TDMM32 Information Security Second Course

Security in IEEE 802.11 Wireless Networks

By
Nicolas Aubry 820927-P512
Justin Yancey 840202-P417

Supervisor
David Byers

Security in IEEE 802.11 Networks

Justin Yancey, Nicolas Aubry

Linköping University, Sweden
Email jusya331@student.liu.se, nicau408@student.liu.se

Abstract

This paper analyses the current encryption technologies associated with wireless, starting from Wired Equivalency Privacy (WEP), continuing on to WEP's temporary replacement, Wifi Protected Access (WPA), and then to a more permanent solution for addressing the flaws in wireless security, Robust Security Network (RSN). It will also discuss Denial of Service attacks on wireless networks and mitigation methods to lower the vulnerability of attacks like those mentioned. A discussion on physical interference in wireless networks explains that attacks are not the only problems associated with implementing a wireless network. It then presents a series of recommendations in regards to creating a secure and practical wireless network according to the business size and privacy requirements. To finish, a description and discussion of the practical attack that was launched will be given.

1. Introduction

Data transmission techniques are going through a profound evolution, and wireless networking has appeared over the last few years from this evolution. Now 802.11 networks are implemented in many companies, but can wireless networks be considered as secure as the "old" wired network?

This new technology brings many new physical problems that didn't exist in wired networks, thus making it vulnerable. Despite the advantage this technology offers of being able to be connected everywhere one goes, it can also be seen has a disadvantage and a risk for the company. Many mechanisms and encryption processes have been, and continue to be, created to help secure wireless network, but are they all effective and efficient?

The aim of this paper is to help the reader understand the different security issues of this new technology and to make some recommendations on implementing a secured wireless network.

2. Wireless Security Technologies

2.1 WEP & its weaknesses

2.1.1 What is WEP?

WEP (or Wired Equivalency Privacy) was the first encryption mechanism in the 802.11 specifications, and its goals are to provide confidentiality and data integrity, and to protect access to the network infrastructure by rejecting all non-WEP packets. The packet is encrypted using the RC4 algorithm. This generates a keystream as a function of the 24 bit initialization vector (IV) and the 40 bit secret key. The cipher text results from applying the XOR function to the plaintext (with CRC) and the keystream. The cipher text and the IV are then transmitted via radio.

2.1.2 Problem 1: IV length is too short, so IV values are reused

Since the IV used in WEP is only 24 bits, there is around 16.7 million possible IV's, which are transmitted in clear text and readable to anyone [1]. On a high volume network this number can be achieved in just a few hours, in which case the reuse of IV's is unavoidable. The storage requirements are only around 24Gb for all possible keystreams, so an attacker can sniff network packets (or insert his own) and recover all possible keystreams by looking for frames with known contents (i.e. MIME header contents etc).

2.1.3 Problem 2: Weak keys

Having a "Weak Key" generally means that there is a more obvious relationship between the key and the encrypted output than there should be. Certain key value combinations do not produce sufficiently random data for the first few bytes, so the attacker can collect these frames and find the pattern, then use the pattern to determine the key. The consequence of this is that it has been made possible to create software that will scan a captured file containing sniffed network traffic that will recognise packets encrypted with weak keys, and from these packets it can perform a comparison. The comparison finds patterns between the packets with weak keys and thus can determine the key used for encryption. It is possible to mitigate this problem by extending the key length, however the vulnerability is still there, extending the key length will only increase the amount of captured traffic required.

2.1.4 Problem 3: Poor Key Management

WEP requires the use of static key entry, thus making the administration of WEP keys difficult to do on large networks. Because of this, there is a tendency for users to change keys very infrequently, which gives an attacker ample time to collect enough data to launch an attack on the system. In addition, the WEP keys are used directly for the encryption process, rather than being used for the generation of temporary keys. Using temporary keys would mean that by the time an attacker had captured traffic and determined the key, a new key would have been produced from the master key and the temporary key they have found would no longer be valid. However, since WEP uses only the master key, if the key is found, all stations that use the network must be reconfigured with a new key.

