

Risks In Using Commercial Wireless Networks

Dennis Luxen

<mh2k3@dennisluxen.de>

Abstract

Over the past months wireless networks emerged from expensive and hard to get to can be found nearly everywhere. The most popular standard is IEEE 802.11b, also known as WLAN or Wi-Fi. But can it be used as trusted means of communication? This paper discusses which techniques can be used to enhance and penetrate built-in security measures of wireless networks. In addition a few methods are described to enhance the precautions already taken.

Introduction

Over the last few month wireless networks using the IEEE 802.11b standard have become more popular and more widespread than ever before. Not only has Apple supported this particular standard from the very early days with the 'AirPort' products. The company adapted the successor standard IEEE 802.11g very early in its 'AirPort Extreme' products. This support of innovative technology is very commendable. The most used and supported standard right now and for the foreseeable future is 802.11b. As every technology, it not only has advantages, but also a few drawbacks, which have to be dealt with in order to achieve a more or less life easing way to use wireless networks. Besides vulnerabilities in certain firmwares or encryption algorithm implementations, the downsides are not vendor specific at all. Furthermore, the approach of how they are seen often does not only apply to wireless networking, but to a variety of security related fields of interest.

A Baseline

As wireless networking becomes more and more utilized in the private and corporate sector, wireless security becomes an important issue.

In 1990 the IEEE formed the 802.11 Working Group to develop the specifications of a wireless networking standard operating in the ISM bands. The ISM (or Industrial, Scientific and Medical) frequency ranges are used for unlicensed low power radio transmissions, typically 900MHz or 2.4 and 5 GHz. Seven years later, in 1997, the group released the first wireless standard. Another two years later, in 1999, the group released the 802.11b specification. This particular standard introduced speeds up to 11Mbit/s and operates on the 2.4GHz frequency range. Besides faster data transmission, this standard also features wide interoperability between different vendors. Eleven separate channels are available for use, but because these channels overlap each other commonly only three of all channels are used, namely channel 1, 6 and 11. Some vendors also feature products with 13 channels using a broader frequency band. Overlapping channels are known to cause bad interference. So it's always a good idea to check for already existing WLANs in the area when deploying your own and it's especially a great idea to be a nice neighbor.

Interception of radio transmissions has always been a great concern as long as people used radio communications to transmit and receive information. Whilst private communications like letters and phone calls are generally quite boring to a third party, the internal communication of a company might be very, very interesting to a competitor. Not to mention governments and their special needs to protect their communications or to know what a foreign power might be doing or not. This is of course a very large field and usually large amounts of resources are spent to reach such objectives.

In the 1980's attackers used automated devices or scripts to systematically dial all telephone numbers in an area to discover modems. One number was dialed and when a modem answered the call, this specific number was written into a log file for later use and the next number was dialed to see if a computer is answering. And so on, until a certain number of potential targets was

reached or all numbers in a particular area were tested. This type of information gathering by mass-dialing phone numbers was known as war dialing. As WLANs have become the potential target of an attack, a new technique of mass harvesting the location of good targets emerged. People started to drive or walk around equipped with a map and a portable device capable of receiving the signal of wireless networks. These devices are often PDAs or notebooks, which can be operated without the need for a fixed power line for quite some time. Using specialized software, it's very easy to discover networks, their name, channel (frequency) and a lot more properties. Even scanning systems which are hooked up to a GPS are available. So, the idea of driving around the city and logging where someone is broadcasting his or her radio waves into the air has been dubbed as 'war driving', coined as a reference to its target collecting predecessor in the eighties.

Protocol Insecurities

People have always been using cryptography to secure communications. Beginning with simple letter shifting techniques used by the roman empire, today's complex methods rely on elliptic curves or prime number factorization problems. If not compromised, these techniques have been more than useful to protect communication. Knowing this, the inventors of IEEE 802.11b implemented a security mechanism into their standard to provide a networking platform ready for secured communication. And for example, especially in sensitive areas like battle fields or emergency rooms trustworthy information is crucial, because it can and probably will save lives.

