WLAN Attacks and Risks

Kimmo Hiltunen (39195V)
kimmo.hiltunen@ericsson.com

***Abstract*—Wireless LANs (WLAN) introduce the concept of complete mobility provided by air travel; communication is no longer limited to the infrastructure of wires. This provides new opportunities and challenges.**

This very air-borne nature of WLANs opens it to intruders and attacks that can come from any direction. WLAN traffic travels over radio waves that cannot be constrained by the walls of a building. As a result of this, intruders and would-be hackers can potentially access the network from the parking lot or across the street.

In this paper some of the most common attacks and threats, e.g. denial-of-service, eavesdropping and manipulation, are briefly explained. Furthermore, some possible counteractions are presented also.

I. Introduction

WLAN (802.11x) networks have unique vulnerabilities that make them an ideal avenue of attack. Wireless networks cannot be physically secured the same way a wired network can be. An attack against a wireless network can take place anywhere: from the next office, the parking lot of the building, across the street, or possibly several miles away.

Understanding the details of various attacks against the wireless infrastructure is critical to determining an appropriate defense strategy. Some attacks are easy to implement but are not particularly dangerous. Other attacks are, however, much more difficult to mount but can have devastating consequences. Like any other aspect of security, wireless security is a game of risk. By knowing the risks involved in the network and making informed decisions about security measures, the wireless network operator has a better chance to protect itself, its assets, and users.

In this paper some of the most common attacks and threats are briefly explained. Furthermore, some possible countermeasures are presented also.

II. An Example Network

In this paper, the example network shown in Fig. 1 is assumed [1]. The network is split into three segments: the Internet, a wireless network containing access points and wireless clients, and a wired network containing workstations, servers, and other devices. A gateway mediates the traffic between these three segments. All of these network components must work together, and implement complimentary security, to establish a secure network.

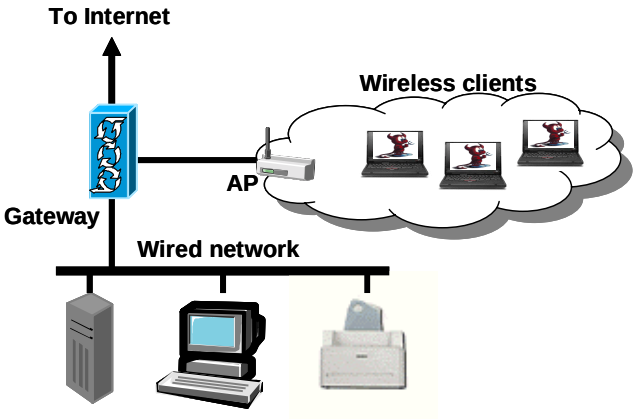

Fig. 1. Structure of an example network.

III. Denial-of-Service Attacks

Denial-of-Service (DoS) attacks, which aim to prevent access to network resources, can be devastating and difficult to protect against. Typical DoS attacks involve flooding the network with traffic choking the transmission lines and preventing other legitimate users from accessing services on the network.

DoS attacks can target many different layers of the network. At the application and transport layers, there is nothing fundamentally different between DoS attacks on wireless and wired networks. However, there are critical differences in the interaction between the network, data-link, and physical layers that increase the risk of a DoS attack on a wireless network.

Next, the DoS attacks on the various network layers are briefly gone through. Most of the information is taken from [1], but also [2] and [3] has been used. Finally, a lot of detailed information can also be found in [4].

A. Application (OSI Layer 7)

An application-layer DoS is accomplished by sending large amounts of otherwise legitimate requests to a network-aware application, such as sending a large amount of page requests to a web server, swamping the server process. The goal of this type of attack is to prevent other users from accessing the service by forcing the server to fulfill an excessive number of transactions. The network itself may still be usable, but since the web server process cannot respond to the users, access to service is denied.

