expand the wireless network with a number of AP's utilising the same channel or utilise different channels to boost aggregate throughput.

Figure 5 WLAN Infrastructure Mode
Source: EUSSO [64]

2.5 WLAN APPLICATIONS

The following tables summarize some of the many applications made possible through the power and flexibility of wireless LANs.

Table 3 Showing WLAN Topologies and Application Areas. [8]

WLAN Topology	Application
Infrastructure (Point-to-point link)	Cross-building interconnect
Infrastructure (Cell configuration)	LAN extension
Infrastructure (Cell configuration)	Nomadic access
Ad hoc (Peer-to-peer)	Ad hoc networking

Table 4 Organizations/Scenarios, WLAN Applications and Advantages [8]

Organization/Scenario	Application	Advantage
Health Care/ Hospital	Patient monitoring and instant access to patient information	▪ Mobility ▪ Flexibility
Consulting or accounting audit engagement teams or small workgroups	Quick network setup	▪ Increased productivity
Network managers in dynamic environments	Minimize the overhead of moves, adds, and changes with wireless LANs	▪ Reduction in the cost of LAN ownership
Manufacturing	Network connectivity for machinery in open locations and hazardous environments	▪ Mobility ▪ Flexibility ▪ Increase in productivity
Conference Centres	Provide connectivity to attendees with enabled devices	▪ Rapid deployment ▪ Quicker decision making
Education	Connectivity to facilitate access to information, information exchanges, and learning.	▪ Mobility
Inventory Control	Connectivity for portable inventory devices with central storage facility	▪ Real-time reporting
Residential	Quick setup of low cost network infrastructure	▪ Low cost networking solution
Multimedia Resources	Provide wireless access to multimedia resources	▪ Shared Resources
Tactical/Military	Rapid establishment of network with mobility support in hazardous environments	▪ Mobility ▪ Rapid network deployment
Small Office/Home Office (SOHO)	Quick setup of low cost network infrastructure	▪ Low cost networking solution
Travel/Train	Provide instant access to internet to travellers	▪ Mobility ▪ Flexibility
Retail Outlets/Hot Spots	Quick access to internet to the public	▪ Mobility ▪ Flexibility ▪ Instant access

CHAPTER THREE

3 WIRELESS LAN STANDARDS

3.0 INTRODUCTION

Wireless technologies conform to a variety of standards and offer varying levels of security features. The principal advantages of standards are to encourage mass production and for interoperability of products from different vendors. For this paper, the discussion of wireless standards is limited to the IEEE 802.11 family.

3.1 THE IEEE 802.11 FAMILY OF STANDARDS

IEEE 802.11 is a family of standards for wireless local area network (WLAN) computer communication, first created in 1997 by the Institute of Electrical and Electronics Engineers (IEEE) LAN/MAN Standards Committee (IEEE 802) in the 5 GHz and 2.4 GHz public spectrum – Industrial, Scientific and Medical (ISM) - bands.
The 802.11 specifications is the fundamental standard for WLAN. The standard defined the following functions and technologies: WLAN architecture, MAC layer services such as association, re-association, authentication and privacy, frame formats, signalling functions, and WEP algorithm. It also defined what comprises a Basic Service Set (BSS) – two or more fixed, portable, and/or moving nodes or stations communicating with each other over the air within a range, and specified two configuration modes: ad hoc and infrastructure. The 802.11 was designed to support medium-range, higher data rate applications, such as Ethernet networks, and to address mobile and portable stations.

3.1.0 IEEE 802.11b

802.11 only supported a maximum network bandwidth of 2 Mbps - too slow for most applications. In July 1999, IEEE expanded on the original 802.11 standard creating the 802.11b specification. 802.11b supports bandwidth up to 11 Mbps, which is comparable to traditional Ethernet. It operates at the same 2.4 GHz unlicensed frequency band as the original 802.11 standard using direct sequence spread-spectrum (DSSS) technology.

3.1.1 IEEE 802.11a

While 802.11b was in development, IEEE created a second extension to the original 802.11 standard called 802.11a. 802.11b gained popularity much faster than 802.11a even, though; they were created at almost the same time. 802.11b is more cost effective than 802.11a, as a result, 802.11a are commonly found on business networks whereas 802.11b serves the home market. 802.11a supports bandwidth up to 54 Mbps and operates in a licensed frequency spectrum around 5 GHz using orthogonal frequency division multiplexing (OFDM) technology to reduce interference. Comparatively, 802.11a covers a shorter range and has more difficulty penetrating walls and other obstacle as it operates at a higher frequency than 802.11b. The two technologies are incompatible with each other as they operate at different frequencies.

3.1.2 IEEE 802.11g

In 2003, the IEEE published 802.11g amendment. 802.11g attempts to combine the best of both 802.11a and 802.11b. 802.11g supports bandwidth up to 54 Mbps, and it operates at the 2.4 GHz frequency for greater range, using OFDM technologies. 802.11g is backwards compatible with 802.11b, by still supporting the complimentary code key (CCK) modulation.

3.1.3 IEEE 802.11n

The newest IEEE 802.11 family of standards is 802.11n. It was designed to improve on 802.11g in the amount of bandwidth supported by utilizing multiple transmitter and receiver antennas – called multiple input, multiple output (MIMO) technology - instead of one. It is anticipated that 802.11n connections should support data rates of over 100 Mbps when finalized. With its increased signal intensity, 802.11n will offer somewhat better range over earlier 802.11 standards, and it will be backward compatible with 802.11g.

3.2 OTHER IEEE 802.11 WORKING GROUP STANDARDS

The IEEE standards (802.11a, 802.11b, 802.11g and 802.11n) discussed above are the general purpose ones in the world of wireless networking, and are referred to as the Wi-Fi standards. Beside these four general-purpose Wi-Fi standards, other IEEE 802.11 working group standards like 802.11h, 802.11j and 802.11i exit. They are extensions or offshoots of Wi-Fi technology and each serve a very specific purpose. However, there are

various other standard tasks and WGs involved with promoting the overall functionality of the 802.11 protocol.

3.2.0 THE IEEE 802.11i STANDARD

Ratified on June 24, 2004, IEEE 802.11i – also referred to as WPA2 - is an important standard that directly addressed security limitations in the 802.11 protocols. It superseded the previous security specification, Wired Equivalent Privacy (WEP), which was shown to have severe security weaknesses. IEEE 802.11i is based on the Wi-Fi Protected Access (WPA), which is a short term solution for the WEP weaknesses. 802.11i makes use of the Advanced Encryption Standard (AES) block cipher; WEP and WPA use the RC4 stream cipher. The AES (CCMP) protocol provides WLANs with a stronger encryption (confidentiality) capability, and message integrity than WPA (TKIP). Also, it incorporates replay protection. The future of WLAN deployments is moving towards CCMP as the accepted compliance standard.

The IEEE 802.11i has the following key components:

- **Temporal Key Integrity Protocol (TKIP):** a data-confidentiality protocol designed to improve the security of products that implemented WEP. TKIP uses a message integrity code, called Michael, which helps devices to authenticate that the data are coming from the claimed source. Also, TKIP uses a per-packet key mixing function to de-correlate the public initialization vectors (IVs) from weak-keys. TKIP uses the RC4 stream cipher with 128-bit keys for encryption and 64-bit keys for authentication. TKIP mitigates the WEP key derivation vulnerability significantly, but does not provide complete resolution for the weaknesses.

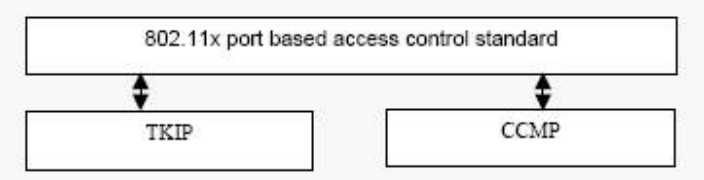
- **Counter-Mode/CBC-MAC Protocol (CCMP):** a data-confidentiality protocol that handles packet authentication as well as encryption. AES counter mode and Cipher Block Chaining Message Authentication Code (CBC-MAC) are two sophisticated cryptographic techniques. CCMP uses AES in counter mode for confidentiality and CBC-MAC for authentication and integrity. This gives a robust security protocol between the mobile client and the access point. AES on its own is a very strong cipher, but with counter mode it is difficult for an eavesdropper to spot patterns. Also the CBC-MAC message integrity method ensures that messages are not tampered with. In IEEE 802.11i, CCMP uses a 128-bit key. CCMP protects some fields that aren't encrypted. The additional parts of the IEEE 802.11 frame that get protected are known as additional authentication data (AAD). AAD includes the packets source and destination and protects against attackers replaying packets to different destinations.

- **IEEE 802.1x**: is simply a standard for passing EAP over a wired or wireless LAN. IEEE 802.1x offers an effective framework for authenticating and controlling user traffic to a protected network, as well as varying encryption keys

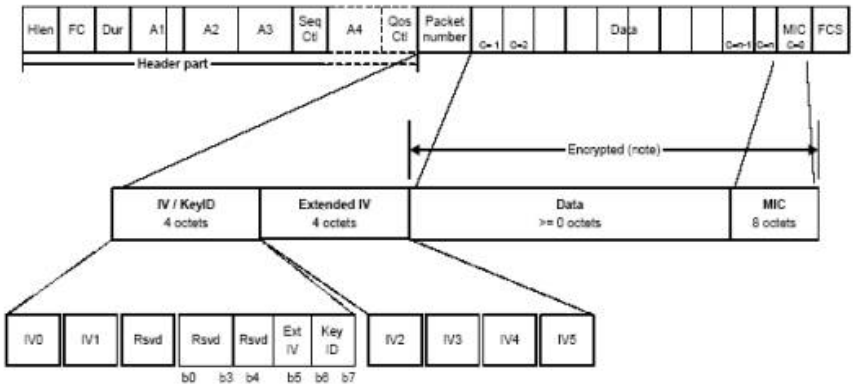
dynamically. It is included in the 802.11i standard to provide MAC layer security enhancements. 802.1X ties a protocol called EAP (Extensible Authentication Protocol) to both the wired and wireless LAN media and supports multiple authentication methods.

