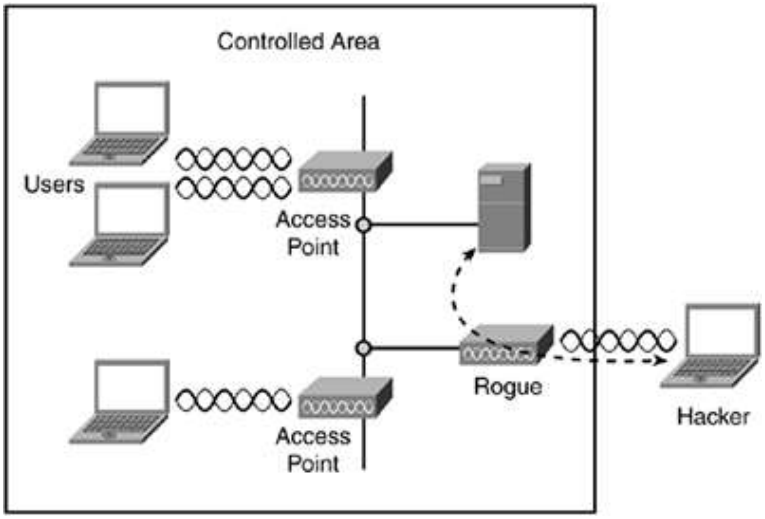
Figure 8-2.) A rogue access point is an unauthorized access point on the network. An employee might purchase an access point and install it within his office without knowing the security implications. A hacker could also plant a rogue access point within a facility by purposely connecting an unprotected access point to the corporate network.

Figure 8-2. Rogue Access Points Offer an Open Port for Hackers to Exploit



A rogue access point can be exploited because it probably won't have any encryption activated, which provides an open door for someone to easily access the corporate network from outside the facility. For that reason, a company should continually monitor for the presence of rogue access points. Keep in mind that this is a problem whether a wireless network is in place or not. Someone could connect a rogue access point to a completely wired Ethernet network.

To counter unauthorized access, the wireless network should deploy mutual authentication between client devices and the access points. Authentication is the action of proving the identity of a person or device. The wireless network should implement methods for client de-

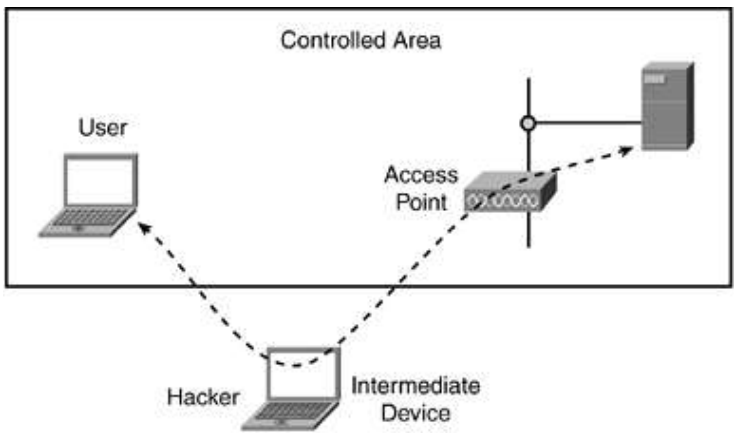
Exhibit 1010
Page 228 of 292

vices to prove identity to base stations and vice versa. This ensures the validity of the user and proves that the user is connecting to a legitimate access point. In addition, access points should authenticate with the switches to disallow the successful connection of a rogue access point.

Man-in-the-Middle Attacks

The use of encryption and authentication techniques improves the security of a wireless network; however, smart hackers can still find vulnerabilities because of the way that networking protocols operate. A definite weakness is a man-in-the-middle attack, which is when a hacker places a fictitious device between the users and the wireless network. (See **Figure 8-3**.) For example, a common man-in-the-middle attack exploits the common address resolution protocol (ARP) that all TCP/IP networks utilize. A hacker with the right tools can exploit ARP and take control of the wireless network.

