Wireless Security

Merritt Maxim and David Pollino

CHAPTER 2

Wireless Threats

Tremendous advantages can be realized by using wireless technology. Wireless technology gives users the freedom of mobility, gives network designers more options for connectivity, and gives many new devices the capability to connect to networks. However, wireless technology brings significantly more threats than traditional wired networks. In order to design a secure wireless application, the threats or attack vectors that wireless technology gives attackers must be realized. Please note: Applications are never totally secure, but you should still investigate the potential risks of wireless technologies. Therefore, we must realize the potential attacks that exist, so we can design our networks to prevent the common attacks and prepare our processes to mitigate the uncommon attacks.

The Uncontrolled Terrain

The major difference between wired and wireless networks is the anonymous, uncontrolled coverage areas between the end points of the network. In wide area cellular networks, the wireless medium cannot be controlled at all. Current wireless networking technology offers little to control the

coverage area. This enables attackers in the immediate vicinity of a wireless network to perform a number of attacks that are not found in traditional wired networks. This chapter will review the threats that are unique to wireless environments, the equipment required by the attacker to successfully leverage the threats, the problems that occur when roaming from one cell to another, the covert wireless channels, and the cryptographic pitfalls prone to open medium communications.

Eavesdropping

The most widely known problem with an open, uncontrolled medium like wireless technology is that it is susceptible to anonymous attackers. The anonymous attacker can passively intercept radio signals and decode the data being transmitted as shown in Figure 2-1. The equipment used to perform eavesdropping on the network can be as simple as the equipment used to gain access to the network itself. This equipment is sometimes given away with mobile phone activation. At the time of this writing, wireless networking cards can be purchased for under a hundred dollars. All wireless devices have the hardware required to send and receive on the wireless network. With little or no modification, the devices can be configured to capture all traffic on a particular network channel or frequency. The attacker must be in proximity to the transmitter in order to receive the transmission. These types of attacks are nearly impossible to detect and even harder to prevent. The use of antennas and amplifiers enables

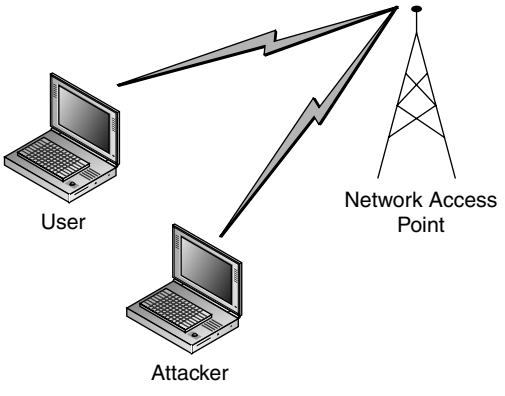


Figure 2-1

Wireless attacker eavesdropping on wireless communications

an attacker to be a considerable distance away from the target during an attack. Recent tests of 802.11 wireless networking equipment show that an attacker can be nearly 20 miles away from a target and still receive a signal, thereby eavesdropping on wireless network communications.

Eavesdropping is used to gather information on the network under attack. The primary goals of the attacker are to understand who uses the network, what is accessible, what the capabilities of the equipment on the network are, when it is used least and most, and what the coverage area is. This information is needed to launch an attack on the target network. Many commonly used network protocols transmit sensitive data such as username and password information in cleartext. An attacker may use captured data to gain access to network resources. Even if communications are encrypted, an attacker is still presented with the ciphertext, which can be stored and analyzed at a later time. Many password encryption algorithms such as Microsoft NTLM can be easily broken.

Active eavesdropping is possible when an attacker can connect to a wireless network. Active eavesdropping on a wireless local area network (LAN) normally involves *Address Resolution Protocol* (ARP) *spoofing*. This technique was originally designed to sniff a switched network. Essentially, this is a man-in-the-middle attack (MITM) (discussed later in the chapter) at the data link layer. The attacker sends out unsolicited ARP replies to target stations on the LAN. The target stations will send all traffic to the attacker instead of the intended destination and the attacker will then forward the packet to the originally intended destination. Therefore, it is possible for a wireless station to sniff the traffic of another wireless client that is out of signal range or a wired client on the local network.

dsniff

dsniff is a suite of network utilities that may be used to sniff passwords, read e-mail, monitor web traffic, and perform active sniffing.

