

Wireless LAN Security



The Growth of Wireless LANs

Until recently, wireless local-area network (LAN) products were used primarily in certain vertical markets—such as retail, education, and health care—where mobile users with a need for LAN access were satisfied with data-transfer rates of 2 megabits per second (Mbps) or less. Even though most wireless LANs were extensions of wired LANs, the proprietary nature and slow speeds of wireless LANs forced organizations to manage wireless LANs as unique entities. To make wireless LANs more “mainstream,” customers pressed vendors to develop a high-speed wireless LAN standard that would encourage interoperability, reduce prices, and provide the bandwidth needed by today’s business applications.

In 1999, the Institute of Electrical and Electronics Engineers (IEEE) ratified an extension to a previous standard. Called IEEE 802.11b, it defines the standard for wireless LAN products that operate at an Ethernet-like data rate of 11 Mbps, a speed that makes wireless LAN technology viable in enterprises and other large organizations. Interoperability of wireless LAN products from different vendors is ensured by an independent organization called the Wireless Ethernet Compatibility Alliance (WECA; see <http://www.wi-fi.com>), which brands compliant products as “Wi-Fi.” Dozens of vendors market Wi-Fi products, and organizations of every size and type are considering, if not deploying, wireless LANs.

Demand for wireless access to LANs is fueled by the growth of mobile computing devices, such as laptops and personal digital assistants, and a desire by users for continual connections to the network without having to “plug in.” There will be over a billion mobile devices by 2003, and the wireless LAN market is projected to grow to over US\$2 billion by 2002.

The Need for Centralized Security Management

Now that wireless LANs have become mainstream, organizations want to tightly integrate wireless LANs with wired LANs. Network managers are reluctant or unwilling to deploy wireless LANs unless those LANs provide the type of security, manageability, and scalability offered by wired LANs.

The chief concern is security, which encompasses access control and privacy. Access control ensures that sensitive data can be accessed only by authorized users. Privacy ensures that transmitted data can be received and understood only by the intended audience.

Access to a wired LAN is governed by access to an Ethernet port for that LAN. Therefore, access control for a wired LAN often is viewed in terms of physical access to LAN ports. Similarly, because data transmitted on a wired LAN is directed to a particular destination, privacy cannot be compromised unless someone uses specialized



equipment to intercept transmissions on their way to their destination. In short, a security breach on a wired LAN is possible only if the LAN is physically compromised.

With a wireless LAN, transmitted data is broadcast over the air using radio waves, so it can be received by any wireless LAN client in the area served by the data transmitter. Because radio waves travel through ceilings, floors, and walls, transmitted data may reach unintended recipients on different floors and even outside the building of the transmitter. Installing a wireless LAN may seem like putting Ethernet ports everywhere, including in your parking lot. Similarly, data privacy is a genuine concern with wireless LANs because there is no way to direct a wireless LAN transmission to only one recipient.

The IEEE 802.11b standard includes components for ensuring access control and privacy, but these components must be deployed on every device in a wireless LAN. An organization with hundreds or thousands of wireless LAN users needs a solid security solution that can be managed effectively from a central point of control. Some cite the lack of centralized security as the primary reason why wireless LAN deployments have been limited to relatively small workgroups and specialized applications.

First-Generation Wireless LAN Security

The IEEE 802.11b standard defines two mechanisms for providing access control and privacy on wireless LANs: service set identifiers (SSIDs) and wired equivalent privacy (WEP). Another mechanism to ensure privacy through encryption is to use a virtual private network (VPN) that runs transparently over a wireless LAN. Because the use of a VPN is independent of any native wireless LAN security scheme, VPNs are not discussed in this paper.

SSID

One commonly used wireless LAN feature is a naming handle called an SSID, which provides a rudimentary level of access control. An SSID is a common network name for the devices in a wireless LAN subsystem; it serves to logically segment that subsystem. The use of the SSID as a handle to permit/deny access is dangerous because the SSID typically is not well secured. An access point, the device that links wireless clients to the wired LAN, usually is set to broadcast its SSID in its beacons.

