Commerce Department's National Institutes of Standards and Technology (NIST) organization chose AES to replace the aging Data Encryption Standard (DES). AES is now a Federal Information Processing Standard, which defines a cryptographic algorithm for use by U.S. government organizations to protect sensitive but unclassified information. The Secretary of Commerce approved the adoption of AES as an official government standard in May 2002.

The problem with AES is that it requires more processing power than what most access points on the market today can support. As a result, the implementation of AES will require companies to upgrade their existing wireless LAN hardware to support the performance demands of AES. An issue, however, is that AES requires a coprocessor (additional hardware) to operate. This means that companies need to replace existing access points and client NICs to implement AES.

Wi-Fi Protected Access

The Wi-Fi Protocol Access (WPA) standard provided by the Wi-Fi Alliance provides an upgrade to WEP that offers dynamic key encryption and mutual authentication. Most wireless vendors now support WPA. WPA clients utilize different encryption keys that change periodically. This makes it more difficult to crack the encryption.

WPA 1.0 is actually a snapshot of the current version of 802.11i, which includes TKIP and 802.1x mechanisms. The combination of these two mechanisms provides dynamic key encryption and mutual authentication, something needed in wireless LANs. WPA 2.0 offers full compliance with the 802.11i standard.

Virtual Private Networks

If wireless users will be roaming into public areas, such as airports and hotels, strongly consider virtual private network (VPN) solutions. Even though VPNs are not foolproof, they provide an effective means of end-to-end encryption. VPNs are also effective when clients roam

Exhibit 1010
Page 240 of 292

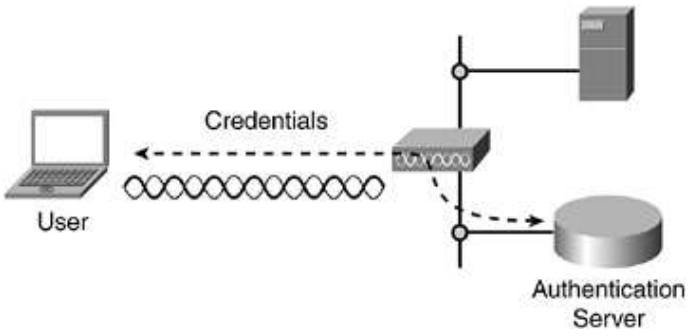
across different types of wireless networks because they operate above the dissimilar network connection levels.

Exhibit 1010
Page 241 of 292

Authentication

The use of mutual authentication is important in a wireless network. This will guard against many security issues, such as man-in-the-middle attacks. With mutual authentication, the wireless client and the wireless network must prove their identity to each other. This process uses an authentication server, such as Remote Authentication Dial-In User Service (RADIUS), to perform the authentication. Figure 8-6 illustrates the process of authentication.

Figure 8-6. Authentication Verifies the Identity of Users and Client Devices Through Credentials, Such as Passwords and Digital Certificates



802.11 Authentication Vulnerabilities

WEP only provides a method for authenticating radio NICs to access points, not the other way around. As a result, a hacker can reroute data through an alternate unauthorized path that avoids other security mechanisms. Instead of one-way authentication, wireless net-

Exhibit 1010
Page 242 of 292

works need to implement mutual authentication to avoid this problem.

When a wireless client becomes active, it searches the medium for beacons broadcast by access points. By default, the access point broadcasts beacons containing the service set identifier (SSID) of the access point, as well as other parameters. The access point only enables association if the client SSID matches the access point SSID. This process offers a basic, but weak, form of authentication.

The major vulnerability is the fact that the SSID is sent unencrypted, which makes it visible to wireless packet sniffers. Because of this, a hacker can easily identify the SSID within the beacon frame and authenticate with the wireless network. Even if the access point is set not to broadcast the SSID—an optional feature available in only a few access points—sniffers can still obtain the SSID from association request frames sent from client devices to the access point.