Figure 8-3. Intermediate Devices Enable Man-in-the-Middle Attacks



ARP is a crucial function used by sending a wireless or wired NIC to discover the physical address of a destination NIC. The physical address of a card is the same as the medium-access control (MAC) ad-

Exhibit 1010
Page 229 of 292

dress, which is embedded in the card by the manufacturer and unique from any other NIC or network component. The MAC address is analogous to the street address of your home. Just as someone must know this address to send you a letter, a sending NIC must know the MAC address of the destination. The NIC only understands and responds to the physical MAC address.

The application software that needs to send the data will have the destination IP address, but the sending NIC must use ARP to discover the corresponding physical address. It gets the address by broadcasting an ARP request packet that announces the destination NIC's IP address. All stations will hear this request, and the station with the corresponding IP address will return an ARP response packet containing its MAC address and IP address.

The sending station will then include this MAC address as the destination address in the frame being sent. The sending station also stores the corresponding IP address and MAC address mapping in a table for a specified period of time (or until the station receives another ARP response from the station having that IP address).

A problem with ARP is that it introduces a security risk resulting from ARP spoofing. For example, a hacker can fool a station by sending, from a rogue network device, a fictitious ARP response that includes the IP address of a legitimate network device and the MAC address of the rogue device. This causes all legitimate stations on the network to automatically update their ARP tables with the false mapping.

Of course, these stations will then send future packets to the rogue device rather than to the legitimate access point or router. This is a classic man-in-the-middle attack, which enables a hacker to manipulate user sessions. As a result, the hacker can obtain passwords, capture sensitive data, and even interface with corporate servers as if they were the legitimate user.

Exhibit 1010
Page 230 of 292

In order to circumvent man-in-the-middle attacks using ARP spoofing, vendors such as OptimumPath implement secure ARP (SARP). This enhancement to ARP provides a special secure tunnel between each client and the wireless access point or router, which ignores any ARP responses not associated with the clients on the other end of the tunnel. Therefore, only legitimate ARP responses provide the basis for updating ARP tables. The stations implementing SARP are free from spoofing.

The use of SARP, however, requires the installation of special software on each client. Consequently, SARP is not practical for public hotspots. Enterprises, though, can install SARP on clients and be much freer from man-in-the-middle attacks.

Denial of Service

A Denial of Service (DoS) attack is an assault that can cripple or disable a wireless network. The possibility of such an attack is something that anyone deploying wireless networks should consider. Be sure to think about what could happen if the wireless network becomes unavailable for an indefinite period of time.

The severity of the DoS attack depends on the impact of the wireless network becoming inoperative. For example, a hacker could disable someone's home wireless LAN, but the result will probably just inconvenience the homeowner. A DoS attack that shuts down a wireless inventory system, however, could cause major financial loss.

One form of DoS attack is the brute-force method. For example, a huge flood of packets that uses all of the network's resources and forces the network to shut down is a DoS brute-force attack. There are tools on the Internet that enable hackers to cause excessive flooding on wireless networks. A hacker can perform a packet-based brute-force DoS attack by sending useless packets to the server from other computers

Exhibit 1010
Page 231 of 292

on the network. This adds significant overhead on the network and takes away usable bandwidth from legitimate users.

Another way of stopping most wireless networks, especially those that use **carrier sense access**, is using a strong radio signal to dominate the airwaves and render access points and radio cards useless. Protocols such as 802.11 are very polite and let the DoS attack signal have access to the medium for as long as it wants.

The use of strong radio signals to disrupt the network is a rather risky attack for a hacker to attempt, however. Because a powerful transmitter at a close range must execute this type of attack, the owners of the wireless network can find the hacker through the use of homing tools available in network analyzers. Once the jamming source is found, authorities can stop it and possibly apprehend the culprits.

