MACQUARIE UNIVERSITY

Department Of Computing

Securing Wireless LANs and Wireless MANs

ITEC810 Final Report

Supervised by Dr. Michael Hitchens

Peter Nicola
Student# 41584929
peter.nicola@students.mq.edu.au

5/6/2009

ABSTRACT

Wireless networking is being extensively used nowadays on both home and enterprise levels. It is becoming a central part of work and leisure activities of many people. Two common forms of wireless networks are WLANs and WMANs. As with other networking schemes, sensitive data such as credit card details or confidential documents are always expected to be travelling through them. Attackers are mainly targeting this type of data to use it for their benefits. A certain level of security is required to maintain a relatively safe environment for data communication. This document will discuss the details of work carried during the lifetime of this project. This includes, studying existing technologies and their way of operation, learning and analysing existing threats and vulnerabilities, and based on research, best practices and suggestions are provided on how to protect both WLANs and WMANs against these threats. It ends with some possible improvements for the existing technology.

ACKNOWLEDGMENTS

I could have not completed this project without Dr. Michael Hitchens who not only served as my supervisor, but also encouraged me and provided me with ideas and challenges throughout the lifetime of the project. Also, I would like to thank Professor Robert Dale for his support and prompt responses whenever questions arose during the semester. Finally, I would like to thank my family and beloved ones for giving me support from day one until the end of the project.

TABLE OF CONTENTS

1. INTRODUCTION

1.1. SECURITY INTRODUCTION

A general definition of security would be a trade-off between using something and protecting it from undesired usage[1]. Security is a broad term that applies to all aspects of life. In this project, the focus will be on wireless communication security which is a variation of communication security itself.

The idea of securing communication started in the pre-computer era, maybe thousands of years ago. In Egypt, many documents were found to be written in non standard hieroglyphs (ancient Egyptian language). It is believed that this was done as way of ciphering text to ensure that only the right people would understand what these documents said. (Cypher Research Laboratories Pty. Ltd.) Also, the Greeks had their Scytale[2] device they used to cipher text. It was mainly used by the Spartan army to exchange messages. (Fred Cohen & Associates, 1995) In that era, communication was based on tangible written messages being transmitted from senders to receivers by a messenger or some other method (e.g. carrier pigeons). The messages were ciphered so that if someone captured the courier, they would have not been able to interpret what the message said.

With the information revolution, new methods of transmitting messages have been introduced (these include, telegraphs, Morse code, telephones, faxes, computer networks, etc...); however, the same threat existed. There were always people in the middle trying to capture and interpret what these messages contain. The reasons why attackers hack and try to intercept communication vary. Some attackers do such action for political reasons or to help their countries while others would aim for personal benefits or revenge. In all cases, communicating parties are encouraged to know what threats exist to the communication method they use, and try protecting their assets against these malicious threats.

Many threats have been already discovered and controls were developed to mitigate their impacts. On the other hand, attackers are working hard to discover other vulnerabilities and exploit them.

As mentioned earlier, wireless communication security is the focus of this project; the previous lines were discussing what security is, focusing on general communication security. They have gone through some historical facts that showed how old security existence is. They also stated how important security is. In the following sub-section, the focus will move

[1] According to ITEC854 – Information Security Management lecture notes, week 1 – semester 2-2008, slide 20 by Milton Baar

[2] See Glossary for definition.

from security to wireless communication; however, it is important to keep the reasons why we need to secure networks in mind, because this is where this project applies security concepts.

1.2. Wireless Networks Introduction

Data communication can be classified into wired communication and wireless communication. The main difference is in the transmission medium used. In wired communication, the medium is usually cables or wires. These are made of different material such as copper, fibre optics, and others; on the other hand, wireless communication uses a wireless transmission medium; this can be such as void or air where electromagnetic radiation is used to carry the information through.

Because of wireless networking numerous advantages, it is becoming more and more popular these days. These advantages include mobility (which leads to time saving – users are not required to go to a specific spot to use the service), less cost, and room saving since they do not need cable connectivity anymore.

The idea of wireless communication goes a couple of hundred years back. In fact the first successful intentional wireless transmission was done by the German physicist, Heinrich Hertz, between 1886 and 1888. (Wikipedia) He based his studies on Maxwell's work done between the years 1861 and 1865; however, it is believed that the work on wireless waves began many years before that. Scientists such as Gian Domenico Romagnosi in 1802, and Hans Christian Ørsted in 1820, worked on electromagnetism and had a series of experiments on it. (Wikipedia) These concepts and theories were used to develop radios, and other wireless devices which were used in World War II as methods of communication between army bases and sites.

These days, there are lot of wireless communication forms; these include mobile phones, computer networks, satellite communication, television and radio broadcasts, and many others. Every category of these can be decomposed into many types and protocols. This document is focusing on computer networks, specifically on two common forms of wireless computer networks, WLANs, and WMANs. A detailed description of each is given later on in sections 2, and 3. The concern now is that these two types are the implementation of other wired computer network types. For instance, WLAN is the wireless version of LAN which is a small network connecting compatible devices together. Similarly but on a greater scale, WMAN. It is the solution ISPs would use for wireless broadband access. It is typically used to deliver ISP services to remote areas having no cable infrastructure.

As stated previously, the difference between wired and wireless networks is in the transmission medium. In a wired network, to control client connectivity to the network,

cables and connectors can be plugged in or removed. Physical connection is a must for access which increases security. That is, if the attacker does not have physical access to the network, they will not be able to access it. On the other hand, wireless waves are everywhere within the transmission range. They can be captured by anyone who is in that range, the same as radio broadcasts.

The following section (Section 2) will start discussing WLANs stating their details and security concerns. Later on, the same will be done for WMANs (Section 3), and also their security concerns will be assessed and discussed. Both of WLANS, and WMANs, are built on layer models. The security focus in this document is mainly focusing on protecting the lower layers since this low layer protection is a fundamental requirement for higher layer protection; the same idea in buildings, protecting the entrance would increase the protection for the apartments in higher floors.

2. REVIEW OF WLAN[3]

2.1. WHAT IS IT?

A Local Area Network (LAN) in general is a small network limited in its area of coverage. It consists of a group of devices equipped with a Network Interface Card (NIC) working on the same protocol. A protocol is the language they speak. Currently, The Institute of Electrical and Electronics Engineers (IEEE), a non-profit organization[4], is the responsible entity for approving and standardizing such protocols.

IEEE assigns a unique number to each standard. The family, to which LANs belong, is given the reference IEEE 802. There are various protocols used in LANs. These include Ethernet (IEEE 802.3), Token Bus (IEEE 802.4), Token Ring (IEEE 802.5), and many others.

Ethernet is commonly used now due to its proven efficiency and low cost. In a typical Ethernet LAN, the main component is a switch[5]. Devices such as computers are connected to the switch via cables such as copper twisted pair cables.

[3] This section summarizes information from these sources: (LAN MAN Standards Committee of the IEEE Computer Society, 1997) (Wang, et al., 2008) (Beck, et al., 2008) (Borisov, et al., 2001) (Hardjono, et al., 2005) (LAN MAN Standards Committee of the IEEE Computer Society, 2007)

[4] Full information available at http://www.ieee.org/web/aboutus/home/index.html

[5] Originally hubs were being used; however, switches are much faster and more efficient. The reason why they were not used is because of their high cost. Now they are very cheap. See Glossary for hub and switch definitions

Figure 1 below[6] shows a typical LAN.

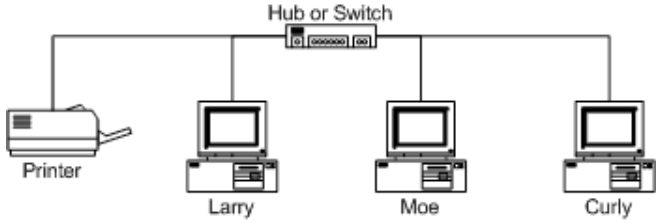

FIGURE 1: SIMPLE LAN

In many cases, a router[7] or a server[7] is connected to the switch as well to allow other devices to access the internet or other resources.

WLAN (IEEE 802.11) is the solution of having a LAN with all its benefits, but at the same time getting rid of much of the cabling. Network administrators and operators have always had problems because of the mess caused by high client numbers, which is the case most of the time. WLAN for them was a dream coming true. It was the solution that will help minimizing the cable numbers, and allowing more users to access the network easily and at anytime without the need to find an empty slot and a cable for the connection.

Figure 2 below[8] shows a simple WLAN.

FIGURE 2: SIMPLE WLAN

[6] Figure obtained from http://wlwhipple.com/TechTips/SimpleIPnetwork.gif
[7] See Glossary for definition
[8] Figure obtained from http://www.minesite.com.au/images/WLAN_Schematic_metal.jpg

The first standard for WLANs was published in 1997 by IEEE. (LAN MAN Standards Committee of the IEEE Computer Society, 1997) The main equipment in a typical WLAN is called Access Point (AP); it does the same jobs as switches in a LAN. In order for devices such as PDAs and computers to be connected to a WLAN, they must be equipped with a Wireless Network Interface Card (WNIC).