The security mechanism used in 802.11b is called 'Wired Equivalent Privacy' or WEP for short. As the name suggests the idea was to make radio transmission as secure as its wired counterpart and to interconnect them without having to worry about possible security hassles. WEP is not simply an encryption technique, but instead it tries to serve two purposes. The first is of course to provide encryption. The cipher used is RC4 and is a symmetric algorithm and as such it is encrypting and decrypting the stream of data with the same key. As a result of using a symmetric cipher, the key has to be present on all communication devices taking part in the transmission. The second intention of WEP is to provide an authentication method. When a new network node connects to an access point a random number is sent to it and the connecting node sends the number received back to the access point, but this time encrypted using the key. If it matches the number encrypted with the key on the other machine, then both machines are using the same key and the authentication has been successful.

But unfortunately the WEP mechanism has some flaws. And these problems diminish the security it provides greatly. First of all WEP simply ignores key management. The used encryption key has to be configured manually on all network nodes. Some implementations allow the rotation of a few keys, but there is no real key management behind it. The key in use is still known to all parties and all the problems remain.

The bigger a wireless network grows the more likely it is that one node on the network will be compromised somehow. When using only one key on the whole network, then you have to trust every client on the network, because anyone is able to decrypt any traffic with that key. For small networks it might be relatively easy to know all users and establish a relationship to them, which makes it easier to tell if they are trustworthy or not. But as soon the number of users becomes double-digit or even higher, then it isn't realistic to trust all users. Furthermore it is very likely that there will be a so called 'human leak' somewhere and sometime. One should never underestimate the power of social engineering. If a key is not changed on a regular basis the more likely it is, that the network will be compromised, because the the key could be brute-forced and because security declines every minute as we will see later. For the purpose of trying to cope with this lowered security of WEP keys, it might be a good idea to change these keys on a regular basis. WEP allows to specify more than one key to be stored in the wireless devices configuration. But again, the number of keys is very limited and thus is the security achieved by it.

The key length of the RC4 encryption is 40 bits by default. The IEEE chose this length because it is exportable under most laws. Modern computer hardware is able to brute force such a 40 bit key in a matter of hours. Furthermore the authors of [FLU2001] describe "Weakness in the key Scheduling Algorithm of RC4". They don't show a weakness in the encryption algorithm itself, but in the way it is implemented in WEP. The authors' conclusion is, that once you enough encrypted traffic has been captured, it is possible to start a cryptanalytic attack on the WEP key. Also, one would expect the time needed to attack a WEP key would rise exponentially with its length.

However, because of the weakness in the scheduling algorithm, the time rises only linear, which means that it only takes twice as long to crack a 100 bit key than to attack a 50 bit one. So, the move of some vendors to upgrade from a 40 (64) bit key to a 104 (128) bit key does not solve the problem of a quite easily crackable encryption. And as soon an attacker obtains the key all gates are open. When the authors of [FLU2001] published their paper in 2001, this attack was only theoretical. But it took a short time only until the first exploits hit the streets and today there are a variety of tools for a variety of computer platforms available including MacOS X, Linux and Windows. Often these tools are available for download accompanied by their source code, so a port to a future, more powerful hardware platform might be easy. Therefore the current WEP standard must be regarded as an insufficient security mechanism to protect your wireless network.

Besides all that or maybe in addition to that is another problem of WEP. Some vendors implemented the IV of the WEP key in a faulty way. Some nearly never rotate the IV as long as a connection exists. Others make it very easy for an attacker to identify the pattern how the IV is shifted and as such rendering the shifting quite useless and allowing cyrptoanalytic attacks to reach their aim faster.

Denial of Service

In addition to vulnerabilities described above it is quite easy to start a denial of service attack on a wireless network. As WLANs use high frequency radio waves and not wires to communicate, this type of attack is different from denial of service attacks known from the wired world. It is unique to wireless networks, because it directly attacks the way data is transmitted. Wireless networks working through the 802.11b standard transmit on the 2.4GHz ISM band. An attacker can use a device, which produces noise on the ISM band. Similar to the situation when two people are talking, if the noise is loud enough, then any communication must fail, because people can't understand each other anymore. So, using a noise generator, which is transmitting noise on the appriopraite frequency and with a sufficient strength (loudness), it is quite simple to take down a wireless network. These jamming devices are cheap and easy to get. Some cordless phones or microwave ovens are very effective jammers. Unfortunately there is very little one can do about it. The only countermeasure to protect ones network is to regularly watch out for people in range of your network, who might be jamming on a regular basis. But who wants to do that in densely populated areas like downtown Manhattan, where virtually thousands of people pass by your place every day?

