Overview of WLAN and its vulnerabilities

Wireless LAN’s (WLAN) are LAN's networked wirelessly using the air interface as the medium of the network. The wireless technology being used is nothing but radio frequency waves. WLAN can run on three different physical media, two based on the spread spectrum and one on diffused infrared. [Peterson & Davie, 2003- P.132]. The fact that wireless networks make use of the air interface as the medium of the network makes them susceptible to threats by attackers. Attacks are carried out with various attacker objectives [Sankar et. al., 2005 - P.126]. E.g. an attacker just might want to check the network traffic, or might want to access resources on the network.

An attack is any action carried out to compromise the security of any information belonging to an organization. [Stallings, 2003 – P. 4]. Furthermore Stallings classifies two types of attacks; Active and Passive attacks. Passive attacks are those in which the attacker obtains information being transmitted / received by the network, these types of attacks are usually difficult to detect as there is no modification of the contents by the attacker. Whereas active attacks involve the attacker changing the information / content or even sometimes generating fraudulent information into the network. These types of attacks are malicious in nature and can result in severe losses for the victims [Stallings, 2003 – P.11, Prasad, 2005 – P. 96].

The following figure represents a general classification of attacks according to Stallings.

Security Attacks

<table>
<thead>
<tr>
<th>Active Attacks</th>
<th>Passive Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Masquerade</td>
<td>Traffic Analysis</td>
</tr>
<tr>
<td>Replay</td>
<td>Release of msg.contents</td>
</tr>
<tr>
<td>Modification of message</td>
<td></td>
</tr>
<tr>
<td>Denial of Service</td>
<td></td>
</tr>
</tbody>
</table>

Fig1. Taxonomy of Active and Passive attacks

Wired Equivalent privacy (WEP) is a security algorithm employed by WLAN’s, the main goal of WEP is not to secure the network but completely secure the data so that the attackers do not have access to the information and if they do, it will be secured with the WEP algorithm. The notion of WEP is important as in many of the attacks on WLAN which I am going to describe; the WEP algorithm’s vulnerability is exploited and broken. More material on attacks on WEP algorithms can be found in “Hacking Exposed” [McClure et. al., 2003 – P.471].

Coming towards more specific attacks on wireless networks. One of the conference papers of The International Association Of Science And Technology For Development – IASTED titled “Wireless LAN Attacks And Protection Tools” gives a very good taxonomy of active and passive attacks on WLAN’s, whereas the amount of information provided in this paper is quite brief. The taxonomy of the attacks on a WLAN is as follows. [IASTED, 2004].

Fig2. Taxonomy of Active and Passive attacks on WLAN

1. Passive Attacks On WLAN

There are two types of passive attacks an attacker can mount:

a. Traffic Analysis
b. Passive Eavesdropping

1a. Traffic Analysis

The first step to any type of hacking is footprinting [McClure et. al., 2003 – Chp. 1], and wireless footprinting is done by carrying out traffic analysis. The attackers before mounting an active attack have to obtain sufficient information about the network. This operation of traffic analysis gives the attacker some basic information about the network, like, the network activity going on, the protocols being used by the network and also the active access points (AP’s) of the network.

The determination of the active AP’s is employed by a process known as Wardriving [IASTED, 2004]. This is a process where the attacker physically moves around (usually in a car and hence the name wardriving is derived) to find out about the active AP’s of the network to be attacked. By finding out about the active AP the attacker can use the AP as a starting point to mount his/her attack. This is done by detecting and capturing the beacon frames sent out Periodically by the AP’s. [IASTED, 2004, Sankar et. al., 2005 - P.133].

1b. Passive Eavesdropping

This attack is very similar to the traffic analysis attack [IASTED, 2004], as this also discloses the information about the network but at the same time the attacker can access and read the message contents. If the Message is encrypted, this will require the attacker to break the encryption and read the message.

The attacker can mainly gain two types of information by mounting this sort of an attack; he/she can read the data transmitted in the session and also get various information about the packet characteristics. Therefore the impact of passive eavesdropping is the compromise of information and privacy [Welch – June 2003].
2. Active Attacks on WLAN

The several types of active attacks an attacker can mount against WLAN are:

- Unauthorized Access
- Rogue Access Points
- Man In the Middle Attack (MITM)
- Session Hijacking
- Replay
- Denial of Service

2a. Unauthorized Access

The attack is not aimed at a particular user, but by doing this, the attacker gains unauthorized access to the whole network. This attack in turn gives rise to more malicious attacks such as MITM, ARP poisoning.

