WHITE PAPER

Symantec Enterprise Security

Securing Enterprise Wireless Networks

INSIDE

Contents

Executive summary

Similar to the way handheld devices running Palm OS and Pocket PC made their way into enterprises through the back door in the late 1990s, mobile and wireless technology is appearing in the enterprise environment. Workers upgrading their laptops to access a wireless network at home, in hotels, or at airports, will want the same mobility in the workplace. If the workplace does not provide wireless access, or a clear policy regarding the usage of wireless networks, workers might go as far as creating their own networks. This could unintentionally create serious security risks for the company. Network administrators need to address wireless networking needs before this happens.

In a recent survey of CTOs, the greatest barrier to deploying wireless technology is security.[1] Because administrators have had years of experience in securing wired networks, the security risks and measures to address them are well defined and understood. However, wireless networking is relatively new; the technology and its risks are not always understood. Without a clear understanding of the technology and how to securely deploy a wireless network, it is far too easy to create an entry point that allows intruders to bypass existing network security measures and gain access to confidential data.

This paper assists administrators in developing a strategy for deploying a secure wireless network. It explains the base 802.11 networking technologies and features, and newer standards that provided enhanced security for wireless networks. This is followed by a summary of the potential security risks involved in wireless networking, and describes the more common security attacks. Finally, the paper presents methods for securing a network, including wireless security standards, security best practices, and the enterprise-class security technologies available.

Wireless LAN technology

The word “wireless” is an umbrella term for a wide variety of completely different technologies, including handhelds, residential cordless phones, cellular/mobile phones, and wireless networks, including those using both infrared and radio frequencies. This white paper addresses only the wireless networking technologies defined by the IEEE 802.11 specifications, including 802.11b (Wi-Fi), 802.11a, and 802.11g. It does not cover Bluetooth, two-way paging, infrared (IrDA), or the many cellular communications standards.

802.11 WIRELESS LAN STANDARDS

In 1999, the IEEE published the 802.11b standard for a group of technologies governing wireless Ethernet connectivity. 802.11 wireless networks are essentially Ethernet networks without cables. Currently, a family of IEEE 802.11 standards is available in various stages of approval, from draft to ratified or approved. Approved standards include 802.11a and 802.11b. Several draft and proposed standards are also in the works, including 802.1x, 802.11g, 802.11i, and 802.11e.

The 802.11b standard was the first to be ratified and is the most frequently used version of the 802.11 standard today. It can, under ideal conditions, transmit and receive at a raw data rate of up to 11 Mbps, but typically operates at speeds of 1 to 5 Mbps. The 802.11a and 802.11g standards provide speeds up to 54 Mbps.

[1] Infoworld, “Enterprises find freedom without wires,” Oliver Rist, March 3, 2003, Issue 9, pp. 38-39.

The following table compares the three available 802.11 standards that provide for the transmission and reception of data through radio frequencies . Note that these are the maximum values for speed and range; the values achieved in practice are dependent upon the hardware used and the surrounding environment, including nearby structures.

Wireless Standard	**802.11a**	**802.11b**	**802.11g**
Technology	OFDM (Orthogonal Frequency Division Multiplexing)	DSSS (Direct Sequence Spread Spectrum)	Both DSSS and OFDM technologies
Max. Speed per Channel	54Mbps	11Mbps	22 – 54Mbps
Radio Frequency	5GHz	2.4GHz	2.4GHz
Range	24 meters (80 feet)	100 meters (328 feet)	100 meters (328 feet)
Channels	12 (8 in US)	14	14
IEEE Ratification Status	Ratified in early 2002	Ratified in 1999 Commonly referred to as "Wi-Fi"	Not yet ratified as of April 2003 (expected Summer 2003) Devices available today by early implementers using the draft standard

Beyond the transportation of the data, the IEEE 802.11 also includes standards to enhance the security and capabilities of a wireless network:[2]

- 802.11e boosts the Quality of Service (QoS) and multimedia capability of the other 802.11 standards while maintaining backward compatibility.
- 802.11i boosts security with improved key-distribution methods using 802.1x and advanced encryption technologies such as AES and TKIP.
- 802.1x provides a framework for stronger user authentication for 802.11 wireless LANs.

There are also standards that can potentially enhance the performance of 802.11:

- 802.16a extends the wireless range of 802.11 to several miles and lets signals bounce around obstacles and penetrate walls. It also provides enhanced security and adds high-quality phone calls.
- 802.20 extends the wireless range of 802.11 to several miles and promises high-speed links in cars and trains traveling at speeds exceeding 120 miles per hour.

