

802.11 WLAN Security

Introduction

802.11 wireless LANs continue to gain market momentum. Higher speeds, larger bandwidth and improved quality of service are helping businesses realize the potential business benefits that wireless networking delivers. Now, with this growing adoption of 802.11 wireless LANs, security has become a focal point regarding the decision to deploy a wireless LAN.

While wireless networking has several advantages over a traditional wired LAN, it introduces security risks that a wired LAN is not susceptible to. Without a robust wireless security solution, organizations leave themselves vulnerable to attack through their WLAN. Although malicious attacks are a non-controllable reality, companies can take action to integrate a solid wireless security solution that prevents unauthorized users from accessing confidential company information.

Authentication and data encryption are the key components of wireless LAN security to help prevent unauthorized users from accessing the network and compromising confidential information. Standard 802.11 security has two major issues: 1) authentication of wireless clients is missing, so unauthorized users may be able to access network resources, and 2) weak encryption results in minimal effort for attackers to decipher data transmissions.

Security Threats and Types of Attacks

Before examining the security solutions available today, it is important to define some of the security risks faced by WLANs. All LANs, wired or wireless, are vulnerable to two types of attack: 1) active attacks; hackers gain access to the LAN to destroy or alter data and, 2) passive attacks; hackers gain access to the LAN, but can only eavesdrop to transmitted data. Wireless LANs are more susceptible to both types of attacks because hackers do not require a physical connection to the premises.

Active Attacks: A direct attack by intruders, with specific intent to disrupt network operations or access data. These are profiled below:

Spoofing: One of the most basic types of active attacks whereby the intruder configures their wireless terminal to appear to have the same MAC address as an authorized access point or wireless terminal. When spoofing an access point, the intruder's terminal appears as the authorized access point, with the intent to associate with an authorized wireless terminal and access the data on that device. When spoofing a wireless terminal, the intruder's terminal appears as the authorized terminal, with the intent to gain unauthorized access to the wireless network.

Denial of Service (DoS): A denial of service attack disrupts a network by flooding the bandwidth with meaningless data to bring the network to a halt. To initiate a DoS attack, the intruder discovers an access point on the wireless network and then sends it a continuous stream of meaningless information. The data stream overwhelms the access point, causing it to become unusable. DoS attacks may be as sophisticated as spoofing

802.11 disassociation management frames to the wireless terminals, or as simple as using an RF generator in the 2.4 GHz band to jam the RF channel.

Replay Attacks: The intruder monitors and captures transmitted packets between a wireless terminal and access point. This is achieved via a passive monitoring utility called a ‘sniffer’; such as Air Snort, which is readily available on the Internet as freeware. Once the packet is captured, the hacker can do one of two things:

- Initiate a DoS attack by repeatedly transmitting through the access point. Because the packet contains valid data, the access point forwards it to the host server to process and respond with a data receipt message. The host server overloads if the packet is transmitted with enough frequency.
- Accelerate the data flow on the network to reduce the time required to collect enough data to crack a WEP encryption key.

Passive Attacks: One of two types; 1) collect data in transit, without the interruption of communication between authorized devices, or 2) penetrate a wireless network through a security hole. 802.11 wireless technology is inherently open to data interception by any 802.11 radio. Consequently, a passive attack does not require sophisticated methods or tools in order to eavesdrop and collect data.

War-driving: The most common form of passive attack. The RF signal of 802.11 networks may extend beyond the confines of a building. With a wireless laptop or terminal, a hacker simply drives through business districts passively listening for a strong RF signal. Without good security, little effort is then required to penetrate the network.

Man-in-the-Middle: An attack that requires sophisticated software and can cause significant disruption or data loss. The hacker inserts themselves between an access point and a wireless terminal to capture packets in transmission. The wireless terminal sees the hacker as an authorized access point, while the access point sees the hacker as an authorized wireless terminal. Both authorized devices fail to detect the intruder and continue transmitting information. The intruder captures legitimate information and is also able to inject false data into the network, or initiate a DoS attack.