802.11 offers, by default, a form of authentication called open systems authentication. In this mode, the access point grants approval for any request for authentication. The client simply sends an authentication request frame, and the access point responds with an authentication approval. This allows anyone having the correct SSID to associate with the access point.

The 802.11 standard also includes shared key authentication, an optional, more advanced form of authentication. This is a four-step process:

1. The client sends an authentication request frame.

2. The access point responds with a frame containing a string of characters called challenge text.

Exhibit 1010
Page 243 of 292

3. The client then encrypts the challenge text using the common WEP encryption key. The client sends the encrypted challenge text back to the access point, which decrypts the text using the common key and compares the result with the text originally sent.

4. If the decrypted text matches, the access point authenticates the client.

This seems adequate for authentication, but a problem is that shared key authentication only proves that the client has the correct WEP key.

MAC Filters

Some wireless base stations offer medium access control (MAC) filtering. When implementing MAC filtering, the access point examines the source MAC address of each incoming frame. The access point will deny frames without a MAC address that matches a specific list programmed by the administrator. As a result, MAC filtering provides a primitive form of authentication.

MAC filtering, however, has some weaknesses. For example, WEP encryption does not encrypt the MAC address field of the frame. This allows a hacker to easily sniff the transmission of frames and discover valid MAC addresses. And, a hacker can use freely available software to change the MAC address radio NICs to match a valid MAC address. This enables the hacker to masquerade as a real user and fool the access point when the legitimate user is not present on the network.

In addition, MAC filtering can be tedious to manage when there are several users. An administrator must enter each user's MAC address in a table, and then make applicable changes when new users come about. For example, an employee from another company location might need access to the wireless LAN during a visit. The administra-

Exhibit 1010
Page 244 of 292

tor must determine the MAC address and program it in the system before the visitor can access the network. MAC address filtering might be adequate for smaller home and office applications, but the hands-on nature of this approach is not desirable by administrators of enterprise wireless networks.

Authentication Using Public Key Cryptography

In addition to protecting information from hackers, stations can use public key cryptography to authenticate themselves to other stations or access points. This might be necessary before an access point or controller allows a particular station to interface with a protected side of the network. Likewise, the client can authenticate the access point in a similar manner.

A station authenticates itself by encrypting a string of text within a packet using its private key. The receiving station decrypts the text with the sending station's public key. If the decrypted text matches some predetermined text, such as the station's name, the receiving station knows that the sending station is valid. The encryption of a particular string of text in this case acts as a digital signature. Figure 8-7 illustrates the concept of using public key encryption for authentication.

Figure 8-7. Public Key Encryption Enables Authentication

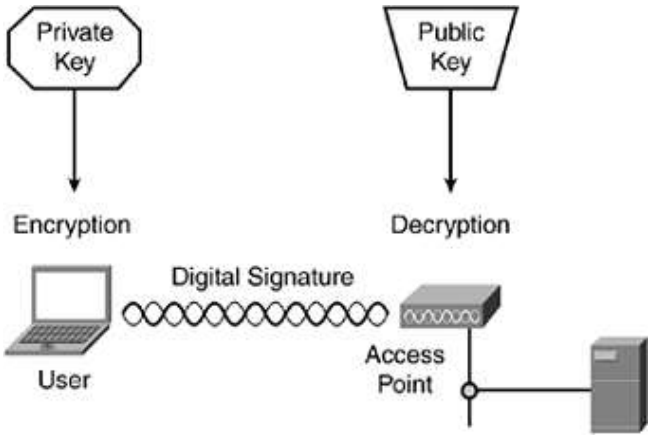


Exhibit 1010
Page 245 of 292

802.1x

The use of IEEE 802.1x offers an effective framework for automatically authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. 802.1x ties a protocol called Extensible Authentication Protocol (EAP) to both the wired and wireless network media and supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, and public key authentication.