2.1.5 Problem 4: Vulnerable to Replay attacks

The way that Shared Key authentication works in WEP involves the client demonstrating to the Access Point (AP) that he has knowledge of the shared WEP key. This is done by encrypting a challenge sent by the AP on the client. The replay problem arises when a monitoring attacker observes the challenge from the AP and the encrypted response. From those, he can determine the keystream that was used to encrypt the response, and later use that stream to encrypt any challenge he receives in the future. This process does not require the attacker to have knowledge of the key. However, if he wishes to communicate further, he does require the key. The replay attack is most useful for a Denial of Service attack on the access point rather than breaking encryption.

2.1.6 Problem 5: Message integrity checking is ineffective

Although WEP does have a message integrity check, however it has also proven to be flawed. The ICV of the message is a linear function, meaning that a bit that is changed in a certain section of the encrypted packet results in a predictable bit change in the ICV. This allows attackers to change messages and recompute a new IC value to match the modified message, without requiring knowledge of the key or keystream. This makes the checking ineffective against tampering attacks.

2.2 WPA and how it improves WEP

The root of the problem in WEP is that its encryption keys are static rather than dynamic. This means that in order to change the keys, a network technician has to visit each computer. The alternative is to leave the keys unchanged, which will make the network highly vulnerable to hackers. This problem is what the Wi-Fi alliance has set out to solve, and has done so in developing the Wi-Fi Protected Access protocol, or WPA. WPA prevents attacks from hackers by periodically generating a unique encryption key for each client on the wireless network. One of the major advantages of WPA is that it is software upgradeable from WEP, and does not require any hardware upgrades, making it very appealing to businesses with an existing wireless network. WPA was developed as a temporary solution to patch the security holes in WEP, thus was developed with the strict limitations that it must be hardware compatible with the current 802.11b products on the market. The following paragraphs list and describe three major improvements that were implemented with WPA.

2.2.1 Improvement 1: Better Key Generation and Distribution through TKIP

WPA implements a new protocol known as TKIP (Temporary Key Integrity Protocol), which extends the IV to 48 bits (as opposed to WEP's 24), a function used for the creation and distribution of keys as well as a mechanism for constructing a key for each packet. The TKIP procedure starts with a 128-bit temporal key, which is generated from the master key, of which all wireless clients and access points on the network will have. Each packet combines the temporal key, the client's MAC address and a 48 bit TKIP sequence number through a key mixing function to produce the key that will be used for encryption. This method ensures that each client uses different key streams for each data packet they transmit, thus avoiding the weak key problem in WEP. The key mixing function has two stages. Stage one combines the MAC address of the wireless interface and the temporal key by iteratively XORing each of their bytes to produce an intermediate key. This key is used to encrypt the TKIP sequence number, thus producing a 128 bit per-packet encryption key. TKIP uses the same encryption method as WEP, using RC4 to perform the encryption, but TKIP is made to change temporal keys every 10,000 packets. This provides a dynamic distribution method that significantly enhances the security of the network. [2]

2.2.2 Improvement 2: Better Message Integrity Checking

It also implements a feature known as a message integrity code, or MIC, similar to that of a CRC. A cryptographic "tag" is calculated and attached to transmitted data, and the recipient generates its own MIC and compares it to the one that was sent.

2.2.3 Improvement 3: Implements 802.1x Authentication with EAP

WPA also employs the use of the 802.1x mechanisms, which allows for mutual

authentication for wireless network users. Mutual authentication is where both the client and the server must prove their identities, in the case of 802.1x it is through the use of certificates or smartcards. User authentication is generally missing in WEP, but it implemented in WPA through the use of the Extensible Authentication Protocol (EAP). WEP controls access to a wireless network based on a computer's hardware-specific MAC address, which is fairly simple to sniff out and steal. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

2.3 Robust Security Network, (RSN or WPA2)

WPA2 (also known as RSN, Robust Security Network) has become a new security standard known as 802.11i, and provides the highest level of security to date. It has taken wireless security to a whole new level, and in the next few years it is certain to become commonplace amongst most corporate networks. The following paragraphs will list and describe some of the major benefits provided by WPA2.