Attacks by unauthorized users are not the only threats to WLAN’s. Many 802.11 networks are installed without proper measures to secure configuration and management functions. Also, companies may not enforce security policies or provide education to help employees understand the wireless network and its security implications. For example, in an effort to minimize the time to get a WLAN up and running, some wireless equipment vendors offer their devices with certain features turned off; including security mechanisms. This can cause undue exposure to an attack. It is important to understand and properly manage WLAN equipment in order to minimize the risk of an attack.

An example of an internally caused network risk could be an employee that introduces an unauthorized ‘rogue’ access point into the company network. Today’s plug-and-play wireless equipment requires minimal configuration, and the individual can quickly have their own wireless network up and running. Without proper security mechanisms, the individual has unintentionally created a security hole. If the RF signal is sufficiently strong, a ‘war-driver’ could pick up the signal and gain access to the company network.

Vulnerabilities of standard 802.11 security

Today's tools and knowledge enable hackers to easily compromise first generation 802.11 security. In 2000, researchers from the University of California Berkley published a paper detailing WEP vulnerabilities, including ways to compromise it. Vulnerabilities include weak encryption (keys no longer than 40 bits), static encryption keys, and a lack of a key distribution method. Various academic and commercial studies show that persistent hackers can quickly breach WLAN security even with WEP enabled. WEP is only effective against casual snoopers, and the Wi-Fi Alliance warns against WEP as a standalone security solution by stating:

“It is important to emphasize that WEP was never intended to be a complete end-to-end security solution. It protects the wireless link between the client machines and access points. Whenever the value of the data justifies such concern, both wired and wireless... should be supplemented with additional higher-level security mechanisms such as access control, end-to-end encryption, password protection, authentication, virtual private networks, or firewalls.”

Another modest security technology is SSID (Service Set Identifier) that acts as a network name or password for the WLAN. In an open system architecture, the access point transmits its SSID in clear-text, allowing any correctly configured wireless client to connect to any access point. In an effort to increase security, many wireless equipment vendors use a closed system architecture where the access point does not transmit its SSID - only clients configured with the same SSID as the access point are granted access. However, this provides minimal defense against a malicious attack as the SSID is broadcast in clear-text in and can be intercepted by an intelligent hacker with the right tools.

The greatest risk attack comes when no security measures are implemented. Although WEP vulnerabilities have been documented, it still requires effort to compromise and should be enabled whenever possible.

Security solutions for today's 802.11 WLAN

To combat standard 802.11 security weaknesses, organizations such as the IEEE, Cisco Systems and Fortress Technologies have introduced enhanced security solutions developed around standards based technologies. The IEEE's 802.1X Port Based Network Access Control standard provides strong authentication and network access control for 802.11 networks. Cisco developed the Lightweight Extensible Authentication Protocol (LEAP); built on the principles of the Extensible Authentication Protocol (EAP). Fortress Technologies' AirFortress FIPS 140-1 certified security solution is built on the National Institute of Standards and Technology (NIST) cryptographic standards and provides strong data encryption for 802.11 networks. Information on each of the technologies can be found below:

IEEE 802.1X Port Based Network Access Control

802.1X is a standard that provides a means to authenticate and authorize devices for network access; a security mechanism absent from 802.11. 802.1X provides a port-based network access control solution for networking technologies such as Ethernet, 802.11, Token Ring and FDDI.

802.1X has three components that combine to deliver authentication: the Supplicant, Authenticator and Authentication Server (AS). The wireless terminal is the supplicant and the access point is the authenticator. The most common type of AS is RADIUS (Remote Authentication Dial-In User Service) - typically a stand-alone software package installed on a standard PC platform. Authentication requests occur during system initialization and are

initiated by wireless terminals or access points, after the terminal has associated to the access point. Various authentication methods such as digital certificates, smart cards and one-time passwords can be used to provide credential information for authentication. Of course, without successful authentication, network access is denied.