For more information, visit http://monkey.org/~dugsong/dsniff.

Communications Jamming

Jamming occurs when an intentional or unintentional interference overpowers the sender or receiver of a communications link, thereby effectively rendering the communications link useless. An attacker can apply jamming in several ways.

Denial of Service (DoS) Jamming

Jamming the entire network can cause a denial of service (DoS) attack. The entire area, including both base stations and clients, is flooded with interference so that no stations can communicate with each other as shown in Figure 2-2. This attack shuts down all communications in a given area. This type of attack can require a significant amount of power if applied to a broad area. DoS attacks on wireless networks may be difficult to prevent and stop. Most wireless networking technologies use unlicensed frequencies and are subject to interference from a variety of different electronic devices.

Client Jamming Jamming a client station provides an opportunity for a rogue client to take over or impersonate the jammed client as shown in Figure 2-3. Jamming also can be used to DoS the client so that it loses connectivity and cannot access the application. A more sophisticated attack may attempt to interrupt connectivity with the real base station to then reattach with a rogue station.

Base Station Jamming Jamming a base station provides an opportunity for a rogue base station to stand in for the legitimate base station as shown in Figure 2-4. The jamming can also deprive clients of service or a telecom company from revenue.

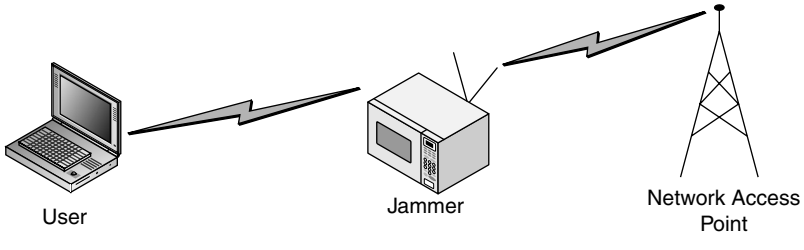


Figure 2-2
Jamming attack on wireless communications

Figure 2-3

Jamming attack against client to hijack communications

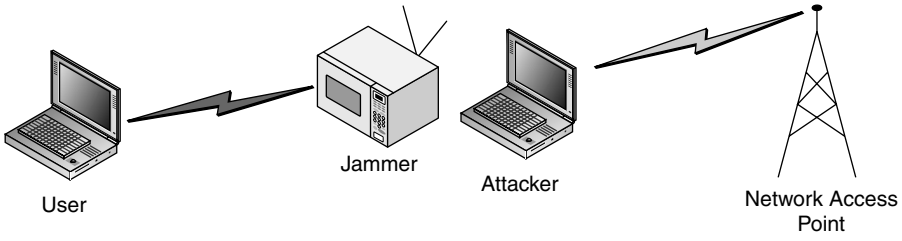
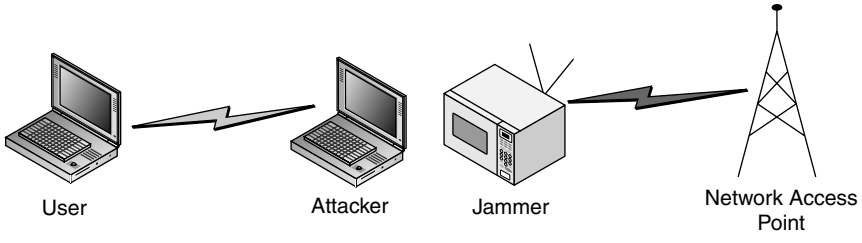


Figure 2-4

Jamming attack against access point to hijack communications



As stated before, most of the wireless networking technologies utilize unlicensed frequencies. Therefore, many devices such as cordless phones, baby monitors, and microwave ovens may interfere with wireless networking and effectively jam the wireless communications. To prevent this kind of unintentional jamming, site surveys are recommended before spending significant money on wireless equipment. These surveys will help to verify that other devices will not interfere with communications and may prevent unneeded capital expenditure on useless equipment.