2.3.1 Benefit 1: Provides a more secure protocol and cipher

The new security protocol used in WPA2 is called Counter mode CBC-MAC Protocol (or CCMP). Unlike WEP and WPA, which use a stream cipher (RC4), WPA2 uses the CCM mode (or "Counter mode") of the Advanced Encryption Standard (AES), which is a block cipher. By running AES in Counter mode, it is transformed from a block cipher to a stream cipher. [3]

2.3.2 Benefit 2: Uses longer keys, avoiding key scheduling problems

WPA2 uses a key with 128 bits and a block size of 128 bits, which is long enough to prevent a brute force attack. With this longer key size, it is possible to use AES to encrypt all packets sent over the network. A key with 128 bits can create 2^{128} key combinations, which is approximately
339,000,000,000,000,000,000,000,000,000,000,000
keys (give or take a couple trillion). [4]

2.3.3 Benefit 3: Has improved Message Integrity

The CCMP combines the counter mode (CTR) for data confidentiality and the Cipher Block Chaining Message Authentication Code (CBC-MAC) for data integrity, using an 8-octet MIC (Message Integrity Code) and a 2-octet Length field. CCMP also provides MIC protection over both the frame body and nearly the entire header in a MAC frame, which prevents an adversary from exploiting the MAC headers. In addition, CCMP uses a 48-bit Packet Number (PN) to prevent replay attacks

2.3.4 The Disadvantage: Why it is not so popular

Unfortunately, the cost of implementing this security standard is quite high, especially for companies with existing wireless networks. Unlike WPA, WPA2 requires hardware upgrades in both the clients and the access points, and there are very few products available that are capable of using WPA2 (in comparison to WPA). The hardware is also more expensive, since all encryption is done at the hardware level it requires newer more capable chipsets. The encryption process is too resource intensive to perform at the software level. This is its primary hindrance in mass implementation, as upgrading an entire system would require a large amount of financial resources.

3. Denial of Service Attacks

The bases for a secured network is to fit to the CIA (Confidentiality Integrity Availability) model. However, most of wireless networks were focused primarily on Confidentiality and integrity, rather than availability. Denial-of-service (DoS) is a threat against availability. The definition given in Wikipedia [5] is: "An attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim system."

Denial of Service attacks are a common network security problem and without a physical infrastructure it's more affordable for an attacker, more flexible to decide where and when to attack and be still anonymous due to the difficulty to locate the source of wireless transmission. The result of this kind of attack could be a disruption of a physical network component, consumption of computational resources (bandwidth, CPU etc) or disruption of configuration information (routing tables etc)

802.11 nodes are identified at the MAC layer. For management and control messages, standard 802.11 networks do not include any mechanism for verifying the correctness of the self-reported identity. Consequently, an attacker may "spoof" other nodes and request various MAC-layer services on their behalf. This leads to several distinct vulnerabilities.

3.1 Deauthentication

When a station wants to connect to an AP, it first exchanges authentication frames and then association frames. It can participate in network communications

after it is authenticated and associated. However, any station can spoof a disassociate or deauthenticate message, pretending to be another station. The AP disassociates the targeted station, which cannot send traffic until it is associated again. By repeatedly sending these frames, an attacker can keep one or more stations off a network indefinitely. Figure 1 demonstrates this.
The advantage of this attack is the flexibility for the attacker to select specific clients to deny or limit is access.

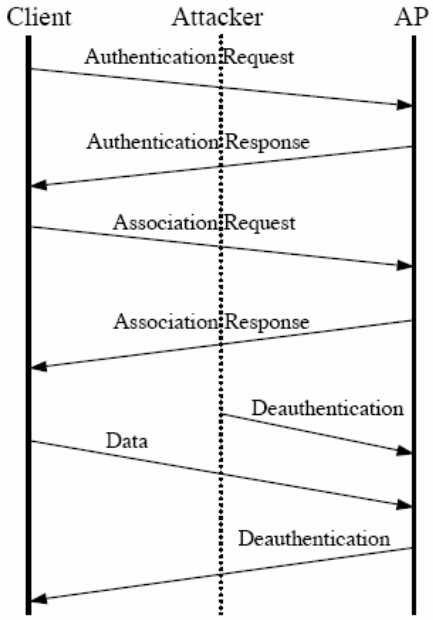

Figure 1. Deauthentication attack

3.2 Disassociation

A Disassociation attack is quite similar to the previous one. A client can be authenticated to many access point in the same time, that's why the association frame exist to select the AP the client will take. The same as with the authentication frame, the association frame is unauthenticated, by sending a similar deauthentication frame in spoofing the address of the client, the attacker can disassociate the target. However, the deauthentication attack is more effective than the disassociation attack because it needs a re-association after the authentication, so the victim has more work to do.