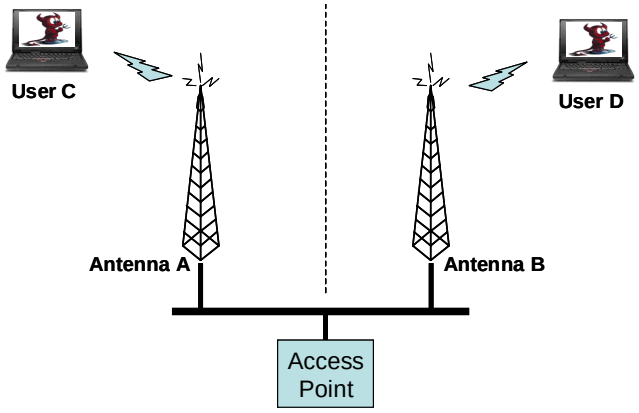

Fig. 2. Attack against improperly provisioned diversity antennas.

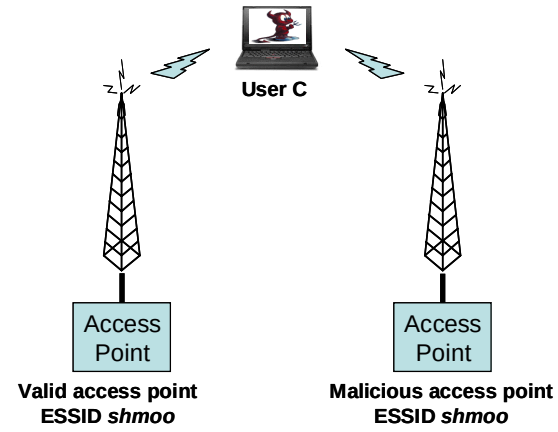

Fig. 3. Malicious AP overpowering valid AP.

B. *Transport (OSI Layer 4)*

A transport-layer DoS involves sending many connection requests to a host. This type of attack is typically targeted against the operating system of the victim's computer. A typical attack in this category is a SYN flood. In a SYN flood (SYN packets are the first step of a TCP connection), an attacker sends an excessive number of TCP connection requests to a host hoping to overwhelm the operating system's ability to track active TCP sessions. Most operating systems have a limit to the number of connections per second they will accept and a limit on the maximum number of connections they will maintain. A successful SYN flood will overwhelm the operating system on one of these two limits, thereby denying access to the services running on that host. As is the case in the application-based DoS, the network is usually still functional, but the target host is unresponsive.

C. *Network (OSI Layer 3)*

If a network allows any client to associate, it is vulnerable to a network-level DoS attack. Since an 802.11 network is a shared medium, a malicious user can flood the network with traffic, denying access to other devices associated to the affected access point. As an example, an attacker can associate to a victim 802.11b network and send an ICMP flood to the gateway. While the gateway may be able to withstand the amount of traffic, the shared bandwidth of the 802.11b infrastructure is easily saturated. Other clients associated to the same AP as the attacker will have a very difficult time sending packets.

Given the relatively slow speed of 802.11b networks, a network DoS may happen inadvertently due to large file transfers or bandwidth-intense applications. A few bandwidth-hungry applications on a WLAN can hamper access for all associated stations. With the deployment of higher-speed WLAN technologies, these unintentional attacks will become less frequent.

D. *Data-Link (OSI Layer 2)*

At the data-link layer, ubiquitous access to the medium again creates new opportunities for DoS attacks. Even with the Wired Equivalent Privacy (WEP) turned on, an attacker has access to the link layer information and can perform some DoS attacks. Without WEP, the attacker has full access to manipulate associations between stations and access points to terminate access to the network.

If an AP is incorrectly utilizing diversity antennas, an attacker can potentially deny access to clients associated to the AP. The use of diversity antennas is normally intended to compensate for multipath fading. However, diversity antennas are sometimes used also to cover a larger area with an AP by using antennas that cover disparate physical regions.

If the diversity antennas do not cover the same region of space, an attacker can deny service to associated stations by exploiting the improper set-up, as shown in Fig. 2. There, diversity antennas A and B are attached to an AP, and are set-up to cover both sides of the wall independently. User C is on the left side of the wall, so the AP will choose antenna A for the sending and receiving frames. User D is on the opposite side of the wall, and will therefore send and receive frames with antenna B. User D can take user C off the network by changing his MAC address to be the same as user C's. Then user D can guarantee that his signal is stronger on antenna B than user C's signal on antenna A by using an amplifier or other enhancement mechanism. Once user D's signal has been detected as the stronger signal on antenna B, the AP will send and receive frames for the MAC address on antenna B. As long as user D continues to send traffic to the AP, user C's frames will be ignored.

