IEEE 802.11 Security Considerations

There are two characteristics of a wired LAN that are not inherent in a WLAN.

- In order to transmit over a wired LAN, a station must be physically connected to the LAN. On the other hand, with a WLAN, any station within radio range of the other devices on the LAN can transmit. In a sense, there is a form of authentication with a wired LAN, in that it requires some positive and presumably observable action to connect a station to a wired LAN.
- Similarly, in order to receive a transmission from a station that is part of a wired LAN, the receiving station must also be attached to the wired LAN. On the other hand, with a WLAN, any station within radio range can receive. Thus, a wired LAN provides a degree of privacy, limiting reception of data to stations connected to the LAN.

➢ Access and Privacy Services

IEEE 802.11 defines three services that provide a WLAN with these two features:

- **Authentication:** Used to establish the identity of stations to each other. In a wired LAN, it is generally assumed that access to a physical connection conveys authority to connect to the LAN. This is not a valid assumption for a WLAN, in which connectivity is achieved simply by having an attached antenna that is properly tuned. The authentication service is used by stations to establish their identity with stations they wish to communicate with. IEEE 802.11 supports several authentication schemes and allows for expansion of the functionality of these schemes. The standard does not mandate any particular authentication scheme, which could range from relatively unsecure handshaking to public-key encryption schemes. However, IEEE 802.11 requires mutually acceptable, successful authentication before a station can establish an association with an AP.
- **De-authentication:** This service is invoked whenever an existing authentication is to be terminated.
- **Privacy:** Used to prevent the contents of messages from being read by other than the intended recipient. The standard provides for the optional use of encryption to assure privacy.

➢ Wireless LAN Security Standards

The original 802.11 specification included a set of security features for privacy and authentication that, unfortunately, were quite weak. For privacy, 802.11 defined the Wired Equivalent Privacy (WEP) algorithm. The privacy portion of the 802.11 standard contained major weaknesses. Subsequent to the development of WEP, the 802.11i task group has developed a set of capabilities to address the WLAN security issues. In order to accelerate the introduction of strong security into WLANs, the Wi-Fi Alliance promulgated Wi-Fi Protected Access (WPA) as a Wi-Fi standard. WPA is a set of security mechanisms that eliminates most 802.11 security issues and was based on the current state of the 802.11i standard. As 802.11i evolves, WPA will evolve to maintain compatibility.

Endpoint devices identify wireless networks using a service set identifier (SSID) along with a set of security parameters. The real security for a wireless network comes from the selection of a proven security technique, there have been a number of different security techniques deployed that have been broken. As of this writing the most secure technique is **IEEE 802.11i** which is also known as **WPA2**. This standard provides two different modes of operation including one typically referred to as Personal or Pre-Shared Key (PSK) and Enterprise:

- **WPA2-Personal** - utilizes a shared key that is communicated to both sides (AP and client) before establishing a wireless connection; this key is then used to secure the traffic.
- **WPA2-Enterprise** - utilizes the IEEE 802.1x protocol to authenticate a wireless client using an authentication server before traffic is allowed.

➢ Common Wireless Threats

There are a number of main threats that exist to wireless LANS, these include:

- Rogue Access Points/Ad-Hoc Networks
- Denial of Service
- Configuration Problems (Misconfigurations/Incomplete Configurations)
- Passive Capturing

Let's go through each of these in more detail.

- **Rogue Access Points/Ad-Hoc Networks**

One method that is often used by attackers targeting wireless LANS is to setup a rogue access point that is within the range of the existing wireless LAN. The idea is to 'fool' some of the legitimate devices into associating to this access point over the legitimate access points.

- **Denial of Service**

Anybody familiar with network security is aware of the concept of denial of service (DoS). It is one of the simplest network attacks to perpetrate because it only requires limiting access to services. This can be done by simply sending a large amount of traffic at a specific target. Of course, the amount of traffic required to affect a target device can be much higher than the capabilities of a single machine.

A denial of service attack can also be used in conjunction with a rogue access point. For example, a rogue access point could be setup in a channel not used by the legitimate access point and then a denial of service attack could be launched at the channel currently being used causing endpoint devices to try to re-associate onto a different channel which is used by the rogue access point.

- **Configuration Problems**

Simple configuration problems are often the cause of many vulnerabilities, this is because many consumer/SOHO grade access points ship with no security configuration. A novice user can set up one of these devices quickly and gain access. However they also open up their network to external use without further configuration.

Other potential issues with configuration include weak passphrases, weak security deployments (i.e. WEP vs WPA vs WPA2), and default SSID usage among others.

- **Passive Capturing**

Passive capturing is performed by simply getting within range of a target wireless LAN and then listening and capturing data. This information can be used for a number of things including attempting to break existing security settings and analyzing non-secured traffic. It is almost impossible to really prevent this type of attack because of the nature of a wireless network; what can be done is to implement high security standards using complex parameters.

➢ Summary

The nature of a wireless network is to provide easy access to end users, but this ease of access creates a more open attack surface. Unlike a wired network that requires an attacker to physically access part of the network, a wireless network only requires that the attacker be in close proximity (and even this is relative).

The best attitude to take towards wireless security it to be constantly vigilant; ensure that the security used on a wireless network is adapted as the standards change to ensure a high level of security.