Enterprise Solutions for Wireless LAN Security

Wi-Fi Alliance
February 6, 2003

Executive Summary

The threat to network security from improperly secured WLANs is a real and present danger for today's enterprises. The good news for enterprise managers is that there is a range of strong, vendor neutral solutions available today that addresses the vulnerabilities inherent with the original 802.11 security implementation known as WEP (Wired Equivalent Privacy). For protection against nontargeted attacks enterprises can use 802.1X-based authentication to provide a dynamic keying mechanism for WEP. At the other end of the spectrum, for protection against active, targeted attacks, IT can isolate the WLAN from the corporate network by use of firewall and Virtual Private Network (VPN) technologies.

In the first half of 2003, Wi-Fi Alliance vendors will begin shipping a strong, standards-based solution called Wi-Fi® Protected Access (WPA) that will address all known WEP vulnerabilities, and provide adequate protection for even the active, targeted attacks. Wi-Fi Protected Access will be available both in new Wi-Fi CERTIFIED wireless LAN hardware and as a software upgrade for most existing Wi-Fi CERTIFIED wireless LAN hardware. WPA uses many of the same security components that will be used by IEEE 802.11i when it is completed.

The key point for enterprise managers to understand about WLAN security risks is that like any network it must be secured. One of the biggest issues in today's corporate environment is the rogue AP that is installed by an employee seeking the convenience of a WLAN in their work area. Unfortunately, these APs are often installed without adequate security and leave the corporate network open to attack.

This paper considers these issues and provides recommended actions to address them, allowing employees secure access to the productivity offered by WLAN technology.

The Wi-Fi Alliance is a nonprofit international association formed in 1999 to certify interoperability of wireless local area network products based on IEEE 802.11 specifications. Wi-Fi product certification began in March of 2000. One of the goals of the Wi-Fi Alliance is to ensure that consumers realize maximum benefit from their Wi-Fi products in a secure and productive environment.

Table of Contents

I. Introduction

Most industry estimates suggest that more than 50% of all enterprises will have at least one WLAN installation by 2003[1]. The Wi-Fi Alliance believes it is critical for CIO's and IT managers to understand the risks of WLANs and immediately take prudent action to secure their installation.

The critical topics covered in this white paper include:

I. WLAN security breaches
II. Causes of WLAN security issues
III. Strong vendor-neutral WLAN security solutions for enterprise campuses
IV. Wi-Fi® Protected Access adds significant new security in 2003
V. Secure corporate access from home and hot spot WLANs, using VPNs
VI. Wi-Fi Protected Access 2 Revamps 802.11 Encryption
VII. WLAN security best practices

II. WLAN Security Breaches

There are two aspects of WLAN security: data protection (encryption) and network access control (authentication). Breaches can occur at the network level via the wireless access point (AP), or at an individual PC - either attached to a network or operating in ad hoc mode and communicating in a peer-to-peer fashion.

The result of a wireless privacy breach is the same as it would be for a physical wire-based network privacy issue: corporate data is at risk for third party recovery or modification. Because of the broadcast nature of wireless, however, providing data protection is much more challenging with wireless networks.

Network breaches range from someone taking unauthorized enterprise network bandwidth to connect to the Internet, to attempts at accessing corporate secrets. Without prudent measures, WLANs can represent uncontrolled entry into an otherwise secure network.

Much of the present threat is caused unintentionally by an enterprise's employees. Vulnerability is created when, for the sake of their own convenience, employees deploy a "rogue" AP which has not been authorized by a network administrator. This effectively leaves a door open to the corporate network. These rogue APs are often installed with no security protection activated and behind the firewall. In this situation, these APs allow virtually open access to the corporate network. This risk of rogue AP deployment is exacerbated by organizations that refuse to implement wireless solutions and prompt employees to take action themselves.

III. Causes of WLAN Security Issues

The original IEEE 802.11 security standard had modest security goals in WEP that are now easily defeated[*]. In general terms this included native authentication, where the user is required to prove he is authorized for access and encryption to provide data protection.