If a client is not using WEP authentication (or the attacker has knowledge of the WEP key), then the client is vulnerable to DoS attacks from spoofed APs. Clients can generally be configured to associate with any access point or to associate to an access point in a particular ESSID (Extended Service Set Identifier). If a client is configured to associate to any available AP, it will select the AP with the strongest signal regardless of the ESSID. If a client is configured to associate to a particular ESSID, it will select the AP in the ESSID with the strongest signal strength.

Either way, a malicious AP can effectively black-hole traffic from a victim by spoofing the desired AP. For example, if a

client is configured to associate to APs in the SSID *shmoo*, the client will look for all available APs in that SSID. It will then associate with the AP for which it has the strongest signal. A malicious AP with the SSID *shmoo* can make sure it has the strongest signal by using a larger or directional antenna, signal amplifier etc, as shown in Fig. 3. The client will associate to the malicious AP, and the malicious AP can drop or monitor all traffic sent to it by the client.

E. Physical (OSI Layer 1)

A physical DoS attack against a wired network requires very close proximity to the victim host. However, this is not the case with a wireless network. The medium is everywhere and attacks can launch a physical attack from much farther distances. Instead of being inside of a building to perform a physical DoS attack against a LAN, an attacker can be outside of the building. Unlike a wired network where is usually evidence of a physical attack (destroyed cabling, removed cable, attackers on video surveillance cameras), there are no visible signs that something has changed.

The 802.11 PHY specifications define a limited range of frequencies for communication. The 802.11 devices that use a specific PHY are constrained to these frequency ranges. An attacker can create a device that will saturate the 802.11 frequency bands with noise. If the attacker can create enough RF noise to reduce the signal-to-noise ratio (SNR) to an unusable level, then the devices within range of noise will be effectively taken offline. The devices will not be able to pick out the valid network signal from all the random noise being generated and therefore will be unable to communicate.

Creating a device that produces a lot of noise at 2.4 GHz is a relatively easy and inexpensive to construct. However, there are common commercial devices available today that can easily take down a wireless network. Unfortunately, many 2.4 GHz cordless phones that can be purchased in electronics stores have the capability to take an 802.11b network offline. While not a refined electronic weapon, these phones can interfere or completely disable a WLAN. Cordless phones use several different modulation techniques and can overlap on the frequencies used by 802.11b. This overlapping is simply noise to an 802.11b radio. The cordless-phone-induced noise can drop the SNR enough to bring down any WLAN network nearby.

There are also problems with a DoS from other networking protocols. In particular, Bluetooth uses the same ISM (Industrial, Scientific and Medicine) band as 802.11b and 802.11g. The DSSS modulation in 802.11b is susceptible to interference from the modulation used in Bluetooth networks. While there are potential solutions to prevent Bluetooth from stepping on 802.11b transmissions, large-scale Bluetooth deployments may still interfere to the point of inoperability with 802.11b networks. As time passes, the 2.4 GHz ISM band will become more crowded, making unintended DoS attacks against 802.11b networks commonplace.

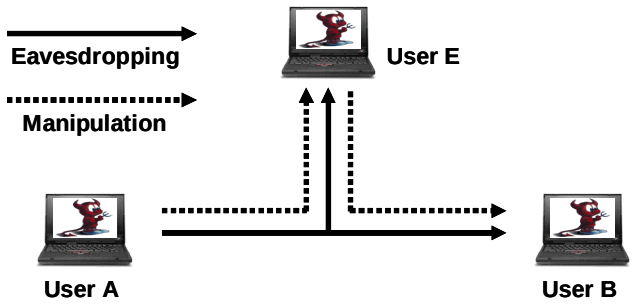

Fig. 4. Eavesdropping versus manipulation.