802.1x Operation

Initial 802.1x communication begins with an unauthenticated supplicant (wireless client device) attempting to connect with an authenticator (wireless base station). The base station responds by enabling a port for passing only EAP packets from the client to an authentication server located on the wired side of the base station. The base station blocks all other traffic, such as HTTP, DHCP, and POP3 packets, until the base station can verify the client's identity using an authentication server, such as RADIUS. Once authenticated, the base station opens the client's port for other types of traffic based on access rights held by the authentication server.

To get a better idea of how the 802.1x process takes place, the following specific interactions occur among the various 802.1x elements:

1. The client sends an EAP start message. This begins a series of message exchanges to authenticate the client; think of this as a group of visitors entering the front gate of a theme park and the group's leader (client) asking the gatekeeper (base station) whether they can enter.
2. The base station replies with an EAP request identity message. In the case of the theme park, the gatekeeper will ask the leader for her name and driver's license.

Exhibit 1010
Page 246 of 292

3. The client sends an EAP response packet containing the identity to the authentication server. The leader in this example will provide her name and driver's license, and the gatekeeper forwards this information to the group tour manager (authentication server), who determines whether the group has entry rights.
4. The authentication server uses a specific authentication algorithm to verify the client's identity. This could be through the use of digital certificates or another EAP authentication type. In this example, this process simply involves verifying the validity of the leader's driver's license and ensuring that the picture on the license matches the leader. Assume the leader is authorized.
5. The authentication server will their send an accept or reject message to the base station. In this case, an accept means the group tour manager at the theme park tells the gatekeeper to let the group enter.
6. The base station sends an EAP success packet to the client. The gatekeeper informs the leader that the group can enter the park. The gatekeeper, of course, would not let the group in if the group tour manager had rejected the group's admittance.
7. If the authentication server accepts the client, the base station will transition the client's port to an authorized state and forward additional traffic. This is similar to the gatekeeper automatically opening the gate to let in only people belonging to the group cleared for entry.

The basic 802.1x protocol provides effective authentication regardless of whether you implement 802.11 WEP keys or no encryption at all. Most major wireless network vendors, however, are offering proprietary versions of dynamic key management using 802.1x as a delivery mechanism. If configured to implement dynamic key exchange, the 802.1x authentication server can return session keys to the base station along with the accept message.

The base station uses the session keys to build, sign, and encrypt an EAP key message that is sent to the client immediately after sending the success message. The client can then use contents of the key mes-

Exhibit 1010
Page 247 of 292

sage to define applicable encryption keys. In typical 802.1x implementations, the client can automatically change encryption keys frequently to minimize the risk of eavesdroppers having enough time to crack the key in current use.

Authentication Types

It's important to note that 802.1x doesn't provide the actual authentication mechanisms. When utilizing 802.1x, you need to choose an EAP type (such as EAP Transport Layer Security [EAP-TLS], EAP Tunneled Transport Layer Security [EAP-TTLS], or Cisco's Lightweight EAP [LEAP]), which defines how the authentication takes place. The software supporting the specific EAP type resides on the authentication server and within the operating system or application software on the client devices.

Exhibit 1010
Page 248 of 292

Security Policies

One of the first steps in providing wireless network security is to formulate effective policies and corresponding enforcement processes. Carefully analyze security requirements and invoke an adequate level of protection. For example, encryption should be part of all wireless network implementations. WEP might be fine for home and small office deployments, but utilize better methods— such as WPA—for corporate applications. An effective mutual authentication method, such as LEAP or EAP-TLS, is also important for corporate applications.

Assessment Steps

After deploying a wireless network, you need to implement a security assessment that ensures that the WLAN complies with security policies. For most situations, this is necessary whether the network implements effective security mechanisms. Don't put too much trust in the design of a system. It's best to run tests to be certain that the network is hardened enough to guard against unauthorized persons attacking company resources.

In fact, companies should conduct regular, periodic security reviews to ensure that changes to the wireless LAN don't make the system vulnerable to hackers. An annual review might suffice for low-risk networks; but a review each quarter or more often might be necessary if the network supports high-risk information, such as financial data, postal mail routing, and manufacturing control functions.