[1] Gartner – Technology Adoption and Value: Survey Results – December 2002

[*] 802.11 security applies equally to 802.11a, b, and g – the three physical level (speed/distance) implementations of 802.11 LANS.

Weak Authentication
IEEE 802.11 authentication is offered by three mechanisms: 1) Open System Authentication, where only the APs publicly available network name – also known as Service Set Identifier (SSID) is used; 2) Shared Key Authentication, where a static, manually preset WEP key on both the AP and the stations is used; and 3) configuring the AP to only accept selected MAC addresses. Whether used separately or in combination, these measures are easily overcome with widely available hacker's tools. Open System Authentication depends on an attacker not learning the SSID—but this can always be learned using a packet sniffer, even when the SSID broadcast has been disabled. Shared Key Authentication is poorly designed, and an attacker with a packet sniffer can reuse information gathered from one valid authentication to authenticate himself. Finally, any Wi-Fi card MAC address can be changed to that of any other (spoofed), so access control via MAC address lists is ineffective and not scalable.

In the name of "plug-and-play", the default authentication is only Open System Authentication, which is why default AP security is said to be off.

WEP Is Easily Defeated
When the AP and stations are configured to use the static key for authentication, that same key is used to drive an encryption process that was intended to keep data confidential as it is transmitted between station and AP. This is an abuse of cryptography, as attacks against the key for one function help develop information to attack the key in the next use. In addition, WEP has fundamental design flaws that render its protection ineffective. It is possible to decrypt the data without even cracking the encryption key due to key reuse; a repeated key can be recovered directly from the WEP packet. Even worse, it is possible to forge properly encrypted WEP packets without the encryption key, and the 802.11 equipment will accept these as genuine.

While applying WEP can deter the occasional drive by or unintentional visitor, it will not prevent an attacker using automated, readily available tools from gaining access to the WLAN network.

Other Security Risks
CIOs and IT managers should be aware of at least two WLAN-related scenarios that lead to compromised enterprise networks or devices.

a. Masquerading illegitimate APs - This is a different type of rogue AP, not part of the corporate network, but instead attached to an attacker's network with the intent to steal user credentials by pretending to be a corporate AP. The 802.1X mutual authentication capability described later in this paper provides an effective means to thwart this attack, as long as users follow a policy of associating only with known APs.

b. WLAN cards operating in ad hoc mode open user data and credentials to theft. 802.11 and other security measures, until Wi-Fi Protected Access 2 (discussed below), do not protect a user's system from unwanted access, if the card is left in ad hoc mode. Consequently IT managers should look for operating system enforcement mechanisms and user education as tools to minimize ad hoc mode threats.

IV. Strong Vendor-Neutral WLAN Security Solutions for Enterprise Campuses

Standards-based solutions exist today that enable enterprise managers to guard campus installations against targeted attacks, where the corporate network is a pre-determined goal, and nontargeted attacks, where the attack is made opportunistically against any available network.

802.1X Protects Against Non-Targeted Attacks

802.1X significantly enhances WLAN security by supporting mutual authentication and dynamic key management. Mutual authentication helps ensure clients are communicating with known networks and dynamic key management reduces exposure to key attacks. When combined with current WEP-based WLAN implementations, an 802.1X solution is often labeled "dynamic WEP" and is an effective deterrent against the non-targeted attack. (see 802.11i sidebar for more information on 802.1X)

A more robust solution, however, is needed against targeted attacks. Since dynamic WEP addresses only key reuse, and not the other WEP flaws, the network remains vulnerable to active attacks such as message forgery, replays, etc.

Action: IT managers should select the Extensible Authentication Protocol EAP type(s) and RADIUS authentication servers for their networks and begin implementing an 802.1X capability as soon as possible to: 1) increase the security of today's WLANs, and; 2) prepare an infrastructure that will be used with upcoming Wi-Fi Protected Access in 2003.