Sometimes a DoS occurrence on a wireless network is unintentional. For example, 802.11b operates in a crowded radio spectrum. Other devices such as cordless phones, microwaves, and Bluetooth can cause a significant reduction in 802.11b performance. The interference can keep a wireless network from operating.

In addition, some security mechanisms are prime targets for DoS attacks. Wi-Fi Protected Access (WPA), for example, is vulnerable to a type of DoS attack. WPA uses mathematical algorithms to authenticate users to the network. If a user is trying to get in and sends two packets of unauthorized data within one second, WPA will assume it is under attack and shut down.

The only completely effective way to counter DoS attacks is to isolate your computer in a room with heavy security and unplug it from all networks, including the Internet. This means not using a wireless network, of course. The U.S. government uses this method to protect their most sensitive data, but this solution is not practical for any enterprise

Exhibit 1010
Page 232 of 292

or home application, where there are benefits for deploying wireless networks.

The most fundamental defense against DoS is developing and maintaining strong security practices. Actions such as implementing and updating firewalls, maintaining updated virus protection, installing up-to-date security patches, ensuring strong passwords, and turning off network devices when they are not needed should be routine practices for all companies and homeowners.

You can protect a wireless LAN against DoS attacks by making the building as resistant as possible to radio signals coming in. Here are some steps to help reduce radio signal leakage:

- If interior walls use metal studs, make sure they are grounded.
- Install thermally insulated copper or metallic film-based windows.
- Use metallic window tint instead of blinds or curtains.
- Use metallic-based paint on the interior or exterior walls.
- Run tests to determine how far the signal actually leaks outside of the building. Adjust transmitter power accordingly until the leakage is eliminated or reduced to the point that it would be easy to locate a hacker.
- Aim directive access point antennas toward the inside of the building.

Because there's no way of completely countering all types of DoS attacks, consider a plan B if a DoS attack will cause significant damage. For example, have a process for switching to batch processing or paper-based methods if the application is subjected to a severe DoS attack. You certainly don't want potential weaknesses in the wireless network to bring down your company!

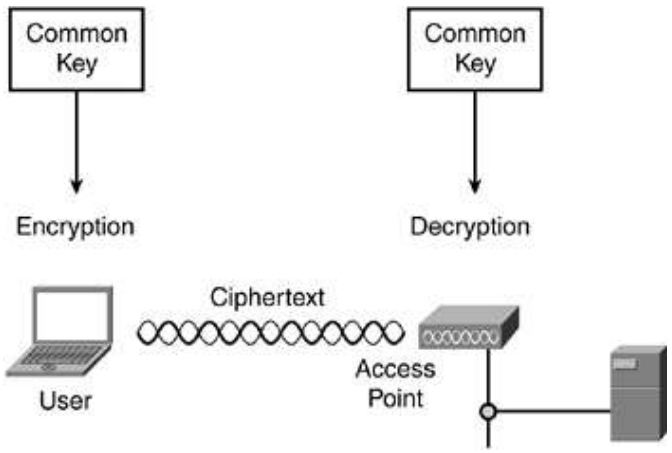
Exhibit 1010
Page 233 of 292

Encryption

Encryption alters the bits of each data packet to guard eavesdroppers from decoding data, such as credit card numbers. Before encryption the data is called plaintext, which is easy to decode by using sniffing tools. The encryption converts the plaintext into ciphertext, which someone can decode only through the use of a proper secret key.

Many encryption methods, such as the 802.11 Wired Equivalent Privacy (WEP), are symmetric—that is, the same key that does the encryption is also the one that performs the decryption. **Figure 8-4** illustrates this process.

Figure 8-4. Symmetric Encryption Uses a Common Key



For example, the radio NIC uses key xyz to encrypt a data packet, and an access point uses key xyz to perform the decryption. This requires both the sending and receiving stations to trust each other, as is the case with a private wireless network application such as an enterprise

wireless LAN. It's not practical to use symmetric keys in a public application, however, because anyone, including hackers, could obtain the key.