WEP

The IEEE 802.11b standard stipulates an optional encryption scheme called wired equivalent privacy, or WEP, that offers a mechanism for securing wireless LAN data streams. WEP uses a symmetric scheme where the same key and algorithm are used for both encryption and decryption of data. The goals of WEP include:

- *Access control*: Prevent unauthorized users, who lack a correct WEP key, from gaining access to the network.
- *Privacy*: Protect wireless LAN data streams by encrypting them and allowing decryption only by users with the correct WEP keys.

Although WEP is optional, support for WEP with 40-bit encryption keys is a requirement for Wi-Fi certification by WECA, so WECA members invariably support WEP. Some vendors implement the computationally intense activities of encryption and decryption in software, while others, like Cisco Systems, use hardware accelerators to minimize the performance degradation of encrypting and decrypting data streams.

The IEEE 802.11 standard provides two schemes for defining the WEP keys to be used on a wireless LAN. With the first scheme, a set of as many as four default keys are shared by all stations—clients and access points—in a wireless subsystem. When a client obtains the default keys, that client can communicate securely with all other stations in the subsystem. The problem with default keys is that when they become widely distributed they are more likely to be compromised. In the second scheme, each client establishes a “key mapping” relationship with another station. This is a more secure form of operation because fewer stations have the keys, but distributing such unicast keys becomes more difficult as the number of stations increases.

Authentication

A client cannot participate in a wireless LAN until that client is authenticated. The IEEE 802.11b standard defines two types of authentication methods: open and shared key. The authentication method must be set on each client, and the setting should match that of the access point with which the client wants to associate.



With open authentication, which is the default, the entire authentication process is done in clear-text, and a client can associate with an access point even without supplying the correct WEP key. With shared-key authentication, the access point sends the client a challenge text packet that the client must encrypt with the correct WEP key and return to the access point. If the client has the wrong key or no key, it will fail authentication and will not be allowed to associate with the access point.

Some wireless LAN vendors support authentication based on the physical address, or Media Access Control (MAC) address, of a client. An access point will allow association by a client only if that client's MAC address matches an address in an authentication table used by the access point.

Security Threats

Theft of Hardware

It is common to statically assign a WEP key to a client, either on the client's disk storage or in the memory of the client's wireless LAN adapter. When this is done, the possessor of a client has possession of the client's MAC address and WEP key and can use those components to gain access to the wireless LAN. If multiple users share a client, then those users effectively share the MAC address and WEP key.

When a client is lost or stolen, the intended user or users of the client no longer have access to the MAC address or WEP key, and an unintended user does. It is next to impossible for an administrator to detect the security breach; a proper owner must inform the administrator. When informed, an administrator must change the security scheme to render the MAC address and WEP key useless for wireless LAN access and decryption of transmitted data. The administrator must reencode static encryption keys on all clients that use the same keys as the lost or stolen client. The greater the number of clients, the larger the task of reprogramming WEP keys.

What is needed is a security scheme that:

- Bases wireless LAN authentication on device-independent items such as usernames and passwords, which users possess and use regardless of the clients on which they operate

- Uses WEP keys that are generated dynamically upon user authentication, not static keys that are physically associated with a client

Rogue Access Points

The 802.11b shared-key authentication scheme employs one-way, not mutual, authentication. An access point authenticates a user, but a user does not and cannot authenticate an access point. If a rogue access point is placed on a wireless LAN, it can be a launch pad for denial-of-service attacks through the "hijacking" of the clients of legitimate users.

What is needed is mutual authentication between the client and an authentication server whereby, both sides prove their legitimacy within a reasonable time. Because a client and an authentication server communicate through an access point, the access point must support the mutual authentication scheme. Mutual authentication makes it possible to detect and isolate rogue access points.