Table 1. Proprietary Alternatives Available Today

Several WLAN vendors provide robust, but proprietary, solutions to address WEP shortcomings.

These solutions combine a standards–based 802.1X implementation with a proprietary version of TKIP (see 802.11i sidebar). Since they address known WEP flaws, these solutions have been shown to be effective at providing a robust wrapper for WEP and therefore should serve as an effective deterrent even for the active techniques that may be used in a targeted attack.

The primary tradeoff for this path is that an enterprise must use WLAN APs and client interfaces that support the same proprietary approach, either from a common vendor, or its licensees.

Generally, vendors offering proprietary options will enable their customers to migrate to standards-based solutions via software/firmware upgrades, once Wi-Fi Protected Access solutions become available; IT managers should check with their vendors on specifics.

VPN's and Network Firewalls Protect Against Targeted Attacks

For networks or selected segments where targeted attacks are considered likely, enterprise managers can isolate current WLANs from the wired LAN using the well-proven combination of a network firewall and Internet Protocol Security (IPsec) based Virtual Private Networks (VPN). While the use of VPN-firewalls typically builds on an enterprise's remote access experience with the same technology, there are potential additional licenses and VPN gateway hardware purchases to consider as this solution is scaled to a larger number of campus WLAN users.

V. Wi-Fi Protected Access Adds Significant New Security in 2003

In response to the need for standards-based mutual authentication and strong encryption, the Wi-Fi Alliance in conjunction with the IEEE, has driven an effort to bring strongly enhanced, interoperable Wi-Fi security to market in the first half of 2003. The result of this effort is Wi-Fi Protected Access, or WPA.

Wi-Fi Protected Access will be forward-compatible with the IEEE 802.11i specification currently under development by the IEEE (see 802.11i sidebar) and is a subset of the current 802.11i draft that includes, 802.1X, PSK and TKIP.

Wi-Fi Protected Access will provide wireless LAN users with a high level of assurance that their data will remain protected and that only authorized network users can access the network. Independent cryptographers have reviewed Wi-Fi Protected Access and verified that it appears to meet its security claims, by addressing all known WEP vulnerabilities, and therefore providing an effective deterrent against nontargeted and targeted attacks. For most enterprises, after the transition to Wi-Fi Protected Access is complete, there will be minimal need for incremental security solutions such as VPN-firewall technology.

Significantly, Wi-Fi Protected Access is designed as a software upgrade to Wi-Fi CERTIFIED devices, requiring no additional hardware. Wi-Fi Protected Access support will be available from vendors of WLAN equipment in early 2003. The Wi-Fi Alliance plans to begin interoperability certification testing on Wi-Fi Protected Access during the second quarter of 2003, enabling multivendor WLAN security solutions.

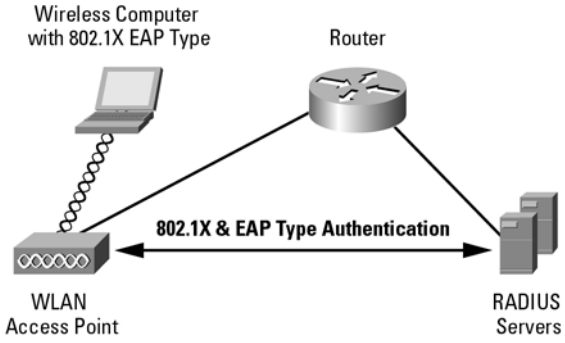

Figure 1. 802.1X & EAP Type

As Wi-Fi Protected Access becomes available, IT managers should update WEP-based installations at both APs and client stations and make sure that new purchases support Wi-Fi Protected Access. For enterprise networks, implementing Wi-Fi Protected Access will involve deploying:

1. 802.1X infrastructure, including:
    - Selection of EAP types that will be supported on stations, APs, and authentication servers
    - Selection and deployment of AAA or RADIUS-based authentication severs
2. Wi-Fi Protected Access software upgrades for APs
3. Wi-Fi Protected Access software upgrades for clients

Also note that most Wi-Fi Protected Access capable APs will support both WEP-based security and Wi-Fi Protected Access with client stations. In this transition mode, security is determined by the minimum mode allowed by the AP (i.e., WEP). Prudent IT managers will therefore quickly move their AP from transition mode to Wi-Fi Protected Access only, in order to gain the security benefits of Wi-Fi Protected Access.