- **EAP encapsulation over LANs (EAPOL):** is the key protocol in IEEE 802.1x for key exchange. It allows WLAN clients to communicate with an authentication server to validate their credentials, and supports strong mutual authentication and key management. There are two main EAPOL-key exchanges defined in IEEE 802.11i: the 4-way handshake and the group key handshake.

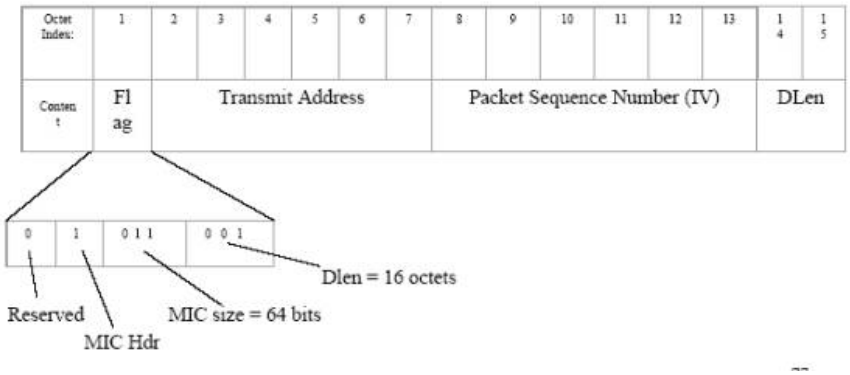
Figure 6 below is a diagram depicting the IEEE 802.11i protocol structure:
IEEE 802.11i Components:



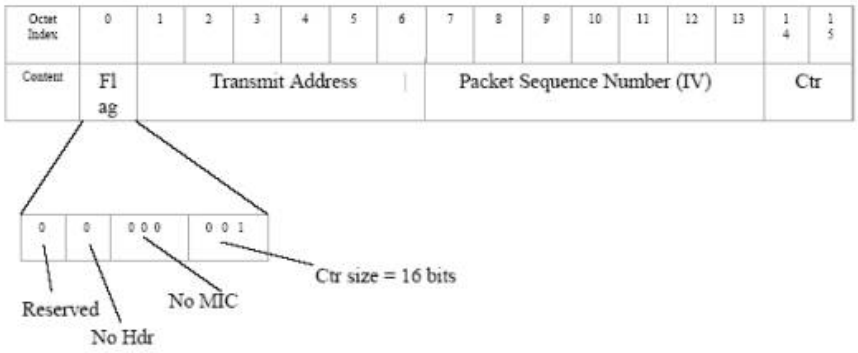
CCMP MPDU Format



CCMP CBC-MAC IV format



CCMP CTR Format



TKIP MPDU Format

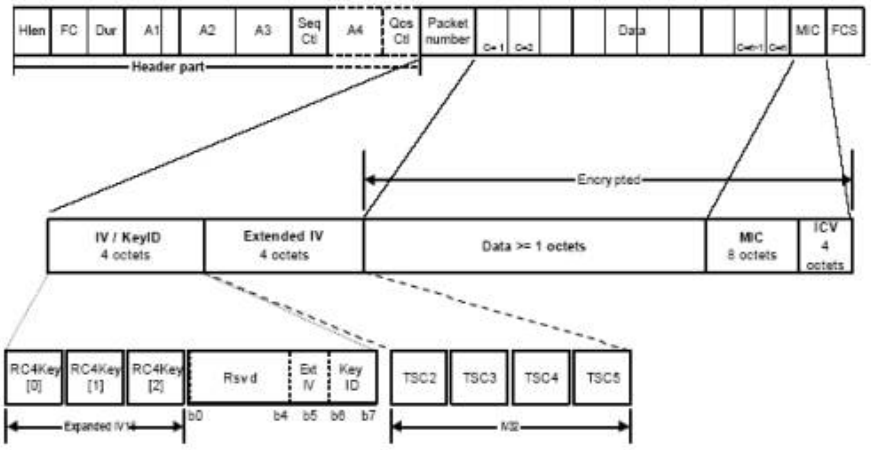


Figure 6 Protocol Structure - IEEE 802.11i: WLAN Security Standards**.**
Source: Javvin. [17]

3.3 THE 802.1x AUTHENTICATION PROCESS

IEEE 802.1x provides a framework to authenticate and authorize devices connecting to a network. It prevents a device from accessing the network until such device is authenticated. In WLANs, three entities are involved in the authentication process: *a supplicant* – which is the user or client that needs to be authenticated, *the authentication server* – typically a RADIUS server that does the authentication, and *the authenticator* – a device in between the other two, for example a wireless access point. IEEE 802.1X also provides a framework to transmit key information between authenticator and supplicant. The 802.1X protocol is an end-to-end communication authentication process between the supplicant and the authentication server (AS), the authenticator serves as the channel for the passage of the authentication messages. EAP encapsulation over LAN (EAPOL) protocol is the means of communication between the supplicant and the authenticator, whereas the authenticator and the AS communicate through RADIUS. 802.1x protocol

supports several other different authentication protocols in addition to RADIUS such as Diameter, and Kerberos. Also, the 802.1x can be implemented with different EAP types. Figure 7 illustrates the communication paths of the supplicant, the authenticator and the authenticator server, and the 802.1X authentication process.

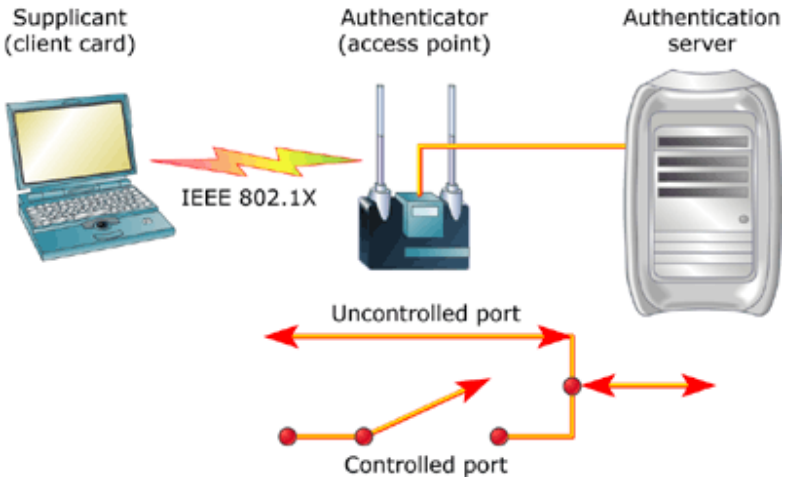


Figure 7 802.1x Authentication Process (WPA2)
Source: Embedded.com [15]

- Supplicant request access with AP.
- Authenticator detects supplicant association and enables the supplicant's port.
- Port is forced into an unauthorized state to forward only 802.1x traffic (all other traffic is blocked).
- The authenticator passes request to the authentication server.
- The authentication server and client exchange authentication messages for server to verify supplicant's identity. Mutual authentication is also possible, where supplicant is verifies the authentication server's identity.
- The authentication server instructs the authenticator via a RADIUS-ACCEPT message to let the supplicant onto the network if it has satisfied the authentication criteria. If not, an RADIUS-REJECT message is sent to the authenticator.
- Upon receipt of the RADIUS-ACCEPT message, the authenticator transitions the supplicant port to an authorized state allowing the supplicant onto the network

The initial 802.11 standard has undergone several revisions since it was ratified, through different task groups of the IEEE 802.11 Working Group (WG), to improve the technology and address security issues. In table 5 shown in the next page, I summarized the existing IEEE 802.11 family of standards.

Table 5 IEEE 802.11 family of standards [10]

Specification	Description	Main Purpose	Pros	Cons
IEEE 802.11 (June, 1997)	The earliest standard, allowing 1-2 Mbps of bandwidth in the 2.4 GHz band; uses FHSS, DSS, and IR in the physical layer, covering typical range of 50-100m.	Basic wireless technology standard		
IEEE 802.11a (Sep., 1999)	Second revision to the original 802.11 standard; bandwidth of 54 Mbps in 5 GHz RF band; uses OFDM; typical range is 50-100m.	Higher Performance	Fast maximum speed; no signal interference as it operates in licensed frequency.	Highest cost; short signal range that is more easily obstructed.
IEEE 802.11b (Sep., 1999)	First revision to the original 802.11 standard; bandwidth of 11 Mbps in 2.4 GHz RF band; uses DSSS/CCK; typical range is 50-100m.	Performance Enhancements	Lowest cost; good signal range that is not easily obstructed	slowest maximum speed; interference with home appliances on the unlicensed frequency band
IEEE 802.11d (2001)	Defines physical layer requirements to satisfy regulatory domains not covered by the existing standards; enable client adjusts its frequencies, power levels and bandwidth accordingly.	Promote Worldwide Use		
IEEE 802.11e (2005)	Defines a set of Quality of Service enhancements for wireless LAN applications through modifications of the Media Access Control (MAC) layer to support applications such as such as VoIP and video.	QOS Enhancements		
IEEE 802.11F (2003)	A standard designed to enforce interoperability of multi-vendor APs within a WLAN network infrastructure. It uses the Inter-Access Point Roaming Protocol, which lets a roaming user transparently switch from one access point to another while moving around.	Interoperability		
IEEE 802.11g (June, 2003)	Fourth revision to the original 802.11 standard; bandwidth of 54 Mbps in 2.4 GHz RF band; uses OFDM/PBCC; typical range is	Higher Performance with 802.11b Backward	Fast maximum speed; good signal range	Costs more than 802.11b; chances of interference on

Specification	Description	Main Purpose	Pros	Cons
		Compatibility	that is not easily obstructed	the unlicensed frequency band.
IEEE 802.11h (2003)	Originally designed to solve regulatory requirements for operations in the 5 GHz band in Europe, but now applies to many other countries. It provides Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) to the 802.11a MAC	European Regulation Compliance		
IEEE 802.11i (June, 2004)	Specification for wireless networks security mechanisms. This standard is based on the AES (Advanced Encryption Standard) and can encrypt transmissions that run on 802.11a, 802.11b and 802.11g technologies.	Security Improvements		
IEEE 802.11j (2004)	Designed to ensure that WLAN operation in the 4.9 to 5 GHz band conform to the Japanese rules for radio use.	Japan Compliance		
IEEE 802.11k (Proposed 2007)	A proposed amendment to IEEE 802.11 standard for radio resource management. It defines and exposes radio and network information to facilitate the management and maintenance of seamless roaming in the WLAN environment.	Radio Resource Management		
IEEE 802.11m (2007)	An initiative to perform editorial maintenance, corrections, improvements, clarifications, and interpretations relevant to documentation for the IEEE 802.11 family specifications.	Editorial Maintenance		
IEEE 802.11n (In progress)	Upcoming industry standard that will significantly improve network throughput over previous standards, such as 802.11b and 802.11g, by using multiple-input multiple-output (MIMO) technology and 40 MHz operation at the physical layer.	Higher Performance	Fastest maximum speed and best signal range; more resistant to signal interference	Costs more than 802.11g; use of MIMO may cause interference with nearby 802.11b/g networks.