The 802.1X authentication process uses the Extensible Authentication Protocol (EAP) to pass authentication information between the supplicant and the AS. EAP effectively creates a session with the AS for the terminal to forward its credentials. If the EAP version supports mutual authentication, then the AS provides its credentials to the wireless terminal within the same session. The EAP session allows a wireless terminal limited access to the network for terminal authentication purposes only. Once authentication is complete, the session is terminated and the wireless terminal is granted access.

EAP is a general protocol and is ‘extensible’ in that it supports multiple authentication mechanisms. 802.1X supports such EAP types as Message Digest 5 (MD-5), Transport Layer Security (TLS), Tunneled Transport Layer Security (TTLS) and Protected Extensible Authentication Protocol (PEAP).

The authentication dialog between the terminal and authentication server is carried in EAP frames. The encapsulated form of EAP, known as EAP over LAN, or EAPOL, is used for all communication between the supplicant and authenticator.

The access point acts as an EAP proxy between the terminal and AS, accepting EAPOL packets from the terminal and forwarding them to the AS over a protocol such as RADIUS. In turn, the access point forwards all AS EAP packets over EAPOL to the wireless terminal.

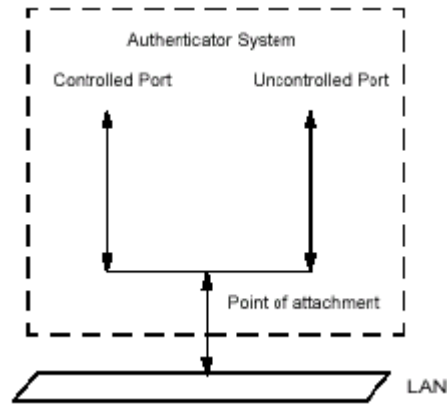
Figure 1. illustrates the IEEE 802.1X setup. The supplicant sends its authentication credentials to the AS via the authenticator. The AS confirms the supplicant’s credentials and directs the authenticator to allow supplicant access to the network. The access point communicates with the wireless terminal and submits the terminal credential information to a suitable AS to determine correct authorization.

Figure 1. The IEEE 802.1x Setup



Figure 2. illustrates how 802.1X port-based access control has the effect of creating two distinct points of access to the authenticator system’s point of attachment to the LAN. The two distinct points of access are referred to as the “controlled” port and “uncontrolled” port.

Figure 2. Controlled and Uncontrolled ports



Uncontrolled ports and controlled ports are considered part of the same point of attachment to the LAN. In 802.11, the LAN point of attachment is the *association* between the wireless terminal and the access point.

The controlled port only accepts packets from authenticated clients - the MAC address is on the list of authenticated MAC addresses. The access point uses the uncontrolled port to exchange EAP protocol information between the wireless terminal and the AS. Protocol exchanges between the access point and the authentication server can be conducted via one or more of the access point's controlled or uncontrolled ports.

EAP/MD5: Simple, one-way handshake in which the AS authenticates the client. Credentials are based on mutual knowledge of a shared secret such as username and password. MD5 requires little memory and is simple to implement and manage; making it ideal for wireless terminals with limited memory and processing power.

EAP/TLS: Two-way (mutual) authentication in which the AS authenticates the client, and in turn, the client authenticates the server. This mutual authentication secures against man-in-the-middle-attacks. TLS uses digital certificates to provide credential information and secures against dictionary attacks.

EAP/TTLS: Two-way (mutual) authentication of the client and AS based on TLS. TTLS only requires server-side certificates, eliminating the need to install and configure certificates for each wireless client. User authentication occurs via a security database already in use on the corporate LAN, such as Windows domain controllers, SQL, or LDAP. TTLS securely forwards client authentication information after a TLS tunnel is established.

EAP/PEAP: Similar in functionality to TTLS in that, it too specifies mutual authentication, uses TLS to establish a secure tunnel between the wireless client and authentication server, and only requires server-side certificates. The difference is that you would deploy an authentication method defined by EAP on the wireless client.

WEP is used in conjunction with 802.1X to protect packets from eavesdroppers. 802.1X EAP types such as TLS, TTLS and PEAP introduce strong improvements to how WEP keys are generated, managed and distributed by enabling 'per user/per session WEP keying'.

