WLAN standards and Wireless networking security

Markus Kujala
Helsinki University of Technology
Telecommunications Software and Multimedia Laboratory

May 28, 2003

Abstract

This paper focuses on the WLAN standards currently in use and on what is being done to develop the technology further. A special focus is on the security point of view, as it appears that there may be some security flaws with the current technologies. The paper includes an overview of the existing standards, literary research on their security flaws and information on what is being done to fix them. We also suggest some workarounds to avoid the security holes.

1 Introduction

1.1 The purpose of the paper

This paper is written for the Helsinki University of Technology course T-110.551, Seminar on internetworking. The purpose of the paper is to introduce the current Wireless Local Area Network (WLAN) technologies to the seminar audience and also shed light on some of the security risks involved in using these these wireless networks.

1.2 What is WLAN

WLAN or Wireless Local Area Network is a term used for the networks in which a user can have a high bitrate network connection through a wireless (radio) connection. The WLAN networks are usually high in bitrate but relatively short in range. There are several standards that specify the different kinds of WLANs. The IEEE standards for WLAN also include an encryption algorithm called Wired Equivalent Privacy, or WEP. It's purpose was originally to make WLAN connections as safe as regular LAN connections. [6]

The physical architecture of wireless networks is quite simple - Access Points (AP) are connected to the normal wired network and they provide wireless access to clients (e.g. laptops, PDAs) with WLAN Network Interface Cards (NIC). WLANs may also be set up between two devices with a NIC, and it is possible to use the WLAN technology to build larger ad hoc networks as well.

Although originally designed for mainly short range indoors communication, WLAN technology can be modified to build links spanning over several kilometers. These links need special directional antennas to work, but the WLAN community has demonstrated that such an antenna can be built for a very low investment out of potato chip containers. [1] The enthusiasm and interest in the WLAN technology has also brought up several security issues that we will be address in the later chapters of this paper.

2 Research focus

2.1 Research questions

The following chapters will aim to answer these research questions set for this paper:

- What are the current WLAN-standards?
- What are some of the security problems with the currently most widely used standards?
- What is the future of WLAN and are there plans to fix security flaws?

2.2 Research methods

This paper has been conducted as a literary study. The discussion of security issues also refers to some experiments by the author.

3 The current WLAN standards

The WLAN standards are rapidly evolving towards a faster and faster connection while trying to cope with security and collision problems. The first standard was published in 1997 and since several others have been deployed.

Most of the information in this chapter is based on information released by the Institute of Electrical and Electronics Engineers Incorporated, IEEE, standards group 802.11. [6]

3.1 802.11

The evolution of WLAN began in 1997 when IEEE adopted the first WLAN standard, IEEE 802.11. It is based on radio technology operating in the 2.4 GHz frequency and has a maximum throughput of 1 to 2 Mbits per second. The basic purpose of WLAN was just to provide a wireless network infrastructure comparable to the wired Ethernet networks in use.

3.2 802.11b

The currently most spread and deployed standard, IEEE 802.11b, is the successor to 802.11 introduced in late 1999. It operates still in the same 2.4GHz frequency range, but the maximum speed is 11 Mbits per second.

Earlier, this standard was also known as Wi-Fi, short for Wireless Fidelity. The Wi-Fi term, however, was since changed to mean any type of 802.11 network, including 802.11a, 802.11b, dual-band etc. This was done mainly as an attempt to alleviate the confusion with WLAN interoperability issues. [2]

3.3 802.11a and HiperLAN

This standard was also published in late 1999 and amended in 2000 as a supplement to 802.11. It operates in the 5GHz band instead of the 'traditional' 2.4GHz that the earlier WLAN standards used, thus being subjected to less interference. It uses orthogonal frequency division multiplexing or ODFM for short and supports data rates up to 54Mbps. 802.11a is not compatible with 802.11b and therefore it's emergence has been quite slow. However, several manufacturers, such as Proxim and Envara, Inc. have come out with dual mode products, supporting both the 802.11a+b standards. In any case, 802.11a products are still a fairly sparse technology even though the first ones came out almost two years ago.

The spread of this standard was hidnered because of trouble getting the 5GHz range approved for use in Europe due to overlapping frequencies with some military channels. It may be that this affected the 802.11a standard has too much, and that it will be left into the shadow by new emerging standards that are backwards compatible with the 2.4GHz 802.11b equipment. However, 5GHz technologies may become important once again as the 2.4 GHz technologies grow more common. It may be that one day the 2.4 GHz band is so crowded by bluetooth and 4G devices that the 5 GHz band may work much better.