Specification	Description	Main Purpose	Pros	Cons
IEEE 802.11r (In progress)	A new fast roaming standard that will facilitate secure mobility by reducing delay in hand-off in WLANs during transitions between access points, thereby supporting applications like voice and video.	Fast BSS Transitions		
IEEE 802.11s (In progress)	An amendment to 802.11 MAC layer to define an architecture and protocol that support both broadcast/multicast and unicast delivery using radio-aware metrics over self-configuring multi-hop topologies.	For Mesh Networking		
IEEE 802.11T (In progress)	Develop recommended practice for the Evaluation of 802.11 Wireless Performance based on a common and accepted set of measurement methods, performance metrics, and test recommendations.	WLAN Performance Prediction		
IEEE 802.11u (In progress)	Amendment to the 802.11 MAC and PHY layers to add features that enable interworking with external networks.	802.11 MAC & PHY Layers Enhancements		
IEEE 802.11v (In progress)	Amendment to 802.11 MAC and PHY layer to support configuration of client devices while connected to IEEE 802.11 networks in a centralized or in a distributed fashion, and create an Access Port Management Information Base (AP MIB).	802.11 MAC & PHY Layers Enhancements		
IEEE 802.11w (In progress)	An amendment standard to 802.11 MAC layer for management frames security enhancement. 802.11w proposes to extend IEEE 802.11i to cover 802.11 management frames as well as data frames.	Security Enhancements		

In the table 5 above, the 'Pros' and 'Cons' columns were used for comparative analysis of the Wi-Fi standards (802.11a, 802.11b, 802.11g and 802.11n) relative to signal strength and range, cost, RF band, and robustness to signal interference.

CHAPTER FOUR

4 WIRELESS LAN VULNERABILITIES, THREATS AND COUNTERMEASURES

4.0 INTRODUCTION

Wireless security is a real challenge for network administrators and information security administrators alike. Unlike the wired Ethernet LANs, 802.11-based wireless LANs broadcast radio-frequency (RF) data for the client stations to hear. Consequently, anyone with the right tools can capture and transmit wireless signals if he is within range.

In other to prevent unauthorized use risk posed by unsecured wireless access points, Wired Equivalent Privacy (WEP) - a low-level data encryption system – was invented for wireless security purposes. WEP protocol protects link level data during wireless transmission between clients and access points. It does not provide end-to-end security, but only for the wireless portion of the connection. WEP uses the stream cipher RC4 for confidentiality, and the CRC-32 checksum for integrity. The encryption keys must match on both the client and the access point for frame exchanges to succeed. WEP may be applied in 64 or 128 bit mode, in which the WEP keys used are usually 40 or 104 bits long, concatenated with a 24 bit initialisation vector (IV). WEP has many known vulnerabilities resulting from its use of static keys, and a number of weak initialisation vectors.

A successor to WEP is Wi-Fi Protected Access (WPA). Introduced in 2003 as an intermediate measure to take the place of WEP while 802.11i was prepared, WPA avoids most of WEP's vulnerabilities by making heavier use of dynamic/temporal keys, using the Temporal Key Integrity Protocol (TKIP). It encrypts data using the RC4 stream cipher, with a 128-bit key and a 48-bit initialization vector (IV).

Ratified on 24 June 2004, Wi-Fi Protected Access 2 (WPA2) is the follow-on security method to WPA. WPA2 uses the Advanced Encryption Standard (AES). There is virtually no known wireless attack against AES. CCMP is the security standard used by AES. CCMP computes a Message Integrity Check (MIC) using a proven Cipher Block Chaining (CBC) technique. Messages are encrypted using a 128-bit secret key and a 128-bit block of data. The result is an encryption scheme that is very secure.

This chapter evaluates the current known IEEE 802.11 wireless LAN vulnerabilities and threats. It ends with sections that explain how to discover wireless network threats, and what to do to reduce or eliminate the threats. Security mechanisms of wireless LANs are not within the scope of this work. The aim is to encourage network and security administrators to carry out risk assessment so as to identify the risks and threats relating

to their information system, and then deploy adequate control measures to reduce or eliminate possible risk.

4.1 WLAN SECURITY ATTACKS

Attacks on wireless LANs are aimed at the confidentiality and integrity of an information, and network availability. These security attacks can be passive or active.

- **Passive attack:** consist of unauthorized access to an asset or network for the purpose of eavesdropping or traffic analysis, but not to modify its content. This is tricky to detect because data is unaffected. Consequently, emphasis is on prevention (encryption) not detection.

- **Active attacks:** an unauthorized access to an asset or network for the purpose of either making modifications to a message, data stream, or file, or to disrupt the functioning of a network service.

The diagram below shows a general taxonomy of WLAN security attacks.

.

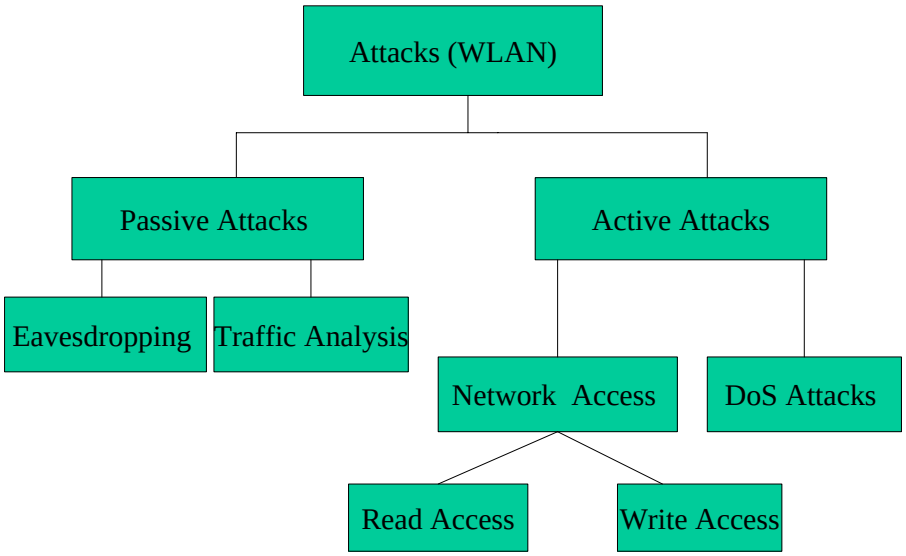


Figure 8 General Taxonomy of WLAN security attacks
Source: K. Fleming [10, 25]

4.1.0 PASSIVE ATTACKS

There are two phases to an attack. The first phase is referred to as the reconnaissance phase, this is a passive attack. During the reconnaissance phase, the goal of an attacker is to discover a target network, and then gather information about the network. The attacker does this in a way that is unnoticeable. However, some of the means of reconnaissance can be detected by an intrusion detection system.

There are two methods used in executing undetectable passive attack: eavesdropping, and traffic analysis.

- **Eavesdropping:** is the capability to monitor transmissions for message content. An attacker listens and intercepts wireless signals between the AP and wireless client.
- **Traffic analysis:** is the capability to gain intelligence by monitoring transmission for patterns of communications, or perform packet analysis. This can be carried out even when the messages are encrypted and cannot be decrypted

There abound a lot of sniffing tools that can aid an attacker in achieving his goal. Sniffing tools are the most effective means to monitor what is happening on a network. Undetectable, sniffing can perform two principal functions: packet capture and packet analysis and display. By analyzing a packet, an attacker is informed about the capabilities of a network, and can gather all sorts of confidential information for exploitation of an organization. Packet capture enables an attacker to recover WEP keys in few minutes, thereby providing him with the capability to read all the data passing between the wireless client and the AP. A wide variety of sniffing tools exit - both as priced and freeware.

War Driving is another technique that can be used for reconnaissance. War Driving is the act of searching for the existence of Wireless LAN (802.11) Networks while driving around a city. Simply, it's locating and logging wireless access points while in motion. With programs like NetStumbler (Windows), Kismet or SWScanner (Linux), FreeBSD, NetBSD, OpenBSD, and DragonFly BSD, and KisMac (Macintosh) and GPS, a WLAN can be detected, plotted and posted to a website. Table 6 provides a list of some popular sniffing tools.