F. Possible Countermeasures

As a countermeasure, the WLAN operator can periodically monitor the network using e.g. a protocol analyzer and a signal strength indicator every time the throughput appears to decrease. Another possible technique that can be considered to minimize the effect of jamming is to turn off the ability of clients and access points to use the RTS-CTS frame sequence. For example, assume that the attacker has modified driver software to continuously transmit RTS (Request-To-Send) frames. As a response to these RTS frames, a sequence of CTS frames are tying up the airway. Alternatively, the attacker could setup the radio Network Interface Card (NIC) (or a 802.11 frame generator) to send a continuous stream of CTS (Clear-To-Send) frames, which mimics an access point informing a particular radio NIC to transmit and all others to wait. The radio NIC being given permission to transmit could be a fictitious user. In both cases, the legitimate radio NICs in end user devices will continually delay access to the medium. The RTS-CTS frame sequence is normally used to overcome the hidden node problem; however, when the RTS-CTS frame sequence is used it can significantly reduce overall network throughput. For this reason most WLAN adapter products by default disable the use of the RTS-CTS frame sequence [2].

IV. MAN-IN-THE-MIDDLE-ATTACKS

Man-in-the-middle (MITM) attacks have two major forms: eavesdropping and manipulation. Eavesdropping occurs when an attacker receives a data communication stream. This is not so much a direct attack as much as it is a leaking of information. An eavesdropper can record and analyze the data that he is listening to. A manipulation attack requires the attacker to not only have the ability to receive the victim's data but then be able to retransmit the data after changing it, as shown in Fig. 4.

A. Eavesdropping

In a wireless network, eavesdropping is easy because wireless communications are not easily confined to a physical area. A nearby attacker can receive the radio waves on the wireless network without any substantial effort or equipment (*passive eavesdropping*). All frames sent across the wireless medium can be examined in real time or stored for later examination.

Although the transmission distance of wireless LANs is normally limited to hundreds of meters, this limitation is based upon the use of small antennas built into PC cards and other form factors used to create wireless network interface cards. When more sensitive antennas are used, it becomes possible to pick up radio frequency transmission of WLANs at a considerable distance from their source. In fact, certain types of antennas with a very high level of directional sensitivity can be used to receive WLAN signals at distances of up to several miles [2]. Because glass windows typically represent a poor shielding it is quite common for RF energy to literally "leak" out of a building.

Several layers of encryption can and should be implemented to obscure transmitted data in an effort to prevent attackers from gleaning useful information from the network traffic. Since the ability of an attacker to eavesdrop on wireless communications is *fait accompli*, the data-link encryption mechanism WEP (Wired Equivalent Privacy) was developed. If the traffic is not protected at the link layer using WEP, then the higher layer security mechanisms must be used to protect the data. If a security mechanism such as IPsec, SSH, or SSL is not used for transmission then the application data is available to anyone with an antenna in the area without any further effort.

Unfortunately, several flaws in WEP have been uncovered, see e.g. [5]. Even with WEP turned on, a determined attacker can potentially log gigabytes worth of WEP-protected traffic in an effort to post-process the data and break the protection. There are several programs, such as AirSnort and Network Stumbler, that can be obtained from the Internet which can reconstruct the WEP key in use if a sufficient number of frames are captured [2]. In addition to the use of software programs, simply capturing several frames with the same Initialization Vector (IV) can enable a frequency analysis to be performed that could result in the contents of an encrypted frame to be decrypted [2].

The weaknesses in WEP drastically increase the risk due to eavesdropping. If WEP is cracked, there is great deal of sensitive data that is passed across networks with no further encryption, such as a user who accesses his mail using the POP or IMAP protocols. These protocols are widely deployed without any form of encryption of authentication or data transport, putting the users at risk when using a wireless network.

Working upon the premise that one cannot decrypt a signal one cannot hear, a valuable countermeasure to eavesdropping that can be utilized is to obscure or hide RF signals from unauthorized third parties. There are several possibilities to obtain this goal [2]:

- Antenna positioning and the use of shielding.
- Control of the use of a particular antenna, when the WLAN device supports antenna diversity.
- Control of transmit signal strength.
- Directional antennas and shielding (for access points).