For symmetric encryption to be effective, the function must minimize the reuse of encryption keys by changing them often, possibly every frame transmission. This decreases the time available for a hacker to break into the network and makes it difficult—if not impossible—to compromise the security of the network. As a result, symmetric encryption mechanisms must have effective key distribution methods.

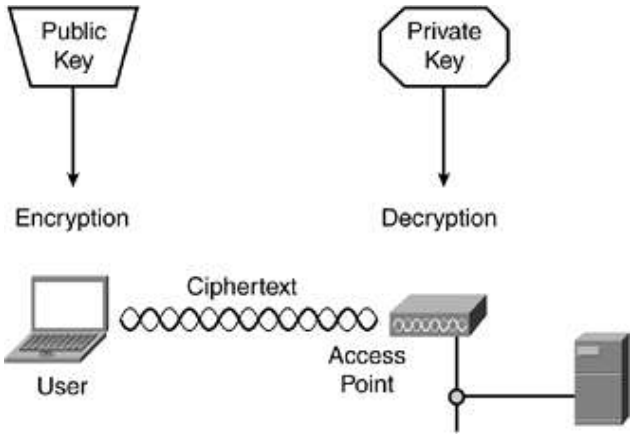
Public key cryptography uses asymmetric keys, with one that is private and another one that is public. As the name applies, the private key is secret; however, anyone can know the public key. This enables more effective encryption and authentication mechanisms because it simplifies key distribution.

An important requirement of public key encryption is that a set of public and private keys must match from a cryptographic standpoint. For example, the sending station can encrypt data using the public key, and the receiver uses the private key for decryption. The opposite is also true. The sending station can encrypt data using the private key, and the receiving station decrypts the data using the public key.

If the goal is to encrypt data, the sending station will use a public key to encrypt the data before transmission; this is shown in **Figure 8-5**. The receiving station uses the matching private key to decrypt the data upon reception. Each station keeps its private key hidden in order to avoid compromising encrypted information. As a result, the process allows any station to use a publicly known key to send encrypted data to any other station.

Figure 8-5. Public Key Encryption Enables All Senders of Encrypted Data to Use a Publicly Available Key

Exhibit 1010
Page 235 of 292



Public key cryptography works effectively for encrypting data because the public key can be made freely available to anyone wanting to send encrypted data to a particular station. A station that generates a new private key can distribute the corresponding public key over the network to everyone without worry of compromise. The public key can be posted on a website or sent unencrypted across the network.

WEP

WEP is 802.11's optional encryption and authentication standard implemented in the MAC Layer that most radio NIC and access point vendors support. When deploying a wireless network, you need to fully understand the ability of WEP to improve security.

WEP Operation

If a user activates WEP, the NIC encrypts the payload (frame body and cyclic redundancy check [CRC]) of each 802.11 frame before transmission using an RC4 stream cipher provided by RSA security. The receiving station, such as an access point or another radio NIC, performs decryption upon arrival of the frame. As a result, 802.11 WEP only encrypts data between 802.11 stations. Once the frame enters the wired side of the network, such as between access points, WEP no longer applies.

As part of the encryption process, WEP prepares a key schedule (seed) by linking the shared secret key supplied by the user of the sending station with a randomly generated 24-bit initialization vector (IV). The IV lengthens the life of the secret key because the station can change the IV for each frame transmission. WEP inputs the resulting seed into a pseudo-random number generator that produces a key stream equal to the length of the frame's payload plus a 32-bit integrity check value (ICV).

The ICV is a checksum that the receiving station recalculates and compares to the one sent by the sending station. It determines whether the transmitted data underwent any form of tampering while in transit. If the receiving station calculates an ICV that doesn't match the one found in the frame, the receiving station can reject the frame or flag the user.