Table 6 Sniffing Tools [10, 32]

Tool	Capability	Source	Notes
tcpick - v0.2.0	Packet capture	http://tcpick.sourceforge.net/	NETwork DUmp data Displayer and Editor for tcpdump tracefiles (Linux, Free BSD, Open BSD)
Sniffit - v0.3.7b	Packet capture	http://reptile.rug.ac.be/~coder/sniffit/sniffit.html	Can track, reassemble and reorder tcp streams (Linux based)

Tool	Capability	Source	Notes
TCPDUMP -v3.8.3	Packet capture & analysis	http://www.tcpdump.org/	Prints out the headers of packets or save packets for later analysis
Sniffit - v0.3.7b	Packet capture	http://reptile.rug.ac.be/~coder/sniffit/sniffit.html	Packet capture library (developed on LINUX), has various functions not offered in any other non-commercial sniffer.
SLSNIF - v0.4.1	Packet capture	http://www.azstarnet.com/	Packet capture library (Linux based)
AirSnort	War Driving (Packet capture & analysis)	Open-source: http://airsnort.shmoo.com	Recovers encryption keys (Windows or Linux Based)
WEBCrack	Packet Analysis	Open-source: http://wepcrack.sourceforge.net	Recovers WEP keys (PERL based scripts)
Sniffer Wireless	Packet Capture & Display	Network Associates (commercial product)	Capability to decrypt WEP-based traffic and quickly detect Rogue APs. (Windows and PDA based)
KRIPP - v0.6	Network passwords capture & display	http://konst.org.ua/kripp	Written in Perl, it uses only the tcpdump utility as an underlying traffic interceptor
Net Stumbler	War Driving; Network Discovery; Packet Capture	Open-source: http://netstumbler.com	Records SSIDs in beacons and interfaces with GPS to map a network. (Windows-based)
Kismet	War Driving; Network Discovers; Packet Capture	Open-source: http://kismetwireless.net /	Most complete War Driving tool. Works with most client cards that support Rfmon mode. Operates on most OS systems.
Wellenreiter	War Driving; Network Discovers; Packet Capture	Open-source: http://www.wellenreiter.net	Perl and C++ based for Linux and BSD systems.
httpcapture -v0.4	Packet capture & analysis/display	http://www.steve.org.uk/Software/httpcapture/	Plugins for capturing, decoding, and displaying some network logins
Ethereal - v0.10.4	Packet capture; Protocol analyzer	http://www.ethereal.com/	Free network protocol analyzer for Unix and Windows

4.1.1 ACTIVE ATTACKS

An active attack is one whereby an unauthorised change of the system is attempted. This could include, for example, the modification of transmitted or stored data, the creation of new data streams or limiting an organization's network availability. Active attacks may take the form of one of four types (or combination): masquerading, replay, message modification, and denial-of-service (DoS).

- **Masquerading:** An active attack in which the attacker impersonates an authorized user and thereby gains certain unauthorized privileges. It could be attempted through the use of stolen logon IDs and passwords, through finding security gaps in programs, or through bypassing the authentication mechanism. The attempt could come from an insider, an employee for example, or an outsider through the public network. Once entry is made and the right access to the organization's critical data is gained, the attacker may be able to modify and delete software and data, and make changes to network configuration and routing information.

- **Replay:** Also known as Man-in-the-Middle attack, a replay attack is one whereby the attacker monitors transmissions (passive attack) and retransmits messages as the legitimate user to trick the receiver into unauthorized operations such as false identification or authentication or a duplicate transaction.

- **Message modification:** The attacker alters a legitimate message by deleting, adding to, changing, or reordering it.

- **Denial-of-service:** The attacker prevents or prohibits the normal use or management of communications facilities. DoS attacks can range from physical destruction of equipment, disruption of certain network services to a specific person or system, prevention of a particular individual from accessing a service to flooding a network, thereby preventing legitimate network traffic. Below are some common practices for accomplishing DoS:
    - Deploy radio-jamming equipment
    - Saturate a network' bandwidth by continually broadcasting frames
    - Conduct disassociation/de-authentication attacks
    - Conduct transmit duration attacks by configuring the transmit duration field to a maximum of 30-packets-per-second rate
    - Saturate AP tables by flooding associations

- Setup a rogue AP and associate users to a bogus network to establish a Man-in-the-Middle attack

To accomplish an active attack, an attacker must have access to the target network with a read and write access right. The overall goal is to have access to network resources or to capture and decrypt data - if encrypted. Read access enables an attacker to intercept and read traffic from a network, thereby providing him with the potential to carry attacks on encryption, authentication, and other protection methods. Having discovered a target network through reconnaissance, and having captured unencrypted or encrypted traffic by sniffing, an attacker has the potential to gain key material and recover encryption keys. Acquisition of the encryption keys provide an attacker full access to the target network, and with write access he has the capability to send traffic to a network entity. The following are some goals of an attacker with network read and write access:

- Recover encryption keys
- Recover key streams generated by encryption keys
- Inject data packets: write encrypted data by replaying captured key stream
- Encrypt data with key and inject the data to the network
- Install spying software on a wireless client and have the capability to read the results
- Setup a rogue AP and control network parameters - such as encryption keys
- Bypass authentication schemes:
  - By deploying MAC address spoofing to evade MAC address filtering
  - By deploying shared-key authentication bypass attacks
  - By performing LEAP Dictionary attacks if network is using 802.1x for authentication
  - By performing PEAP Man-in-the-Middle attacks if network is using 802.1x for authentication
- Install malicious code on a wireless client

WLAN technology on its own has inbuilt security problems in its architecture, as the APs and the clients must advertise their existence through beacon frames. This makes a signal exposed to anyone within range and is capable of listening. Shielding a WLAN by locating it within an area where the RF signals are not cable of escaping minimizes the risk of unauthorized access. However, this is not always a viable solution. As a result other security methods must be deployed such as strong access control and encryption technology.

The techniques for gaining unauthorized access to a WLAN are well-known security issues. Many of these security issues exploiting WLANs have recently been corrected with technology developments in the 802.11i standard. Table 7 is a list of all known security attacks deployed against WLANs categorized by type of threat, and mapped to associated hacker methods and tools.

Table 7 Wireless Security Attacks [45]

❖ **Access control attacks**

These attacks attempt to penetrate a network by circumventing filters and firewalls to obtain unauthorized access. MAC spoofing (also known as identity theft) and Rogue Access Points are more common among these. War Driving, as explained in section 4.1.0 is a technique used for reconnaissance.

Attack	Description	Methods and Tools
War Driving	Discovering wireless LANs by listening to beacons or sending probe requests, thereby providing launch point for further attacks.	DStumbler, KisMAC, MacStumbler, NetStumbler, WaveStumbler,
Rogue Access Points	Installing an unsecured AP inside firewall, creating open backdoor into trusted network.	Any hardware or software
AP Ad Hoc Associations	Connecting directly to an unsecured station to circumvent AP security or to attack station.	Any wireless card or USB adapter
MAC Spoofing	Reconfiguring an attacker's MAC address to pose as an authorized AP or station.	Bwmachak, SirMACsAlot, SMAC,Wellenreiter, wicontrol
802.1X RADIUS Cracking	Recovering RADIUS secret by brute force from 802.1X access request, for use by evil twin AP.	Packet capture tool on LAN or network path between AP and RADIUS server

❖ **Integrity attacks**

These attacks send forged/modified control, management or data frames over wireless to mislead the recipient or facilitate another type of attack. Denial-of-service attacks are the most common of the attacks that can be facilitated by this. DoS has been explained in section 4.1.1. 802.11 Frame Injection, 802.11 Data Replay, and 802.11 Data Deletion are the commonest amongst integrity attacks. Replay and message modification have been briefly explained in section 4.1.1.

Attack	Description	Methods and Tools
802.11 Frame Injection	Crafting and sending forged 802.11 frames.	Airpwn, File2air, libradiate, void11, WEPWedgie, wnet dinject/reinject
802.11 Data Replay	Capturing 802.11 data frames for later (modified) replay.	Capture + Injection Tools 802.11

Attack	Description	Methods and Tools
802.11 Data Deletion	Jamming an intended receiver to prevent delivery while simultaneously spoofing ACKs for deleted data frames.	Jamming + Injection Tools
802.1X EAP Replay	Capturing 802.1X Extensible Authentication Protocols (e.g., EAP Identity, Success, Failure) for later replay.	Wireless Capture + Injection Tools between station and AP
802.1X RADIUS Replay	Capturing RADIUS Access-Accept or Reject messages for later replay.	Ethernet Capture + Injection Tools between AP and authentication ser

❖ **Confidentiality attacks**

These attacks attempt to intercept private or sensitive information sent over wireless associations - whether sent in the clear or encrypted by 802.11 or higher layer protocols. Eavesdropping, WEP Key Cracking, Evil Twin AP (poorly-understood attack) and Man-in-the-Middle (a form of active eavesdropping) are the most common attacks in this category. As shown in general taxonomy of WLAN security attacks (figure 8), eavesdropping is classified as passive attack whereas the rest are members of active attack class.

Attack	Description	Methods and Tools
Eavesdropping	Capturing and decoding unprotected application traffic to obtain potentially sensitive information.	bsd-airtools, Ethereal, Ettercap, Kismet, commercial analyzers
WEP Key Cracking	Capturing data to recover a WEP key using brute force or Fluhrer-Mantin-Shamir (FMS) cryptanalysis.	Aircrack, AirSnort, chopchop, dwepcrack, WepAttack, WepDecrypt, WepLab
Evil Twin AP	Masquerading as an authorized AP by beaconing the WLAN's service set identifier (SSID) to lure users.	cqureAP, HermesAP, HostAP, OpenAP, Quetec, WifiBSD
AP Phishing	Running a phony portal or Web server on an evil twin AP to "phish" for user logins, credit card numbers.	Airsnarf, Hotspotter
Man-in-the-Middle	Running traditional man-in-the middle attack tools on an evil twin AP to intercept TCP sessions or SSL/SSH tunnels.	dsniff, Ettercap

❖ **Authentication attacks**

Intruders use these attacks to steal legitimate user identities and credentials to access otherwise private networks and services. Dictionary attack and brute force attack are the two most common techniques employ here by the attackers to achieve their objectives.

Once succeeded, the attacker impersonates (masquerading) as an authorized user, thereby gaining certain unauthorized privileges. More on masquerading can be found on section 4.1.1.

