ITEC810 Securing WLANs and WMANs

Peter Nicola
Department of Computing
Macquarie University
Sydney, Australia
peter.nicola@students.mq.edu.au

Abstract

Recently, wireless networking has become a central part of the work and leisure activities of many people. It is being widely used on both enterprise and home levels. It is a "dream coming true" to finally get rid of all the cabling and wire mess. Two common forms of wireless networks are WLANs and WMANs. Both of them will be discussed in this paper. Sensitive information such as credit card details, confidential documents, and passwords are always expected to be travelling through wireless communication channels. Attackers are mainly targeting this type of data to use them for their benefits. A certain level of security is required to maintain a relatively safe environment for data communication. The aim of this paper is to identify and explain low level threats, and suggest how to protect wireless networks against them.

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 in all aspects of life. This paper is concerned with wireless communication security which is a variation of communication security itself. Communication security existed in the pre-computer era. According to historians, ancient Egyptians and Greeks used non standard languages and other tools to cipher their messages. That is if someone captures the messenger and steals the message, they would not be able to interpret what it says. The same idea exists in wireless communication. The difference is in the medium and the form of messages. In the following sections, a security assessment for two wireless network schemes will be done discussing different types of attacks and how to reach a relatively satisfactory level of security.

1.2 Wireless Network Introduction

Wireless networks are just another form of computer network. They use a wireless transmission medium instead of using a wired one such as copper cables. This has significant advantages; including getting rid of all the cables and the mess caused by having many connections and in providing mobility to users. On the other hand, since it is wireless, anyone within the range of transmission would be able to capture these waves. Two common forms of wireless networks are WLANs and WMANs. WLANs are often used on home and office level. WMANs however have a greater geographical scale which can cover several kilometres up to an entire city. It is commonly used by ISPs to cover such areas having no cable connectivity. Both forms have security vulnerabilities that give room to attackers to subvert them. Protecting lower levels of networks always helps strengthening the network as whole. The following sections will handle WLAN and WMAN security at low levels.

2 Review of WLAN[2]

WLAN (Wireless Local Area Network) is the implementation of LANs but using a wireless transmission medium. IEEE has standardised this approach in 1997 giving it the reference IEEE 802.11 (LAN MAN Standards Committee of the IEEE Computer Society, 1997). It is also known as Wi-Fi. The main equipment in a typical WLAN would be an AP (Access Point). It con-

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

[2] This section summarizes information from these sources: (IEEE Computer Society, 1999) (Wang, et al., 2008) (Beck, et al., 2008) (Borisov, et al., 2001) (Thomas Hardjono, 2005) (LAN MAN Standards Committee of the IEEE Computer Society, 2007) (Elliott)

nects devices such as computers or PDAs if they are equipped with a WNIC (Wireless Network Interface Card) to a wired network. This scheme is ideal for home and office use. Its coverage range is usually up to 100 metres; however, a new edition of the standard, IEEE 802.11N expands both the range and the former 54Mbps speed. Typically, the difference in WLANs with respect to LANs would be in the first two layers in the OSI model, Physical and Data Link layers. The physical layer is the one where the modulation / demodulation processes are involved. It supports many signalling techniques such as FH (Frequency Hopping), IR (Infrared), and others. Figure 1 below[3] shows the layer of 802.11

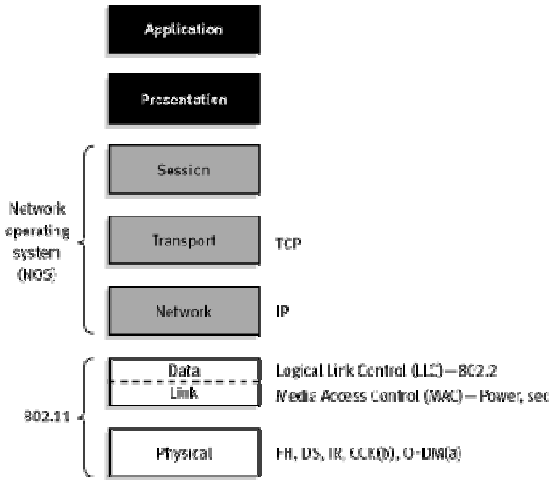

Figure 1: 802.11 Layers

Moving to the upper layer, the Data Link layer, it is divided into two others, LLC (Logical Link Control) and MAC (Media Access Control). Security lies in the MAC sub-layer. The following sub-sections will discuss different security approaches provided by this sub-layer.