How to be Mean

Now, knowing that the built-in security measures are like a fig leaf, how would one try to attack a wireless network? It is important to know how a network can be penetrated, because then it is known what to protect from.

Acquiring a Target

The first step is to discover wireless networks. This is the easiest task and for a lot of private and corporate networks this is all you have to do. Networks can easily be detected with tools like Macstumbler¹. As soon as a wireless network is in range a sound is played and the network is noted in a logfile along-side it's properties, like name, vendor, MAC address, if it is using WEP and other information. Collecting a list of maybe a dozen or more networks normally generates a nice set of potential targets. Additionally, some websites² keep a databases of hot spots sorted by zip code and/ or city name.

Locking on

Assuming a nice target has been found, the next step is to authenticate your machine with the access point. In most cases this is the trickiest part. If an access point is using WEP, then the WEP key must be recovered. This can be done by either attacking the weaknesses of the RC4 implementation as described above or by brute-forcing the key. Both methods are effective and the success is only a matter of time. Alternatively another approach to recover the key is social engineering. The human factor cannot be underestimated. When asked in the right way, people are likely to give away sensitive information. Once the key has been recovered nearly all gates

¹ <http://www.macstumbler.com>

² An example: <http://www.freewebs.com/crackrock>

are open. One last line of defense would be limitation to the network based in MAC addresses, simply denying hosts you do not know. At first sight, this idea sounds very charming. Hosts, which are not registered as known, won't have a chance to use an access point. But remember, the WEP key has already been recovered. While not authenticated, it is not only already possible to capture any traffic passing by, but also decrypting it as needed. This is done in a completely passive way without interacting with the network. As soon as the original host goes down start using the allowed MAC address.

Some drivers have a feature to ignore the hard coded MAC address in the network interface. This feature will be a vital part to gain access. Hosts on a network never stay up for an infinite amount of time. In an office for example workstations are likely to be switched off at the end of working day and especially on the weekend. When the possibility of passively sniffing network traffic, while not associated with the access point, and changing the MAC address of the network card are combined with a pool of allowed addresses currently not in use, then the protective measure of limiting the MAC address space can be easily bypassed.

Now it is time to get associated. Not a big deal at all, when WEP key and valid MAC address are known. The last remaining barrier is a valid IP address. Access points often offer a DHCP service making it very easy for an attacker to get a running connection. DHCP automatically assigns an IP address for the network. If DHCP is switched off or not available, then a method to the one for obtaining a valid MAC address could be used. Sit and listen again. And try to figure out what the settings are for subnet and IP-range. An example: If the access point is using the IP 192.168.2.1 and is communicating with a host answering at 192.168.2.29, you can be pretty sure that it's a class C like network and that the hosts between 1 and 29 are valid as well. Just choose a free address in between or at least in the same subnet.

In the past few paragraphs a network has been found and a host is successfully associated with it using a valid IP address.

An attack on a network might be go like this, but it hasn't to. Let's have a look at a more theoretical approach how an assault might be working.

A Small Theory of Attack and Defense

The chapters above showed a practical view on how someone may get unauthorized access to a network. The following section tries to determine attacks in a more general approach. Here, the main questions of interest here are:

- What is defended,
- What are the principles of an attack,
- What are the strategies and
- How can it be visualized?

As every theory has them, a few axioms and definitions are needed:

Definition:

A system identifies a social or technical technical entity, which provides a certain function.

In general a 'system' is assaulted by the attacker and guarded by the defender. In the real world there might be a lot more than two people, but they are grouped as the player and the defender. In fact, normally there are a lot of people attacking a (well known) target and probably more than one person trying to prevent it. Seen as a game, defender and attacker are direct opponents trying to achieve an opposite goal.