Injection and Modification of Data

Injection attacks occur when an attacker adds data to an existing connection in order to hijack the connection or maliciously send data or commands. An attacker can manipulate control messages and data streams by inserting packets or commands to a base station and vice versa. Inserting control messages on a valid control channel can result in the disassociation or disconnection of users from the network.

Injection attacks can be used for DoS. An attacker can also flood the network access point with connect messages, tricking the network access point into exceeding a maximum limit, thereby denying authorized users access to the network. Bait-and-switch attacks or midstream insertion

attacks are also possible if the upper-layer protocols (discussed in Chapter 3) do not provide real-time integrity checks in the data stream.

Man-in-the-Middle (MITM) Attacks

Similar to injection attacks are MITM attacks. MITM attacks can take many forms and are designed to subvert the confidentiality and integrity of the session. MITM attacks are more sophisticated than most attacks and require significant information about the network. An attacker will normally impersonate a network resource. When a victim initiates a connection, the attacker will intercept the connection, and then complete the connection to the intended resource and proxy all communications to the resource as shown in Figure 2-5. The attacker is now in a position to inject data, modify communications, or eavesdrop on a session that would normally be difficult to decode, such as encrypted sessions.

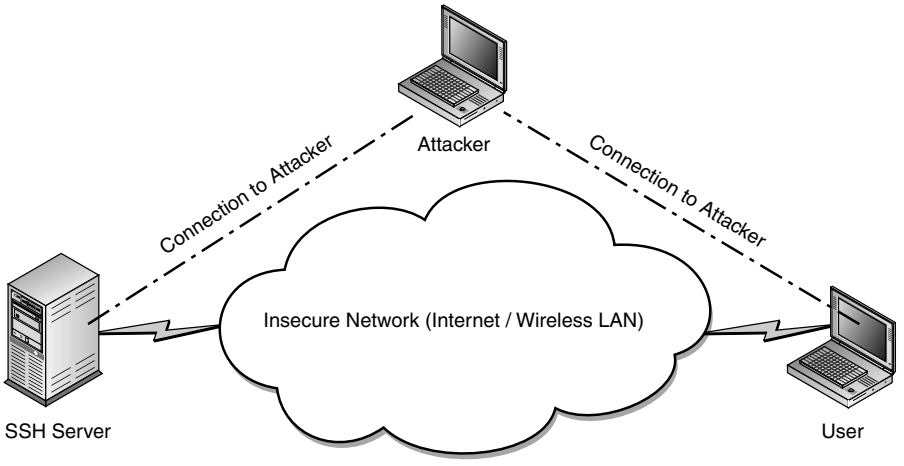
dsniff

Another use for the dsniff utilities is to perform testing of MITM attacks against Secure Sockets Layer (SSL) and Secure Shell (SSH). These tools can serve as a good auditing mechanism for these kind of attacks. Make sure users know what MITM error messages look like; many times users will just disregard the messages.

Rogue Client

After studying a client in the field, an attacker may choose to mimic or clone the client's identity and attempt to gain access to the network and advertised services. The attacker may also be so bold as to steal an access device to attempt to gain access to the network. Securing all wireless devices may be very difficult, for convenience and mobility dictate that most wireless devices are very small. A common wireless security mechanism was supposed to use layer 2 access controls to limit access to