2.1 WEP

WEP stands for Wired Equivalent Privacy. It was meant to provide the same level of security as in wired networks. It came out with the 1997 edition of the standard which is the original version. (LAN MAN Standards Committee of the IEEE Computer Society, 1997) Unfortunately, WEP had a disappointing design; people could break it and get illegal access to the network within minutes. WEP originally used a 40 bit shared key represented in hexadecimal format (which means 16 possibilities per character), + a 24 bit IV (Initialization Vector) that is used in RC4 algorithm. (Wang, et al., 2008) Amendments were proposed to solve this weak design that could be broken easily with a brute force attack; these amendments expanded the 64 bit WEP from 64 bits (Key + IV) to 128 bits, and then to 256 bits. It was slightly better than the standard WEP version, but it had a very critical problem. RC4 is based on an XOR function of the plaintext with the key, if an attacker could capture a sequence of packets, they would be able to reverse the mathematical calculation and obtain the key.

2.2 WPA

Because of WEP's bad reputation, attempts were made to produce a better security technique to enhance security in WLANs. In 2003, the Wi-Fi Alliance introduced WPA (Wi-Fi Protected Access). It became a standard feature in 802.11 in the IEEE document 802.11i-2004. One main difference between WPA and WEP is the key space used. WPA uses ASCII characters, which leads to 95 possibilities per character. Such larger key space leads to longer time when it comes to brute force attacks. The key length can vary from 8 to 63 characters. This scheme is called WPA-PSK (PSK stands for Pre-Shared Key). PSK is still vulnerable to password cracking if a weak paraphrase is used. WPA was definitely an improvement in WLAN security. Considering a brute force attack, it would take the attacker very long time to crack the key. PSK however is not suitable for corporate level networks since it is based on a shared key. In this case, a RADIUS server can be integrated to manage user accounts so that each user would have their own username and password. Another drawback in WPA-PSK is that it used the same encryption algorithm in WEP, RC4. It made it vulnerable to the key derivation from capturing a sequence of packets.

2.3 WPA2

WPA was a sort of remediation to WEP, but it was not up to the security requirements due to the flaws in the RC4 algorithm. Just after WPA was standardized, Wi-Fi Alliance released their new edition of WPA, and gave it the name, WPA2. WPA2 uses a stronger encryption algorithm called PBKDF2. This algorithm is not a stream cipher like RC4; it actually takes the key and processes it in a pseudorandom function with a salt value. This process is repeated hundreds of times before an encrypted text would be finally produced. WPA2 operates in two modes, PSK, and EAP (Extensible Authentication Protocol). Whereas PSK mode is the same as before, but

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

using better encryption techniques, and EAP is the scheme used for enterprise level when integrating the WLAN with a RADIUS server to manage user accounts. Whether WPA2 is operating in PSK mode or EAP mode, it supports two modes of ciphering techniques, these are TKIP and AES. TKIP (Temporal Key Integrity Protocol) mixes the key and an IV generated by the protocol, and then processes them in a hash function. AES is based on DES. AES is being used by the US government. It is a block cipher algorithm offering a very strong encryption algorithm and is very popular now these days because of its high reputation.

2.4 Other Security Approaches

Other than encryption and the discussed approaches, some regular ways exist to help increasing security. Any WLAN has an SSID (Service Set Identifier). It is the name of the wireless connection and is usually represented in ASCII characters. SSIDs are necessary to be connected to the wireless network. By default, SSIDs are broadcasted by APs so that anyone within the transmission range would be able to find the wireless network. SSIDs are not a security approach themselves, but hiding them is considered as a way to help increase the security. Even on cheap APs, there is an option to hide the network. By checking this option, the AP will not broadcast the network name which is required for successful communication. Connection settings have to be manually configured on every device seeking to be connected. This option might seem promising; however, software programmes such as “NetStumbler” can detect all APs within the range of the WNIC including the hidden ones.