WLANs are generally used on home and office levels. They normally have a coverage range of 100 metres and a speed of 54Mbps (version 802.11g). These numbers are now bigger after the introduction of 802.11n, the new edition of the standard, where the coverage range can reach up to 300 metres, and the speed up to 600Mbps. This is achieved by using multiple antennas at both the sender's and receiver's ends[9].

2.2. ARCHITECTURE

Many network types operate on a layered model called the OSI model[10]. This model consists of seven layers. Each of these layers is responsible for certain tasks. The difference between actual physical networks is usually in the lower layers. This would be in the Physical Layer (layer one), which is concerned with the delivery of bits over the physical medium (Forouzan, 2004 pp. 45-48). Also, differences are often in the Data Link Layer (layer two), which is responsible for the delivery of frames to the next node. Data Link Layer is divided into two sub-layers, Logical Link Control (LLC), and Media Access Control (MAC). LLC (IEEE 802.2) is concerned with detection and correction of errors caused by the Physical Layer, while MAC is concerned with security issues along with other tasks (Forouzan, 2004 pp. 239-242).

The network interface for applications, such as email or web browsers, is the Application layer, layer seven. When applications generate data that needs to be delivered to another host by the network, the application layer receives the data and pushes it down through the lower layers. Each of these lower layers does its function until the data is finally transformed into bits that can be sent over the physical medium. The process of data moving from higher layers to lower ones is referred to as Encapsulation.

The following lines will discuss the 802.11 layered architecture for WLANs. They will discuss the layers it operates on, stating what their functionalities are.

[9] Based on the wireless communication MIMO concept, see Glossary for MIMO definition.
[10] See Glossary for definition.

Figure 3 below[11] shows the layers of 802.11

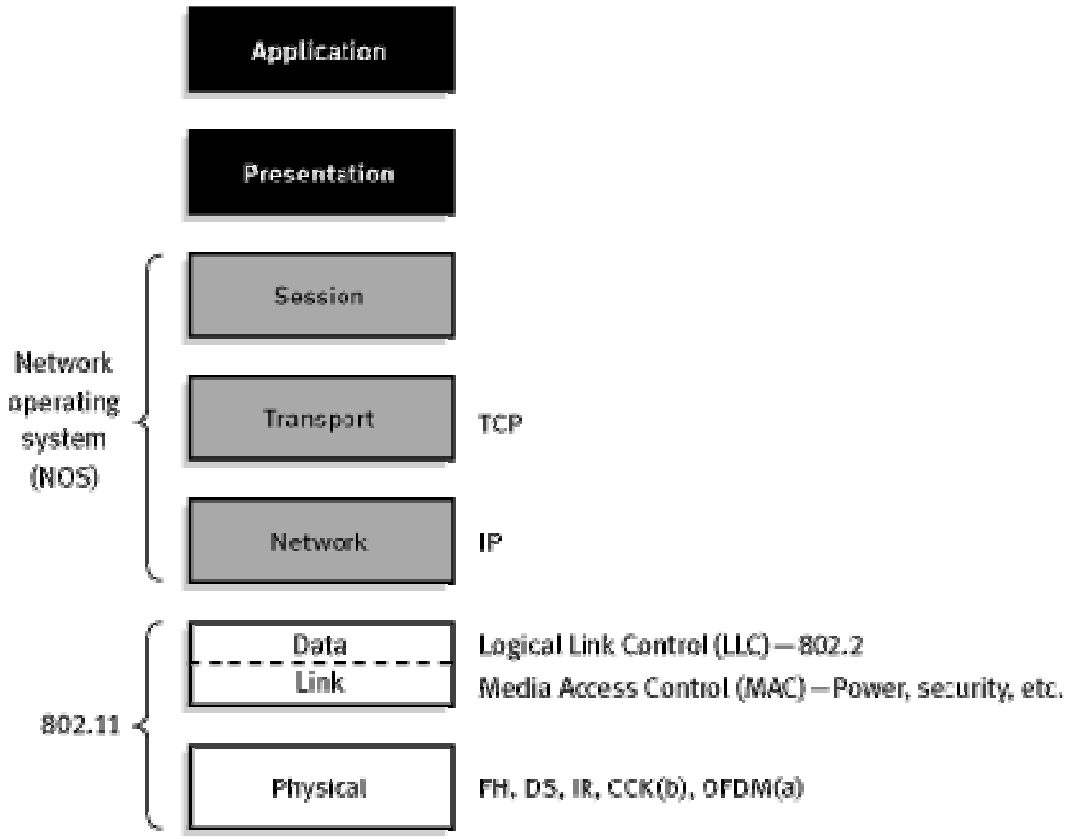

FIGURE 3: 802.11 LAYERS

PHYSICAL LAYER

The Physical layer – from now on will be referred to as PHY layer, is responsible for transmitting the bits over the medium. WLANs use air as their transmission medium. They use signalling techniques such as FHSS, DSSS, IR, OFDM, and HR/DSSS. (LAN MAN Standards Committee of the IEEE Computer Society, 2007 pp. 637-688) Below is a brief description for each of them.

FHSS (FREQUENCY-HOPPING SPREAD SPECTRUM)

FHSS transmits data on the 2.4 ISM (Industrial, Scientific, and Medical) GHz band. Its concept is sending data on a certain frequency for a certain amount of time, then hops to another frequency for the same amount of time, and so on. It keeps hopping until it reaches a defined number of hops. It keeps repeating this cycle while transmitting data. Switching

[11] Figure obtained from http://ntrg.cs.tcd.ie/undergrad/4ba2.01/group1/ISO.gif

from a frequency to frequency, which makes it hard for attackers to capture the signals; this contributes in increasing the network security[12]. (Forouzan, 2004 pp. 363-364)

DSSS (Direct Sequence Spread Spectrum)

DSSS also transmits data on the 2.4 GHz ISM band. This signalling technique replaces each original bit sent by the sender with a sequence of bits called chip code. It uses all the frequency range to transmit the chip code to the other end, as to be delivered at the same time taken if just the original bit was sent. The security goal behind this design is to make it hard to jam signals since it is not easy to get that chip code. Generated chip codes are different, which allows multiple accesses to the same channel. At the receiver's end, a calculation is done to remove the extra bits in the chip code and extract the original data[13]. (Forouzan, 2004 p. 364)

IR (Infrared)

IR was part of the first standard edition in 1997. It has a section in the latest standard edition 2007, but it is no longer maintained in the specifications. IR can be useful in many uses, but its range which covers up to 20 metres and other properties made it not preferable to be used in WLANs. (LAN MAN Standards Committee of the IEEE Computer Society, 2007 pp. 575-590)

OFDM (Orthogonal Frequency Division Multiplexing)

OFDM transmits data on the 5 GHz ISM band. It divides the band into several sub-bands and sends bits in a parallel manner. The advantage behind such scheme is to avoid interference. Also, random usage of sub-band increases security[14]. (Forouzan, 2004 p. 365)

HR/DSSS (High Rate Direct Sequence Spread Spectrum)

HR/DSSS is similar to DSSS, it also operates on the 2.4 ISM band. The difference is that DSSS encodes each bit to a chip code and transmits it to the receiver. HR/DSSS encodes four or eight bits to what is known as (CCK) Complementary Code Keying symbol. This new method increases the speed of transmission since it encodes many bits together.

PHY layer security protects against some types of attacks that will be discussed later; however, in case an attacker succeeds in capturing signals, they should not be able to change the message or even interpret what it says; the same idea as the messenger in the

[12] See (LAN MAN Standards Committee of the IEEE Computer Society, 2007 pp. 487-536) for more details

[13] See (LAN MAN Standards Committee of the IEEE Computer Society, 2007 pp. 537-574) for more details

[14] See (LAN MAN Standards Committee of the IEEE Computer Society, 2007 pp. 591-636) for more details

pre-computer era. The problem here is that, if the WLAN belongs to a financial organization, and someone could capture their traffic, losses can cause the business to cease. In fact many attackers target this type of organization, where their profit would be relatively high.

We Looked at the PHY layer and mentioned what security features it provides. The following lines will discuss how security is provided in the Data Link layer. Security is provided by and operates in its MAC sub-layer. There are some standard mechanisms that will be explained. We first start with encryption algorithms. The first algorithm used in IEEE 802.11 standard is called WEP.

2.3. WEP (WIRED EQUIVALENT PRIVACY)

WEP was introduced in 1997 with the first edition of the standard. The goal of its designers was to achieve a level of security similar to the one existed in wired networks, this is why they gave it the name "Wired Equivalent Privacy". It basically works with a key that is shared among WLAN users. This key is used in the encryption of data transmitted from the client's wireless device to the access point; the encryption algorithm used, is the RC4 algorithm which will be explained in this section. WEP seemed promising at that time where it was meant to provide a satisfactory level of security. Unfortunately, its design and the algorithm used were disappointing. It took only a few minutes to crack the key at that time.