3.3 Power Saving

To conserve energy, clients are allowed to enter a sleep state during which they are unable to transmit or receive, at which stage the access point places into a buffer any data concerning the client. Occasionally the client awakes and polls the AP which transmits data if there is some in the queue. It is possible to spoof the polling message of the client so that the AP discards the packets.

From another point of view, the AP broadcast a Traffic Indication Map message (TIM) periodically when packets are in the buffer to prevent the client from going into sleep mode. The attacker can spoof the TIM message to convince the client that there is no data in the buffer for him.

3.4 Transmit Duration

This is a type of denial-of-service attack based on the Transmit Duration field of the 802.11 frame. Transmit Duration is the collision avoidance mechanism for 802.11 that announces to other nodes how long a frame transmission will last. All stations on the network are then supposed to stay quiet for that amount of time to avoid colliding with that transmission.

An attacker can send a stream of packets with the maximum Transmit Duration (1/30th of a second) set, which prevents other nodes from sending for that amount of time. Thus, a relatively slow 30-packets-per-second rate keeps the network occupied.

3.5 Other DoS attacks

Many others DoS attacks exist against 802.11 networks like on the frame control in the virtual carrier-sense mechanism (RST frames) or emitting interference from traffic using the same radio band. A demonstration has been made with a wireless laptop next to a microwave oven [6]. Denial-of-service can be done via other elements than wireless like EAP in 802.1X authentication.

4. Mitigation methods

Many methods can solve or almost mitigate DoS attacks. For the deauthentication and disassociation, frames are sent as clear text and without verification are simple to spoof. It's possible to authenticate management frames and drop invalid requests. If a data packet arrives after a deauthentication or disassociation request is queued, that request is discarded – since a legitimate client would never generate packets in that order. A timeout of 5-10 seconds applied in the access point for each management request can lower the effect of the denial-of-service attack. For the power saving attack, the mitigation is the Authentication of management frames limits the source of TIM packets to the appropriate access point. The transmit duration time has also the same mitigation: Authentication of management frames to limit the authority of the source of RTS, CTS, and ACK frames.

For interferences, there is no automatic mitigation to this vulnerability. The victim user must track down and physically eliminate the source of the

interference. If the source is naturally occurring, the network has to adapt (change frequencies, location, etc.)

Finally we can deduce that the most efficient solution for this problem is to extend explicit authentication to 802.11 control packets but unfortunately this protection is not currently part of standard implementations, it requires modification of firmware and/or use of third party software

5. Physical aspects of wireless network security

5.1 Interference

Wireless networks can be divided in three groups: 802.11b, 802.11g and 802.11a. 802.11b/g is the most widely implemented wireless, broadcasting at a frequency of 2.4 GHz, it differs from 802.11a which as a wave band of 5GHz. All references about a wireless network in the text below refer to 802.11b/g.

The electromagnetic spectrum of a wireless network is between infrared and microwaves [7], like it said in the previous section, the microwaves ovens are in the same category and so they can create interferences. It is important to install a wireless network free of components emitting radio signals at the same wave band to have the best emission/reception for the network.

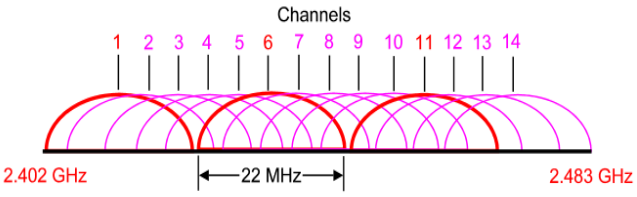

Figure 2, Overlapping frequencies

Other interferences can be due to the network itself. A wireless network is composed of 14 different channel frequencies from 2.402 GHz to 2.484 GHz [8], and many of these channels are overlapping each other (see figure 2), thus creating interferences. In practice, only channels 1, 6 and 11 will not overlap each other. Selecting defined channels allows administrators to discover rogue access point that are broadcasting on a different channel.