COMPONENTS OF A WIRELESS LAN

The following four key components are required by every 802.11 wireless LAN:

- Client computer—Can be a laptop, handheld computer, or a desktop system.
- Communications medium—Consists of radio waves in the 2.4GHz or 5GHz radio frequency band. The frequency band is broken up into channels. The availability of specific channels depends on the local regulations of the country.
- Wireless Network Interface Card (NIC)—A radio that interfaces between the client computer and the communications medium, converting digital data to and from radio waves. These come in a variety of computer interfaces including PC cards, USB, and PCI cards.

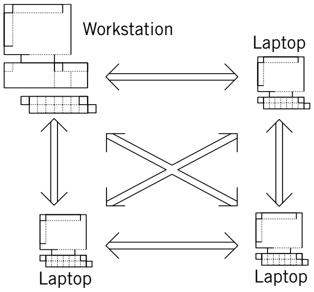
[2] eWeek, February 3, 2003, eweek.com, "Wireless LAN Lockdown," p.34.

- Access point—A hardware device that provides several channels that connect client computers to the wired LAN. Can be a simple bridge, connecting the wireless LAN to a wired LAN, or part of a router. Some wireless NICs can be configured to allow a client computer to act as an access point.

WIRELESS OPERATING MODES

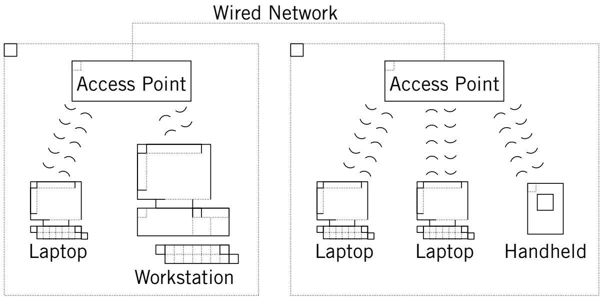
The IEEE 802.11 standard provides two distinct operating modes: Ad-Hoc and Infrastructure.

Ad-Hoc mode, shown in the following figure, allows two or more client computers to create a peer-to-peer network with each other's wireless NICs through a mesh network. This type of network is usually formed on a temporary basis.



Ad-Hoc configuration

Infrastructure mode, shown in the following figure, is the more common operating mode in which the wireless NICs in the client computers communicate with each other via an access point connected to a wired network. The access point is typically a standalone piece of hardware, however, the wireless NICs in some client computers can be configured to act as an access point as well.



Infrastructure configuration

NETWORK IDENTIFICATION – SSID

The Service Set Identifier (SSID) is an alphanumeric code configured on both the wireless NIC (or device) and the access point. Before a device can establish a connection to an access point, the device must provide a SSID. If the SSID matches the SSID of the access point, the connection is established. SSIDs are sometimes referred to as the network names as they provide a name that identifies one wireless network from another.

Benefits and risks of wireless

When first considering the deployment of a wireless network, one must understand both the benefits and risks involved. Not only does this help in making the decision to deploy or not, but an understanding of the risks allows one to implement precautions to mitigate them.

BENEFITS OF WIRELESS

For computer users, the most anticipated benefit is increased employee productivity. As with mobile devices, wireless technology also increases productivity for mobile employees, increases employee and partner collaboration, and increases customer satisfaction. The convenience of immediate communication for mobile users and the ability to stay connected anywhere and anytime are attractive benefits.

For wireless LAN administrators, the benefits include simplified implementation and maintenance as well as reduced Total Cost of Ownership (TCO) and operation. Wireless networks cut out expensive time and overhead to run wires and cables, allowing a more flexible and dynamic infrastructure. Connecting two LANs between buildings through a directional wireless relay can be more cost effective than running wires. The TCO is reduced by the low cost and high availability of wireless hardware and more rapid deployment.

RISKS OF WIRELESS

Unlike wired networks, there is no physical security with wireless networks. Wireless network devices, such as access points, are basically radios that broadcast signals, and these signals often “leak” from buildings to expose networks beyond their intended boundaries. Without proper security measures, anyone in the right location with the right equipment can access a wireless network and any of its resources, including client and server computers. It is crucial to use extra precautions when setting up a wireless network.

Even if the wireless network is completely isolated from the main internal network, eavesdroppers can still “sniff” the network transmission, and extract valuable data, compromising data confidentiality. Worse yet, it is possible for an attacker to modify the packets, compromising the integrity of vital data.

It only takes a single user to deploy a rogue and insecure access point allowing unauthorized access to the corporate networks. Even the most secure network implementations can be thwarted by a single unapproved access point purchased at a computer store for about $100 USD.