WEP specifies a shared secret key to encrypt and decrypt the data. With WEP, the receiving station must use the same key for decryption. Each radio NIC and access point, therefore, must be manually configured with the same key.

Before transmission takes place, WEP combines the key stream with the payload/ICV through a bitwise XOR process, which produces ciphertext (encrypted data). WEP includes the IV in the clear (unencrypted) within the first few bytes of the frame body. The receiving station uses this IV along with the shared secret key supplied by the receiving station user to decrypt the payload portion of the frame body.

In most cases, the sending station will use a different IV for each frame (this is not required by the 802.11 standard). When transmitting messages having a common beginning, such as the sender's address in an e-mail, the beginning of each encrypted payload will be equivalent when using the same key. After encrypting the data, the beginnings of these frames would be the same, offering a pattern that can aid hackers in cracking the encryption algorithm. Since the IV is different for

Exhibit 1010
Page 237 of 292

most frames, WEP guards against this type of attack. The frequent changing of IVs also improves the ability of WEP to safeguard against someone compromising the data.

WEP Issues

WEP is vulnerable because of relatively short IVs and keys that remain static. The issues with WEP don't really have much to do with the RC4 encryption algorithm. With only 24 bits, WEP eventually uses the same IV for different data packets. For a large, busy network, this re-occurrence of IVs can happen within an hour or so.

This results in the transmission of frames having key streams that are too similar. If a hacker collects enough frames based on the same IV, the individual can determine the shared values among them—that is, the key stream or the shared secret key. This, of course, leads to the hacker decrypting any of the 802.11 frames.

The static nature of the shared secret keys emphasizes this problem. 802.11 doesn't provide any functions that support the exchange of keys among stations. As a result, system administrators and users generally use the same keys for weeks, months, and even years. This gives mischievous culprits plenty of time to monitor and hack into WEP-enabled networks.

When to Use WEP

Despite its flaws, you should enable WEP as a minimum level of security. Many people have discovered wireless networks that use protocol analyzers, such as AiroPeek and AirMagnet. Most of these people are capable of detecting wireless networks where WEP is not in use and then use a laptop to gain access to resources located on the associated network.

By activating WEP, however, you significantly minimize this from happening, especially if you have a home or small business network. WEP

Exhibit 1010
Page 238 of 292

does a good job of keeping most people out. Beware: There are true hackers around who can exploit the weaknesses of WEP and access WEP-enabled networks, especially those with high utilization.

Temporal Key Integrity Protocol

The 802.11i standard includes improvements to wireless LAN security. One of the upgrades is the Temporal Key Integrity Protocol (TKIP), initially referred to as WEP2. TKIP is an interim solution that fixes WEP's key reuse problem. In fact, many wireless LAN products already have TKIP as an option.

The TKIP process begins with a 128-bit temporal key shared among clients and access points. TKIP combines the temporal key with the client's MAC address and then adds a relatively large 16-octet IV to produce the key that will encrypt the data. This procedure ensures that each station uses different key streams to encrypt the data.

TKIP uses RC4 to perform the encryption, which is the same as WEP. A major difference from WEP, however, is that TKIP changes temporal keys every 10,000 packets. This provides a dynamic distribution method that significantly enhances the security of the network.

An advantage of using TKIP is that companies having existing WEP-based access points and radio NICs can upgrade to TKIP through relatively simple firmware patches. In addition, WEP-only equipment will still interoperate with TKIP-enabled devices using WEP. TKIP is a temporary solution, and most experts believe that stronger encryption is still needed.

In addition to the TKIP solution, the 802.11i standard includes the Advanced Encryption Standard (AES) protocol. AES offers much stronger encryption. AES uses the Rine Dale encryption algorithm, which is a tremendously strong encryption that replaces RC4. Most cryptographers feel that AES is uncrackable. In addition, the 802.11i standard will include AES as an option over TKIP. In fact, the U.S.

Exhibit 1010
Page 239 of 292