Attack	Description	Methods and Tools
Shared Key Guessing	Attempting 802.11 Shared Key Authentication with guessed vendor default or cracked WEP keys.	WEP Cracking Tools
PSK Cracking	Recovering a WPA PSK from captured key handshake frames using a dictionary attack tool	coWPAtty, KisMAC, wpa_crack, wpa-sk-bf
Application Login Theft	Capturing user credentials (e.g., e-mail address and password) from cleartext application protocols.	Ace Password Sniffer, Dsniff, PHoss, WinSniffer
VPN Login Cracking	Recovering user credentials (e.g., PPTP password or IPsec Preshared Secret Key) by running brute-force attacks on VPN authentication protocols.	ike_scan and ike_crack (IPsec), anger and THC-pptpbruter (PPTP)
Domain Login Cracking	Recovering user credentials (e.g., Windows login and password) by cracking NetBIOS password hashes, using a brute-force or dictionary attack tools.	John the Ripper, L0phtCrack, Cain
802.1X Identity Theft	Capturing user identities from cleartext 802.1X Identity Response packets.	Capture Tools
802.1X LEAP Cracking	Recovering user credentials from captured 802.1X Lightweight EAP (LEAP) packets using a dictionary attack tool to crack the NT password hash.	Anwrap, Asleap, THCLEAPcracker
802.1X EAP	Downgrade Forcing an 802.1X server to offer a weaker type of authentication using forged EAP-Response/Nak packets	File2air, libradiate
802.1X Password	Using a captured identity, repeatedly attempting 802.1X authentication to guess the user's password.	Password Dictionary

- **Availability attacks**

These attacks attempt to inhibit or prevent legitimate use of wireless LAN services. The most common type of availability attack is the denial-of-service (DoS) attack, known as RF Jamming in the wireless world. A brief description of DoS has been given in section 4.1.1.

Attack	Description	Methods and Tools
AP Theft	Physically removing an AP from a public space.	"Five finger discount"
RF Jamming	Transmitting at the same frequency as the target WLAN, perhaps at a power that exceeds regulation Equivalent Isotopically Radiated Power (EIRP).	RF Jammer, Microwave oven, AP with Alchemy/HyperWRT firmware
Queensland DoS	Exploiting the CSMA/CA Clear Channel Assessment (CCA) mechanism to make a channel appear busy.	An adapter that supports CW Tx mode, with a lowlevel utility to invoke continuous transmit
802.11 Beacon Flood	Generating thousands of counterfeit 802.11 beacons to make it hard for stations to find a legitimate AP.	Fake AP
802.11 Associate / Authenticate Flood	Sending forged Authenticates or Associates from random MACs to fill a target AP's association table	Airjack, File2air, Macfld, void11
802.11 TKIP MIC Exploit	Generating invalid TKIP data to exceed the target AP's MIC error threshold, suspending WLAN service.	File2air, wnet dinject
802.11 Deauthentic-ate Flood	Flooding station(s) with forged Deauthenticates or Disassociates to disconnecting users from an AP.	Airjack, Omerta, void11
802.1X EAPStart Flood	Flooding an AP with EAP-Start messages to consume resources or crash the target.	QACafe, File2air, libradiate
802.1X EAPFailure	Observing a valid 802.1X EAP exchange, and then sending the station a forged EAPFailure message.	QACafe, File2air, libradiate
802.1X EAP-of-Death	Sending a malformed 802.1X EAP Identity response known to cause some APs to crash.	QACafe, File2air, libradiate
802.1X EAP Length Attacks	Sending EAP type-specific messages with bad length fields to try to crash an AP or RADIUS server.	QACafe, File2air, libradiate

4.2 PUTTING ATTACKS INTO PERSPECTIVE: RISK ANALYSIS

Risk is chances of threats in getting benefits from defects or weaknesses which are causes of losses and/or damages to assets or groups of assets, effecting an organization directly or indirectly. Risk analysis is an effective tool in WLAN threat management. With this a good security policy can be derived and implemented to defend the WLAN against

possible attacks. On-going monitoring and periodic testing can then be used to verify that a deployed WLAN meets defined objectives. Vulnerabilities discovered in the process are then (re)analyzed so as to refine the policies and/or apply fixes. This iterative process is illustrated in the diagram (figure 9) shown below.

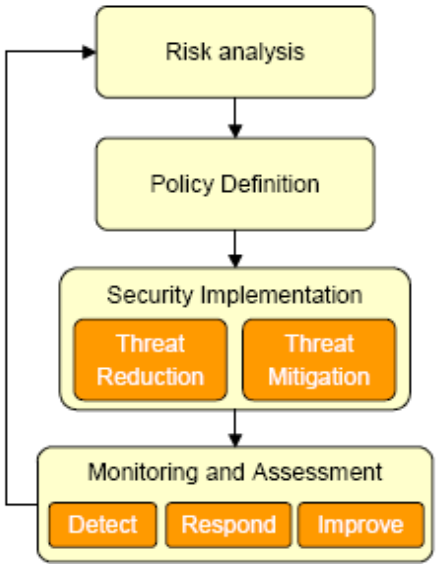


Figure 9 Security as a process
Source: L. Phifer [44]

It's extremely important to understand the attacks that might affect a network. However, it should be noted that some attacks are less likely or more damaging than others. More also, it should be noted that it is not practical or possible to defend any network against all possible attacks. A more realistic goal is to reduce associated risk to an acceptable level. Risks are put into perspective by identifying one's own WLAN's vulnerabilities - the probability that attacker will exploit them - and business impact would occur. The following steps/points are necessary in performing risk analysis.

- Define business needs
- Document who needs WLAN access, and where?
  - Identify users or groups permitted to use 802.11 at the office, on the road, and at home.
- Determine resources reached over wireless
- Which applications, databases, and shares must be opened to wireless users, and when?
- Next, quantify new business risks caused by adding wireless.
- What information do those services and databases contain?
- Consider data that resides on wireless stations and flows over wireless links
- For each asset, estimate the likelihood of compromise and potential cost to business, using quantifiable metrics like downtime, recovery expenses, etc.

Completion of this process provides a prioritized list of at-risk assets. Base on this, a security policy that defends important assets from wireless-borne attack, balancing cost/benefit and residual risk can be written. Next step is to select, install, and configure countermeasures that implement and enforce the security policy.

4.3 CONDUCTING A VULNERABILITY ASSESSMENT

A vulnerability assessment is an explicit study that uses penetration testing and observation to identify security weaknesses that could be exploited, and the risks. The results obtained are then evaluated to determine severity and steps to reduce or eliminate the threats. To be truly effective, assessments should be carried out regularly to spot out newly-introduced vulnerabilities and verify that installed security measures are working as intended. Assessments may be performed by in-house or third-party staff, with full, partial, or no knowledge of the organization network and security implementation.

In the following sections, I present the techniques and tools that can be useful for conducting a WLAN vulnerability assessment: from wireless device discovery and penetration testing, to security event monitoring and spectrum analysis. A sample worksheet, provided in appendix, illustrates how assessment results can be documented for review and remediation.

4.3.0 WLAN DISCOVERY

The first step in any vulnerability assessment is identification of all wireless devices near the site(s) under test. By so doing, all authorized devices will be isolated from the rest - where as the authorized will be subjected to further assessment; the rest will be scrutinized to determine ownership, impact on WLAN operation, and potential threat.

Wi-Fi Stumblers – which are free, easy to use for simple tasks, and available for most Operating Systems – is one of the tools that can be used for this purpose. One limitation of Stumblers is that they can find APs, but not Stations or non-802.11 interference sources. They may supply GPS latitude/longitude, but cannot pinpoint indoor location. For complete vulnerability assessment, a portable WLAN Analyzer that can scan all RF channels, export details about all wireless devices, accurately plot results on floor plans, and make it easy to find newly-discovered devices is ideal.

Using the discovery tools, make a list of observed 802.11 and other devices. Record the following parameters: a) for APs, record their ESSID, MAC address, IP address, channel, SNR, and observed 802.11/802.1X settings, b) generate a similar list of discovered Stations, noting whether they are associated to an Ad Hoc node, probing for multiple ESSIDs, and/or actively associated with specific AP(s). For non-802.11 devices, a spectrum analysis is used to fingerprint type. To locate and indentify the unauthorized devices - including the owner -, use a "find" tool (or WIPS with rogue mapping).

4.3.1 VULNERABILITY/PENETRATION TESTING

The overall objective of penetration testing is to discover areas of the enterprise network where intruders can exploit security vulnerabilities. These tests are typically performed using automated tools that look for specific weaknesses, technical flaws or vulnerabilities to exploit, with the results presented to the system owner with an assessment of their risk to the networked environment and a remediation plan highlighting the steps needed to eliminate the exposures. Various types of penetration testing are necessary for different types of network devices. For example, a penetration test of a firewall is different from a penetration test of a typical user's machine. Even a penetration test of devices in the DMZ (demilitarised zone) is different from performing a scan to see whether network penetration is possible. The type of penetration test should be weighed against the value of the data on the machine being tested and the need for connectivity to a given service.

Tools like Nmap or Superscan are used to scan devices and ports. Active devices are fingerprinted to identify operating systems, server programs, accounts, and shares using tools like Winfingerprint and Xprobe. WEP traffic may be analyzed with a tool like Aircrack-ptw, while PSK authentication messages may be analyzed with coWPAtty. 802.1X/EAP user IDs may be recorded and passwordbased EAPs may be tested using a tool like Asleap.

4.3.2 USING WIRELESS INTRUSION PROTECTION SYSTEM (WIPS) TO MONITOR ACTIVITY

WIPS is a network monitoring tool that runs round the clock and pinpoints attacks or attempted attacks on wireless network. It is an extension of the advanced protection found in wired firewall and virtual private network security systems, but with a focus on wireless local area networks (WLANs). It uses traffic analysis to keep track of attack signatures, protocol errors, atypical behaviour, and policy violations, generating alerts and defensive actions. Within a given RF band, WIPS sensors listen to the air - both in local and remote offices - decoding 802.11/802.1X protocols and analyzing all wireless activity. WIPS servers understand wireless attacks and can enforce real-time wireless security policies - for example, it automatically locks down rogue devices. Intrusion alerts and related evidence are reported to a central database for future reference during routine compliance reporting or post-breach forensic analysis.