A vulnerable wireless network can be costly to a company. The exposure of internal data cannot only lead to a loss in revenue, but can be a legal liability. Any breach in the security of confidential data such as medical, financial, or personal records, leaves an organization wide open to costly lawsuits and fines, as well as a loss of business due to a lack of confidence with the company.

Wireless LAN security considerations

Before installing a wireless network, an administrator must be aware of the security risks involved. How, or even if, a wireless network is installed and configured depends upon how the enterprise decides to address the risks.

RADIO WAVE LEAKS

The greatest benefit of wireless networks is also the greatest security issue. Since radio signals are not limited by the physical boundaries of a building, they "leak" into public areas such as parking lots or roads, allowing unauthorized users access to the network and the data transmitted on it. While a typical antenna connected to a wireless NIC in a laptop might not be able to connect to a network beyond a few hundred feet, more sensitive and focused antennae might pick up the transmissions from more than a mile away.

INTERFERENCE

Radio signals are prone to interference. 802.11g and 802.11b wireless devices operate in the unregulated 2.4GHz frequency band that is crowded and noisy. Interference from a 2.4GHz cordless phone or wireless camera can overwhelm the wireless network causing poor performance or even a complete denial-of-service.

WEAK ENCRYPTION

Because unauthorized users can receive the transmitted data, the 802.11b standard included Wired Equivalent Privacy (WEP) to encrypt the transmitted packets. Unfortunately, the encryption is weak and can be broken after just a few hours of monitoring a high-traffic network.

POOR NETWORK ADDRESS MANAGEMENT

The network SSID must be provided by a user before a connection can be made to a wireless network. As a convenience to the users, access points are frequently configured to broadcast the SSID, advertising the name and availability of the network. Unfortunately, this also announces the availability of the network to unauthorized users.

Even if an SSID is not broadcast, it is a simple task for an attacker to monitor transmissions and retrieve the SSID, which is not encrypted and is transmitted in clear text.

LACK OF USER AUTHENTICATION

The base 802.11a, b, and g standards do not provide any user authentication. An access point can authenticate hardware based on the MAC or IP addresses, but it does not require user authentication.

UNAUTHORIZED HARDWARE INSTALLATION

Between the combination of low cost and ease of installation, it is very tempting for an employee to set up a private access point. While this adds conveniences for the employee—such as getting strong reception and having wireless access directly into the internal network—it bypasses all security measures, granting attackers a gateway into the network.

Attacks on wireless networks

Several types of attacks can be launched on wireless networks. This section briefly describes several of these vulnerabilities and attacks.

TRAFFIC INTERCEPTION

The simplest attack that can be made is for the attacker to monitor the network, and extract valuable data from the transmission, breaching data confidentiality. Once an attacker is able to retrieve the data, he has a foothold with which to launch more invasive attacks.

ONE-WAY AUTHENTICATION

When a client connects to an access point, the access point is responsible for authenticating the client and authorizing the connection. However, the connecting client does not authenticate the access point. Once an attacker knows the SSID for an access point, the attacker can set up an access point with the same SSID and a stronger signal, overshadowing the real access point. Clients will not see the real access point, and instead, will connect to the rogue access point. Once an attacker has overshadowed an access point, clients are susceptible to a man-in-the-middle attack.

MAN-IN-THE-MIDDLE ATTACK

The man-in-the-middle attack is so called because the attacking computer intercepts packets sent by a client computer and retransmits them to the access point. Responses from the access point to the attacker are also retransmitted to the client computer. To the client, the attacker appears to be the access point and, to the access point, the attacker appears to be the client.

SHARED KEY AUTHENTICATION ATTACK

To encrypt data, the client and access point will often share the same key. By observing the plain text challenge and the cipher text response, an attacker can easily reproduce the shared key. This key can then be used to properly encrypt packets to disguise them as being valid. Broadcast ping packets can then be sent to flood the client and access point.

SESSION HIJACKING

With session hijacking, an attacker takes over an existing client/access point connection. When an attacker is able to identify an existing session, the attacker emulates the access point and sends the client a “dissociation” message (dropping the client from the connection). The attacker can spoof the client’s MAC address to emulate the client and continue the connection with the access point.

DENIAL-OF-SERVICE

An attacker might initiate a Denial-of-Service (DoS) attack in which clients are prevented from using the wireless network. One type of a DoS attack is a forged frames attack where the attacker emulates the access point and continuously sends de-authentication and disassociation messages. The clients disconnect from the access point and are unable to re-establish a connection.

An attacker can also prevent users from utilizing the wireless network by jamming the radio signals. By generating enough radio noise in the frequency range used, the attacker blocks the access point and clients from communicating.