5.2 Antennas

The way in which radio waves are emitted depends largely on the antennas. Different types of antennas exist; the basic one is an omni directional antenna *Figure 3* [9]. The others antennas are unidirectional antennas like patch antenna *Figure 4* [9] or parabolic antenna *Figure 5* [9]. The effectiveness of the antenna depends of the type of the antenna used and the geographical place where the wireless is implemented. The choice of the antenna is important and enables administrators to limit the broadcasting of the radio waves outside the desired area. On the other hand, an attacker can choose a Yagi [9] antenna to perform a remote attack far away from the access point without been caught, since he is located outside the standard wireless area.

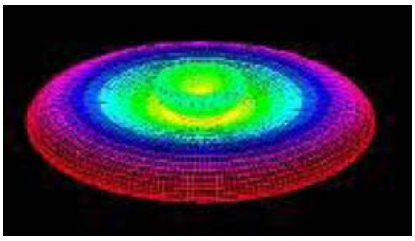

Figure 3: broadcasting of an omni directional antenna

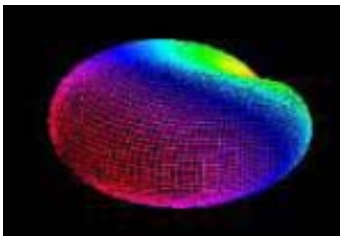

Figure 4: broadcasting of patch antenna

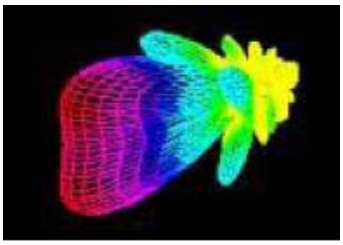

Figure 5: broadcasting of parabolic antenna

Some solutions have been found to minimize physical vulnerabilities. The power regulation of the access point can limit the connected area to a certain building or floor; antennas can also be used to limit emissions to a specific direction. The require signal strength can also be used, for example when a client wishes to connect he must have a signal strength of at least 5.5Mbit/s to allow communications. Many companies that have a wireless connection often provide connection outside their buildings but with a poor quality (1 or 2Mbit/s connection), by using require signal strength the company limit many wild connections.

6. Recommendations for creating a secure wireless network

There is no “best way” to create a secure wireless network. Like all network design, the security of the wireless network depends on the size of the company, the security levels required and the people who will be using the system, as well as the resources available. As such, we shall give different recommendations according to some common scenarios which require different configurations due to these factors. When differentiating between large and small networks, we define a large network as a network that has a centralised user management system with a formal security policy, and a small network as a workgroup style with no user management system.

For a small network, for less than 20-30 users, we recommend using WPA in conjunction with MAC address authentication. WPA provides strong encryption but should never be used without some form of authentication, and for a small network MAC authentication is manageable. In this case, since 802.1x requires an authentication server, it also requires additional resources which will greatly increase the overall cost of the system. This configuration can be done at the access point, so no additional servers are required.

For a large network, with a centralised user management system, we recommend again using WPA, but instead of MAC authentication, which is authenticated at the hardware level, using 802.1x EAP because it is an authentication system based at the user level, so no static configuration would be required. It also provides stronger security against techniques such as MAC spoofing. Large companies will also dedicate more resources for their networks, so the cost of an authentication server is outweighed by the need for a secure system. It is also advisable to set up the access points on a Demilitarised Zone, so that any users who access the system from the outside must first go through the internal firewall, making hacking the system even more difficult.

In both of the above cases, we have not recommended the use of WPA2 (802.11i). This is due to the fact that it is a very recent development and as such it is supported by very few devices (both access points and wireless cards). It requires a large investment, since the products that are available are expensive, and in order to implement WPA2, all access points must be changed and all wireless users must buy new hardware in order for it to work, unlike the upgrade from WEP to WPA. This is due to the AES encryption process being done at the hardware level rather than at the software level, where it was performed before.. However, if the resources are available, we highly recommend this option, as it provides excellent security which far exceeds that of its predecessors, but the fact that it requires a hardware upgrade makes it undesirable for companies which already have a wireless network. We believe that this is currently limiting its growth, but will become much more popular as more hardware supports its use.