The first edition of WEP, often called 64 bit WEP, used a 64 bit key; 40 bits of the key represent the shared key chosen by the user, and the other 24 bits are for the IV (Initialization Vector) used in RC4 algorithm. (Wang, et al., 2008) The 40 bit key chosen by the user is in hexadecimal[15], that is, the number of possibilities for each character is 16 possible characters (0 to 9, and A to F). Since every character is represented with 4 bits, then the maximum length of the key is 10 hexadecimal characters. Each of these characters has 16 possibilities; that means 16^{10} possible keys. It might seem a large number when calculated, but an old computer with a Class C Pentium 100 processor (can generate 1,000,000 combinations per second[16]) can crack the key using a brute force attack in just over 300 hours. Newer processors would crack such password in a few minutes.

Short length and limited key-space are not the only weaknesses in WEP. In fact the major weakness lies in the algorithm it uses, RC4.

[15] See Glossary for definition

[16] According to ITEC851 – Commercial Operating Systems Vulnerabilities lecture notes, week 4 – semester 2-2008, slide 27 by Milton Baar

RC4 algorithm is a stream cipher mechanism. Stream cipher means that it takes the plain text and does an XOR function with the 64 bit key available to produce a key stream that is used to cipher text by an XOR operation.

Figure 4 below[17] shows the encryption operation of WEP

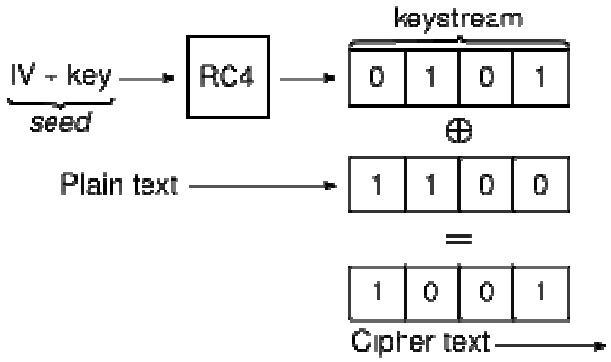

FIGURE 4: WEP ENCRYPTION

The key or the seed, as mentioned earlier, is composed of 40 bit user key, and 24 bit IV. The IV value is calculated randomly; however, due to its limited size (24 bits), it is expected to see IVs being repeated within five hours assuming the WLAN speed is 11 Mbps (much less time with higher speeds). If an attacker could capture two frames with the same IV but different data, which is very possible, another XOR operation would reveal the IV which would lead to obtaining the original data sent. (Wang, et al., 2008) Amendments were suggested, and other versions with longer keys were introduced; 128 bit WEP that uses 104 bit user key (a maximum key length of 26 hexadecimal characters), and 256 bit WEP that uses 232 bit user key (a maximum key length of 58 hexadecimal characters). Maybe user key cracking using brute force became harder because of the length, but on the other hand, it is unfeasible for people to memorize a key with that length, a lot of people would write it on a piece of paper, which if fell into the wrong hands, all the security approaches would not help. Also, the increased length does not solve the major flaw where, using two messages, data can be calculated. (Borisov, et al., 2001)

WEP never had a good reputation in the security world because of its poor design and weaknesses; that lead to its abandonment a few years later and another algorithm called WPA took over. One serious issue remains, although WEP is officially depreciated, and actually not recommended at all to be used, some people still use it until this day. In a later sub-section, 2.7, where threats will be discussed, one of these threats, 'War Driving', will mention another reason why WEP should not be used.

[17] Figure obtained from http://www.prism.gatech.edu/~jfaulk3/images/wep_encryption.png

2.4. WPA (Wi-Fi Protected Access)

Wi-Fi Alliance, another non-profit organization that is composed of more than 300 member companies devoted to promote WLANs[18], researched and came up with an alternative solution that was promised to be better than WEP. This approach was released in 2003, and it took part of the IEEE standard edition 802.11i-2004 (Wong, 2003).

The encryption technique used in WPA will be discussed later on, now one of the big differences making WPA relatively more secure than WEP is the key format used. WPA's key is in ASCII which is more convenient to human beings rather than hexadecimal since meaningful words can be used (recommendations for keys will be discussed later on, in section 2.8). Another issue is the key space. Using ASCII characters means 95 possibilities[19] for each character. Such huge key space makes the password cracking function using brute force attack exceptionally hard if the key meets a certain level of complexity. The key length is enforced to be at least 8 characters, and it can be up to 63 characters. This means, if the key is chosen to be at the minimum length required, we would still have 95^8 possible combinations. On a Pentium Dual processor (can generate 10,000,000 passwords per second), it would take up to 274 months for a brute force attack to crack the key.

Key space expansion is definitely a good step; however, the encryption mechanism is an important factor to be considered. WPA uses the same RC4 technique, but, some modifications we made to make it resistant to message calculation mention in the previous section. Instead of having an IV of 24 bits that keeps changing and at some stage same keys well be reused, in WPA, There is a new key called TKIP (Temporal Key Integrity Protocol) which is derived mathematically from the original key by the user, and then a 48 bit IV is calculated (twice the size of the IV used in WEP), and the final key steam used are based on that derived TKIP which gets changed every while. According to TKIP description, the chance of having a TKIP reused is low. (Hardjono, et al., 2005 pp. 143-154)

So far, WEP and WPA were serving home users more than corporate users. On home level, the key can be shared among inhabitants; however, on the enterprise level, sharing the same key would not be a good idea. We need to avoid employees giving the key to non-employees. The method where one key is being shared by different people is called PSK (Pre-Shared Key). EAP (Extensible Authentication Protocol) is the other method that satisfies enterprise requirements; it uses an authentication server, such as RADIUS, which takes the responsibility of managing people's accounts. Using RADIUS server means, each employee would have their own account that is required to use the WLAN. Using this

[18] Full information available at http://www.wi-fi.org/about_overview.php

[19] 95 possibilities are the sum of as all capital characters (26), small characters (26), numbers (10), and special characters (33)

method helps administrator track what actions were done by who. Also, enforcing policies such as, account cannot be used from two different terminals at the same time, can help improving security, and detecting illegal access.

Although WPA's architecture is better than WEP, and using TKIP for key stream calculations makes it even harder to derive plain text using the XOR operation when capturing a sequence of frames (like what was explained in WEP's section, 2.3), such an attack was still possible. It is also vulnerable to dictionary attacks where the attacker has a list containing likely possibilities, and they try them. This is why short and obvious passwords are not encouraged. If the password or the key is the person's name, birth date, or even a combination of both, then the chances of cracking the password using dictionary attack are very high. The development work to security approaches continued to catch up with security requirements. Given the possibility of key cracking in WPA, the Wi-Fi alliance introduced a newer protocol than WPA, and gave it the name, WPA2; it is discussed in the next section, 2.5. (LAN MAN Standards Committee of the IEEE Computer Society, 2007 pp. 165-185)

2.5. WPA2

WPA fixed many of the problems with the former security protocol, WEP; however, security requirements always change. This change is usually a higher demand for security. Usage of RC4 in WPA mitigated the risk of a successful message derivation, but did not eliminate it. Some flaws existed that made it possible to obtain the key stream from some control messages. (Beck, et al., 2008 pp. 9-11) Wi-Fi Alliance was well aware of the requirements change, and in fact, they released their new edition of WPA, WPA2, about a year after releasing WPA.

WPA2 also supports both PSK, and EAP modes, for key sharing, and for centralizing user account management. All WPA functions are also supported in WPA2; however, more methods and functions were added to increase security, these include, PBKDF2 (Password-Based Key Derivation Function), AES (Advanced Encryption Standard), CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code), and enhanced EAP.

PBKDF2 (Password-Based Key Derivation Function)

Formally, RC4 was used to produce a key stream from the key and the IV that is used to encrypt data, WPA2 Supported another method called PBKDF2[20] for key derivation and AES for encryption. PBKDF2 is one of a series by RSA laboratories. The advantage of this key derivation functions lies in its way of operation. Assuming ASCII characters are being used

[20] See RFC 2898 for more details about PBKDF2 and its series

for PSK, what it does is, it takes the PSK as the key, and the SSID[21] as a salt value[22]. It processes both in a hash function to produce a 256 bit key stream that is used in encryption. This operation is repeated hundreds of times to make it strong enough not to be cracked. An important note though, about SSID, since it used in the key stream derivation, it is not recommended that the SSID is easy to guess. Some websites publish lists of such easy SSIDs[23]. The same concept applies to PSK. More information comes later on in the following sections.

AES (Advanced Encryption Standard)

AES is the new supported encryption algorithm in WPA2. Unlike RC4, AES is a block cipher; it encrypts blocks of plain text using a certain function, and uses another function to decrypt data[24]. AES is adopted by the CSD (Computer Security division) at NIST[25] (National Institute of Standards and Technology), and was announced in 2001. It is based on the former DES algorithm which had very good reputation. AES is actually used by another protocol called CCMP that provides quality encryption as well as integrity checks.

CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code)

CCMP is fully defined in RFC 3610, as mentioned in the previous paragraph; it mainly provides encryption and authentication. Its encryption function uses AES whereas it uses block chaining techniques to provide authentication and integrity check.