Wireless security features

While 802.11 can be thought of as an Ethernet network without wires, in reality it has a more robust feature set than Ethernet that provides wireless connectivity, encryption, authentication, and operating modes.

WIRED EQUIVALENT PRIVACY (WEP)

Wired Equivalent Privacy (WEP) is the standard 802.11 wireless security protocol for data encryption designed to provide wired-like protection. It uses a key to encrypt wireless data transmitted through the radio waves.

When first introduced, WEP included 40-bit keys, but after attackers had broken the encryption, vendors introduced 128-bit WEP. Because 128-bit WEP was not part of the 802.11b specification, it introduced incompatibilities with older wireless NICs that only supported 40-bit WEP. Also, 128-bit WEP was not as strong as anticipated, and soon after its introduction, attackers were able to break its encryption as well.

WEP is marketed as having 128-bit keys, but this is deceptive. 128-bit WEP includes a 24-bit Initialization Vector (IV), leaving only a 104-bit key. While stronger than a 40-bit key, 128-bit WEP is significantly weaker than its name implies.

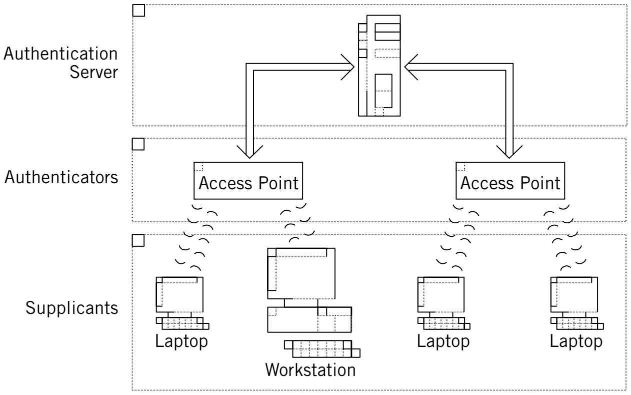
Since every wireless device must be configured with the WEP key, managing and distributing the key can become difficult beyond a small number of devices. A key's lifetime in an enterprise can get very short based on revocation and expiry policies. Every time a key is updated, the new key must be distributed to all users and access points. Also, there is nothing, other than company policy, to prevent a user from redistributing the key to an unauthorized user.

USER AUTHENTICATION – IEEE 802.1X

WEP provides data encryption, but it does not provide user authentication. IEEE 802.1x is a ratified standard that can be used in conjunction with WEP to provide a strong user authentication framework and a centralized security management model.

IEEE 802.1x consists of three components:

- A supplicant—A client machine trying to access the wireless network.
- An authenticator—A Layer 2 device that provides the physical port to the network (such as an access point or a switch).
- An authentication server—Verifies user credentials and provides key management. This can be a Remote Authentication Dial-In User Service (RADIUS) server, an LDAP directory, a Windows NT Domain, or an Active Directory.



IEEE 802.1x components

Extensible Authentication Protocol (EAP) is the upper-layer authentication protocol used by 802.1x components to allow users to authenticate to a central server. Once the server authenticates the client, keys are sent to both the authenticator (the access point) and the supplicant (the client).

Cisco Lightweight EAP (LEAP), also known as Cisco Wireless EAP, is an implementation of EAP using a RADIUS server for authentication. Since standards are still being defined for the use of EAP, many companies use Cisco's proprietary implementation as they await an open and ratified standard.

WI-FI PROTECTED ACCESS (WPA)

Wi-Fi Protected Access (WPA) is a new security standard intended to address the known deficiencies in the WEP algorithms while maintaining backward compatibility with legacy 802.11 hardware. WPA combines the 802.1x authentication with a stronger encryption element from the 802.11i draft called Temporal Key Integrity Protocol (TKIP).

TKIP works like a "wrapper" around WEP, adding multiple enhancements to the WEP cipher engine. TKIP extends the initialization vector (IV), used to encrypt the packet, from 24 bits in WEP to 48 bits to increase the number of possible shared keys, providing protection against replay attacks. In addition, TKIP uses better sequencing rules than WEP to ensure that the IV cannot be reused, even if intruders get hold of it.

To protect against forgery attacks, TKIP also includes a Message Integrity Code (MIC), a 30-bit cryptographic checksum. The checksum of a received packet is compared against the MIC and if they do not match, the packet is ignored.

Although WPA brings a welcome boost to wireless network security, many view it as a temporary fix because future 802.11 equipment will likely use the Counter Mode with CBC-MAC Protocol (CCMP) which is also a part of the 802.11i draft. CCMP uses Advanced Encryption Standard (AES) to provide even stronger encryption. However, AES is not designed for backward compatibility.