Regardless of the size of the network, a wireless system should only be implemented if there is a need for one. Before it is implemented, it should be given careful consideration as to who gets access, what resources are available to wireless users and a security policy should be drafted to make sure the implementation is done properly, to form a secured wireless network. In addition, we recommend the constant use of network monitoring software, to alert the administrators to any signs of suspicious activity so that they may promptly bring a halt to any possible attacks.

7. Practical: Attack on a Wireless Network

7.1 The strategy

In this section we will describe an attack on a wireless network. The attack is based around a system similar to that used on the Linköping University (LIU) network. Although the University is not our target, they are an example which we will use for practicality purposes. This attack could be done on any wireless network that requires a web-based login, including pay & play hotspots at airports, coffee lounges etc.

The system requires all users to be authenticated in order to have access to the network. This authentication is done via a secured web authentication server. The challenge is to steal username/password of the login session via the wireless vulnerabilities.

First of all the attacker brings his laptop in a connected wireless area where students are currently connected to the Linköping University (LIU) network through a wireless connection. The attack requires a laptop running a Linux operation system, with a wireless card based on the Prism2 chipset (so that it can run HostAP [10], to make the laptop into a virtual access point) and a piece of software called airsnarf [11]. It also requires software by void11 [12], which is used to deauthenticate connected users.

The first step starts with a reconnaissance stage. Luckily this is quite easy, as the access points broadcast the SSID, so no special tools are necessary. All the information we need can be found by running the command “iwconfig wlan0” in a terminal session. This information is then used in certain configuration files for the HostAP program.

After getting all the other information (like SSID for masquerading, the MAC address of the access point for flooding, etc) we can start the attack. *Figure 6 (in appendix)* explains what the attack will looks like. This attack can be summarized in two steps:

The attacker will start with the void11 software to deauthenticate the currently connected users. This

software will flood authentication requests to the access point to force it to crash, or denying service by filling up tables of associated stations. The result of this attack will be the deauthentication of the network users; there will be then disconnected from the network.

Now that the users are disconnected, naturally they will want to reconnect. Here the attacker runs HostAP and the Airsnarf script on their laptop to install a rogue AP, having the same characteristics of the access point they previously connected to. Airsnarf is a small and simple utility that works by redirecting DNS requests, sort of like a manual cache poisoning. All queries for domain names will automatically receive a reply that contains the IP address of the attackers wireless interface. Because the original AP is crashed or too flooded to answer the request, the normal user will only receive replies from the rogue access point, which is also hosting a web server with the index page looking identical to that of the legitimate login page. The user will then be asked again to enter their username/ password, and this information is processed by the Airsnarf software and is sent via email to the root account on the laptop.

7.2 The results and some interesting discoveries

After a great deal of installing, building, configuring, testing and hair-loss, we finally managed to create the successful attack. However, we found that there is much more simple way to hijack traffic rather than flooding an AP, potentially drawing unwanted attention from sharp administrators. In the end we just forgot about crashing the access point, and worked on a "mine is stronger than yours" principle. This basically means that if your fake access point gives off a stronger signal than the real access point, the client will by default associate with the strongest signal, in this case the fake. In our tests we found this to be very practical, with a distance difference of a mere 30 cm between the real AP and the fake, the client would always associate with the fake. In the case of a coffee shop, with interference such as walls, people, cell phones etc, it is more than likely you will not need to flood anything.

After implementing this new idea, our attack had just become half as complicated as before, and greatly reduced our chance of discovery. We tested it and it worked, we were able to successfully capture a username and password of users wishing to log in (on our test network, not the LIU network).

We had hoped at first that after obtaining this login, it would be possible to then use an authenticated session along with NAT routing to open up a legitimate channel so that the client can browse the web at the same time as they are being attacked. This would mean that after the attacker had successfully stolen one login, any further clients would not receive an error message, their details would automatically be stored and then the fake AP will grant access over the shared connection. However, there is currently no software available that will provide this function. Airsnarf will only allow redirection to the one page, but after that there is no way to connect, as all DNS queries will continue to point to the login page.