EAP (Extensible Authentication Protocol)

EAP existed in the previous WPA. The same remained in WPA2, but the Wi-Fi Alliance added more features to enhance APs' communication with each other. Many security methods of authentication are used in WPA2 EAP. Details about EAP are available at RFC 3748

In general, WPA2 is proven to be reliable regarding to the current security requirements; however, proper usage and configuration are still the key factors to make use of WPA2 features. Poor configuration would make all the security features useless. WPA2 has a strong design making it recommended to be used by many professionals and experts. (Beck, et al., 2008)

2.6. Other Security Approaches

Sub-sections 2.3, 2.4, and 2.5 discussed the main security approaches in WLAN. They were concerned with encryption involving complex functions. Although WLAN security mainly

[21] SSID is the WLAN name, it will be referred to in the next section, 2.6
[22] See Glossary for definition
[23] See http://www.wigle.net/gps/gps/Stat for list example
[24] See (Federal Information Processing Standards, 2001) for full details
[25] See http://csrc.nist.gov/about/index.html for further details about CSD and NIST

relies on them, there are some other approaches that can help increasing the overall security of a WLAN; however, due to the advanced technology and attacking techniques, the methods mentioned in this section cannot be used alone. They are very easy to be cracked. The next few lines will talk about SSID that was mentioned earlier in sub-section 2.5 (WPA2), and MAC address filtering.

SSID (Service Set Identifier)

SSID is simply the name given to a WLAN; it is represented as alphabet and / or numerical format, and it is needed for clients to be connected. If the SSID changes at any time, clients will not have access until they reconfigure their wireless device with the new SSID. SSIDs are usually broadcasted; anyone with a device equipped with a WNIC would be able see that this specific WLAN exists in this area. The security approach here is that SSID broadcasting can be disabled, in other words, the WLAN can be hidden. This option might seem promising, but actually software programmes such as "Network Stumbler" can detect networks in range, including the hidden ones. (Raymond, 2007). As a result, SSIDs cannot be used alone; we can just assume that not all of the curious people know that such tools exist. This does not mean that SSID should not be cared about since they can be discovered anyway. As mentioned in WPA2's section (section 2.5), SSIDs are used as a salt value for the encryption process, therefore, strong SSID are useful, and in fact they contribute in increasing security.

MAC Filtering

MAC addresses are also known as physical addresses. Any network adapter, whether it is a NIC or WNIC, have a unique address that typically consists of 6 bytes. A common method of controlling who would access the WLAN is enforcing an access list on the AP. This access list filters devices based on their MAC address. There are two main problems in this approach.

1. What if there are 50 APs connected to each other forming one big WLAN? To grant or deny one client access, the update must be done on all 50 APs. This scalability problem would discourage operators from using such method. (Wang, et al., 2008)
2. Although MAC address is supposed to be unique, software programmes such as "MACshift" can forge them, in other words, this software can change the MAC address of a device. Having software programmes capable of doing such thing, makes the method insufficient to be relied on; however, it is still be useful to increase security in certain situations such as at homes and small offices.

2.7. COMMON THREATS

The previous sections discussed many security approaches and techniques where detailed technical information was involved. The user or the network operator, however, cannot do anything more than following some guidelines or best practices (e.g. password complexity policy, or which security mode to use). This section introduces and discusses other existing threats that can be avoided if the network operator has the appropriate knowledge.

EVIL TWIN

Evil Twin attack is a common way of attacking WLANs. The attacker here replicates another WLAN's SSID. For the user, they would not notice that there is a change, or that they are connected to a rogue AP; they search for a specific SSID, and they find it. Another factor is that most of the WNICs get connected to the network with stronger signal. The attacker, on the hand, can capture all their traffic picking these packets containing sensitive data such as passwords, confidential documents, credit card information, etc... Software programmes such as "LucidLink" can help differentiating genuine APs from rogues one. This is discussed in section 2.8. (Elliott)

WAR DRIVING

War Driving is the act of attackers cruising with a car aiming to find an unsecured WLAN, or a WLAN with weak security (e.g. using WEP). Their next typical action is, posting these to the internet so everyone would know about them, and use them for free internet access if applicable, or maybe just capture the traffic of that network. If the network is found to belong to a financial organization, it would be a dream coming true to the attacker. (Elliott) Google maps and www.wifimaps.com are two resources where open and cracked WLANs are posted.

WIRELESS NETWORK VIRUSES

Wireless network viruses are similar to the viruses well known by people. Their characteristic is that they use wireless networks to move from a device such as a computer to another. MVW-WiFi virus is an example of WLAN viruses. Once it infects a computer, it sends probe messages to other networks and forwards itself to these networks. (Gordon, 2006) This type of viruses can be prevented using anti-virus software programmes.

PSK CRACKING

The operation of PSK cracking might seem hard, but in fact, with the current available tools, it would not take a long time to crack WEP and WPA. Tools such as "Aircrack" and "Airsnort" can crack 128 bit WEP within 60 seconds. WPA2 is harder to be cracked.

PACKET SNIFFING

Attackers may have tools to sniff network, these tools are also easy to be obtained[26]. The packets are then analysed, and maybe used for illegal purposes. Quality encryption would not stop sniffers, but it would not allow them to extract useful information for the sniffed packets.

2.8. RESULT – SECURING WLANS

BEFORE WE START

One concept should be conveyed before we get to the outcome of this research; perfect security does not exist. Government systems are well known to be well protected against malicious attacks. They spend fortunes funding security research projects. Their efforts succeed to block a lot of attacks; however, since perfect security does not exist, some attacks might be successful. One of these governments is the US government. It is well known of its strong intelligence system and quality IT infrastructure, and yet it got hacked. Gary McKinnon is a Scotsman who is currently facing charges of hacking many of their systems including those of Air Force, US Army, Navy, the Department of Defence, and some NASA computers. (Boyd, 2008) Our goal is to secure our networks and systems as much as possible with the options we have. The following few lines suggest some approaches based on the study of WLANs done in this research.

RECOMMENDATIONS

After looking at different security mechanisms, and threats, I would make some recommendations for those who are interested in making their WLANs relatively secured. Following the order of the sections, I would strongly recommend using WPA2 whether the WLAN is used at home or office. Almost all WNICs now support WPA2 encryption. AES mode is also proven to be more reliable than TKIP mode.

In PSK mode, choose the key carefully, the more random the better, avoid names, birth dates, and information that can be easily obtained. The longer the key, the better, for the current security situation, for home level, 12 characters would be fine. For offices, 12 characters might not be enough, if it is a highly targeted firm such as financial organizations, then the key should be as long as possible. Use different character groups, i.e. capital letter, small letters, numbers, and special characters. Change the key frequently.

[26] Tools such as wireshark and others, available at http://www.wireshark.org/, and http://www.wildpackets.com/

Hidden SSIDs and MAC filtering help increase security, use these options when applicable. There might be ten curious people, but not all of them know how to crack these. SSID is not recommended to be one of those on the well-known SSID lists[27].

Usage of management software programmes such as "LucidLink" (freeware), and "ManageEngine WiFi Manager" (license required) help discovering rogue APs. These programmes use management protocols, and techniques such as SNMP (Small Network Management Protocol), RF Scan, and others to discover APs in range and create signatures for them based on their MAC address, SSID, vendor, channel used, and other criteria as to identify any rogue APs in range. This would protect WLANs against "Evil Twin", and similar attacks.

Infrastructure design should be made professionals, bearing in mind product interoperability and compatibility. The design includes site surveys to check any possible signal interference, and the possibility of 'dead spots'[28] occurrence. It also includes the choice of proper hardware.

Make sure connections to wired networks are secured. Do not allow physical access to APs or network equipment to non-trusted people. Always keep computers and devices protected against viruses, worms, and Trojans. Some viruses use WLANs to infect all computers in the network as mentioned in section 2.7.

POSSIBLE IMPROVEMENTS

Comparing where WLANs stand with the current security requirements, they have a good security level, if they are properly configured; however, some things still can be added to improve their security. Hardware encryption, where the encryption / decryption functions are done by hardware, makes it harder to be cracked and protect against rogue APs. The key length can be extended to match the technology pace. In some cases, a two-way authentication system can be helpful where the user would have a password and a token or another piece of hardware to allow them access. Another issue that is not clear in (LAN MAN Standards Committee of the IEEE Computer Society, 2007), is how APs handle trust issues in mesh mode. What if an attacker deploys another AP with the same SSID in order to perform an evil twin attack? Why does not the WNIC create a digital identity for APs in order to differentiate rogue APs from genuine ones. The same concept can also be implemented on AP level. APs can store a digital ID of their peers in the same WLAN. This would minimize the possibilities of successfully deploying and operating rogue APs.

[27] See http://www.wigle.net/gps/gps/Stat for list example

[28] A dead spot is a zone between APs that should be covered but it is not or weakly covered.

Generally, WLANs are in a good position now when compared to security requirements; however, there is always room for improvements.