3.4 Wired Equivalent Privacy, WEP

Since eavesdropping on a wireless network is much easier than on a wired network, 802.11a and b standards introduced an encryption algorithm called Wired Equivalent Privacy, or WEP for short. Its purpose was to bring the security of wireless LAN networking to the level of wired networks by encryption methods. The idea is that the traffic is encrypted, so it doesn't matter if someone is able to eavesdrop on it, because they won't be able to understand what is being transmitted.

WEP uses an algorithm called RC4. The idea is that all the nodes on the network know a secret key which can be used to encrypt and decrypt the packets and thus join the network. The RC4 algorthm key is formed by combining the secret key with a 24 bit initialization vector. This vector is sent unencrypted with each sent network frame. The data is decrypted by first using the shared secret key and the initialization vector to reproduce the same key stream as used in encryption and then XOR'ing the encrypted message with the key stream. [18]

In WEP there are two levels of encryption which are defined by the key length. The key package can be either 64 or 128 bits long, of which 24 bits always contain the unencrypted initialization vector. Thus WEP encryption is either 40 or 104 bits strong (although sometimes referred to as 64 or 128 bit encryption).

The RC4 algorithm was designed by Ron Rivest in 1987. It's a symmetric stream cipher algorithm that was publicized in 1994 when someone posted it into several cryptology newsgroups. The algorithm consists of two parts, the Key Scheduling Algorithm (KSA) and Pseudo Random Generation Algorithm (PRGA), whose weaknesses are discussed in more detail by Fluhrer and Shamir. [17] The algorithm produces initiation vectors, some of which are weak and therefore reveal a character of the secret key. This security flaw is quite severe and its impacts are discussed further in the next chapter.

3.5 HiperLAN

Hiperlan, the ETSI standard for the 5GHz range got approved in August of 2001 and since then the 5GHz technology has been spreading in Europe as well. HiperLAN, short for High PErformance Radio Local Area Network, is the European response to the IEEE 802.11 standards. It has already evolved into two different standards:

- HiperLAN/1, a 20 Mbps standard and
- HiperLAN/2: a 54 Mbps standard.

Both of the standards operate in the 5 GHz band. They haven't yet been able to replace the 802.11b technology which spread very rapidly after it's release, probably due to the fact that this standard also requires a total renovation of WLAN hardware. Thus a new standard that takes this problem into consideration is emerging. It's called 802.11g.

3.6 Problems with the current standards

One of the large problems with the standards is that they are not all compatible with each other, since some operate in the 2,4GHz band whereas others work in the 5GHz band. Thus moving to a newer standard often requires the purchase of new equipment. Some manufacturers have tried to circumvent this problem by creating so called "dual mode" devices that support two different standards. This way more networks can be accessed using the same equipment, at the cost increased price to the end customer, of course.

Another problem are the security issues that some of the standards have not addressed with sufficient methods. These problems will be discussed in more depth in the next chapter.

3.7 802.11g

The 802.11g standard is currently scheduled for final approval in the summer of 2003. Drafts of the standard have already been published. 802.11g is a 2.4GHz technology that is backwards compatible with the currently most widespread WLAN-technology, 802.11b.

Reports from the task group state that speeds over 50mbps have been reached, which is very exciting as the 2.4GHz technology generally has a longer range and thus may render the 802.11a and other 5GHz technologies obsolete.

A lot is expected of the 802.11g standard, as it also promises better security than its predecessors. However, many unanswered questions still remain, especially involving connecting the older and newer technologies. A network is only as secure as its weakest link, which means that if it is necessary to revert to 802.11b WEP based security to allow 802.11b clients to connect, the networks may still be insecure. Similarly, if the network has to be slowed down in order for a 802.11b client to understand the traffic, it will take a long time before purchasing the more expensive 802.11g device will be sensible. [5]

4 Security problems

The current WLAN standards have several documented security flaws which have not yet been fixed. Many of these flaws are due to the nature of communication which is very different for the WLAN networks when compared to the traditional physical medium. Although the future standards are hopefully going to repair at least most of these security holes, the current technology is still going to be in use for quite a while and most likely it is going to remain as insecure as it is now. Unfortunately, many network administrators are not even aware of the flaws of WLAN even though they have been under discussion for a long time now.

4.1 WLAN vs Physical medium

Due to its mediumless nature of communication, the WLAN technology is prone to attacks that the traditional networks didn't have to consider.

Eavesdropping on a WLAN network is much easier than for example on a traditional Ethernet network office LAN. Instead of breaking into the office to gain access to the traffic, the eavesdropper simply has to get into the range of the WLAN, which usually can include for example the office parking lot. In order to stop eavesdropping the buidling would have to be insulated to stop the WLAN microwaves from leaking outside. This would be so hard and expensive that it would be much more sensible to simply resort to traditional ethernet cables.