Perhaps the most interesting thing we found was that with LIU's in-house developed open source Netlogon program (for authenticating clients) [13], plus a little time and some modification to the code, Netlogon can be perfectly integrated into this style of attack, and with a little publicity, would most likely become the standard for Man-in-the-Middle attacks. It follows a similar pattern to the Airsnarf program, first it redirects traffic, it processes the traffic (in this case authenticates users rather than logging their details), then allows or denies traffic. The difference is that Airsnarf works by redirecting DNS queries, where Netlogon redirects HTTP queries. This difference can grant the attacker complete transparency, only the first user to log on will be denied (only long enough for the attacker to establish his own connection to then share with other clients).

8. Closing statements

Although there are many weaknesses in wireless technologies, new solutions are constantly being formed by learning from old mistakes. WPA2 will surely take off in the near future, and will provide the same level of security as wired networks. Having said that, wireless networks still have their limitations. While they offer convenience for mobile users, it creates more work for administrators and a another drain on the IT budget for managers. Before implementing wireless on a network, a serious analysis must be done as to what levels of security they require, the type and quantities of equipment they will need and more importantly, whether they will benefit from wireless at all.

9. Research Material

[1] Nikita Borisov, Ian Goldberg, David Wagner, *Analysis of 802.11 Security, or Wired Equivalent Privacy Isn't.* http://www.isaac.cs.berkeley.edu/isaac/wep-slides.pdf MAC Crypto Workshop, Cupertino, CA, February 2001

[2] Jesse Walker *802.11 Security Series, Part 2: The Temporal Key Integrity Protocol*, http://cache-www.intel.com/cd/00/00/01/77/17769_80211_part2.pdf April 2002

[3] Changhua He and John C Mitchell, *Security Analysis and Improvements for IEEE 802.11i,* www.isoc.org/isoc/conferences/

ndss/05/proceedings/papers/NDSS05-1107.pdf
Standford University, 2005

[4] 9 Dollar Domains FAQ section,
http://www.9dollardomains.com/encryption.htm

[5] Wikipedia Online Encyclopedia,
http://en.wikipedia.org/wiki/Denial_of_service

[6] Authors not credited, *Effects of Microwave Interference on IEEE 802.11 WLAN Reliability* http://www.wlana.org/learn/microreliab.pdf Intersil Corporation, May 1998

[7] François Gerthoffert Ludovic Toinel Christophe Malinge, *802.11 Les Réseaux sans fils*, http://www.wireless-fr.org/medias/ebook_sept2003.pdf, Nantes Wireless, September 2003

[8] IEEE Standards for Information Technology, *IEEE 802.11, 1999 Edition, (ISO/IEC 8802-11: 1999)*http://standards.ieee.org/getieee802/download/802.11b-1999_Cor1-2001.pdf

[9] Wikipedia Online Encyclopedia ,
http://en.wikipedia.org/wiki/Yagi_antenna

[10] HostAP, http://hostap.epitest.fi/

[11] Airsnarf, http://airsnarf.schmoo.com

[12] Void11, http://www.wlsec.net/void11

[13] Netlogon, http://www.unit.liu.se/netlogon/

Appendix: Wireless Security/Hacking tools

There are a plethora of Wireless network tools available on the Internet to test for or exploit vulnerabilities in 802.11 networks, and can be categorised into the vulnerability that they exploit. The focus will be on Denial of Service attacks, Man in the Middle attacks, and encryption cracking, as these three forms of attacks have the most software available. In the following section I shall briefly describe the attack category, list and describe some common tools and how they work.

Denial of Service Attacks

A Denial of Service (DoS) attack aims at preventing users from being able to use the wireless network. It does not accomplish much other than to create frustration for users and administrators of the system. However, it can be used in conjunction with other techniques to form serious attacks.

Void11 – A packet injection program that is used to flood wireless networks with de-authentication packets. Authenticated stations will receive these packets and drop their connections. It also has a feature that will crash the access point itself by flooding it with authentication packets.

Airpwn – This is a tool that allows raw frame injection onto a wireless network. It requires two network cards, one for listening and one for transmitting, and can be configured to respond to certain packets with specific answers.