MANAGED ACCESS BY MAC AND IP ADDRESSES

Every wireless 802.11 NIC has a unique Media Access Control (MAC) address hard coded into it. An access point can contain a list of authorized MAC addresses, and only allow NICs with a MAC address in the list to connect. This provides a simple level of security, filtering out connections attempted by devices with unauthorized MAC addresses.

Similarly, some access points also provide the ability to filter connections based upon the IP addresses assigned to the connecting devices. In this situation, the devices attempting to make a connection cannot receive their IP addresses dynamically from a DHCP server and instead must use a static, or manually assigned, IP address.

Securing wireless networks

With all of the possible attacks that can occur, the idea of securing a wireless network can be intimidating. While it is impossible to guarantee a 100% secure wireless LAN, creating a smart company-wide strategy can mitigate most of the risks. This involves following basic wireless security practices using enterprise-class and client protection technologies.

ESTABLISHING AN ENTERPRISE-WIDE STRATEGY

The first step in creating a secure wireless network is to establish an enterprise-wide strategy for wireless network deployment and usage. When developing a strategy, the following areas should be addressed:

- Determine business needs

  Adopt a wireless network plan only after researching the business drivers and needs of the enterprise. Identify clear and achievable objectives, and determine that the benefits outweigh the risks.

- Integrate wireless policies into existing IT policies

  Policies should define corporate standards for devices, infrastructure, and operating systems. Update wireless security policies often by reviewing them and adapting them to new technologies and threats.

- Clearly define wireless network ownership

  This ensures control as well as response when new threats are identified. Many enterprises provide policies for wireless from the IT group with a well-defined architecture and strict safeguards recommended by the security team.

- Protect the existing infrastructure

  Do not place wireless devices directly on the internal network. Instead, provide a separate wireless network with highly controlled gateways to the main network.

- Educate users in wireless policies

  People continue to be a network’s weakest link. Educate your employees and partners about wireless security and how to configure their devices to securely access the network.

WIRELESS NETWORK SECURITY BEST PRACTICES

There are simple steps to securing a wireless network, but many people do not follow them. Administrators erroneously assume that whatever they buy already comes secured. Using the following procedures while setting up the wireless network will allow you to create a secure network.

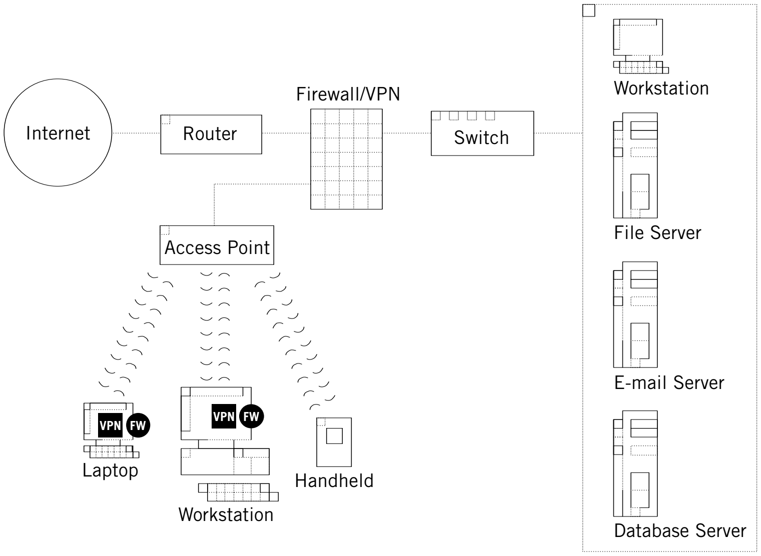
Planning and design

Before installing the wireless hardware, create an implementation plan for the wireless network, at a policy level as well as a physical implementation level.

Evaluate the existing networking policies and amend them for wireless networking. While new wireless-specific policies must be created to ensure overall network security, most of the existing policies should overlay onto the wireless network. Keep one set of policies to simplify security for the administrators and the clients.

Do not install access points on the same network as your other network resources. Install access points on a separate network on the outside of your corporate firewall. This keeps your resources protected from any attackers that have compromised an access point. The following figure illustrates a sample network with the wireless access point isolated from the main company network.

The physical location of the access points must also be taken into consideration. Minimize the number of access points since each one is a potential entry point for an intruder. Install access points away from exterior walls. This provides better coverage inside your offices and reduces the strength of any signals that can be picked up outside.