Review Existing Security Policies

Exhibit 1010
Page 249 of 292

Before getting too far with the security assessment, become familiar with company policies regarding wireless network security. This provides a benchmark for determining whether a company is complying with its own policies. In addition, you'll be able to assess and make corresponding recommendations for policy modifications. Determine whether the policy leaves any room for a disgruntled employee to access company resources.

For example, the policy should describe adequate encryption and authentication mechanisms, keeping in mind that 802.11 WEP is broken. Also, the policy should mandate that all employees coordinate with the company's IT department before purchasing or installing base stations. It's important that all base stations have configuration settings that comply with the policies and provide the proper level of security. In addition, you need to ensure that security policies are disseminated to employees in an effective manner.

Review the Existing System

Meet with IT personnel and read through related documentation to gain an understanding of the system's architecture and base stations configurations. You'll need to determine whether there are any design flaws that provide weaknesses that could allow a hacker inside the system.

Learn as much as possible about existing support tools and procedures to spot potential issues. Most companies, for example, configure the base stations over the wired Ethernet backbone. With this process, the passwords sent to open a connection with a particular base stations are sent unencrypted over the wired network. As a result, a hacker with monitoring equipment hooked to the Ethernet network can likely capture the passwords and reconfigure the base station.

Interview Users

Exhibit 1010
Page 250 of 292

Be sure to talk with a sample of employees to determine whether they are aware of the security policies within their control. For example, do the users know that they must coordinate the purchase and installation of wireless network components with the appropriate department? Even though the policy states this, don't count on everyone having knowledge of the policy. Someone might purchase a base station from a local office supply store and install it on the corporate network to provide wireless connectivity within the office. It's also a good idea to verify that people are using personal firewalls.

Verify Configurations of Wireless Devices

As part of the assessment, walk through the facilities with base stations and use tools to capture the base station configurations. If the company has centralized support software in place, you should be able to view the configuration settings from a single console attached to the wired side of the network. This is to determine which security mechanisms are actually in use and whether they comply with effective policies.

For example, the policies might state that base stations must disable the physical console port, but while testing you determine that most base stations have the ports enabled. This would indicate noncompliance with the policies, and it would enable a hacker to reset the base station to the factory default settings with no security enabled. In addition, look at the firmware version of each base station to see if it's up-to-date. Older firmware versions might not implement the more recent patches that fix encryption vulnerabilities.

Also, investigate base stations' physical installations. As you walk through the facilities, investigate the installation of base stations by noting their physical accessibility, antenna type and orientation, and radio wave propagation into portions of the facility that don't have physical security controls. The base stations should be mounted in a

Exhibit 1010
Page 251 of 292

position that would make it difficult for someone to physically handle the base station and go unnoticed.

A base station simply placed on top of a bookshelf, for example, would make it easy for a hacker to swap the base station with a rogue one that doesn't have any security enabled. Or, the hacker could attach a laptop to the console port to reset the base station. If the base stations are all mounted above the ceiling tiles and out of plain view, however, someone would need to use a ladder and would probably be noticed by an employee or security guard.

Identify Rogue Base Stations

A problem that's difficult to enforce and significantly undercuts a network's security is when an employee installs a personal base station in her office. Most of the time, these installations don't comply with security policies and result in an open, unsecure entry port to the corporate network. In fact, a hacker can utilize sniffing tools to alert him when such an opportunity exists.

As a result, scan for these unauthorized base stations as part of the assessment. Most companies will be surprised to learn how many they find. The most effective method for detecting rogue base stations is to walk through the facilities with sniffing tools. In addition, the company should periodically scan the network for potential rogue base stations from the wired side of the network. This is available in many of the centralized wireless network management systems.

Perform Penetration Tests

In addition to hunting for rogue base stations, try going a step further and attempt to access corporate resources using common tools available to hackers. For example, can you utilize AirSnort to crack through WEP? Is it possible to associate with a base station from outside the company's controlled perimeter? Of course your job will be easy if

Exhibit 1010
Page 252 of 292