In fact, eavesdropping on a WLAN network is incredibly easy. Several applications, such as Airopeek [11] have been developed with this purpose in mind. When testing airopeek we discovered that even an inexperienced user can easily monitor and capture network traffic on an unencrypted WLAN. [12]

4.2 War driving and war chalking

Due to the above, a whole new hacker culture has developed around WLANs. Tools such as Netstumbler [13] have been developed to look for WLANs and place them easily on a map. There is an ongoing mapping project at Netstumbler where users can send in their information of newly discovered WLANs and their status. The easiest way to map WLAN networks like this is to have a laptop with a wireless NIC and a GPS device in your car and when driving around, all you have to do is start netstumbler and it will record the WLAN data and locations for you. This new method of hacking has been given the name war driving, and it's incredibly effective. When we tested wardriving about a year ago in Helsinki, the Finnish capital, we found over 70 separate WLAN access points, approximately half of which were operating without WEP encryption enabled. It is likely that since then these numbers have only grown.

Another hacking method called war chalking has also emerged. In addition to finding the networks, the hackers are marking the places where open networks have been discovered. This may be done by drawing to the pavement or a closeby wall, either with chalk or any kind of pen. Special symbols have been developed so that other war chalkers will know where WLAN spots can be found. [14]

4.3 Denial of service

The 2.4GHz frequency range is unlicensed. Therefore many devices operate on it, which may cause interference. Microwave ovens generate waves in the same frequency range as the WLANs use, and many sources state that old leaky microwave ovens may disturb WLANs. [7, 8, 9] Although we did not get a denial of service effect in our test with a simple microwave oven [12], some interference was definitely visible. This indicates that at least building an interference device out of a microwave oven as described by Wang may be quite feasible [9]

4.4 WEP flaws

As stated before, the WEP or Wired Equivalent Privacy protocol is insecure due to the inherent security flaw contained by the RC4 encryption algorithm it uses. WEP has been proven crackable by several different parties. There are at least two different softwares publicly available on the internet that can be used to automatically crack WEP in order to get the password to access the network. [15, 16]

The crack is based on the fact that the encryption algorithm has initiation vectors, of which some are weak in such a way, that they may reveal a character of the WEP encryption key. When enough traffic is collected, eventually there will be enough packets containing so many weak initiation vectors that all the characters of the encryption key can be discovered.

Once the key has been revealed, the hacker can access the network as if no encryption was in place. As stated in the earlier sections, eavesdropping on an unencrypted network is extremely easy.

In our tests we discovered that the hacking programs are quite hard to install and not very reliable in running. However they were quite convincing and with a relatively small amount of work it would have been quite likely that we would have been able to crack the WEP encryption as well, even though we did not have almost any background information on WEP or WLANs in general. [12]

5 Solutions to the problems

5.1 Current projects

The IEEE 802.11 standards group is struggling to solve the problems described in the previous chapter. However, it may not be easy as the current technology is already flawed and that cannot be changed.

The 802.11g standard is supposed to bring new security enhancements to the WLAN standards world, but because of its backward compatibility with 802.11b it may very well be prone to attacks if an 802.11b device is connected to the network.

The 802.11i workgroup is also striving to find new security solutions for WLANs, but as of yet it has not solved the problems described before. [6]

5.2 Workarounds for the security flaws

One way that has been adopted to use with WLAN is simply accepting that the traffic may be listened on. This is in use at least in some educational facilities in Finland, where the students are simply informed that the WLAN traffic is not encrypted and that they should make sure that they either use a secure way of communicating or their data may be compromised. The problem with this approach is that many end users do not realize how easily they may be revealing critical information. One may think that it's not that bad to download some e-mails that for example only contain jokes sent by friends, but in the process the e-mail account password must be transmitted over the network, and a hacker observing the traffic may capture it as well.

Some manufacturers have produced 802.11b compatible equipment that use WEP, but avoid using the weak initiation vectors. They work just as the regular 802.11b equipment, but simply skip the initiation vectors that may produce weak packets. This is a pretty good workaround for the WEP problem as it is backwards compatible with the existing technology. However, it has its flaws as well. Since the packets are always encrypted by initiation vectors created on the local device, the network is only secure if none of the devices on the network produce weak initiation vectors. There is really no way of blocking a network interface card that produces weak initiation vectors from joining the network, and thus the network may be very easily compromised. If a user with a device that produces weak initiation vectors joins the network, the whole network's security is immediately compromised.