WIPS can be extremely useful during a WLAN vulnerability assessment, as WIPS can triangulate a discovered device's location on a floor plan, making searches more efficient. WIPS helps to spot misconfigured devices, actual attacks that may have occurred recently, problem-prone locations and devices that may warrant additional scrutiny and on-going risky user behaviour by generating policy-based alerts. Also during penetration testing, WIPS can confirm that tests are working as expected. It can teach how to recognize signs of attack. It can record information needed for incident investigation or understanding of its impact, long after the attack ends. WIPS can even combine current

and past observations to suggest how to mitigate threats. Penetration test results can, in the other hand, help to fine-tune WIPS.

4.3.3 USING WIRELESS ANALYZERS FOR INVESTIGATION

WLAN and spectrum analyzers play important role during vulnerability assessment, from start to finish. A combination gives a tool that offers both performance and security monitoring functions for wireless LANs. Where as WLAN analyzers help capture packet on the air to display important information such as the list of access points and stations, per-node and per-channel statistics, signal strength, a list of packets and network connections, protocol distribution charts, etc., spectrum analyzers dig into non-802.11 transmissions – for example, RF interference coming from microwave oven. Portable (laptop or handheld-based) analyzers are useful while penetration tests are in progress as they provide a mobile platform for device discovery, traffic capture, and other eye-raising wireless activity. Remote analyzers - WIPS sensor or AP-based - can help to further investigate potential vulnerabilities at the end of tests. Portable analyzers are efficient for on-site investigation, while remote analyzers are more cost-effective for off-site investigation.

4.4 PUTTING ASSESSMENT RESULTS TO WORK

Wireless vulnerability assessment is an effective tool on which a good security policy that can defend organization assets is hinged on. Assessment reports usually rank identified vulnerabilities by severity and recommend countermeasures. These countermeasures are then installed and configured to implement and enforce the security policy. This is achieved through station and AP hardening, rogue detection and elimination, and deployment of 802.11/802.1X security measures.

- **Rogue Management:** In most cases, during vulnerability assessments, some unknown wireless devices are discovered. Assessment results always list all the discovered devices and their observed properties to facilitate threat assessment, classification, and elimination. For rogue management, a report for example might recommend classifying low-SNR APs as Neighbors so as to use ACLs to block unauthorized associations. It may, as well, recommend physical removal of discovered high-SNR APs connected to the corporate network without permission and stand-alone draft 802.11n APs installed by employees. As a proactive measure rogue management, a report can recommend adding suspicious stations to WIPS watch list to escalate any future alerts pertaining to them. Also, automated actions - like network connectivity checks and temporary wireless blocking - may be configured for malicious rogues that lie off-premises but within RF range.

- **WLAN Infrastructure Hardening:** Wireless access points (WAPs), switches, gateways, web portals, DNS/DHCP servers, and other devices connected to WLANs often need to be hardened to resist network-borne attacks. Recommendations of penetration test results might be countermeasures, like: changing AP defaults, disabling unnecessary services, eliminating unused ports, using stronger admin passwords or authentication methods, disabling wireless-side management and restricting wired-side to specific IP addresses and/or VLANs, using AP filters to prevent route updates or LAN broadcasts from getting to the wired network, fine-tuning DoS thresholds, and applying firmware upgrades/patches.

- **Station Hardening:** Wireless clients such as laptops, PDAs, wireless-enabled desktops, scanners, cameras, printers, VoFi phones, and field terminals also require hardening. Countermeasures and best practices - like personal firewalls - typically used to defend Internet-connected clients, are generally recommended for WLAN clients as well. WLAN-specific vulnerabilities indentified during penetration tests might require that further recommendations like configuring stations to associate only to corporate ESSIDS in infrastructure mode, checking 802.1X server certificates to avoid rogue AP is necessary. Deployment of host-resident Wi-Fi Intrusion Prevention program on every client helps to disconnect unsafe associations automatically. Also, WEP-only capable wireless adapters need to be scraped, and those with vulnerable drives should be patched.

- **Securing Data In Transit:** Assessments help to verify adherence to the corporate security policy, and also identify weaknesses in that policy – if there is any. Test results should be able to list all wireless devices that associate without the mandatory corporate encryption technique. Recommendation could be blocking of employee associations to guest WLAN if the risk analysis shows that the risk is too high. In alternative, guests might be advised to protect themselves with VPN tunnels. Tests report may recommend alternatives to reduce over-the-air vulnerabilities and comply with data privacy regulations. WPA is advised for WLANs with legacy products. However, WPA2 is better for robust data privacy and integrity. But the best practice here is to secure data using VPN for off-site and WPA2 for on-site.

- **Controlling Network Use:** Also, assessments exercise should test the WLAN's Access Control and Authentication mechanisms to determine if there is a breach. And if yes, where? Test results may list plain user identities and crackable credentials that need to be strengthened. One of the consequences of cracked user credentials is unauthorized access to other systems in the corporate network. Here again, recommendations can be made to mitigate vulnerabilities, based on the WLAN's defined security policy. For example, if corporate policy stipulates authentication by PSK, test results should list ESSIDs with weak PSKs, recommending replacement with stronger PSKs or perhaps 802.1X.

Table 8 below shows some of the wireless attacks listed in table 7 above matched against the specific countermeasures to mitigate them. As can be seen from the table, there exists more than one countermeasure for each attack – some are simple, some are complicated. To mitigate an attack, you don't need to implement all, war driving for example. However, a combination of measures makes the network more robust and secured against the attack.

Table 8 Wireless attacks and countermeasures

Attack	Category/Target	Countermeasures
War Driving	Network Access	Change the Access Point default Admin password, always update the Access Point firmware and drivers for the wireless Adapter(s); Use the highest level of WEP/WPA (WPA2/802.11i strongly preferred); Authenticate wireless users with protocols like 802.1X, RADIUS, EAP (including EAP-PAX, EAP-PSK, EAP-TLS, EAP-TTLS, EAP-FAST, EAP-POTP, EAP-IKEv2, PEAP, and EAP-SIM); Use strong encryption for all applications that run over the wireless network, e.g., use SSH and TLS/HTTPS; Encrypt wireless traffic using a VPN (Virtual Private Network), e.g. using IPSEC or other VPN solutions; Create a dedicated segment for Wireless Network, and take additional steps to restrict access to this segment; Use a proxy with access control for outgoing requests (web proxy, and others).
MAC Spoofing	Network Access	Use of 802.11i (TKIP and CCMP) or VPNs (Session Encryption); AP Authentication; User based Authentication; Static ARP Mapping; Port Security.
802.11 De-authentication Flood	Network Availability	Requires strong authentication of management and control frames.
Rogue Access Points	Network Access	Wireless Security Policy; Physical Security; Wired and Wireless Network Separation; Corporate Security Policy/Users Separation; Authentication; Use of Wireless Intrusion Prevention Systems (WIPS); Network Connectivity Checks and Temporary Wireless Blocking; Disabling Unused Ports.
Eavesdropping	Message Confidentiality	Physical Security; T802.1x or VPNs; 802.11i (TKIP & CCMP)
WEP Key Cracking	Message Confidentiality	WPA & 802.11i i.e. TKIP (known as WPA1) and CCMP (also known as WPA2)

Attack	Category/Target	Countermeasures
Man-in-the-Middle	Message Confidentiality	Physical Security; T802.1x or VPNs; Strong Authentication Protocols: PKI, Mutual Authentication, Secret Keys, Passwords e.t.c.
RF Jamming	Network Availability	Mac Filtering; Firewalls (wired); IDS (Wired), DMZ architecture; 802.11i; Dynamic Channel Assignment.
Dictionary Attacks (Crack passwords)	Network Access	Strong Password Policy, 802.1x and VPNs
802.11 Frame Injection	Network Availability	WPA & 802.11i (MIC Algorithm)
Evil Twin AP	Message Confidentiality	Use of Wireless Intrusion Detection or Prevention System; Use of 802.1X Port Access Control for robust mutual authentication; Use of strong Extensible Authentication Protocol (EAP-TLS, EAP-TTLS, or PEAP) to check servers' signature; Use of product like Wavelink Avalanche or Windows Active Directory Group Policy Objects to administer 802.11 and 802.1X parameters on Windows PCs for centrally-manage PCs; Users' education.
Session Hijacking	Network Access	802.11i, 802.1x & VPNs
AP Phishing	Message Confidentiality	Use of Wireless Intrusion Prevention System (WIPS); Use of strong Extensible Authentication Protocol (EAP-TLS, EAP-TTLS, or PEAP) to check servers' signature; Use of Personal Firewalls for Wireless Devices

In summary, there are ten steps that need to be taken in order to deploy a secured enterprise wireless LAN after an assessment has been carried out. They are:

- Document a wireless security policy
- Break the wireless network into SSIDs
- Implement access controls
- Deploy authentication credentials
- Encrypt wireless data
- Harden WLAN infrastructure
- Defend wireless clients
- Monitor wireless traffic
- Prevent wireless intrusions
- Enforce network security [28]

CHAPTER FIVE

5 CONCLUSION, SUMMARY AND FUTURE RESEARCH

5.0 CONCLUSION

This work was done to find out if there are known inherent insecurities that limit enterprise deployments of a WLAN. And if yes, are there countermeasures that can be put in place to fix these known security holes for secure enterprise deployment of wireless networks. The following conclusions were drawn from this work:

1. WLAN technology has inbuilt security problems in its architecture, as the APs and the clients must advertise their existence through beacon frames, thereby exposing the signals to attackers.

2. There exist a wide range of attacks – from passive to active- on wireless LANs, and are aimed at the confidentiality and integrity of an information, and network availability as shown in table 7. Some of the attacks are less likely or more damaging than others, and some are more common than others.

3. The flaws detected in WEP have been fixed with the ratification of the IEEE 802.11i standard, and the rollout of WPA and WPA2. However, a combination of security measures is required to further increase the security offered by WLAN technologies as explained in section 4.4.

4. Security risk assessment is necessary so as to produce a list of threats a network is prone to and the severity each has on the network. Base on this a good security policy is made to defend the network. It is not practical or possible to defend any network against all possible attacks. The goal, however, is to reduce associated risk to an acceptable level.

5. There exist a number of countermeasures to mitigate a network against a particular risk as shown in table 8. Some of these countermeasures are simple, some are complicated. A combination of countermeasures, however, ensures that a network is robust and more secured against an attack.