Figure 2-5
MITM attack

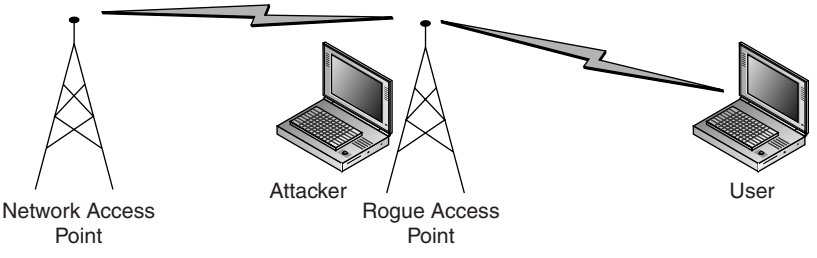


resources. This mechanism proved a failure when it was used by cellular phone companies to limit access to phone numbers by using an Electronic Serial Number (ESN). Then the failure was repeated by the 802.11 wireless LAN standard with Media Access Controls (MACs) that can be easily circumvented by a skilled attacker.

Rogue Network Access Points

An adept attacker can set up a rouge access point to impersonate a network resource. Clients may unknowingly connect to this false access point and divulge sensitive credentials such as authentication credentials. This type of attack can be used in conjunction with directive jamming to block the ears of the legitimate network access point as shown in Figure 2-6.

Figure 2-6
Rogue access point



Users with access to the wired network may also install rouge access points, unknowingly opening up the network to attacks. Users may install a wireless access point seeking the convenience of wireless without knowing the security concerns. Currently, access points can be purchased at almost any electronic store for a minimal cost. These access points can serve as backdoors to the wired network because they are normally installed with the default configuration so they are wide open to attack. Attackers can easily connect to these access points and have the same access that a wired user would have. Most networks rely on firewalls for perimeter security and are not prepared for an attack from an attacker on the inside.

Attack Anonymity

Complete attack anonymity can be achieved through wireless ventures. Without properly laid-out networks to determine locality and direction-finding equipment, an attacker can remain anonymous and hidden anywhere in the wireless coverage area. This can make locating an attacker and forensic work very difficult. I predict that Internet attacks will become increasingly more difficult to solve due to the wide availability of anonymous access through insecure access points. There are many Internet sites that publish the location of insecure access points that may be used for this purpose.

War Driving

War driving is the process of searching for open wireless LANs by driving around a particular area. The name comes from the term "war dialing," which is an old attack method that involves repeatedly dialing different numbers to search for modems and other network entry points. There are many Internet sites devoted to war driving. For less than $300, an attacker can outfit a laptop with a wireless network card and a Global Positioning System (GPS) unit for war driving. War-driving software is freely available on the Internet at www.netstumbler.com.

It is important to note that many attackers are searching out networks not to attack internal resources, but to gain free anonymous Internet access. The access can be used for a malicious attack against other networks. If network operators do not take prudent steps to prevent malicious attackers from using their network, they may be liable for damages inflicted against other networks using their Internet access. Caution must be exercised.

Client-to-Client Attacks

Once on a network, other network clients can be attacked directly. If successful, the attacker may gain the credentials required to gain further access into the corporate or telecom network. Most network administrators do not take the time to harden stations or install personal firewall software. Therefore, successful attacks on wireless-connected clients may reveal sensitive information such as the username and password that can be used to access other network resources. All Internet or wireless-connected stations need to be adequately hardened.

Infrastructure Equipment Attacks

Incorrectly configured infrastructure equipment is a prime target for attackers and usually provides a means for attaining further penetration into the network. These are sometimes referred to as stepping stones and can be used to bypass access controls. Network devices such as routers, switches, backup servers, and log servers are prime targets. Many network administrators rely on layer 2 security mechanisms such as virtual LANs (VLANs) to keep wireless networks separate from wired networks. There are many documented attacks that can be used to bypass VLAN security. There are many attacks depending on the switch, but they break down into three main categories: switch attacks, MAC attacks, and routing attacks.

Switch attacks take many different forms. Some involve flooding the MAC or ARP table in the switch to cause it to fail open. This attack is often caused inadvertently by administrators choosing a low-quality switch. Other attacks against the switch involve manipulating the protocol that switches use to communicate such as spanning tree. MAC attacks include ARP spoofing and other physical layer attacks that can be used to fool network devices into sending the data to unintended recipients. Routing attacks are very difficult and normally involve participating in the routing protocol, such as Open Shortest Path First (OSPF) or Enhanced

Interior Gateway Routing Protocol (EIGRP), to change the flow of traffic for DoS or sniffing.