Recommended wireless network configuration

Hardware selection

The purchase of wireless hardware should be part of the security plan. Do not purchase devices that only support 40-bit WEP. The devices should also have upgradeable firmware to allow hardware upgrades as new security enhancements become available.

To provide the highest degree of compatibility, hardware should come from the same vendor. While the IEEE standard should provide compatibility between devices from different manufacturers, interpretations of the standards and proprietary extensions sometimes prevent full integration between devices of different manufacturers.

Standardizing equipment also simplifies administration. If all of the hardware comes from a single vendor, then all of the hardware can use the same administration software and procedures. There is also only one set of updates that needs to be tracked, and when updates do become available, all of the devices can be upgraded to the same version at the same time.

SSID management

When attempting to make an unauthorized connection to a network, an attacker looks for the SSID. Take steps to protect the SSID from unauthorized users.

A new wireless access point comes with a default SSID. This should be immediately changed. Do not change the SSID to reflect your company's main names, divisions, products or street address. Do not rename SSIDs with provocative names such as “Hackproof” since they only invite trouble. Periodically change the SSID so that any SSIDs gained by unauthorized users become invalid.

If your access point supports it, disable "broadcast SSID." Users will need to manually enter the SSID on their computer to connect, but it helps hide the network from unauthorized users. There are ways to passively monitor the traffic to determine an SSID, but this provides a deterrent.

Change the access point’s default user name and password

When installing a wireless access point or router, immediately change the default username and administrator password. Since wireless access points and routers usually have a Web administration menu, all an attacker must do to gain control of your network is type your router’s IP into a browser. Make your password a non-dictionary word, more than 8 characters, alphanumeric and non-alphanumeric symbols, and do not match it to your SSID.

Scan for rogue access points

Because wireless NICs can be configured to act as an access point, it only takes a user a few mouse clicks to turn a client computer into a rogue access point. Use wireless scanning tools to identify unauthorized access points. After you identify such an access point, walk the area watching the signal strength. As you get closer, the signal will get stronger.

Be aware that scanning alone does not stop rogue access points from appearing; it only identifies ones that are currently active. A combination of educating users about wireless policies and random scanning will help deter rogue access points.

Enable 128-bit (or greater) WEP

WEP encryption should always be enabled. While WEP can be easily cracked, it is more difficult to access a WEP-protected network than an unprotected one. It is not worth the time and effort of cracking a network with WEP enabled when there are so many other wireless networks not using it.

Whenever possible, use at least 128-bit WEP. Some newer access point devices have WEP keys larger than 128-bit but might not be compatible with older wireless NICs.

Enable VPN access

Provide VPN service to allow authorized clients to connect to the main network. This creates connections between authenticated clients and the internal network gateway using a stronger encryption than that which is used between the client and the access point. This makes it more difficult for attackers to decipher the data. Be mindful of “piggyback” connections where an attacker compromises the client computer, then accesses the corporate network through the VPN connection.

Implement user authentication when practical

Require access point users to authenticate. Upgrade the access points to utilize implementations of the WPA and 802.11i standards when they become available. Certification of the new security enhancements in the 802.11i standard is just starting, and products supporting WPA will make their way to market this year (2003).[3]

Leverage existing RADIUS servers

As you implement user authentication on the access points, re-use any existing servers providing authentication for your other network services. This reduces the maintenance overhead and prevents former employees from using old user accounts to access the network.

Restrict access point connections

When you have a known set of wireless clients, you can configure the access point to restrict connections to specific MAC and/or IP addresses.

Most access points allow you to filter access to your wireless network by MAC address. You can add the specific MAC addresses for which you want to grant access. Computers with invalid MAC addresses will be refused connections. It is possible for attackers to spoof a MAC address, but MAC address filtering will provide a deterrent to most attackers.

Some access points will allow you to filter access to your wireless network by IP address. You can add specific static IP addresses for which you want to grant access. If the access point does not support this feature, be sure to configure the firewall behind the access point to place very tight restrictions on which IP addresses are allowed access to the internal network. Like MAC addresses, it is possible for attackers to spoof an IP address, but using IP address filtering provides an additional deterrent to most attackers.

If you do filter by IP addresses, you must disable DHCP services for your wireless clients. Though convenient, IP address filtering cannot be used affectively if DHCP services are automatically assigning IP addresses to client computers.

"War Drive" the parking lot looking for leaks

After you have set up the wireless network and implemented the security measures, you should take on the role of an attacker and examine your network from the outside, looking for potential weaknesses. A simple search of the Internet for "war driving" will provide you with a list of sites providing the latest war driving methods and tools.