3. REVIEW OF WMAN[29]

3.1. WHAT IS IT?

The previous sections discussed WLAN which is a solution ideal for home and business use. Other entities, such as ISPs, were interested in such scheme. It would help them deliver their services to remote areas where no cable infrastructure exists. This would maximize their profit, and give them the option of expanding services. It would also solve one of the great problems ISPs have always had, which is the "last mile"[30] problem. (Yang, et al., 2005)

The last mile problem simply states that, for a given POP (Point of Presence), there is a distribution box that is acting a point to multi-point hop. The number of subscribers increase, but at the same time the physical area available to be used for their equipment remains the same, so the providers are running out of physical slots and wires. Having a wireless solution is one possible solution to this problem.

WLANs, however, are not sufficient to be used by ISPs since they can cover up to a few hundred metres with a maximum speed of 600 Mbps (IEEE 802.11n). ISPs need a method that can cover several kilometres in order to reach remote areas.

WMANs (Wireless Metropolitan Area Networks), is another approach that was designed for wireless broadband requirements. In 1999, IEEE formed a working group to achieve such task, and gave the solution the reference IEEE 802.16. Typically, WMANs' coverage varies from several building, and can reach up to an entire city. (Marks, et al., 2002) Unlike WLANs, WMANs have some more problems. This is due to the incomplete nature of the standard.

One of the main components of a WMAN is called BS (Base Station). A BS, which is located at the ISP's POP, is a tower transmitting wireless signals, and it is the link between the wired network of the ISP and the SS (Subscriber Station) / MS (Mobile Station). BSs are responsible for many tasks including resource allocation, key management, and other functions. (Hardjono, et al., 2005 pp. 190-193) SSs and MSs are the clients' equipment connected to BSs. They can be represented as home connections, office connections, or even Wi-Fi hotspots where public internet access takes place. WMANs are often referred to

[29] This section summarizes information from these sources: (Johnston, et al., 2004) (Marks, et al., 2002) (Hardjono, et al., 2005) (Wright, 2006) (Barbeau, 2005)

[30] Last Mile is the section from the provider's last point till the CPE (Customer Premises Equipment)

as WiMAX (Worldwide Interoperability for Microwave Access); more explanation comes later on in this section.

Figure 5 below[31] shows a simple WMAN / WiMAX topology.

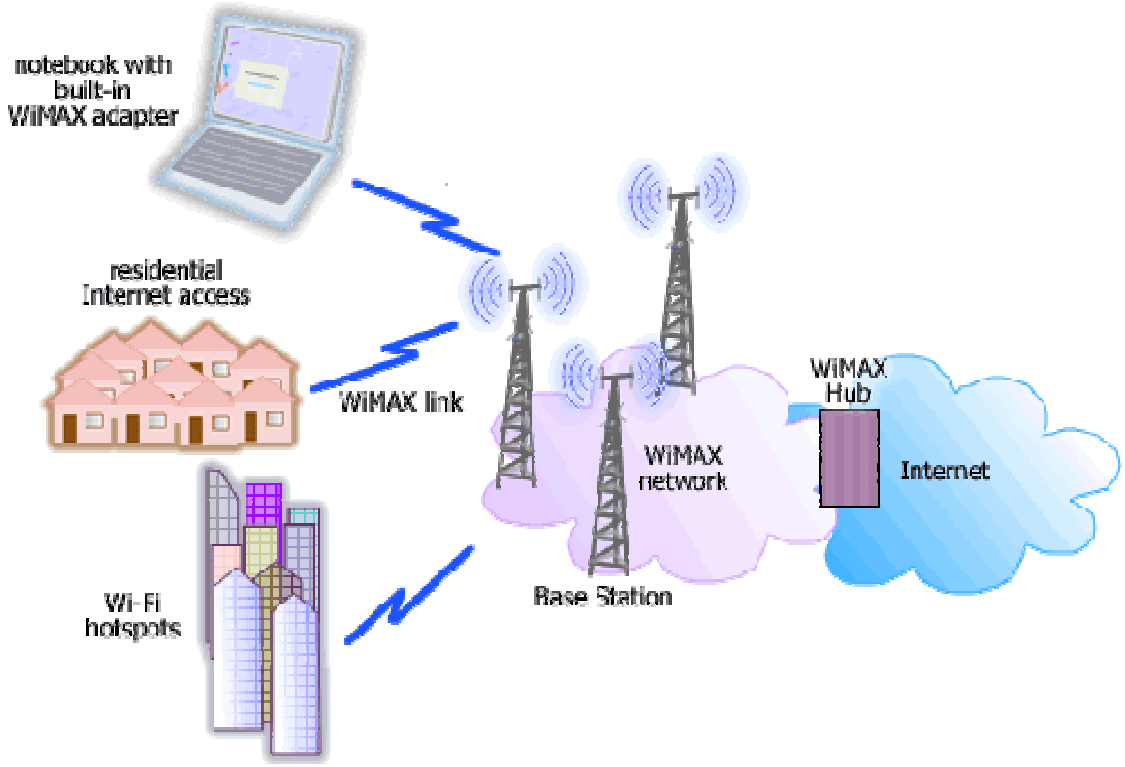

FIGURE 5: SIMPLE WMAN

The name WiMAX was given to WMANs by a non-profit organization consisting of more than 500 member companies and operators devoted to promote WMANs; it is similar to Wi-Fi Alliance in WLANs, but concerned with WMANs. This organization's name is WiMAX forum[32].

Services of WiMAX are not limited to ISPs; governments also showed interest to establishing infrastructure in regional areas. Recently, the NSW government has announced that they have plans to use WiMAX to get regional suburbs connected to the broadband network. (LeMay, 2007) "It is also known that WiMAX is emerging as a complementary technology and that future client devices will be both Wi-Fi and WiMAX enabled" wrote the state.

[31] Figure obtained from http://www.conniq.com/images/Access_WiMAX.gif
[32] Full information available at http://www.wimaxforum.org/about/about-wimax-forum-overview

(LeMay, 2007) The following section will discuss the architecture of WMANs, and later on, security approaches and threats will be handled.

3.2. ARCHITECTURE

WMANs are a component of the IEEE 802 set of standards. They operate on the same seven layered OSI model[33]. The differences, as usual, lie in the first two layer, PHY and Data Link layers.

Figure 6 below[34] shows the 802.16 first two layers, the upper layers are the same as the ones in WLAN (Figure 3).

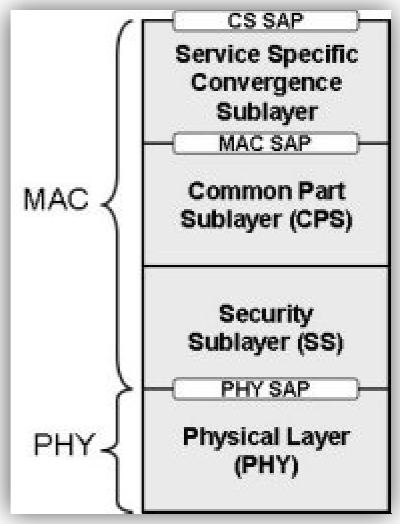

FIGURE 6: 802.16 LAYERS

The physical layer has the same function as the one mentioned in WLANs (refer to section 2.2); however, the signalling techniques are different. The following lines will start describing the physical layer and then move on with layer two explanation.

Before we start, two terms that will be used in many occasions have to be explained. LOS (Line-of-sight transmission), this means that the signals are flowing in a straight line, and that the signals are exposed to reflection, refraction, and other types of attenuation. NLOS (Non-line-of-sight transmission), this is the inverse of line-of-sight transmission where waves can travel through an obstructed path.

[33] See Glossary for definition.
[34] Figure obtained from http://www.dalewright.net/2006/11/29/intro-to-wimax-and-ieee-80216

PHYSICAL LAYER

Since physical layer functions were already stated previously, we will move on to the details regarding this layer in WMANs. There are two directions of communication in WMANS, BS to SS which is known as Down Link, and SS to BS which is knows as Up Link.

The reserved frequency band for WMANs starts from 2 GHz until 66 GHz. This range is divided into three sub-ranges.

- 10 to 66 GHz (licensed bands): In this range, the type of transmission is LOS since the wavelength is short which makes it more vulnerable to attenuation. (Hardjono, et al., 2005 p. 192)
- 2 to 11 GHz (licensed bands): In this range, LOS is not required; however, its existence can significantly increase the performance. (Hardjono, et al., 2005 p. 192)
- 2 to 11 GHz (unlicensed bands): This is similar to the licensed bands, but interference may occur since it is unlicensed. (Hardjono, et al., 2005 p. 192)

In the 10 to 66 GHz range, TDM (Time Division Multiplexing) is used in the Down Link transmission where every SS is allocated a timeslot, while TDMA (Time Division Multiplexing Access) is used in the Up Link transmission. TDM is used in the Down Link because it s coming from a fixed node, in other words, BS does not move; however, since TDMA supports transmitting from different nodes, it is used in the Up Link because SS/MS might change its location during the transmission.