In some security architectures when the attacker accesses the wireless network, he/she also gets access to the wired components of the network. Where as in other security architectures the wired components are contro lled by access control, usually implemented using ACL’s (Access Control Lists). However the access control rights can be bypassed by spoofing the victim’s MAC address [IASTED, 2004]. Spoofing is the same as Masquerading. The main motive of the attack is to give the attacker the access to services or privileges he/she is not authorized to access [Prasad, 2005 – P.95].

2b. Rogue AP’s

These can be thought of as sub divisions of the AP’s. Rogue AP’s are setup by the users for their convenience [IASTED, 2004, Sankar et. al., 2005 - P.154]. E.g. an AP is not in the range of the user’s current position; the user will setup a rogue AP for the purpose of boosting the range and getting the AP’s signal unto him. The rogue AP has no or minimal security, due to this it becomes a very massive back door for attackers. Even if the rogue AP’s are secured using for example WEP, an attacker can attack and exploit the WEP algorithm using various methods [McCure et. al., 2003 – P.471]. An Attacker can setup a rogue AP to gain future access to the network or even to obtain user a/c information. Some AP’s serve as public gateways like hotspots, etc. An attacker can set up a fraudulent rogue AP for the respective AP and then mirror the AP’s registration page to get hold of people’s user name and password. Rogue AP’s play and essential part in mounting a MITM attack. [Sankar et. al., 2005 - P.154].

2c. Man In The Middle Attacks (MITM)

These attacks have an indirect Perspective of attacking data confidentiality. Although the organizations might have employed security measures such as VPN or IPSec. These countermeasures only protect from a direct data confidentiality attack. This attack comprises the integrity of messages as they can be read and/or modified by the attacker. The attacker appears to the AP as the user and to the user as the authentic AP. Hence this fools both the AP and the user and all data is passed through the Attacker [Welch – June 2003]. Masquerading/spoofing is the technique employed by the attacker to fool the participants of the connection. [IASTED, 2004].

2d. Session Hijacking

This attack is also attacking the victim indirectly as the MITM attack. Session High jacking involves taking control of the session. The attacker will take control of the session and the victim will think that the session is no longer in operation whatever the cause. Whereas the session will be live and in the hands of the attacker, which he/she can exploit for many purposes. Session hijacking is basically done by obtaining MAC of the AP and the victim, after the victim is authenticated by the AP the attacker impersonates as the AP by using its MAC and sends a MAC-Disassociate message to the victim. The victim then closes the session but the real AP has the session open, and the attacker then acts as the victim by using its MAC and gains control over the session. This attack happens in real time and also compromises the integrity aspect. Further information in [Welch – June 2003, IASTED, 2004].

2e. Replay

A replay attack has the same objectives as the MITM and the session hijacking, but this attack happens offline, rather than in real time. The attacker can capture data of a session and can use it later to exploit the victim’s information [IASTED, 2004]. The information can be the user’s session information, which could be the authentication information. Therefore by introducing timeouts in a message, replay attacks could be avoided.

2f. Denial of Service (DoS)

This works well on WLAN and is one of the very famous attacks, to bring down the system. The main aim is to bring down the system so that it doesn’t respond to the users request. This can be done by sending huge traffic at the AP, making it unable to respond [IASTED, 2004]. Hence this attack deals with the attacker trying to keep the user from accessing the information or the resources of the system. The DoS attacks in case of wireless technologies can be carried out just by introducing interference in the form of noise, whereas flooding packets performs a DoS attack on the network.

Conclusion

The attacks which I have described above are quite brief and further information can be obtained by following up the references. The attacks have countermeasures to them which are not covered in this paper. Cryptographic techniques are sometimes employed to protect against some of the attacks. Although this particular taxonomy used in this paper is not a set standard, but it can be used as a starting point for a WLAN network designer. He/she can analyse these and understand the risks involved and hence implement a wireless network which can counter the active and passive attacks against the WLAN.
References

1. IASTED (2004) 
   International Association of Science and Technology for Development 
   URL: www.iasted.com 

   McGraw Hill: NY, U.S.A.

   Morgan Kaufmann Publishers: CA, U.S.A.

   802.11 WLANs and IP Networking: security, QoS, and mobility 
   Artech House Universal Personal Communication: Boston, London

   Cisco wireless LAN security:Expert guidance for securing your 802.11 networks 
   Cisco Press: U.S.A.

   Prentice Hall: New Jersey, U.S.A.

   Wireless Security Threat Taxonomy 
   Proceedings of the 2003 IEEE workshop on information assurance United States Military 
   Academy West Point, NY, June 2003