Attacker Equipment

The equipment used by the casual attacker can minimally consist of a wireless network interface. This can either be a wireless Ethernet network interface card (NIC), a General Packet Radio Service (GPRS), or a Cellular Digital Packet Data (CDPD) cellular telephony handset connected to a laptop either as a Personal Computer Memory Card International Association (PCMCIA) card or through some communications link. Advanced attackers will sometimes employ this wireless interface in conjunction with jammers and specialized software. A sample is shown in Figure 2-9. Cellular network attackers will generally use a configuration as depicted in Figure 2-7 because the network coverage is understood and generally covers a large area.

On the other hand, wireless Ethernet networks generally cover a smaller area. Attackers will first detect the networks and determine the coverage area to find the best position to mount an attack. The preferred position is one that provides cover sometimes behind landscaping or in a

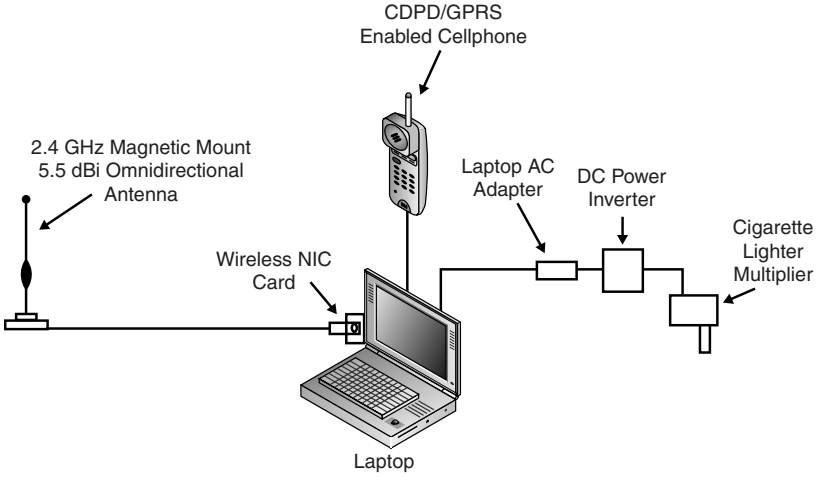


Figure 2-7

Attacker hardware configuration

different building and optionally an easy escape route. The basic network discovery setup consists of a laptop, a GPS unit, an antenna, an amplifier, and a wireless Ethernet NIC. In order to perform long-duration sweeps, extra power can be obtained by using an inverter for converting 12V DC into 120V AC to power the laptop or any other equipment one may be using (such as a jammer or a low-noise amplifier [LNA]). Some attackers have been known to remove dashboard cigarette lighters and replace with DC inverters to provide power for an extended period of time. Once the basic coverage is determined, the attacker, utilizing various antenna apparatus, determines the best link from which to mount attacks.

Attackers will utilize various antenna types when mounting an attack, depending on the situation and the desired effect. Antenna types are generally characterized by the amount of gain or increase in received or transmitted signal strength and beam width. The beam width of an antenna indicates how electromagnetic radiation emanates. The three most common antenna types are the omnidirectional antenna, the yagi, and the parabolic.

The omnidirectional antenna has a beam width of 360 degrees and is usually deployed to survey or jam a wide area (see Figure 2-8). Electromagnetic radiation is received from all sides and therefore, unless in an array, direction cannot be determined with a single station utilizing an omnidirectional antenna. Omnidirectional antennas also have little to no gain, unless they are assembled in a collinear array where gain can be as high as 8 dBi.