In the 2 to 11 GHz range, the PHY layer is divided into more than one sub-layer to support different air interfaces; however, in this document we just mention two of them; WirelessMAN-OFDM, and WirelessMAN-OFDMA. OFDM concept was explained earlier in WLANs (refer to section 2.2); OFDMA is the multi-user version of OFDM, the same concept of TDM / TDMA. For further details regarding the PHY layer and its sub-layers refer to (IEEE Computer Society and the IEEE Microwave Theory and Techniques Society, 2006 pp. 317-650)

The designers of 802.16 used resources to avoid glitches like those in 802.11. They tried to learn from the inefficient WEP, and used another set of standards called DOCSIS (Data Over Cable Service Interface Specification). DOCSIS is a standard supported by prominent networking companies, and it is concerned with many networking issues including MAC (Media Access Control) layer security[35]. The problem is that DOCSIS is designed for cable services; it does not really care about PHY layer, on the other hand, WMANs are wireless, anyone within the transmission range can capture the signals and maybe tamper with them

[35] Full Information available at http://www.docsis.org/

if they have the right equipment. This made WMANs vulnerable to PHY layer attacks, which is one of the issues that can be improved.

MAC LAYER

As shown previously in figure 6, the MAC layer of 802.16 is divided into three sub-layers; Service Specific Convergence sub-layer (CS), Common Part sub-layer (CPS), and the Security sub-layer (SS). This is the reason why some references describe the model as a four layer model. Each of these sub-layers is responsible for certain tasks. We will go through the three sub-layers from bottom to top.

- ***SECURITY SUB-LAYER***
  The Security Sub-layer is responsible for encryption and cryptography, authentication and key management, which will be discussed soon in section 3.3. SA (Security Association) is used for security parameter exchange between BSs and SSs. SAs are identified by SAID (Security Association Identifier) (Marks, et al., 2002 pp. 102-107) (Wright, 2006)

- ***COMMON PART SUB-LAYER***
  The Common Part Sub-layer is responsible for managerial tasks such as bandwidth allocation, QoS (Quality of Service), manage communication with CS and SS, and other tasks. (Marks, et al., 2002 pp. 102-107) (Wright, 2006)

- ***CONVERGENCE SUB-LAYER***
  The Convergence Sub-layer is responsible for receiving data from upper layers in their format (typically ATM or IP), and converting them into the appropriate MAC format. (Marks, et al., 2002 pp. 102-107) (Wright, 2006)

After having an overview of the MAC layer, we move to the core of WMANs security. The main security feature in WMANs or WiMAX is called PKM (Privacy Key Management), which will be discussed in the following section. After some steps are performed by the SS (Subscriber Station), comes the authentication phase which involves PKM. These steps include, detecting a BS, synchronizing with it, retrieving parameters, and other steps[36].

[36] See (Hardjono, et al., 2005 pp. 194-196)

3.3. PKM (PRIVACY KEY MANAGEMENT)

Since WMANs are designed for broadband access, they have to support multi-user access, which they do; they also need to authenticate them (achieved using PKM).

PKM operates in the Security Sub-layer. The normal flow of sequence starts with the SS requesting to join the network, this request is made to a BS. As in client-server architecture, the SS is the client, whereas BS is the server. The client sends a request to the server and the server replies. The communication between both ends uses 3DES for encryption, which is a quality encryption algorithm that proved its reliability. Also the BS uses X.509 certificates[37] to authenticate clients. For further security, the certificate at the client side is actually embedded in hardware by the device manufacturer. This is used to protect them from being extracted and tampered with. Hardware also contains the device the private key used in encryption / decryption processes, MAC address (48 bits), vendor, and other information. (IEEE Computer Society and the IEEE Microwave Theory and Techniques Society, 2006 pp. 269-272)

The SS now sends the BS a copy of the certificate, followed by a number of parameters including the serial number, SAID, cryptographic capabilities, along with other information. On the other side, the BS verifies the certificate and other parameters such as cryptographic capabilities, and if they are found to be valid and supported, the BS sends what is called AK (Authorization Key). This key is used during the authorization process to encrypt the rest of the authorization operation. AK is sent to SS encrypted with the public key available in the certificate, but since AK has its private key embedded, it is able to decrypt the message and obtain the AK. The message sent by BS also contains the key lifetime (one to 70 days), its sequence number (4 bits), and SA descriptors to be used later on.

SS has to maintain a valid AK at all time; therefore, it has to do a reauthorization process before its key expires. During the reauthorization process, the SS is not required to send the initial message to let the BS know its identity since it is already known from the previous active session. The goal behind having two active AKs is to avoid service interruption for reauthorization process. Once the reauthorization process is over, the older key is declared invalid. (IEEE Computer Society and the IEEE Microwave Theory and Techniques Society, 2006 pp. 272-275)

[37] See Glossary for definition

Figure 7 below[38] shows the process of obtaining the AK; it also shows the process of obtaining TEK which is explained below.

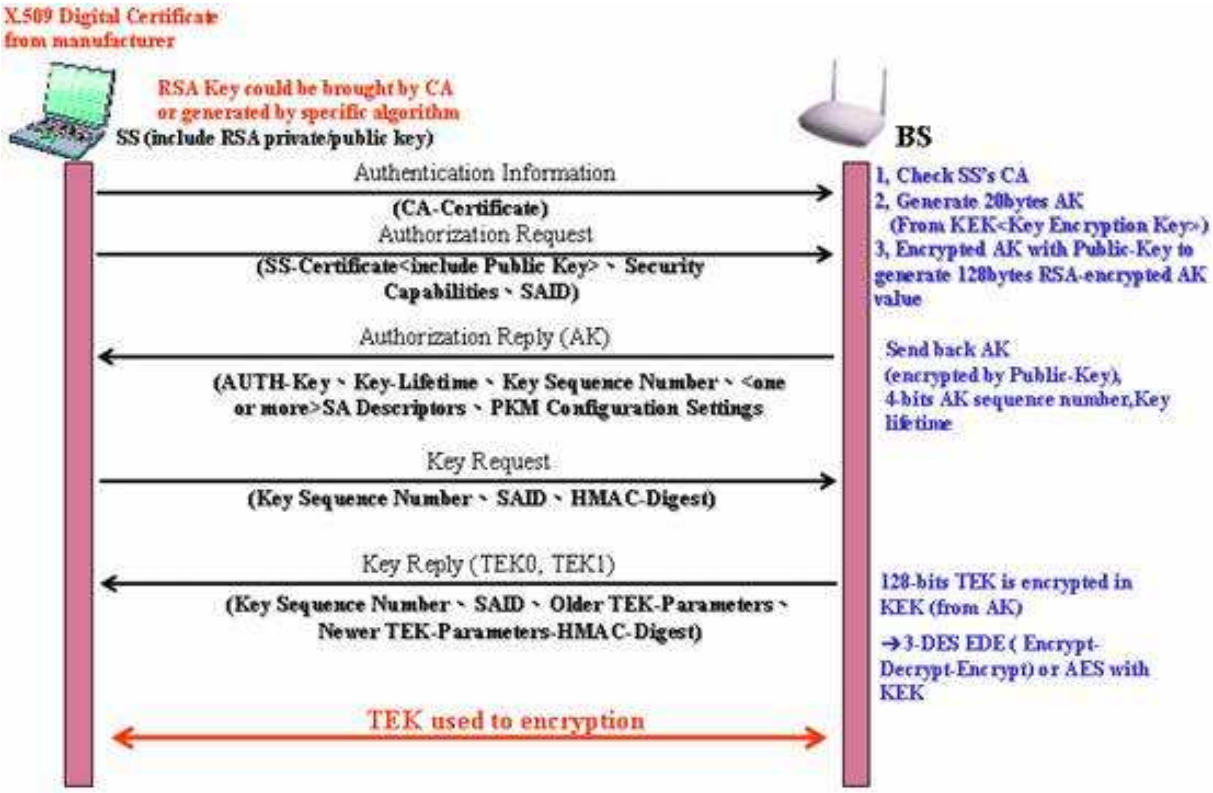

FIGURE 7: PKM AUTHORIZATION

Once the AK is obtained, the process of obtaining TEK (Traffic Encryption Key) begins. TEK is used to encrypt the user's traffic during the session lifetime. The same concept of the SS having two AKs at a given time also applies to TEKs (that is why there are two TEKs in figure 7). TEK's lifetime can vary from twelve hours to seven days. A request for a new TEK is made before it expires. The process of obtaining a TEK is similar to AK's one.

Since the SS has an AK, it is now authorized to request a TEK. It starts by sending a *key request* message. This message contains a set of parameters; these include, SAID, the SS's serial number, MAC address, public key, HMAC-Digest (used as identity proof) and other information.

BS receives the request from SS, checks its integrity, and validates it (using the HMAC-Digest); if it is found to be genuine and unmodified, the BS then generates and replies with

[38] Figure obtained from http://loda.zhupiter.com/80216security/image004.jpg

TEK, its sequence number, lifetime, HMAC-Digest, and other parameters. The life time sent by BS helps the SS identifying when the next TEK request should be scheduled. (IEEE Computer Society and the IEEE Microwave Theory and Techniques Society, 2006 pp. 272-275)

In this section we looked at how PKM works, what it uses for encryption, and the measures taken to secure communication between BSs and SSs / MSs. Some of the information mentioned, such as the lifetime of AKs and TEKs, use of certificates, and others, will be referred to in the next section for security assessment.