Other Threats

Standard WEP supports per-packet encryption but not per-packet authentication. A hacker can reconstruct a data stream from responses to a known data packet. The hacker then can spoof packets. One way to mitigate this security weakness is to ensure that WEP keys are changed frequently.

By monitoring the 802.11 control and data channels, a hacker can obtain information such as:

- Client and access point MAC addresses
- MAC addresses of internal hosts
- Time of association/disassociation

The hacker can use such information to do long-term traffic profiling and analysis that may provide user or device details. To mitigate such hacker activities, a site should use per-session WEP keys.



Addressing Security Threats

In summary, to address the security concerns raised in this section, a wireless LAN security scheme should:

- Base wireless LAN authentication on device-independent items such as usernames and passwords, which users possess and use regardless of the clients on which they operate
- Support mutual authentication between a client and an authentication (RADIUS) server
- Use WEP keys that are generated dynamically upon user authentication, not static keys that are physically associated with a client
- Support session-based WEP keys

First-generation wireless LAN security, which relies on static WEP keys for access control and privacy, cannot address these requirements.

A Complete Security Solution

What is needed is a wireless LAN security solution that uses a standards-based and open architecture to take full advantage of 802.11b security elements, provide the strongest level of security available, and ensure effective security management from a central point of control. A promising security solution implements key elements of a proposal jointly submitted to the IEEE by Cisco Systems, Microsoft and other organizations. Central to this proposal are the following elements:

- Extensible Authentication Protocol (EAP), an extension to Remote Access Dial-In User Service (RADIUS) that can enable wireless client adapters to communicate with RADIUS servers
- IEEE 802.1X, a proposed standard for controlled port access

When the security solution is in place, a wireless client that associates with an access point cannot gain access to the network until the user performs a network logon. When the user enters a username and password into a network logon dialog box or its equivalent, the client and a RADIUS server (or other authentication server) perform a mutual authentication, with the client authenticated by the supplied username and password. The RADIUS server and client then derive a client-specific WEP key to be used

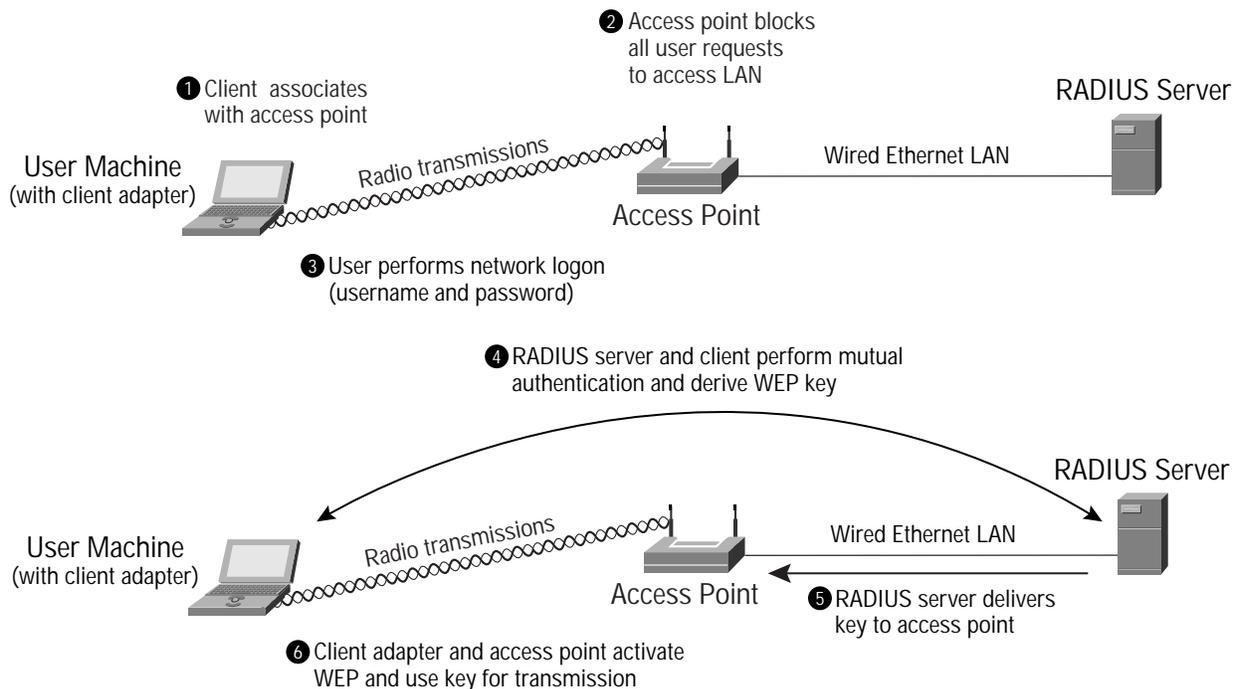
by the client for the current logon session. All sensitive information, such as the password, is protected from passive monitoring and other methods of attack. Nothing is transmitted over the air in the clear.