Any device equipped with a WNIC has a physical address; it is usually a unique 6 byte hexadecimal address. APs can filter clients based on that address, but again software programmes such as “MACshift” were created to forge this address. The point here is that hiding SSIDs and using access lists to filter MAC addresses are not sufficient to achieve a fair level of security, but they can help increasing security and mitigate the risk. There might be ten curious people within the range of a WLAN, but not all of them know how to discover a hidden WLAN, or forge MAC addresses.

2.5 Common Threats

The previous sub-sections discussed advanced threats in WLANs. That means they require special hardware equipment and software programmes to successfully attack them. Attacking hidden SSIDs and forging MAC addresses are not considered as advanced attacks. Along with these two come a lot of other threats, varying from amateur level to advanced ones. Below are some of these threats. Network operators are encouraged to know about what threats could affect their network and try to protect their networks from these malicious threats.

Evil Twin attack is a famous way of attacking WLANs. The attacker in this type of attack replicates another WLAN 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. 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...

War Driving is the act of attackers cruising with a car aiming to find an unsecured WLAN, or a WLAN with weak security. Their next typical action is to post these on the internet so everyone would know about them and maybe 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.

Wireless network viruses are similar to the viruses well known by people. The difference is, they use wireless network 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) These can be prevented using anti-virus software programmes.

2.6 Result - Securing WLANs

Perfect security does not exist in the real world. Many of the most secured networks on the planet such as governments and intelligence systems got hacked. Gary McKinnon is a Scotsman who is currently facing charges of hacking many US government systems including Air Force, and the Department of Defence. (Boyd, 2008) The objective is to secure the network as much as possible. As for the focus of this section, some recommendations can be made based on the previous experience studied in this section. It is strongly recommended that WPA2 is used in a WLAN. The PSK would not be less than 12 characters, and the more the better actually. It should contain characters from different characters groups, i.e. capital letters, small letters, numbers, and special characters. PSK is encouraged to be a non guessable word. Using first names and birthday dates are

easy to guess. It is encouraged that PSKs get changed frequently. AES is recommended for encryption. Usage of access lists on APs helps minimizing risks. Keeping the SSID hidden minimizes the number of people who can know it exists, therefore less hacking attempts. Usage of management software programmes such as "LucidLink" (freeware), and "ManageEngine WiFi Manager" (license required) can help detecting rogue access points. These programmes use management protocols to store the AP information, and use it to differentiate between genuine APs from rogue ones. Remediation exists for a lot of threats, but unfortunately nothing can protect against human failures. People are actually one real threat to any security systems. Kevin Mitnick mentioned in his book "The Art of Intrusion" that in many times of his successful hack attempts, people on the inside were the tool that made it happen not just the technology he used. In the end, it is extremely important to keep WLANs secured, but the risk will always exist.

3 Review of WMAN[4]

WLAN is commonly known to have a coverage range up to 100 metres and a speed of 54 Mbps (802.11g). ISPs on the other hand, are interested in a scheme that would help them deliver their services i.e. broadband connectivity to remote area where no cable infrastructure exists. WMAN (Wireless Metropolitan Area Network), also known as WiMAX is the solution for such requirement. Is covers a wider area, and have a higher speed than WLAN. Its coverage can vary from a few buildings to an entire city. ISPs showed interest in using such scheme since it will help them accomplish their task resulting in more revenue. Governments have also shown an interest in WiMAX. 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. (LeMay, 2007)

WMAN solved the "last mile" problem ISPs have always suffered from (Yang, et al., 2005). Last mile by definition is the area between ISP's POP (Point of Presence) and the CPE (Customer Premises Equipment). ISP's last point is usually an equipment commonly known as a distribution box. The problem is that the number of subscribers increases, while the ISP's equipment has limited slots. Here comes the role of WiMAX technology offering a solution for such problem.