3.4. Security Issues

As mentioned earlier, the designers of WMAN tried to learn from the previous mistakes and technologies while developing this standard; however, due to the differences of the application natures, some problems and vulnerabilities exist.

Security in many applications is measured by the CIA (Confidentiality, Integrity, and Availability) triad. Confidentiality is the target of making information accessible for authorized entities only. Integrity means data should not be modified by unauthorized entity. Availability means data / service should be available whenever it is needed. (Nichols, et al., 2002 p. 84) The three components the triad are vulnerable to be violated in the current WMAN standard.

Physical layer

We first start with physical layer attacks. The physical layer is left relatively unsecured in the current 802.16 model. The signalling technique used is OFDM / OFDMA as mentioned in section 3.2 is a reliable technique, it is efficient and adaptable to channel changes, but it is vulnerable to attacks such as “water torture”.

Water torture attack is when an attacker sends a stream of frames which causes the receiver’s battery to drain. (Johnston, et al., 2004) This violates the Availability requirement in the CIA triad.

DoS

Another famous way to violate the Availability component is DoS (Denial of Service) attack. DoS attacks aim to deny the server (BS in our case) from providing its services to clients. DoS attacks have numerous techniques. They are not discussed here[39]; however, the relatively unprotected physical layer allows attackers to jamming the radio spectrum if they have the appropriate equipment, thus denying the service from all parties. This adds

[39] Refer to RFC 4732 at http://tools.ietf.org/html/rfc4732 for further information regarding DoS.

another method to accomplish successful DoS attacks on WMANs to the existing ones such as sending requests for connection initialization. (Johnston, et al., 2004)

The transmitted signals are always vulnerable to be captured if proper equipment is used, nothing can prevent that. Here comes the layer two security function; if attackers successfully capture signals, they should not be able to interpret the message; the same idea is mentioned in WLANs and in the pre-computer era. One point to be emphasized; WLANs are moving from LOS architecture to NLOS architecture; this makes it easier for attackers, since they don't have to be between the BS and SS.

MAC LAYER ATTACKS

There are a number of existent threats for the MAC layer. First of all, the current authentication scheme in the PKM protocol allows only BSs to authenticate SSs. By using this method, the BS would know that the SS is eligible to acquire services, but the SS cannot know whether the BS is genuine or rogue. In WLANs, this was easy since every network operator manages their AP; on the other hand, in WMANs, BSs belong to some ISP (can be national, regional, or local ISP); SSs have no management rights over them. This lack of mutual authentication poses a number of threats including, "Evil Twin" which was referred to earlier in section 2.7; however, it is harder to implement such attack in WMANs because of the BS size, cost, and the needed experience to configure and operate it; yet, it is still possible to be done. In some cases, RS (Relay Station), a type of equipment used to extend WMAN signals is used; attackers can deploy them and just be a hop in the middle between SSs and the BS.

Other threats can also use the lack of mutual authentication. Data can be intercepted in the middle; contents can be modified and forwarded to the customer or to the attacker's equipment; generally, man-in-the-middle, and the related attacks (replay attack, relay attack, etc...). All these attacks violate the other two components of the CIA triad.

OTHER VULNERABILITIES IN EXISTING WMAN MODEL

Although strong encryption mechanisms are used in WMANs (3DES), the long lifetime of the keys makes them vulnerable to be cracked. For instance, AK's lifetime varies from one to 70 days, and the TEK's life time from twelve hours to seven days. It might take the attacker a long time to crack the keys; however, these numbers are enough for the attackers to accomplish their mission. Again, mutual authentication can solve this problem. (Johnston, et al., 2004). Mutual authentication is taking a part of the new version of PKM, PKMv2. (IEEE Computer Society and the IEEE Microwave Theory and Techniques Society, 2006 pp. 275-296)

The sequence number of the keys is another threat. The AK has a sequence number of four bits; this can easily be cracked. This small range increases the chances of replay attacks.

Another concern, but it is not discussed in this paper, is security in mesh mode. How would different BSs authenticate each other if they do not have certificates? Also, roaming support, when the client is moving from one BS to another does not have an explicit definition for how it is handled. This needs to be clearer than what is mentioned in (IEEE Computer Society and the IEEE Microwave Theory and Techniques Society, 2006).

In this section, we have discussed different attacks threatening current WMAN model. These attacks can violate the three components of the CIA triad.

3.5. Result – Securing WMANs

Before We Start

I'll start this section by referring to the same concept in section 2.8. Perfect security does not exist. The goal is achieve the highest possible level of security. This level of security in WMANs is limited because of its incomplete nature. Some security holes are expected at this stage. When WLAN was first release, its security measures were disappointing. Many amendments are already in progress to improving such standard[40].

This section contains the result of efforts to improve WMANs security. The results are inspired by some previous work discussed earlier in the document, and a continuation to some of them.

What can be improved?

As a result to the previous section, the first possible improvement, and it is actually in the implementation phase now, is mutual authentication. Mutual authentication will not just help SSs to authenticate BSs; it will mitigate the risk of many attacks such as man-in-the middle attack, replay attack, and relay attack. Another method that can help is time stamping the transmitted packets. Time stamps are not existent in (IEEE Computer Society and the IEEE Microwave Theory and Techniques Society, 2006). They are simple, but extremely useful. Usage of time stamps mitigates the risks of man-in-the-middle and similar attacks. When the packet is received, the time stamp gets checked, if its value is found to be older than what is expected, which the case if it was captured and changed in the middle, it gets discarded.

Another great issue that needs to be patched is physical layer security. Although jamming signals can be detected using spectrum analysers, they cannot stop the attack. Research on

[40] See Current work in progress at http://ieee802.org/16/tgs.html

physical layer security is active, and trying to find solutions. Suggestions and papers can be submitted to entities[41]. Maybe the previous experience of WLANs can be taken into consideration, and make WMANs support other signalling techniques if the current ones used are vulnerable to some physical layer threats. TDM (Time Division Multiplexing), for instance, is harder to be attacked since it is time related; it is hard for an attacker to capture packets, change them, and then resend them in the right timing. It is practically easier to do such task in FDM (Frequency Division Multiplexing); all the attacker needs to obtain is the frequency on which the victim's traffic is submitted.

The idea of embedding certificates in hardware is proven to be effective. It makes the cost of a successful attack (i.e. extraction of information from hardware) more than what the attacker would gain. A supporting solution for this approach is keeping track of the location of the connected devices based on the signal strength or visibility by other BSs (same idea as mobile phone tracking), maybe using the serial number or a digital ID of hardware for the device as a primary key to uniquely identify different devices. If this device attempts to access from a different location within a short period of time, this might be because its identity has been stolen.

Lifetimes of AK and TEK can be minimized. According to the application of WMAN, where it is used broadband access, the lifetime of the keys cannot be just an hour, this would overload the network with added traffic; however, if the AK lifetime can have a maximum value of less than a day, and the TEK lifetime can have a maximum lifetime of a day, the risk of successful key cracking would be mitigated assuming the current encryption mechanism is in use.

In 2004, IEEE published their document IEEE 802.1X which discusses a lot of security concerns. 802.16 can be integrated with some sections of the document such as the EAP protocol mentioned earlier. EAP can be used along with the certificates for enhanced authentication mechanism.

This section discussed some possible improvements that can contribute in increasing WMAN's security. Although it is already widely used (currently in use in more than 135 countries)[42], and the position where it stands with respect to security world is not bad, development in its security architecture is expected to match security requirements that are increasing rapidly.

[41] See http://www.newcom-project.eu:8080/Plone/news/jcwn-on-wireless-physical-layer-security
[42] See http://www.wimaxforum.org/ for more information

4. CONCLUSION

Recently, wireless networking has become more popular. It is growing in technology and popularity as well. Many reasons are supporting its growth; these include, mobility, room saving, less cost than LANs, and others. There are two common forms of wireless networking, WLANs and WMANs. WLANs are commonly used on home and office levels, while WMANs are used for wireless broadband access. Due to the sensitivity of data transmitted over networks, security is a requirement that cannot be waived. On the other hand, attackers are eagerly watching and trying to exploit vulnerabilities to subvert networks or get illegal access and take advantage of them.

We started with WLANs, and explained their architecture and layers in sections 2.1 and 2.2. Then, in sections 2.3 to 2.6, security topics were discussed explaining how WEP, WPA, WPA2, and other security approaches work. Their strengths and weaknesses were identified and analysed. In section 2.7, we discussed available threats that might not be known by many people. Evil Twin and War Driving, for example, are threats the can be implemented by non-experts, and they can have great impacts. It is recommended that WLAN operators know about them, and be able to protect their networks and assets from damage or loss posed by these threats. Possible remediation for them was discussed later in section 2.8; this includes usage of management software programmes, and certain password complexity level to secure WLANs as much as possible. Also, as a result to the research done, some possible improvements, such as two way authentication, were suggested to contribute with the development of the protocol; however, with respect to the current security requirements, WLANs have decent defensive methods to keep them relatively protected.