The sequence of events follows:

- A wireless client associates with an access point.
- The access point blocks all attempts by the client to gain access to network resources until the client logs on to the network.
- The user on the client supplies a username and password in a network logon dialog box or its equivalent.
- Using 802.1X and EAP, the wireless client and a RADIUS server on the wired LAN perform a mutual authentication through the access point. One of several authentication methods or types can be used. With the Cisco authentication type, the RADIUS server sends an authentication challenge to the client. The client uses a one-way hash of the user-supplied password to fashion a response to the challenge and sends that response to the RADIUS server. Using information from its user database, the RADIUS server creates its own response and compares that to the response from the client. Once the RADIUS server authenticates the client, the process repeats in reverse, enabling the client to authenticate the RADIUS server.
- When mutual authentication is successfully completed, the RADIUS server and the client determine a WEP key that is distinct to the client and provides the client with the appropriate level of network access, thereby approximating the level of security inherent in a wired switched segment to the individual desktop. The client loads this key and prepares to use it for the logon session.
- The RADIUS server sends the WEP key, called a session key, over the wired LAN to the access point.
- The access point encrypts its broadcast key with the session key and sends the encrypted key to the client, which uses the session key to decrypt it.
- The client and access point activate WEP and use the session and broadcast WEP keys for all communications during the remainder of the session.



Figure 1 With the Cisco security solution, authentication is based on username and password, and each user gets a unique, session-based encryption key.



Support for EAP and 802.1X delivers on the promise of WEP, providing a centrally managed, standards-based, and open approach that addresses the limitations of standard 802.11 security. In addition, the EAP framework is extensible to wired networks, enabling an enterprise to use a single security architecture for every access method.

It is likely that dozens of vendors will implement support for 802.1X and EAP in their wireless LAN products. Knowing the customer benefits of 802.1X, Cisco Systems supports the forthcoming standard today, offering a complete, end-to-end security solution that is fully compliant with 802.1X. The solution is available when a site uses Cisco Aironet® wireless client adapters and access points and the Cisco Secure Access Control Server. More information is available through Cisco Connection Online at <http://www.cisco.com>.

With the Cisco Systems wireless LAN security solution in place, an organization:

- Minimizes the security threats of lost or stolen hardware, rogue access points, and hacker attacks
- Uses user-specific, session-based WEP keys created dynamically at user logon, not static WEP keys stored on client devices and access points
- Manages the security for all wireless users from a central point of control

Cisco wireless security services closely parallel security available in a wired LAN, fulfilling the need for a consistent, reliable, and secure mobile networking solution.



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems Australia, Pty., Ltd
Level 17, 99 Walker Street
North Sydney
NSW 2059 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the
Cisco Connection Online Web site at <http://www.cisco.com/offices>.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam •

All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement. Printed in the USA. Aironet, Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other brands, names, or trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0011R)