Per user/per session keying: Once mutual authentication is successfully complete, the client and authentication server each derive the same high-level encryption key, known as

a session key. Using a secure channel on the wired LAN, the authentication server sends the session key to the access point, which the access point stores. The access point generates a set of WEP keys that it transmits to the wireless terminal as multiple EAP protocol messages, which are protected by encrypting the messages with the session key. The terminal uses its derived session key to decrypt the EAP protocol messages to get at the WEP keys that are used for encrypting subsequent data transmissions. The result is per-user, per-session WEP keys. The length of a session is defined on the authentication server. When a session expires or the client roams from one access point to another, re-authentication occurs and a new session key is generated, which in turn generates new WEP keys. The re-authentication is transparent to the user.

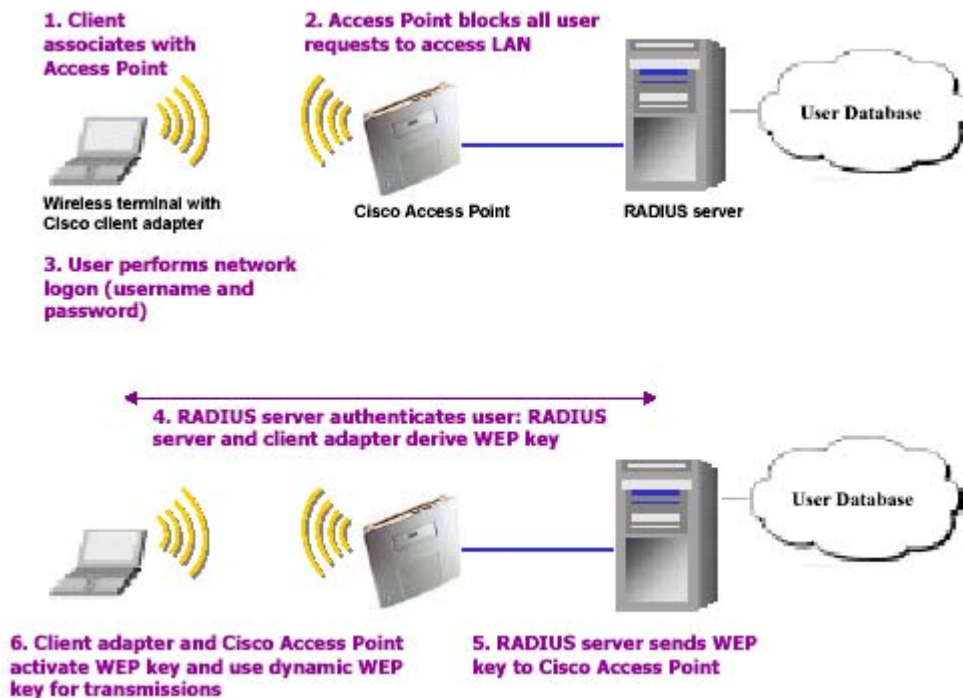
Even if an intruder intercepts a WEP key, a new WEP key is generated after a specified period of time rendering the captured key invalid.

LEAP

LEAP is Cisco's solution for providing strong authentication and is supported with Cisco's Aironet wireless infrastructure; client credentials are based on username and password. By enabling WEP, LEAP mitigates the risk of a hacker intercepting and cracking a WEP key through dynamic generation of per user/per session WEP keys, as described above.

The Cisco Secure Access Control Server (ACS) or the Cisco Access Registrar (AR) RADIUS server determine session length. When a session expires or the client roams from one access point to another, re-authentication occurs and generates a new session key – totally transparent to the user. Figure 3. illustrates the LEAP authentication process and the derivation of the dynamic WEP key.

Figure 3. Cisco LEAP authentication



Cisco recently announced a no-cost licensing program called the Cisco Compatible Extensions program (CCX), specific to wireless client products. CCX makes Cisco technology (including LEAP) available to industry leading silicon suppliers that manufacture embedded and stand-alone wireless clients. CCX participants include Agere Systems, Atheros, Atmel, HP, IBM, Intel, Intersil, and Texas Instruments. Many have already begun integrating Cisco extensions into their product designs. Extensive third party testing ensures interoperability between CCX products and Cisco Aironet products.