In 2001, the first edition of standards for WMANs was released by IEEE. They called it 802.16. (Roger B. Marks, 2002)

The developers of 802.16 tried to learn from the glitches in previous standard 802.11 and used parts of DOCSIS (a standard supported by prominent networking companies, and it is concerned with many networking issues including MAC layer security) to try minimizing the security risks. The problem here is that DOCSIS is concerned with wired connections. DOCSIS actually stands for Data Over Cable Service Interface Specification. WMANs on the other hand use wireless transmission medium, anyone can capture the signal if they are within its range of transmission. That makes it vulnerable to physical layer attacks.

WMANs operate on a two layer model; PHY (Physical) and MAC (Media Access Control) layers. MAC layer is divided into three sub-layers, CS (Convergence Sub-layer), CPS (Common Part Sub-layer), and SS (Security Sub-layer). Some references mention that it is a four layer model (PHY, CS, CPS, and SS). Figure 2 below[5] shows the 802.16 layer model.

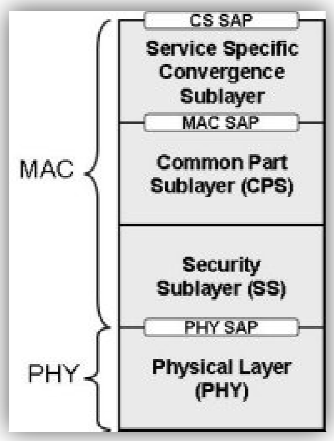

Figure 2: 802.16 Layers

Each of these sub-layers has a certain responsibility. The CS receives data from layers (typically ATM or IP) and coverts it to the appropriate MAC format. (Roger B. Marks, 2002) (Wright, 2006) The CPS manages tasks such as bandwidth

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

[5] Figure obtained from http://www.dalewright.net/2006/11/29/intro-to-wimax-and-ieee-80216

allocation, and QoS (Quality of Service). (Roger B. Marks, 2002) (Wright, 2006) SS's tasks are concerned with security issues such as encryption and authentication. (Roger B. Marks, 2002) (Wright, 2006) The last layer in the WMAN model is the PHY layer which is responsible for the transmission process over wireless channels (2-11 GHz, and 8-66 GHz). Regarding the equipments used, WMANs generally have one main component which is the BS (Base Station). The client side is usually called SS (Subscriber Station) or MS (Mobile Station). These can be represented in PCs, handheld devices, or even Wi-Fi hotspots.

3.1 PKM (Privacy Key Management)

Since WMAN is used in applications such as broadband access, authentication cannot rely on a PSK like in WLAN. It needs an authentication technique to check whether the SS is allowed access or not. PKM is the protocol used to achieve that. To secure communication, PKM uses X.509 certificates along with 3DES encryption mechanism for both keys, AK (Authorization Key) and TEK (Traffic Encryption Keys). AK is the key used for authorization; it has nothing to do with user's traffic. It is actually used to obtain TEK which is responsible of securing user's traffic.

3.2 Security Issues And Threats

Having all security techniques lying in the SS sub-layer and since it only protects its layer and the upper ones, the PHY layer is left relatively unprotected, which makes it vulnerable to many types of attacks. One famous threat to WMANs is often called 'water torture'. In this type of attacks, the attacker sends a stream of frames to drain receiver's battery. (Johnston, et al., 2004)

Lack of MIC (Message Integrity Check) is another serious issue in WMAN security. There is no mechanism used for data integrity and authenticity from the SS towards the BS. Authentication is only done in one way, BS authenticating the SS. If an attacker could manage to get a radio transmitter, it is actually possible to capture traffic, and tamper it. Obtaining traffic can also result in key calculation which is a very hard process, but still doable. In some cases an intermediate device, often called RS (Relay Station), is used to extend WMAN coverage. The attacker could use their rogue device, and seem as an RS to intercept user's traffic. Since the receiver does not have a mechanism to verify if the message was changed or not, they will process the message as a normal one coming from the expected source. This type of attacks is called 'relay attack'.

Another similar attack is 'man-in-the-middle attack'. The attacker here captures the messages as well, but instead of forwarding them to their original destination, they would forward them to their own device.