The other major section in the document was discussing WMANs. It also started with a description of what they are in section 3.1. We then moved from a general view of the standard to the details of its operation. This included looking at WMANs' relatively unprotected physical layer in section 3.2, which makes them vulnerable to several physical layer attacks, such as water torture and jamming. Going deeper in security, we moved to the MAC layer which provides the main security features for WMANs. For example, PKM, which is used for authentication, is a strong technique; however, it is not free of flaws. Its flaws and other existent security problems in the standard, such as the lack of mutual authentication, were discussed in section 3.4. In the end, the result of research and evaluation work took place in section 3.5 where possible improvements, such as shortening the keys' lifetime, and physical layer security, were suggested.

One concept remains, perfect security does not exist. Attackers will always try to discover vulnerabilities and exploit them. Network operators should be aware of the existent threats in order to be able to mitigate the risks caused by these threats.

5. ABBREVIATIONS

AES	Advanced Encryption Standard
AK	Authorization Key
AP	Access Point
ASCII	American Standard Code for Information Interchange
ATM	Asynchronous Transfer Mode
BS	Base Station
CCK	Complementary Code Keying
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code
CPE	Customer Premises Equipment
DOCSIS	Data Over Cable Service Interface Specification
DoS	Denial of Service
DSSS	Direct Sequence Spread Spectrum
FDM	Frequency Division Multiplexing
FHSS	Frequency Hopping Spread Spectrum
HR/DSSS	High Rate Direct Sequence Spread Spectrum
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IR	Infrared
ISM	Industrial, Scientific, and Medical
IT	Information Technology
LLC	Logical Link Control
LOS	Line Of Sight
MAC	Media Access Control
MIMO	Multiple Input and Multiple Output,
MS	Mobile Station
NIC	Network Interface Card
NLOS	Non Line Of Sight
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiplexing Access
PBKDF2	Password-Based Key Derivation Function
PHY	Physical
PKM	Privacy Key Management
POP	Point Of Presence
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
SA	Security Association
SNMP	Small Network Management Protocol
SS	Subscriber Station
SSID	Service Set Identifiers

TDM	Time Division Multiplexing
TDMA	Time Division Multiplexing Access
TEK	Traffic Encryption Keys
TKIP	Temporal Key Integrity Protocol
WEP	Wired Equivalent Protection
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WNIC	Wireless Network Interface Card
WPA	Wi-Fi Protected Access

6. REFERENCES

Barbeau, Michel. 2005. *WiMax/802.16 Threat Analysis.* Ontario, Canada : Carleton University, 2005. ACM 1-59593-241-0/05/0010.

Beck, Martin and Tews, Erik. 2008. *Practical attacks against WEP and WPA.* November 8, 2008.

Borisov, Nikita, Goldberg, Ian and Wagner, David. 2001. *The Insecurity of 802.11.* Rome, Italy : s.n., 2001. ACM ISBN 1-58113-422-3/01/07.

Boyd, Clark. 2008. Profile: Gary McKinnon. [Online] BBC News, July 30, 2008. [Cited: May 27, 2009.] http://news.bbc.co.uk/2/hi/technology/4715612.stm.

Cypher Research Laboratories Pty. Ltd. A Brief History of Cryptography. [Online] [Cited: May 22, 2009.] http://www.cypher.com.au/crypto_history.htm.

Elliott, Christopher. 6 Wireless Threats To Your Business. [Online] Microsoft. http://www.microsoft.com/smallbusiness/resources/technology/broadband-mobility/6-wireless-threats-to-your-business.aspx#wirelessthreatstoyourbusiness.

Federal Information Processing Standards. 2001. *Announcing the ADVANCED ENCRYPTION STANDARD (AES).* s.l. : NIST, November 26, 2001. FIPS Publication 197.

Forouzan, Behrouz. 2004. *Data Communications and Networking.* 2004. ISBN 007-123241-9.

Fred Cohen & Associates. 1995. A Short History of Cryptography. [Online] 1995. [Cited: May 22, 2009.] http://all.net/books/ip/Chap2-1.html.

Gordon, Jon. 2006. Invisible wireless dangers stalk the unwary. *www.fortinet.com.* [Online] South China Morning Post, October 31, 2006. http://www.fortinet.com/news/media/apac2006/Anti-virus01031.pdf.

Hardjono, Thomas and Dondeti, Lakshminath. 2005. *Security in wireless LANs and MANs.* 2005. ISBN-10:1-58053-755-3.

IEEE Computer Society and the IEEE Microwave Theory and Techniques Society. 2006. *IEEE Std 802.16e™-2005.* New York, United States of America : IEEE Computer Society, February 28, 2006. Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems.

Johnston, David and Walker, Jesse. 2004. *Overview of IEEE 802.16 security.* s.l. : Intel, 2004. IEEE 1540-7993/04.

LAN MAN Standards Committee of the IEEE Computer Society. 2007. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.* USA : IEEE, 2007. ANSI/IEEE Std 802.11, 2007 Edition.

—. 1997. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.* USA : IEEE, 1997. ANSI/IEEE Std 802.11, 1997 Edition.

LeMay, Renai. 2007. NSW calls for free Wi-Fi builders. [Online] ZDNet Australia, January 29, 2007. http://www.zdnet.com.au/news/communications/soa/NSW-calls-for-free-Wi-Fi-builders/0,130061791,339273255,00.htm?feed=pt_network.

Marks, Roger B., et al. 2002. *IEEE Standard 802.16: A Technical Overview of the WirelessMAN™ Air Interface for Broadband Wireless Access.* 2002. IEEE C802.16-02/05.

Nichols, Randall K. and Lekkas, Panos C. 2002. *Wireless Security Models, Threats, and Solutions.* s.l., United States of America : The McGraw-Hill Companies, Inc., 2002. 0-07-138038-8.

Raymond. 2007. How To Discover Hidden Wireless Network. *Raymond.cc.* [Online] November 4, 2007. [Cited: March 20, 2009.] http://www.raymond.cc/blog/archives/2007/11/04/how-to-discover-hidden-wireless-network/.

Wang, Maocai, et al. 2008. *Security Analysis for IEEE802.11.* 2008.

Wikipedia. Heinrich Hertz. *Wikipedia, the free encyclopedia.* [Online] [Cited: May 24, 2009.] http://en.wikipedia.org/wiki/Heinrich_Hertz.

—. History of radio. *Wikipedia, the free encyclopedia.* [Online] [Cited: May 24, 2009.] http://en.wikipedia.org/wiki/History_of_radio.

Wong, Stanley. 2003. *The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards.* 2003.

Wright, Dale. 2006. Intro to WiMax and IEEE 802.16. [Online] 2006. [Cited: May 20, 2009.] http://www.dalewright.net/2006/11/29/intro-to-wimax-and-ieee-80216/.

Yang, Fan, et al. 2005. *An Improved Security Scheme in WMAN based on IEEE Standard 802.16.* Wuhan, China : s.n., 2005. 0-7803-9335-X/05.

7. GLOSSARY

HEXADECIMAL

Hexadecimal is a numeral system with a base of 16. When compared to decimal numbering system, they match from 0 to 9, then 10 in decimal is A in hexadecimal, 11 is B, up to 15 which is F. [See http://en.wikipedia.org/wiki/Hexadecimal]

HUB

A hub is a device connecting different computers / network devices together. It is less efficient than switches and bridges because of its mode of operation. [See http://en.wikipedia.org/wiki/Network_hub]

MIMO (MULTIPLE INPUT AND MULTIPLE OUTPUT)

MIMO is the technique of using multiple antennas for transmitting and receiving data which can result in higher speed and wider range of coverage. [http://en.wikipedia.org/wiki/MIMO]

OSI MODEL

OSI model is developed by ISO to represent networking functions in different layers. It consists of seven layers. Each of these layers is responsible for different tasks. It starts with Physical layer (Layer one), and ends with Application layer (Layer seven) [See http://en.wikipedia.org/wiki/Osi_model]

ROUTER

A router is device used to connect different networks together, and deliver data from a network to another. [http://en.wikipedia.org/wiki/Router]

SALT

Salt is usually a number of random bits used in cryptography to be used along with the key for better encryption; however, in some cases, it is not a randomly generated value, but a word used to hardening the encryption key [See http://en.wikipedia.org/wiki/Salt_(cryptography)]

SCYTALE

Scytale is a method of encryptions used by the Spartan army. Its idea is wrapping a thin sheet of papyrus around a stick, and writing the message down the length of the staff. If the sheet is then unwrapped, it would be unreadable. It has to be wrapped around an identical stick so people could read it. [See http://en.wikipedia.org/wiki/Skytale]

SERVER

A server is commonly known to be a computer / entity offering service to other entities commonly known as clients. [See http://en.wikipedia.org/wiki/Server_(computing)]

SWITCH

A switch has the same goal of a hub; however, it is more efficient because of due to its method of operation. [See http://en.wikipedia.org/wiki/Network_switch]

X.509 CERTIFICATE

X.509 certificates are usually used in authentication. They consist of a number of entries, these include, issuer, serial number, creation date, expiry date, public key, and other information. Each host has two keys, private key, and a public key. Data is encrypted with one of both and decrypted with the other. [See http://en.wikipedia.org/wiki/X.509]