Aireplay – This program takes a captured packet and simply reinjects it onto the network. This takes advantage of the lack of reply protection in WEP. Since the aim is simply to flood the network, the contents of the WEP packet do not matter, the program just takes one packet and sends it out hundreds of times per second. If the packet requires a response from the target, a huge amount of traffic is generated, and the flood is a success.

Man in the Middle Attacks

A Man in the Middle (MitM) attack is perhaps one of the most common forms of attack, as it can enable an attacker to retrieve sensitive information such as usernames and passwords. The tools in this category work by creating a fake access point that poses as a legitimate access point and have the client connect to them rather than the real access point.

Airsnarf – A program that masquerades as a genuine access point on the network. The attack begins when the client connects to the fake access point. He tries to connect to the internet, but his browser is redirected to a login page (a very commonly used system for authentication). The login page is hosted on the attackers laptop, but the user will not notice the difference. He will then proceed to send all authentication data to the fake access point.

Encryption cracking

Encryption cracking refers to the process of capturing and analysing traffic, recovering the key (or keystreams) from the captured data and thus enabling the attacker to decrypt WEP encrypted packets. There are a few tools that enable this.

WEPCrack – A set of 4 Perl scripts that exploit the key scheduling weakness in WEP. A capture file is obtained, decoded and the possible weak IV's are identified. One byte is encrypted with a key from command line and matched up to a corresponding IV in the list and written to a file. This file is then parsed and the secret key is produced.

CoWPAtty – A program that utilises the weak passphrase vulnerability in WPA. The program is run with a word generator as input (such as John the Ripper, which uses a large dictionary for word generation) and uses a brute force attack to discover the passphrase that was used to generate the Pre-Shared Key.

WEPWedgie – This tool is used for determining WEP keystreams and injecting traffic with known keystreams. The WEP keystreams can be used for an offline attack to determine the secret key that was used to encrypt.

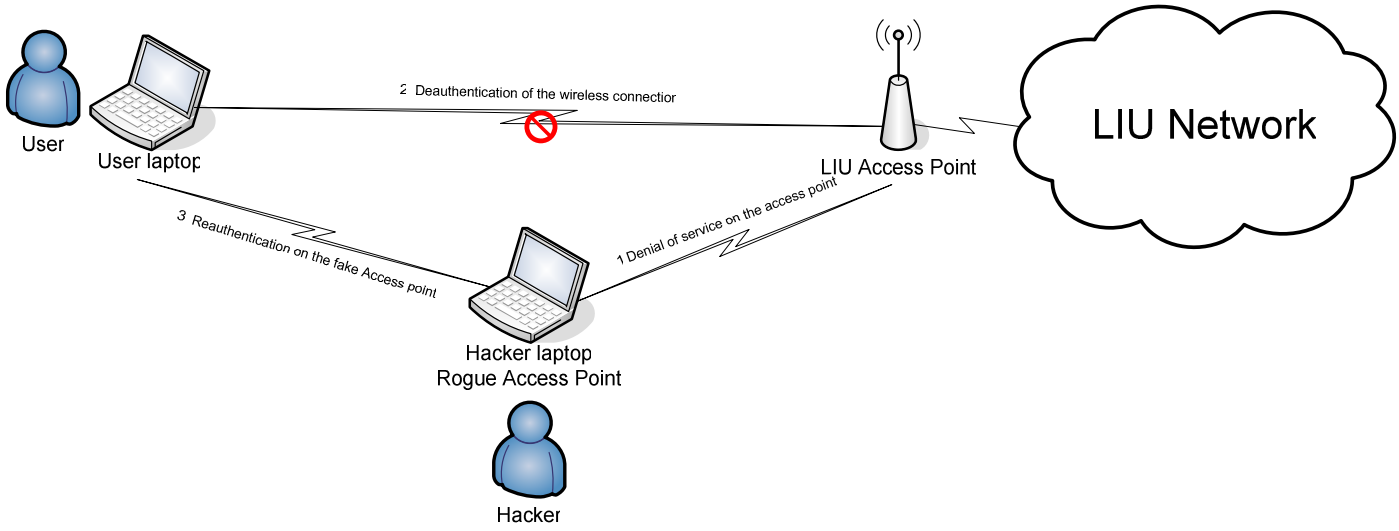

Figure 6: Representation of the practical attack on the Wireless network of Linköping University