Axiom:

An attacker will always choose the strategy of the easiest way to achieve a certain goal.

The strategy of the easiest ways means a strategy directed to reach a certain aim with the minimal effort possible. When trying to reach a goal, it is in the human nature to always choose the easiest way. Choosing an aim has to mean to choose an idea how to achieve it as well. Without this idea trying to reach an the aim is quite useless, because normally things don't happen on their own. They have to be pursued. This is not only true in a personal manner, but also applies to the context of trying to break security measures. So, as a result of that an attack is directed in

order to try to reach ones aim as easy as possible and because the strategy chosen always has to be easy, one can postulate the following

Implication:

Attacks are always goal oriented.

Up until now, we only had an informal description of what a defender is trying to do. As stated above, the defender is trying to hamper the attacker from reaching the goal of circumventing the security measures taken. Despite, that the defender ought to have an idea of how to protect a system, the attacker has the initiative. In most cases the offense can choose its strategy freely, while the defensive strategy is a reaction to that. Consequently, to stop an attack a defender has to prepare the defensive strategy to match one or more offenses. So, a defender has the task to ensure the functionality of a system, thinking of as many possible attacks as possible. The attacker can choose between different strategies to fit the aim.

Unfortunately the security of a system can't be measured in numbers. Any statement on the security of a system is more a qualitative than a quantitative figure. Sure, there are estimations of how long a cryptographic attack on a specific cipher might take, but this estimation can be either a very long period of time or there are other factors, like yet unknown vulnerabilities or other similar factors. Although the longer an attack takes, the more likely it is that the attacker loses interest. But because of the unquantitive measurement, any statement is based on a certain probability only.

To measure the security in a qualitative way, it is important to know that the level of security diminishes as time passes by. The following picture visualizes this issue.

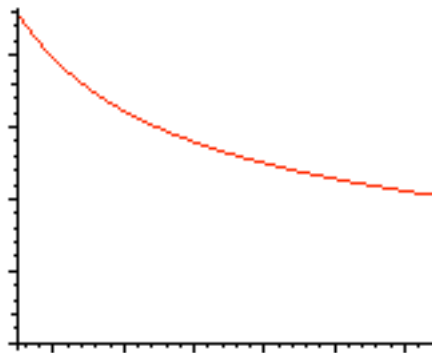


Figure 1. Security diminishment

When a security system is introduced it has a certain (qualitative) level of security. Over time, vulnerabilities become known and as computer equipment becomes cheaper and more powerful literally every day, a brute force attack becomes a more and more potential attack. Very similar to that is the next graph. It shows the abilities of an attacker over time. Both graphs are only very rough idealizations.

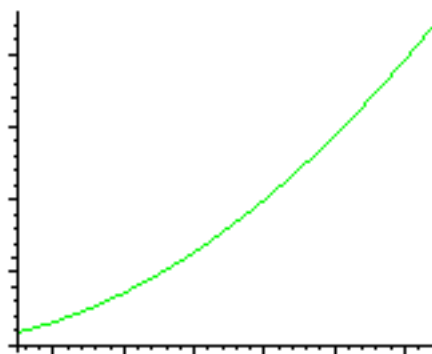


Figure 2. Attacker Abilities

A successful attack can only occur, if the abilities of the attacker meet at least the security precautions taken. In other words: The attacker has to know how to defeat the barrier of the defense. The next figure shows a combination of the previous two. The hatched area shows where the abilities exceed security precautions.

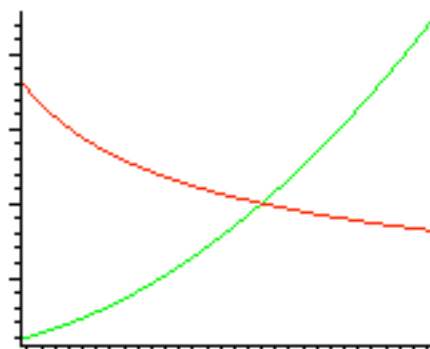


Figure 3. Combined Graph

Keeping this theory in mind is a tremendous help to understand how attacks work in wired and as well a wireless world. How can this knowledge be applied when securing a network?