AirFortress

AirFortress™ provides a simple, efficient and robust Layer 2 encryption security solution for 802.11 wireless networks. Developed by Fortress Technologies Inc, AirFortress is a FIPS 140-1 approved security technology (Certificate # 231) that supports current and legacy operating systems for a total solution.

The AirFortress solution is comprised of three components:

Wireless Security Gateways: provide perimeter security by bridging encrypted wireless communications to the wired LAN, or remotely between point-to-point connections. The Wireless Security Gateway encrypts and decrypts communication to/from a Secure Client or other Wireless Security Gateway, thereby preventing unauthorized network access.

Secure Client: a DOS or Windows based driver that secures a wide range of mobile devices. The Secure Client encrypts and decrypts communication to/from a Wireless Security Gateway and during peer-to-peer communication between mobile devices thereby preventing unauthorized access to the mobile device from other devices.

Access Control Server (ACS): a software application database designed to monitor and manage the authentication and access control of wireless clients.

The AirFortress solution utilizes a number of methods to enhance security. *Frame Manipulation* hides the entire Layer 3 (Network Layer) header and utilizes a unique MAC protocol ID only recognized by AirFortress products. *Frame Authentication* ensures integrity through SHA-1 hashing, preventing session hijacking. *Payload Compression* disguises original frame length and its contents to combat analytical and brute force attacks. Dynamic Per Session Keys are generated using an encrypted dual Diffie-Hellman key exchange to prevent man-in-the-middle attacks and spoofing. The encryption of ARP packets and unique bridging design prevents ARP poisoning attacks. *Replay Protection* guards against data being captured and then being re-injected into the network after it has been compromised.

A unique *Access ID* prevents unauthorized clients and intruders from performing a key exchange by providing a mechanism to segment communications and control network access. A *Physical Device ID* is a system generated, unique hardware identifier bound to a specific device and used to distinguish AirFortress devices. The closed architecture design restricts both the wireless client and security gateway to encrypted communications to deliver the protection of a firewall without the complexity. Figure 4. illustrates an AirFortress implementation:

Figure 4. AirFortress™ implementation



The AirFortress solution is based on *Wireless* Link Layer Security (wLLS) - a true security protocol that operates on the Data Link layer and provides point-to-point encryption of wireless communications. wLLS is designed using standard encryption methods and a dual Diffie-Hellman key exchange to automatically build security associations. wLLS uses industry standard algorithms including AES, 56-bit DES, 128-bit IDEA or 168-bit 3DES - if necessary, other algorithms can be customized into the product.

wLLS is an efficient, self-contained software driver that saves processing cycles and memory. The protocol performs all key exchanges, encryption and authentication at the Data Link layer. Unlike other security protocols, wLLS requires only 2 steps to complete a key exchange making wLLS up to 20 times faster than other key exchange methods. wLLS can be combined with WEP, but is strong enough to be utilized by itself. Because the Fortress driver compresses data, significantly increased bandwidth and shorter transmit times result. The Layer 2 (Data Link layer) encryption renders information unreadable during transport while critical internal addressing information is protected.

wLLS is a FIPS (Federal Information Processing Standard) approved security protocol certified under the U.S. Government's FIPS 140 cryptographic validation process. FIPS based security solutions are the required source of security for the U.S. Federal government.

Table 1. illustrates the security solutions available across the Psion Teklogix family of products.

Table 1.