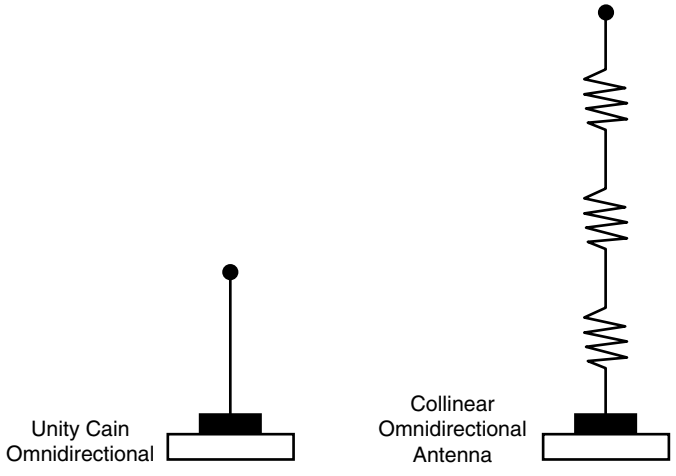
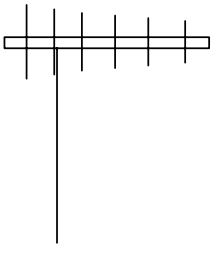


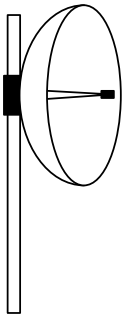
Figure 2-8

Common omnidirectional antenna

The yagi antenna has special properties that focus the electromagnetic radiation from a driven element into a directed pattern. A yagi antenna, shown below, typically exhibits a beam width of 10 to 20 degrees and a gain of 10 to 18dBi. The yagi is usually deployed when one cannot gain direct access to the coverage area using an omnidirectional antenna. A typical yagi antenna has a gain of 10 to 18 dBi. A yagi can also be used when the jamming of a particular device or group of devices sharing a geographical area is desired. Using a tripod designed for a camera or a telescope can prove effective for aiming a yagi in the field.



The parabolic antenna, shown below, has the narrowest beam width of all, typically between 4 and 10 degrees. The parabolic antenna is generally deployed when concealment is of concern and great distances are to be covered. The parabolic antenna is difficult to use due to the narrow beam width, but this characteristic can be used to determine location. This antenna can also be used to support jamming functions as well as very precise attacks, perhaps to avoid detection systems.



Survey software for collecting packet reception locations in a log file categorized by longitude and latitude is commonly used to discover the location and coverage of unknown wireless Ethernet networks. The longitude/latitude coordinates are supplied by a GPS device. Wireless coverage

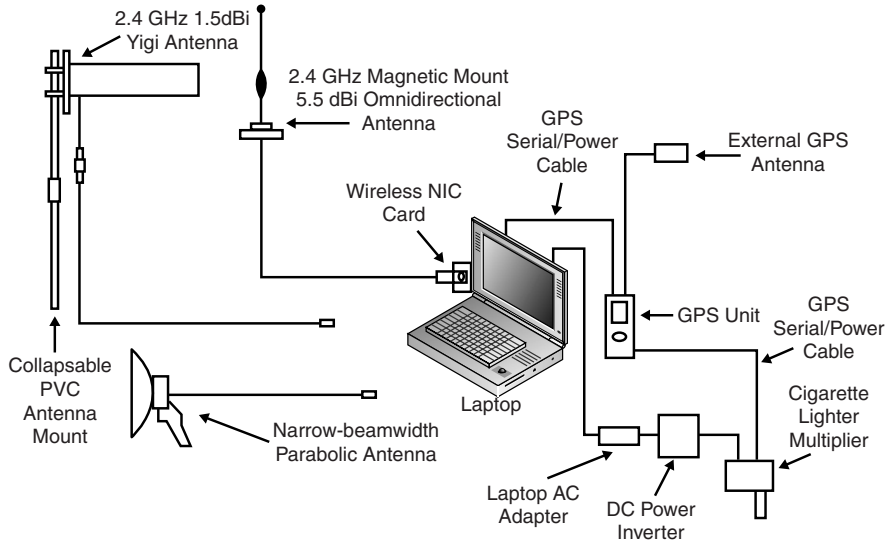


Figure 2-9

Wireless assessment/war-driving hardware setup

of a given area can then be clearly identified when plotted on a map. Typical attacker hardware configuration is shown in Figure 2-9.