'Replay attack' is the third attack from the same family. Such attack is represented in an attacker capturing and keeping some messages, say ones containing passwords, and sending them when they need to. Time stamping is a typical way to protect against such attack.

TEK uses quality encryption mechanisms. Usage of certificates makes it even stronger. They practically make it very hard to crack the key; however, in the key cracking world, time is one of the greatest factors. Having a key that changes every minute would make it hard for an attacker to crack the key and use it. If the key changes once every month, attackers would definitely have greater chance to crack this key. A vulnerability in TEK is its lifetime. Its lifetime can vary from twelve hours up to seven days. Maybe keys can be too complex to be cracked now, but technology is growing at lightning speed. Faster processors and newer cracking mechanisms shall be available soon. Seven days is definitely enough time for the key to be cracked. (Johnston, et al., 2004)

Many of WLAN threats exist in the WMAN world as well. 'Evil Twin' attack may exist; however it is much harder to actually use it. APs are cheap; anyone can buy and configure them. BSs are huge, too complex, expensive, and require experts to configure them, not just reading a manual.

Maybe DoS attacks were not a big issue of concern in WLANs due to their limited are of coverage and speed. WMANs are being used by service providers to connect hundreds if not thousands of users. DoS attack to a BS would cause serious damage to the users not to mention the ISP. DoS attacks have many ways to be achieved. The unprotected PHY layer in WMANs adds one more way to achieving a successful DoS attack. This way is using a jamming device that would jam the radio spectrum which results in disabling the service to everyone.

3.3 Result - What Can Be Improved?

Since IEEE 802.16 is still an incomplete standard, it is normal to have glitches and security holes. The problem is that WMAN is gaining more popularity as time goes by. Many entities already started using it, and others like NSW government have plans to make use of such technology. The ongoing research process in different universities

and RNA departments has revealed a lot of these security threats seeking to be patched before they are undesirably used by attackers. Among these, the authentication mechanism used; it can result in some serious problems due to its unidirectional flow, BS authenticating SS. If a mutual authentication scheme could be used, so that BS authenticates SS, and SS authenticates BS, it could solve some problems mentioned earlier such as relay attacks, man-in-the-middle attacks, and replay attacks.

PHY layer protection is another great issue that should be improved; having nil security for PHY layer is one of the major threats in WMANs. Some of the PHY layer attacks can be avoided using primitive methods. For instance, the use of a spectrum analyser can detect jamming signals; however, it cannot prevent it from happening. Many researching entities are accepting suggestions and papers[6] on how to secure the physical layer in wireless communication in general, which also applies to WMANs. The right choice of signalling technique would actually help securing the PHY layer. For instance, usage of TDD (Time Division Duplexing) would make it harder for attackers to capture the message, parse it, change it, and then resend it in the right timing. It is practically easier to achieve that in FDD (Frequency Division Duplexing); sending the message on a certain frequency is easier than trying to spot the right timeslot.

4 Conclusion

Wireless networking has a lot of advantages; whether it is being looked at from a financial or practical point of view. Mobility is a common interest for most people. They dream of having a small device that would allow them to be connected on the move to the internet or other services. In either forms, WLAN or WMAN, attackers have their eyes wide open to exploit vulnerabilities and use them for financial benefits or mental satisfaction. A lot of these vulnerabilities were already discovered and fixed. Others are still waiting to be patched. Network operators and administrators should make themselves aware at all times of these vulnerabilities and what threats exist to their network, and try fix them before they get discovered by an unwanted person. This paper introduced some of these threats, discussed them and suggested some ways to protect against them.

[6] http://www.newcom-project.eu:8080/Plone/news/jcwn-on-wireless-physical-layer-security

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. http://news.bbc.co.uk/2/hi/technology/4715612.stm.

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.

Fred Cohen &Associates. 1995. A Short History of Cryptography . [Online] 1995. 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.

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

—. 2007. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.* USA : IEEE, 2007. ANSI/IEEE Std 802.11, 2007 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.

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

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

Wright, Dale. 2006. Intro to WiMax and IEEE 802.16. [Online] 2006. 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.