Building a Rampart

The tendency when protecting a network is to keep the abilities as below as you can from the level of security. The wanted situation is, when the graphs of ability and security level don't cross. Ideal would be, if they'd never come close. Unfortunately it isn't that simple. At least a few categories of wireless networks exist.

A simple classification consists of three categories. The first category is comprised of public networks. These are the nets present at hotels, coffee shops, lounges and similar places. They are intended to offer internet service to a customer. As the service is wanted to be available to a general public, it wouldn't make sense to turn on encryption, because of two reasons. First, connecting to the network should be as simple as possible. Most users aren't IT specialists and don't know about configuration of computers or networks. They simply want to use the service. Second reason is, that with the WEP standard it is quite useless to hand out encryption keys. The cipher is symmetric and therefore encrypting and decrypting with the key just handed out, but security of keys relies on non-proliferation. Often these networks use an own authentication method. Connection to the WLAN is allowed to everyone, but routing of traffic is based on MAC or IP address and for paying customers only. For an attacker this guest access might be enough because, when connected it is possible to sniff for traffic on the net using ethernet sniffers like Ethereal³.

The next category consists of small scale private networks, often used to hook up one or more computers to an internet connection. Normally, the number of machines is fixed or does change only quite seldomly and because the uplink bandwidth is limited and a more or less expensive good, encryption and authentication methods should be used. Despite the fact, that WEP isn't enough, it is always a good idea to turn it on, because it raises the bar and the nonrecurring war driver will stay out. In fact, most access points are poorly configured by default. Encryption is turned off, every MAC address is allowed and connecting hosts receive an IP address via DHCP. So, it's a good idea to turn that off and increase the level of security. The casual war driver can't use the access point anymore and a sophisticated knowledge is already required to gain access.

The thirds category are corporate networks. Companies have a special need for information security and integrity. Knowing the internals of a particular marketing campaign for example could be more than interesting to a competitor. If wireless networks are used in a company, very good preparation is needed prior the deployment. Besides the built-in security measures like WEP and

³ <http://www.ethereal.org>

alike another layer of security should be introduced. WEP is only a barrier for the occasional hacker. Mechanisms like virtual private networks (VPN) add a second layer of security, because before data is transmitted it is encrypted. So, if an attacker breaks the WEP encryption there is still no clear text to read. This layer could also be introduced in private networks, if there is special need to secure communication. The disadvantage is, that with such a second layer the administration effort increases and as a result the costs for deploying and maintaining a wireless network.

Hiding any information about your network is always a good thing. It helps staying unidentified. WLANs offer the feature to identify themselves over a name. Some names disclose information like website address or company name, which makes it very easy to identify the physical location of the access point. [POT2003] delivers a technical introduction into the problem. Some access points have the possibility to turn that off. It's a good idea to do so if possible or change it to a non-meaningful name like 'network'.

Conclusion

Many would say, that wireless networking is a hopeless case, when it comes to security. It's an important topic for sure and there are problems, which have to be addressed. A lot of enhancements have surfaced to the original standard and a lot more will do in the coming months or years. Wireless networking is still a very young technology and as such, it will have to grow up like others did before. Maybe there will be only one common standard for all use cases, ranging from small, private networks at home to hooking a game console up to the internet to large scale corporate networks. Maybe there will be different standards for different applications, but a lot of people and organizations are investing a lot of resources right now to extend today's standards. Lots of things are still waiting to be discovered.

The author of [WHA2002] says, "Security is about reducing risk, not eliminating it. In most cases, elimination is not possible."

Bibliography

[ISS2003] Internet Security Systems, Inc. Internet Risk Impact Summary for January 1, 2003 - March 31, 2003. <https://gtoc.iss.net/documents/summaryreport.pdf>

[FLU2001] Scott Fluhrer et al. Weaknesses in the Key Scheduling Algorithm of RC4.

[POT2003] Bruce Potter et al. 802.11 Security. O'Reilly & Associates, Sebastopol, CA. 2003.

[WHA2002] Sean Whalen. Introduction to Wireless Auditing, 2002.