Avoid 2.4 GHz cordless phones or X10 wireless video

The 2.4Ghz frequency range is used for a variety of wireless devices including cordless phones and wireless video. These can interfere with a wireless network by overpowering one or more channels. Avoid or minimize the use of such devices around access points. If this is not possible, you might want to consider using the 802.11a devices which work within the 5 GHz spectrum.

[3] eWeek, "Standards Will Fill Holes in WEP Authenticaion and Encryption," Francis Chu, February 3, 2003,
http://www.eweek.com/article2/0.3959.857267.00.asp.

Secure the client computers

Every client computer utilizing a wireless network is more vulnerable to an attacker than when connected to an internal network behind a firewall. Once an attacker has access to the wireless network, he potentially has access to all of the computers on the wireless network. Worse yet, if an exposed client computer is using VPN to access the internal network, an attacker could piggyback off that same VPN connection and gain access to the internal network as well.

Protect the client computers the same way you protect your internal network. Install client firewall software to prevent attackers from infiltrating the computers and using them to piggy-back their connections to the internal network or initiate attack attacks on other client computers on the network. Use virus protection software to prevent security-breaching viruses from infecting the computers.

ENTERPRISE-CLASS SECURITY TECHNOLOGIES FOR WIRELESS NETWORKS

Similar to the wired network, use enterprise-class security solutions to secure wireless networks at the gateways, servers, and clients. More and more security products are being enhanced to address 802.11 wireless-specific vulnerabilities and threats. In addition to commercial security software, many free wireless hacker tools are available on the Internet.

Firewalls

For best security, employ a Layer 7, full-application inspection firewall on the demilitarized zone (DMZ) and deploy client firewalls on each desktop. Firewalls, such as the Symantec Gateway Security and Symantec VelociRaptor appliances, or the Symantec Enterprise Firewall with VPN, should either be integrated into or connected behind the wireless access points to catch upstream attacks. Both incoming and outgoing traffic should be monitored.

Because wireless networking clients are more accessible by outside users, the network perimeter has been pushed to the desktops. Clients must enable firewalls to protect their individual systems from unauthorized use. Enterprise-aware products, such as the Symantec Client Security and Symantec Enterprise VPN Client, provide firewall technology for each desktop and are centrally managed and administered.

VPN

VPN services should be used to encrypt all traffic to and from the wireless devices. This is one of the most often used mechanisms to secure wireless network traffic once the connection is authenticated. Most firewalls include VPN technology.

IDS

Intrusion detection systems (IDS), such as network-based Symantec ManHunt and host-based Symantec Host Intrusion Detection, should be used to detect and stop attacks on servers. Both Symantec Gateway Security appliance and Symantec Client Security include integrated IDS that can communicate with the integrated firewall in response to an attack.

Antivirus software

Viruses can travel through a wireless network as easily as a wired network. Antivirus software should be used at the gateways, servers, and desktops. Antivirus software should be configured to automatically scan at regular intervals and update signatures.

Vulnerability assessment

Wireless networks should be scanned regularly for known vulnerabilities. Vulnerability assessments locate security weaknesses before an attacker does, allowing security administrators to prioritize and correct each deficiency. Assessment tools will identify many wireless vulnerabilities and recommend mitigation strategies. Since access points do not run on a server, network-based scanners are required.

Policy compliance

Required and forbidden services, as well as password strength checks and updated patches, are common to both wired and wireless networks. Policy compliance tools help measure an enterprise for compliance to industry-wide standards and regulations, such as ISO 17799 and HIPAA.

Conclusion

Wireless networking is the fastest growing computer technology since the Internet. The benefits of being able to connect to the network anywhere in an office, without having to plug in a cable are strong, but the security risks involved in creating a wireless network are just as great. Once set up, it is just a matter of time before unauthorized users locate and attempt to compromise the availability, integrity, and confidentiality of your enterprise network.

You can build a wireless network that keeps attackers out. Creating a secure network starts long before the installation of the first access point with the creation of a strategy. Design security into your network; install firewalls to keep the wireless network isolated from the internal network. Use the wireless security standards, such as WEP, even if they are less than perfect.

As you implement wireless network security, do not forget about the clients. Be sure to create a clear wireless networking policy and take the time to communicate it to the users. Also, since wireless clients are potentially exposed to the outside, protection, such as client firewalls, must also be installed on the client computers to prevent them from becoming back doors into your corporate network.

Creating secure wireless networks is a complex and ongoing task. Attackers will constantly attempt to breach the security in a variety of ways. However, with a well-designed network, you can provide your users with the benefits of mobile computing, yet maintain a secure network that protects the enterprise assets.