Finally, on top of these methods, one could also consider of using a distributed antenna system to shape the WLAN coverage area in a more controlled way [6].

B. Manipulation

Manipulation takes eavesdropping a step further. An attacker who can successfully manipulate data on a network can effectively send data masquerading as a victim computer. Furthermore, the attacker can gather sensitive data by introducing a rogue access point into the WLAN coverage area [7]. The rogue AP can be configured to look like a legitimate AP and, since many wireless clients simply connect to the AP with the best signal strength, users can be "tricked" into inadvertently associating with the rogue AP. Once a user is associated, all communications can be monitored by the attacker through the rogue AP (*active eavesdropping*). The attacker may, for example, change the content of emails, instant messages, or database transactions. The attacker can also choose not to forward packets along, effectively denying use of the network from the victim.

1) Masquerade

The ability of an unauthorized third party to masquerade as a legitimate user of a wireless network can range from being a very simple to complex undertaking, with the degree of complexity based upon the security in effect. If the victim's WLAN does not employ any security it becomes a relatively simple process for an unauthorized third party to determine the SSID in use by an access point and gain access to victim's network. If the WEP is enabled gaining access to victim's network becomes more difficult, but not impossible due to the weaknesses of the WEP. Depending on the security used by the WLAN it can be made extremely difficult to near impossible for an unauthorized third party to masquerade as a legitimate user. However, even if they gain an RF capability to the victim's network, an additional barrier can be added through the use of authentication, authorization and accounting (triple-A) [2].

2) Data Modification

A data modification attack results from the fact that the integrity check value (ICV) used by WLANs is a CRC-32. The CRC-32 is linear with respect to a bit flipping process. This means that flipping bit n in the message results in a deterministic set of bits in the CRC that must be flipped to produce a correct checksum on the modified message. Because flipping bits carries through after an RC4 decryption, this allows the attacker to flip arbitrary bits in an encrypted message and correctly adjust the checksum so that the resulting message appears valid.

Because the ICV is linear it is possible to change both frame data and the composition of the ICV. This means that it is possible to encrypt the 802.11 frame within a layer 3 (network layer) wrapper to preclude the ability of a third party to tamper with frames such that the tampering can go undetected. Encrypting and wrapping the 802.11 frame can be accomplished via several methods which includes the use of a

Web browser's built-in security feature, using IPSec or via the creation of a VPN, which is likely to be based upon the use of IPSec. Another option is to use equipment that supports the Temporal Key Integrity Protocol (TKIP), which represents a series of measures that harden WLANs to include preventing undetected tampering of frames.

V. Rogue Access Points

Because the cost of access points have fallen to the point where they can be acquired for petty reimbursement, many organizations now face the threat of rogue APs due to the fact that many departments in large organizations are setting up their own WLANs. While the use of a WLAN can certainly enhance productivity and facilitate the addition or relocation of stations within an office, when performed without appropriate coordination this network can also represent a security problem. This is because the use of one or more rogue access points is not coordinated with the network manager or the LAN administrator due to their very nature of being "off-the-cuff" equipment. Because rogue access points are unknown to the rest of the organizational network, the use of hardened security techniques is normally omitted. This can result in rogue APs becoming the weakest link in an organization's network. Thus, by installing a rogue AP on an established LAN, a user can create a backdoor into the network, subverting all the hard-wired security solutions and leaving the network open to hackers.

As a countermeasure the network managers and LAN administrators can use various types of monitoring tools to locate rogue access points, and to take the necessary actions to examine the security features of the rogue wireless equipment and initiate any appropriate action to harden the device.

VI. Illicit Use

Illicit use of a wireless network involves an attacker using the network because of its connections to other networks. Attackers may use a network to connect to the Internet or to connect to the corporate network that lives behind the AP. Illicit use may not cause any operational problems, but it still may be unwanted and unlawful use of the wireless network. An attacker in this case may simply be someone who drove up near the AP, associated to the network and is checking his mail. Alternatively, the attacker may be sending spam to thousands of email addresses. The attacker may even be attempting to exploit a file server that lives on the same network as the AP or use the AP as a mask to hide the source of illegal actions, such as hacking other networks.