An antenna is by far the most useful tool for a network designer or an attacker, but an amplifier can also be used to boost reception over a long distance. Amplifiers will increase the signal as well as the noise, so getting a good quality amplifier is important. Using amplifiers may violate Federal Communications Commission (FCC) regulations, so great care needs to be taken.

Covert Wireless Channels

There is a final vector that wireless implementers must consider when evaluating or designing a wireless network. Due to the low cost of wireless access points and the ease of creating software-based access points consisting of a standard desktop or laptop computer and a wireless NIC, one must be vigilant in detecting incorrectly configured or unintentionally deployed wireless equipment on the wired network, such as the network backdoor shown in Figure 2-10. This equipment can poke very damaging holes in the fabric of the wired infrastructure, which will be exposed to attackers within several miles of a target network.

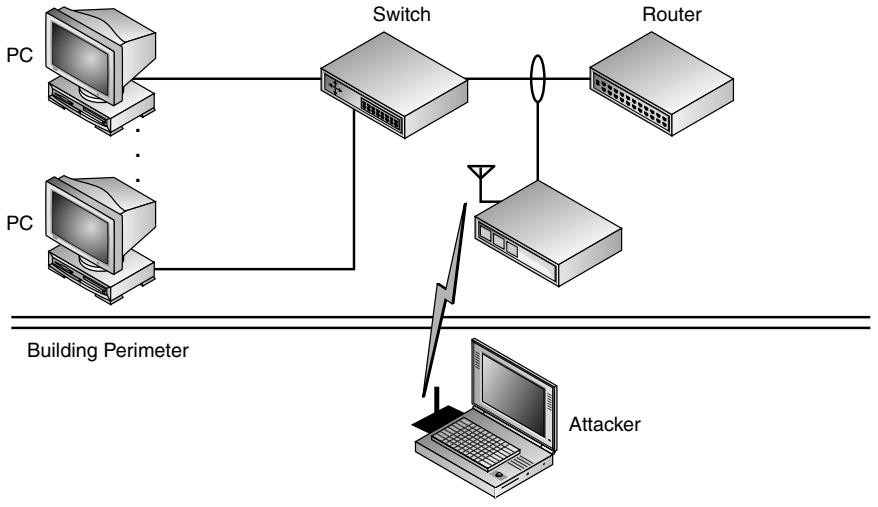


Figure 2-10
Access point network backdoor

A similar configuration can also bridge air-gap networks via a wireless channel and funnel data from an air-gapped network outside a protective building by chaining access points together until the final leg of the link leaves the confines of the building as shown in Figure 2-11. This configuration can effectively increase the amount of coverage area to many miles. The equipment needed for this configuration is very inexpensive and may be purchased at most electronic stores.

Roaming Issues

Another major difference between a wireless and a wired environment is end-point mobility. The concept of roaming on Code-Division Multiple Access (CDMA), Global System for Mobile Communications (GSM), and wireless Ethernet are all very similar. Many Transmission Control Protocol/Internet Protocol (TCP/IP) network applications require the IP address of the server and the client to remain static; however, when roaming among a network, you will undoubtedly be required to leave and join across subnets. This requirement is the drive behind mobile IP and other wireless network roaming mechanisms.