Model	7035	8255 / 8260	8560	8570	7535	NetPad	9150
OS	DOS	DOS	Win 2000 / XP	Win 2000 / XP	CE.NET 4.2	CE.NET 4.1	VxWorks
WEP 64 or 128 Bit	Yes	Yes	Yes	Yes	Yes	Yes	Yes
802.1X	Yes	Yes	Yes, with Windows 2000 SP3 and upgrade patch or SP4, with Windows XP	Yes, with Windows 2000 SP3 and upgrade patch or SP4, with Windows XP	Yes	Yes	Yes
Cisco LEAP	Yes with Cisco radio	Yes with Cisco radio	Yes with Cisco radio	Yes with Cisco radio	Yes with Meetinghouse client	Yes with Cisco radio	LEAP only supported on Cisco Aironet wireless infrastructure
AirFortress	Yes	Yes	Yes	Yes	Q4/2003	Q4/2003	Yes

Emerging 802.11 security standards

IEEE 802.11i Enhanced Wireless Security standard

The IEEE 802.11 TGi working group is currently working on ratifying (expected early 2004) the 802.11i Enhanced Wireless Security standard, also known as Robust Security Network (RSN).

802.11i incorporates user authentication mechanisms and stronger data encryption, effectively representing second-generation 802.11 security to address security concerns for legacy hardware and new hardware in AP and ad-hoc (peer-to-peer) based 802.11 networks. 802.11i specifies user authentication through 802.1X and data encryption through the Temporal Key Integrity Protocol (TKIP) and Counter Mode with CBC-MAC Protocol (CCMP).

TKIP targets legacy 802.11 equipment and will be available as a firmware or software upgrade. TKIP implements counter-measures to reduce the rate at which a hacker can make message forgery attempts, down to two packets every 60 seconds; after which new encryption keys are generated. The counter-measures reduce the probability of successful forgery and amount of information an attacker can learn about a key.

By contrast, CCMP requires new 802.11 hardware with greater processing power and increased memory. Based on the Advanced Encryption Standard (AES), CCMP is a FIPS-197 certified algorithm approved by NIST. AES replaces the Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES) for all government transactions.

AES operates in a Counter Mode within 802.11i with CBC-MAC (CCM). Counter Mode is used for data privacy and CBC-MAC (Cipher Block Chaining Message Authentication Code) is used for data integrity and authentication. Message Authentication Code (MAC) provides the same functionality as MIC, used with TKIP.

Wi-Fi Protected Access (WPA)

The Wi-Fi Alliance realizes the immediate need for stronger wireless security and has teamed with the IEEE to introduce Wi-Fi Protected Access WPA; a subset of 802.11i security with many of the same data encryption and user authentication components. WPA fills the security gap

until the ratification of 802.11i, and WPA certification of 802.11 hardware began in February 2003. WPA will be mandatory for Wi-Fi certification before the end of 2003.

WPA utilizes TKIP to provide strong data encryption, and offers two user authentication and key management methods. In enterprise environments with a centralized AS, user authentication is based on 802.1X and mutual authentication based EAP. In home or office environments where a centralized authentication server or EAP framework is not available, user authentication is based on a 'Pre-Shared Key' method (PSK). With Pre-Shared Key authentication, the home or office user manually enters a password (Master Key) in the Access Point or Wireless Router and enters the same password in each client device that accesses the wireless network. The manually configured WPA password (Master Key) automatically starts the TKIP data encryption process.

The first version of WPA addresses security requirements for AP-based 802.11 networks only. The Wi-Fi Alliance will adopt the full 802.11i security standard as WPA version 2, featuring security requirements for AP-based and ad-hoc (peer-to-peer) 802.11 infrastructures.

Summary

802.11 wireless LAN deployments will continue to grow with each passing year. Higher data rates, increased bandwidth and improved quality of service coupled with increased productivity through mobility are making wireless LANs an attractive network solution for many customers. Along with improved wireless technology performance, organizations such as the IEEE, Wi-Fi Alliance, Fortress Technologies and Cisco Systems are providing enhanced security solutions for 802.11 networks to prevent unauthorized access to confidential data.

Companies that are deploying a wireless network should become familiar with 802.11 wireless technologies to help them create a more efficient and secure network. It is important to understand today's security solutions in order to choose the right solution for their requirements. Enhanced wireless security solutions such as 802.1X, AirFortress, LEAP and WPA deliver the significant benefit of security to the other features of a wireless network.

Rosario Macri
Product Manager
Psion Teklogix