It is essential that organisations put in place suitable protective measures for their wireless network. Though wireless group of standards IEEE 802.11 provide basic security, it is not foolproof enough to give the level of protection required for organizations network infrastructure. Vulnerability assessment is necessary to determine the combination of measures that should be implemented to mitigate the risks associated with the use of wireless technologies.

5.1 SUMMARY

Wireless LANs undoubtedly provides higher productivity and cost savings. In light of this, many organisations are beginning to deploy wireless LAN technologies not only for cost savings, but also for convenience and flexibility of use. But the fundamental question plaguing the industry today is if wireless networks can be deployed securely without compromising organization's assets - information. This study was undertaken to find out if wireless networks are inherently insecure thereby limiting enterprise deployment. If yes, what are the known holes, and can they be fixed? The following are the contributions to knowledge this work has made through exhaustive and broad literature study:

1. This study has shown that wireless LANs are prone to many different kinds of attacks. Attempt to secure wireless LANs, suitable for enterprise deployment, initiated a move from weak WEP to more robust WPA2.

2. This work also showed that the most effective security solution for Wireless LANs involves a combination of security technologies.

3. It demonstrated that a thorough vulnerability assessment and risk analysis is essential for development of effective security policy and determination of appropriate security measures, or combination of measures that are most effective.

4. It also showed that countermeasures and best practices - like personal firewalls, antivirus, intrusion detection systems e.t.c. - typically used to defend Internet-connected clients, are generally recommended for WLAN clients as well.

5. On-going monitoring and periodic testing are necessary to verify that a deployed WLAN meets defined objectives.

5.2 FUTURE RESEARCH

Wireless security is a broad area. In this work, the emphasis was on managing the attendant risks with vulnerability assessment. Below are areas in which I suggest future research work to be carried out on:

1. Performance evaluation of security implemented using WPA and WPA2 relative to robustness against attacks, bandwidth usage and running/maintenance cost.

2. Comparative analysis of security policy developed using vulnerability assessment and without vulnerability assessment: How robust are they? Long term maintenance cost.

3. Development of a robust and secured centralized management solution for large enterprises implementing both WPA and WPA2 in their infrastructure.

4. There is, virtually, no known attack against AES which is used by CCMP in counter mode for confidentiality. I suggest future researchers should use penetration tools to see if any technical flaw, weakness or vulnerability will be exposed.

REFERENCES:

1. W. Stallings, *Wireless Communications and Networks*. Pearson Education, India, 2006, pp 448-492.

2. R. Pejman, & L. Jonathan, *802.11 Wireless LAN fundamentals: A Practical Guide to understanding, designing and operating 802.11WLANs.* Cisco Press, Indiana, pp 21-34.

3. W. Noonan, *Hardening Network Infrastructure: Bulletproof Your Systems Before You are Hached! ,* McGraw-Hill Professional, New York, 2004.

4. W.Stallings, *Cryptography and Network Security Principles and Practice*, 4th edn, Pearson Education, India, 2006.

5. C. Doru, 'Telecommunication System: Wireless Local Area Network', Blekinge Institute of Technology, Nov. 2005, pp 1-54.

6. Y. Jui-Hung, C. Jyh-Cheng & L. Chi-Chen, 'WLAN Standards: In Particular, The IEEE 802.11 Family,' *Potentials, IEEE,* Vol. 22, Issue 4, Oct.-Nov. 2003, pp 16 – 22.

7. D. Smith, 'What Makes up a WLAN', Techrepublic, May 2007, retrieved 27 June 2008, < http://articles.techrepublic.com.com/5100-10878_11-1048092.html>

8. J. Burell, 'Wireless Local Area Networking: Security Assessment and Countermeasures: IEEE 802.11 Wireless Networks', Dec. 2002, retrieved 16 May 2008, <telecom.gmu.edu/publications/Jim-Burrell-December-2002.pdf>

9. G. Ollman, 'Securing WLAN Technologies: Secure Configuration Advice on Wireless Network Setup', Technicalinfo , retrieved 18 April 2008, <http://www.technicalinfo.net/papers/SecuringWLANTechnologies.html>

10. K. Fleming, 'Wireless Security Initiatives' May 2005, retrieved 16 May 2008, < http://telecom.gmu.edu/publications/Kieth-Fleming-Wireless-Security-Project-f2-May-2005.doc>

11. J. Epstein, '802.11w Fills Wireless Security Holes', Network World, April 2006, retrieved 05 July 2008, <http://www.networkworld.com/news/tech/2006/040306-80211w-wireless-security.html>

12. F. Mlinarsky, '802.11T Puts WLANs To The Test', Network World, March 2006, retrieved 05 July 2008, <http://www.networkworld.com/news/2006/031306-wireless-lans-80211t.html>

13. D. Molta, '802.11r: Wireless LAN Fast Roaming' *The Promise of Secure Wi-Fi Mobility*, Network Computing, April 2007, retrieved 02 July 2008, <http://www.networkcomputing.com/showArticle.jhtml?articleId=198900107>

14. D. Stanley, 'Standards Corner: IEEE 802.11m - 802.11 Standard Maintenance', The Edge, June 2007, retrieved 04 July 2008, <https://edge.arubanetworks.com/article/standards-corner-ieee-802-11m-802-11-standard-maintenance>

15. D. Halasz, 'IEEE 802.11i and wireless security', Embedded.com, August, 2004, retrieved 06 July 2008, <http://www.embedded.com/columns/specialreports/34400002?_requestid=402884>

16. C. Jyh-Cheng, J. Ming-Chia, & L. Yi-wen, 'Wireless LAN security and IEEE 802.11i' *Wireless Communications, IEEE,* Vol. 12, Issue 1, Feb. 2005, pp 27 – 36.

17. IEEE 802.11i: WLAN Security Standards, Javvin Network Management & Security, retrieved 01 July 2008, < http://www.javvin.com/protocol80211i.html>

18. WiFi – Introduction, Kioskea, retrieved 01 July 2008, <http://en.kioskea.net/wifi/wifiintro.php3>

19. B. Mitchell, 'Wireless Standards - 802.11b, 802.11a, 802.11g and 802.11n' *The 802.11 family explained,* About.com, retrieved 02 July 2008, <http://compnetworking.about.com/cs/wireless-80211/a/aa80211standard.htm>

20. B. Mitchell, 'IEEE 802.11 Working Group Standards', About.com, retrieved 02 July 2008, <http://compnetworking.about.com/cs/wireless80211/a/aa80211standard _2.htm>

21. J. Mallery, J. Zann, P. Kelly, W. Noonan, P. Love, E.S. Seagren, R. Kraft, & M.O'Neill, *Hardening Network Security: Network Security,* McGraw-Hill Professional, New York, 2005, pp 323-349.

22. K. Sankar, Cisco *Wireless LAN Security: Expert Guidance for Securing Your 802.11 Networks,* Cisco Press, Indianapolis, 2004, pp 125-155.

23. J.Koziol, *Intrusion Detection with Snort,* Sams Publishing, Indianapolis, 2003.

24. E. Sithirasenan, S. Zafar, & V. Muthukkumarasamy, 'Formal Verification of the IEEE 802.11i WLAN Security Protocol', *J. IEEE Computer Society,* Issue 18-21, April 2006, pp 181-190.

25. D. Welch, & S. Lathrop, 'Wireless Security Threat Taxonomy', *J. IEEE Systems,* Issue 18-20, June 2003, pp 76 – 83.

26. Sinha, I. Haddad, T. Nightingale, R. Rushing, & D. Thomas, 'Wireless Intrusion Protection System Using Distributed Collaborative Intelligence' *J. IEEE IPCCC*, Issue 10-12, April 2006.

27. S. McQuerry, *Wireless LANs: Extending the Reach of a LAN*, Cisco Press, 2008, retrieved 09 July 2008, <http://www.ciscopress.com/articles/article.asp?p=15668&seqNum=3>

28. L. Phifer, *Ten Steps to Wireless LAN Security*, Search Networking, retrieved 09 July 2008, < http://searchnetworking.techtarget.com.au/tips/24729-Ten-steps-to-wireless-LAN-security>

29. Network security- Learning Space, *Threats to Communication Networks*, retrieved 10 July 2008, <http://openlearn.open.ac.uk/mod/resource/view.php?id=183172>

30. B. Potter & B.Fleck, *802.11 Security: Attacks and Risks*, Search Networking, 2003, retrieved 10 July 2008, <http://searchnetworking.techtarget.com/generic/0,295582, sid7_gci1050371_tax303099,00.html>

31. NetworkDictionary, *How to Install Network Sniffing Tools for Effective Traffic Monitoring?*, retrieved 11 July 2008, < http://www.networkdictionary.com/howto/NetworkSniffer.php>

32. LOT3K, Sniffing Networks: *The Complete Documentation*, retrieved 11 July 2008, <http://www.l0t3k.org/security/tools/sniffing/>

33. Javvin Technologies, *Network Packet Analyzer CAPSA 6.8*, retrieved 11 July 2008, <http://www.javvin.com/packet.html>

34. CERT, *Denial of Service Attacks*, retrieved 12 July 2008, <http://www.cert.org/tech_tips/denial_of_service.html>

35. TECHWEB, *Replay Attack*, retrieved 12 July 2008, <http://www.techweb.com/encyclopedia/defineterm.jhtml?term=replay+attack>

36. L. Phifer, *Lesson 1: How to counter wireless threats and vulnerabilities*, Search Networking, 2006, retrieved 12 July 208, < http://searchnetworking.techtarget.com/general/0,295582,sid7_gci1172482,00.html?track=wsland>

37. Rapid7, *Penetration Testing Augments Vulnerability Management*, retrieved 12 July 2008, <http://www.rapid7.com/services/pentest.jsp>

38. 3Com, *New 3Com Systems Keep Wireless LANs Safe from Rogue Devices, Hackers and Vulnerabilities*, retrieved 13 July 2008, <http://www.3com.com/corpinfo/en_US/Pressbox/press_release.jsp?INFO_ID=265117>