Glossary

802.1x: The IEEE standard to enhance the security of IEEE 802.11 wireless networks by providing an authentication framework.

802.11: The IEEE standard that specifies wireless connectivity between fixed, portable and moving stations within a local area at data rates of 1 and 2Mbps.

802.11a: The IEEE standard for data rates up to 54Mbps in the 5GHz frequency band.

802.11b: The IEEE extension to the initial 802.11 standard for data rates up to 11Mbps in the 2.4GHz frequency band.

802.11g: The IEEE extension to the initial 802.11 standard for data rates up to 54Mbps in the 2.4GHz frequency band.

Access Point: An interface between the wireless network and a wired network.

Bandwidth: The measurement that specifies the amount of the frequency spectrum that is usable for data transfer. It identifies the maximum data rate that a signal can attain on the medium without encountering significant loss of power.

Bluetooth: A standard published by the Bluetooth Special Interest Group (SIG) for 1Mbps data rates in the 2.4GHz frequency band at relatively short ranges. It is not considered a wireless network, but is a wireless Personal Area Network (PAN).

De-Militarized Zone (DMZ): A computer host or small network inserted as a ‘neutral zone’ between a private network and the outside public network.

Dynamic Host Control Protocol (DHCP): A DHCP server issues IP addresses automatically within a specified range to devices such as PCs when they are first powered on. The device retains the use of the IP address for a specific license period that the system administrator can define.

Extensible Authentication Protocol (EAP): A protocol for message exchange during an authentication process.

Health Insurance Portability and Accountability Act (HIPAA): A set of US national standards to protect the privacy of personal health and medical records that are either transmitted or maintained electronically, and the paper printouts created from these records.

Institute of Electrical and Electronic Engineers (IEEE): A US-based standards organization participating in the development of standards for data transmission systems.

ISO 17799: The International Organization for Standardization’s information technology code of practice for information security management.

Local Area Network (LAN): A collection of computer devices located in a single building, or in multiple buildings on a single site, which are connected to one another so that users can share information, programs, printers and other computing resources and services.

Network Interface Card (NIC): A computer circuit board or card that is installed in a computer so that it can be connected to a network.

Network Sniffer: A tool for monitoring network traffic.

Personal Area Network (PAN): A very low powered wireless network typically used by portable or wearable computer devices to communicate with other nearby computers and exchange information.

Service Set Identifier (SSID): A configurable identification that allows wireless clients to communicate with the appropriate Access Point.

Spread spectrum: A modulation technique that spreads a signal's power over a wide band of frequencies. Using this technique the signal is much less susceptible to interference from other radio sources.

Virtual Private Network (VPN): A private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.

Wireless Fidelity (Wi-Fi): A standard for interoperability sponsored by the Wireless Ethernet Compatibility Alliance (WECA). 'Wi-Fi' is a brand that signifies IEEE 802.11 interoperability with other Wi-Fi certified products.

Wired Equivalent Privacy (WEP): An optional IEEE 802.11 function that offers transmission privacy similar to that of a wired network. WEP encrypts transmitted data to avoid disclosure to eavesdroppers.

Wireless Network Interface Card: A Network Interface Card (NIC) that is installed in a computer so that it can be wirelessly connected to a network.

SYMANTEC, THE WORLD LEADER IN INTERNET SECURITY TECHNOLOGY, PROVIDES A BROAD RANGE OF CONTENT AND NETWORK SECURITY SOLUTIONS TO INDIVIDUALS AND ENTERPRISES. THE COMPANY IS A LEADING PROVIDER OF VIRUS PROTECTION, FIREWALL AND VIRTUAL PRIVATE NETWORK, VULNERABILITY MANAGEMENT, INTRUSION DETECTION, INTERNET CONTENT AND EMAIL FILTERING, REMOTE MANAGEMENT TECHNOLOGIES, AND SECURITY SERVICES TO ENTERPRISES AROUND THE WORLD. SYMANTEC'S NORTON BRAND OF CONSUMER SECURITY PRODUCTS LEADS THE MARKET IN WORLDWIDE RETAIL SALES AND INDUSTRY AWARDS. HEADQUARTERED IN CUPERTINO, CALIF., SYMANTEC HAS WORLDWIDE OPERATIONS IN 38 COUNTRIES.

FOR MORE INFORMATION, PLEASE VISIT WWW.SYMANTEC.COM.

WORLD HEADQUARTERS

20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
1.408.253.9600
1.800.441.7234

www.symantec.com

For Product Information
In the U.S., call toll-free
800-745-6054.

Symantec has worldwide
operations in 38 countries.
For specific country
offices and contact numbers
please visit our Web site.