No matter what the attacker is doing, his use of the network is unacceptable. However, the different types of illicit use pose varying degrees of problems for the organization running the WLAN. Again, in a wired network, illicit use is not a likely problem. In order to use a wired network, an attacker must have physical access to the network infrastructure. However, in most wireless networks, an attacker has much more freedom and is less likely to be caught attempting to use the network.

Access points are not difficult to find. An attacker can simply drive around an area looking for unprotected APs using war-driving software such as NetStumbler. Furthermore, special databases have also been created, removing the war-driving step. An attacker can query any of these public databases to determine nearby APs to use as a launching point. Once an attacker finds an open AP, he can use it for whatever illicit use he desires.

Illicit resource use is a risk for several reasons. An attacker may launch attacks against external servers. These attacks will be seen as originating from the IP addresses of the owner of the access point. If these exploits are detected by remote administrators, they will be tracked down to the owner of the AP. The AP owner may be subject to punishment from his ISP or even a criminal investigation. Without a clear and complete audit trail, this form of illicit use may cause large problems for the AP owner.

In addition, the AP owner may be paying for transit to the Internet on a usage basis. If an attacker is using relatively large amounts of bandwidth, his usage may cost the AP owner money. Even when Internet access is not paid for on a usage basis, the attacker may be using enough bandwidth to infringe on the legitimate use by other clients using the same Internet connection.

VII. Other Risks And Threats

On top of the risks and threats already discussed in this paper, [2] mentions a number of additional security risks and threats, such as:

- The Service Set Identification (SSID)
- File sharing
- Encryption attacks
- Implementation of the Simple Network Monitoring Protocol (SNMP)
- Accessing a management console
- Theft of hardware
- Broadcast monitoring

VIII. Conclusion

The combination of free spectrum, efficient channel coding and cheap interface hardware have made 802.11-based access networks extremely popular. However, this same widespread deployment makes 802.11-based networks an attractive target for potential hackers.

Because they use radio waves, wireless LANs are open to hackers trying to access sensitive information or spoil the operation of the network. In fact, most WLANs do not implement any form of reliable security, enabling access to just about anyone [3].

In this paper a brief description of some of the most common attacks and threats, e.g. denial-of-service, eavesdropping and manipulation, have been given. Furthermore, some possible counteractions have been presented also.

REFERENCES

[1] B. Potter, B. Fleck, *802.11 Security*. O'Reilly & Associates Inc, 2003, ch 2, pp. 18-29.
[2] G. Held, *Securing Wireless LANs*. John Wiley & Sons Ltd, 2003, ch 5, pp. 113-148.
[3] J. Geier, "Minimizing WLAN Security Threats" [Online]. Available: http://www.wi-fiplanet.com/tutorials/article.php/1457211
[4] J. Bellardo, S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions" [Online]. Available: http://ramp.ucsd.edu/~bellardo/pubs/usenix-sec03-80211dos-html/aio.html
[5] N. Borisov, I. Goldberg, D. Wagner, "(In)Security of the WEP Algorithm" [Online]. Available: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
[6] K. Hiltunen, "Using Distributed Antenna Systems to Extend WLAN Coverage", to be presented at S-72.333 Postgraduate Course in Radio Communications 2003-2004.
[7] Airdefense Inc, "Wireless LAN Security: Enterprise Rouge Detection" [Online]. Available: http://www.airdefense.net/whitepapers/roguewatch_request2.php4
[8] C.W. Klaus, "Wireless LAN Security FAQ" [Online]. Available: http://www.iss.net/wireless/WLAN_FAQ.php

HOMEWORK 20.4.2004

Provide brief answers to the following questions:

1. Explain why WLAN is in general more vulnerable to attacks than wired LAN.

2. Explain the difference between active and passive attacks. Name a couple of examples on both. (http://www.psionteklogix.com/assets/downloadable/80211_Security.pdf)

3. Name and explain the three basic types of DoS attacks.

4. Explain why a careful WLAN RF coverage planning and monitoring is an effective countermeasure against e.g. eavesdropping.