Another better aproach for now is additional encryption. Many of the current WLAN security holes can be circumvented by stacking another protocol layer on top. If the traffic on the WLAN is tunneled through a VPN or an SSH connection, it becomes much harder, if not impossible, for the hacker to capture the traffic. If only tunneled traffic is allowed, the hacker won't be able to join the network to perform man-in-the-middle attacks either. The problem is that many network administrators do not know how to set up an environment like this, or won't bother with it. The easiest way to set this up is to install a VPN or SSH server right behind the WLAN access point, so that it only allows encrypted traffic to the WLAN direction. In addition to the trouble this of course brings additional costs as additional procurements in the form of encryption servers are required.

The interference denial of service problem cannot be solved with the above solution. The only way to fight it would be to change frequencies. For example the 5GHz range is much better protected from interference. However, since the current standards are on the 2.4GHz band, migration is very difficult.

6 Conclusion

In conclusion, the current WLANs in use are prone to many different kinds of attacks. Network administrators need to be aware of these attacks and take appropriate steps to defend against them in order to keep their WLAN connected networks secure. It would be in the best interest of the WLAN community if the evolution moved towards the 5GHz range products as not only is implementing fast connections with them already been done, but also interference from other devices is much less likely. However, since only technology compatible backwards with the currently most widespread technologies is likely to thrive, the migration to 5GHz range is going to take a long time if it's ever going to happen.

In any case it is very important that in the future standards the security issues are taken much more into consideration than what was done when the first standards were released. Fortunately it seems that this is already being done, but nevertheless eyes should be kept open for new flaws discovered, especially as visions of implementing the 4G (4th generation) of mobile phones partially on top of WLAN technology are emerging. [10]

References

[1] Flickenger, Rob *Wi-Fi Pringles Can Yagi Antenna* http://www.3nw.com/pda/wireless/wi_fi_pringles_can_yagi_antenna.htm July 2001.

[2] Webopedia *Wi-Fi* http://www.webopedia.com/TERM/W/Wi_Fi.html Jupitermedia 2003.

[3] Webopedia *HiperLAN* http://www.webopedia.com/TERM/H/HiperLAN.html Jupitermedia 2003.

[4] Conover, Joel *802.11a: Making Space for Speed* Mobile & Wireless Technology Workshop http://www.networkcomputing.com/1201/1201ws1.html January 2001.

[5] Marks, L. Victor *The 802.11g standard – IEEE* IBM developerWorks Wireless articles http://www-106.ibm.com/developerworks/wireless/library/wi-ieee.html

[6] IEEE 802.11 work group *IEEE 802.11 Wireless Local Area Networks* http://grouper.ieee.org/groups/802/11/ The Institute of Electrical and Electronics Engineers, Inc. (IEEE), 2003.

[7] Leira, Jardar *Wireless Networks* http://www.uninett.no/wlan/radio.html The Norwegian academic and research data network, March 2003.

[8] Boncella, Robert J. *WLAN Security* http://www.washburn.edu/cas/cis/boncella/WLANSecurity.ppt

[9] Wang, Sean *Threats and Countermeasures in Wireless Networking* http://www.sans.org/rr/wireless/threats.htm December 2000.

[10] AT&T Labs - Research *Wireless LANs and Cellular Systems* http://www.research.att.com/ macsbug/Mobile_Interdomain_Roaming/Cellular_WLANs/WLAN-Cellintro.html AT&T 2003.

[11] Airopeek http://www.wildpackets.com/products/airopeek Wildpackets, Inc. 2003.

[12] Kujala, M and Savolainen, M *Wireless Local Area Network Security* T-110.452 Special seminar course for practical information systems security Telecommunications Software and Multimedia Laboratory Helsinki University of Technology, March 2003.

[13] Netstumbler http://www.netstumbler.com/ Netstumbler, 2003.

[14] Maijala, Ville *Warchalking - the big threat or a key to more secure WLANs?* T-110.501 Seminar on Network Security Telecommunications Software and Multimedia Laboratory Helsinki University of Technology, November 2002.

[15] Airsnort http://airsnort.shmoo.com/ The Shmoo Group, 2003.

[16] Rager, Anton *Wepcrack - An 802.11 key breaker*

[17] Fluhrer, Mantin and Shamir *Weaknesses in the Key Scheduling Algorithm of RC4* http://www.drizzle.com/ aboba/IEEE/rc4_ksaproc.pdf

[18] Ailus S. and Hedberg J. *T-110.452 Practical security of IEEE 802.11b* T-110.452 Special seminar course for practical information systems security Telecommunications Software and Multimedia Laboratory Helsinki University of Technology, March 2003.