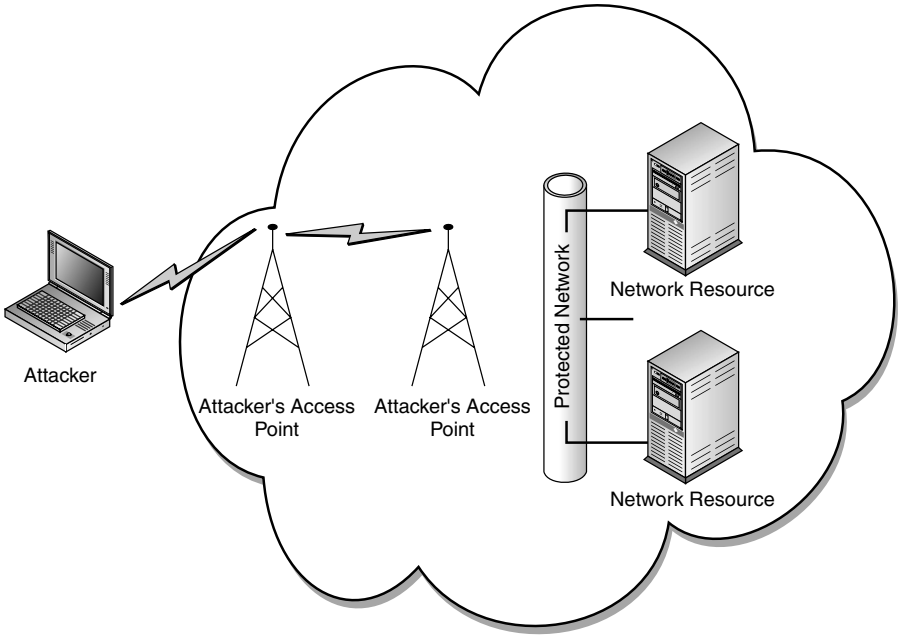


Figure 2-11

Attacker extending range by chaining access points

The basic idea behind mobile IP is location registration and packet redirection. A location-independent address is used to keep TCP/IP connectivity alive, while a temporary location-dependent address is used to provide connectivity to the local network resources. There are three other mandatory requirements of a mobile IP system. There is the mobile node (MN), home agent (HA), and the foreign agent (FA). The MN is the wireless user device, the HA is a server located on the MN's home network, and the FA is a server residing on the roamed-to network. When an MN roams to a network, it obtains a temporary location-dependent IP address and registers with a FA. The FA then communicates with the HA, notifying the HA that the MN is attached to it, and that all packets should now be routed through the roamed-to FA to be delivered to the MN.

There are some obvious problems with this schema. Replay attacks of the registration process can be performed by a rogue station in a different cell to attempt to capture outbound traffic from the network. One can also imitate a valid station and illegitimately obtain network service.

Cryptographic Threats

CDMA and GSM cellular networks and wireless Ethernet networks have employed cryptographic mechanisms in order to deter eavesdropping and stymie unauthorized network usage. However, in both networks, oversights resulted in the compromise of communications and fraudulent use.

Wired Equivalent Privacy (WEP) is a cryptographic mechanism designed to provide security for 802.11 networks. Implementation flaws and key management issues have proved WEP almost useless. WEP was designed with a single static key that was to be used by all users. Controlling access to these keys, changing the keys frequently, and detecting compromises is nearly impossible. An examination of the implementation of the RC4 algorithm in WEP has revealed weaknesses that enable an attacker to completely recover the key after capturing minimal network traffic. Tools are available on the Internet that allow an attacker to recover the key in a number of hours. Therefore, WEP cannot be relied on to provide authentication and confidentiality on a wireless network.

Using these cryptographic mechanisms is better than not using them, but due to the known vulnerabilities, other mechanisms are needed to protect against the aforementioned attacks. All wireless communication networks are subject to the attacker eavesdropping on phases of contact, namely, connection establishment, session communication, and connection termination. The very nature of wireless communication eliminates out-of-band management and control, thus requiring protection. Key management, as always, presents additional challenges when being applied to roaming users and a shared open medium. We will discuss commonly used cryptographic mechanisms in the following chapter.

Conclusion

Understanding the threats to wireless technology is the first step in securing wireless implementations. The advantages of using wireless are tremendous. Therefore, these threats need to be considered, but should not stop the deployment of wireless applications. Taking a few simple security measures can dramatically reduce the impact of many common attacks. The following chapter will help to show what steps can help to reduce wireless threats.