39. Verisign, *An Introduction to Network-Vulnerability Testing*, retrieved 22 July 2008, <http://www.verisign.co.uk/static/029888.pdf>

40. Motorola, *Enterprise Wireless LAN Security*, March 2008, retrieved 22 July 2008, <http://www.motorola.com/staticfiles/Business/_Documents/static%20files/WLAN_Security_WP_0308_New.pdf>

41. L. Phifer, *Wi-Fi Vulnerability Assessment Checklist*, SearchSecurity, Mar 2006, retrieved 19 July 2008, <http://searchsecurity.techtarget.com/generic/0,295582, sid14_gci1167666, 00.html>

42. Cisco Systems, *Five Steps to Securing Your Wireless LAN and Preventing Wireless Threats*, 2006, retrieved 11 July 2008, < http://www.cisco.com/en/US/prod/collateral/ wireless/ps5678/ps6521/prod_white_paper0900aecd8042e23b_ns386_Networking_Solutions_White_Paper.html>

43. R. Apinantrakul, S. Malisuwan, & K. Kasemsan, *The Risk Analysis of WLAN Security Systems for Organizations in Thailand*, retrieved 21 June 2008, <http://www.rsu.ac.th/ grad/research/paper/2006/RiskAnalysisWLAN.pdf>

44. L. Phifer, *Managing WLAN Risks with Vulnerability Assessment*, AirMagnet, retrieved 11 July 2008, < http://www.airmagnet.com/assets/whitepaper/WLAN_ Vulnerabilities _White_Paper.pdf>

45. L. Phifer, *Wireless attacks, A to Z,* SearchNetworking, April 2006, retrieved 11 July 2008, <http://searchnetworking.techtarget.com/generic/0,295582,sid7_gci1173698, 00.html>

46. Intermec, *Wireless Security: It's Like Securing Your Home*, June 2003, retrieved 11 July 2008, <http://epsfiles.intermec.com/eps_files/eps_wp/WirelessSecurity_wp _web.pdf>

47. M. Kujala, *WLAN Standards and Wireless Networking Security*, May 2003, retrieved 11 May 2008, < http://www.tml.tkk.fi/Studies/T-110.551/2003/papers/3.pdf>

48. Flextronics, *Trends in WLAN Technology*, 2005, retrieved 1 July 2008, <http://www.futsoft.com/pdf/wlan_trends_note.pdf>

49. 'Wireless *Security* – Information for CIOs', February 2006, retrieved 27 June 2008, <http://www.ag.gov.au/agd/WWW/rwpattach.nsf/VAP/(7A188806B7893EBA0402BC1472412E58)~Wireless+Security++Overview+CIOs.PDF/$file/Wireless+Security+ -+Overview+CIOs.PDF>

50. N. Chendeb, B. Hassan & H. Afifi, 'Performance Evaluation of the Security in Wireless Local Area Networks (WiFi)', *J. IEEE I&CT*, April 2004, pp 215- 216.

51. S. Radack, *Security for Wireless Networks and Devices*, retrieved 15 April 2008, <http://www.itl.nist.gov/lab/bulletns/bltnmar03.htm >

52. D. Nayak, N. Rajendran, D.B.Phatak & V.P.Gulati, 'Security Issues in Wireless Local Area Networks' *J. IEEE*, vol 3, May 2004, pp 1637 – 1640.

53. B. Issac & L. A. Mohammed, 'War Driving and WLAN Security Issues — Attacks, Security Design and Remedies', *J. ISM*, Vol. 24, Issue 4, January 2007, pp 289 – 298.

54. K.H. Lim, *Security Guidelines for Wireless LAN Implementation*, August 2003, retrieved 18 April 2008, <http://www.sans.org/reading_room/whitepapers/wireless /1233.php>

55. Y. Jiang, C. Lin, H. Yin & Z. Chen, 'A Mutual Authentication and Privacy Mechanism for WLAN Security' *J. Wirel. Commun. Mob. Comput*., Vol. 8, Issue 1, September 2006, pp 101 – 112.

56. Mishra, N.L. Petroni Jr, W.A. Arbaugh, & T. Fraser, 'Security Issues in IEEE 802.11 Wireless Local Area Networks: A Survey', *J. Wirel. Commun. Mob. Comput*., vol. 4, Issue 8, November 2004, pp 821-833.

57. N. Wei, J. Zhou, Y. Xin, & L. Li, 'A Security Architecture for IEEE 802.11 Wireless Networks in Large-scale Multinational Corporations', *ITS Telecommunications Proceedings*, June 2006, pp 846-849.

58. R. Zhang, & J. Welch, 'A Survey on Current Practices in Enterprise Wireless Networking and Security Management', *J. Information Systems*, vol. 8, issue 2, 2007, pp 279-382.

59. N. Borisov, I. Goldberg, & D. Wagner, *Security of the WEP Algorithm*, UC Berkeley, retrieved 18 April 2008, <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>

60. Symantec, *Wireless LAN Security: Enabling and Protecting the Enterprise*, Symantec Enterprise Security, May 2002, retrieved 24 May 2008, < http://www.symantec.com /avcenter/reference/symantec.wlan.security.pdf>

61. V. Bhargava, & M.L. Sichitiu, 'Physical Security Perimeters for Wireless Local Area Networks', *J. Network Security*, vol.3, issue 2, September 2006, pp124-135.

62. Cisco, *A Comprehensive Review of 802.11 Wireless LAN Security and the Cisco Wireless Security Suite*, 2002, retrieved 18 April 2008, <http://www.cisco.com/warp /public/cc/pd/witc/ao1200ap/prodlit/wswpf_wp.pdf>

63. AirWave, *Best Practices Guide: Eight Things You Can Do TODAY to Improve Wireless Network Security*, 2008, retrieved 16 April 2008, < www.airwave.com/ resource-center/>

64. EUSSO, *54Mbps Wireless-G Cardbus Adapter: Linking your Computer with Wireless G network*, retrieved 16 April 2008, <http://www.eusso.com/Models/Wireless/UGL2454-01R/UGL2454-01R.htm#Diagram>

65. WLANA, retrieved 16 April 2008, <www.wlana.org>

APPENDIX

Wi-Fi VULNERABILITY ASSESSMENT CHECKLIST

1. Nearby wireless devices discovery

The first step in any vulnerability assessment is identification of all wireless devices near the site(s) under test. Document the following:

- Channels with active traffic in the 2.4 GHz band.
- Channels with active traffic in the 5 GHz band.
- Sources of non-802.11 interference in these frequency bands.
- Document for each discovered 802.11 access point:
  - Media Access Control (MAC) address
  - Extended service set identifier (ESSID)
  - Channel
  - Average/Peak signal-to-noise ratio (SNR)
  - Beaconed security parameters (i.e., WEP, TKIP or AES-CCMP)
  - Approximate location and probable owner
- Document for each discovered 802.11 station:
  - MAC address
  - Associated ESSIDs
  - Associated AP(s) or peer station(s)
  - Average/Peak SNR
  - If visible, 802.1X identity
  - Approximate location and probable owner

2. Investigate rogue devices

The next step is to use spectrum analyzers to locate non-802.11 sources of interference (e.g., microwave ovens, Bluetooth, cordless phones). For 802.11 devices, an existing inventory should be used to isolate unknown devices for further investigation. Search for activities in the bands and channels not in use helps to catch devices trying to escape detection.

3. Testing access points

The following questions are to guide you in testing your APs:

- Is the AP running the latest firmware and security patches?
- Is it still having the factory default ESSID?
- Has the default administrative login/password been changed?
- Can the administrative password be easily cracked?
- Are stronger authentication options available (e.g., private keys)?
- Are there any unnecessary open ports (e.g., telnet, http, snmp, tftp)?
- Are those open ports vulnerable to known exploits?
- Are there available encrypted administrative interfaces (e.g., ssh, https)?
- Have security alerts or logs been turned on (e.g., syslog, traps)?

- Have filters been used to prevent unauthorized protocols (e.g., ARP, RIP, SNMP, NetBIOS) from passing through the AP into the wired network?
- Are filters available/used to block user-to-user wireless?
- Is the right ESSID and channel in use by the AP?
- Are AP's security parameters consistent with defined policy?
- How long does it take to crack the key if WEP is in use?
- Is the AP emitting any known weak initialization vectors (IVs)?
- Is the AP's PreShared Key (PSK) is easily crackable, if it is in use?
- If the AP is not using WPA2, are WPA2 upgrades available?
- Can the AP withstand simulated 802.11 DoS attacks (e.g., Authenticate floods)?

4. Testing own stations

Carry out the following checks on each wireless station that you own:

- Is the station running the latest OS and application security patches?
- Is boot or OS authentication used to prevent lost/stolen/unintended use?
- Are current antivirus and antispyware programs running?
- Is the wireless interface protected by a personal firewall?
- Are there unnecessary ports open (e.g., netbios-ns/ssn, microsoft-ds, ssdp)?
- Are there unnecessary protocols bound to wireless (e.g., file/printer sharing)?
- Are potential wireless intrusions (e.g., blocked sessions) being logged?
- Is the wireless client willing to associate to ANY network? ANY Ad Hoc?
- Is the client automatically re-associating with home or hotspot SSIDs?
- Are there wireless user credentials (e.g., passwords) saved on disk?
- Is the station scanning the right bands and using the right ESSID(s)?
- Are its security parameters consistent with defined policy?
- Is the station emitting any known weak IVs?
- If the station is using 802.1X, is its identity visible?
- If using 802.1X, is it using a vulnerable EAP type (e.g., LEAP)?
- If using 802.1X, is it checking the server's certificate?
- If not using WPA2, are WPA2 upgrades available?
- If a VPN client is used over wireless, is it configured properly?

5. WLAN infrastructure testing

The security of all the devices in your network infrastructure that participate in your wireless subnet, including wireless switches, firewalls, VPN gateways, DNS servers, DHCP servers, RADIUS servers, Web servers running captive portal login pages and managed Ethernet switches should be assessed using the same penetration test used for the APs.

The RADIUS server's ability to gracefully reject badly-formed EAP messages, including bad EAP lengths and EAP-of-death should be tested. [41]