Table 2. 802.11i Overview for Enterprise

Native WLAN security will be significantly improved when the IEEE workgroup TGi completes the 802.11i specification, expected by the end of 2003. This specification will apply across 802.11 versions a, b and g—ultimately all physical layer versions of 802.11.

Upon completion, 802.11i will address WLAN security issues by specifying the following:

- *Use of 802.1X, an IEEE authentication standard since August 2001, for both new and existing 802.11 hardware*.* 802.1X creates a framework for mutual authentication between a client station and the AP, by including an authentication server (often RADIUS-based) and one of several possible Extensible Authentication Protocols (EAP) types. After mutual authentication, a key is derived for encryption. Since 802.1X derives a fresh key for each new session between a station and the AP, it is providing dynamic key management and replaces native 802.11 static keys.
- *A security update for existing 802.11 hardware*. The Temporal Key Integrity Protocol (TKIP) specified by the 802.11i specification, will offer a robust software/firmware "wrapper" for existing WEP hardware to address the fundamental flaws of WEP. Measures are provided to fix WEP encryption vulnerabilities (key re-use and weak key attacks), and threats to message integrity (forgeries and replays).
- *A security plan for new AP hardware.* The Advanced Encryption Standard (AES) will provide enhanced encryption and require new hardware in the AP. AES will be used in counter cipher-block chaining mode (CCM), and represents a "ground-up" upgrade to WLAN security that is expected to satisfy US Government security requirements. Additionally, the AES-based scheme will enable security for stations operating in ad hoc mode.

*An alternative authentication scheme using a pre-shared key (PSK) methodology is included in the 802.11i specification, for homes and small businesses that do not have the resources to deploy an 802.1X infrastructure.

VI. Secure Corporate Access from Home and Hot Spot WLANs, Using VPNs

Employees access the corporate network via the Internet when connected to a home or public (hot spot) WLAN, and in most cases use a VPN for this remote access.[*] While using a VPN protected connection and personal firewall, corporate data and network access are protected, even while connected from an unprotected WLAN.

WLAN security measures applied on the enterprise campus should have no impact on employee ability to connect to hot spot or home WLANs, since 1) most hot spots operate with no local data protection (encryption) in order to remain open to all potential customers, and 2) users will set up their own credentials (password) for access to home APs.

VII. Wi-Fi Protected Access 2 Revamps 802.11 Encryption

The full implementation of 802.11i, tentatively called Wi-Fi Protected Access 2 (WPA2), will upgrade the fundamental 802.11 WLAN encryption algorithm from TKIP/WEP to an Advanced Encryption Standard (AES) based approach (see 802.11i sidebar). Wi-Fi Protected Access 2 will utilize the same 802.1X authentication used with Wi-Fi Protected Access (version 1), and will enable a graceful transition from the earlier version. A mixed mode is expected to be supported on Wi-Fi Protected Access 2 APs that will allow both WPA1 and WPA2 clients. And since version WPA1 remains a strong encryption solution, the transition to all WPA2 clients and APs can be done gradually, driven by the pace of an enterprise's AP replacement.

[*] Employees should use enterprise provisioned devices and not potentially misconfigured personal devices for corporate access.

The 802.11i specification is targeted for completion by the end of 2003. Since Wi-Fi Protected Access 2 will utilize this specification, vendor products and Wi-Fi certification testing for WPA2 are expected during 2004.

WLAN - A Necessity

WLANs offer employees productivity gains as they stay connected with corporate resources while moving about the workplace. Enterprises can bolster corporate wide security by deploying secure Wi-Fi WLANs today, thereby reducing employee motivation to install rogue APs - and by emphasizing user education.

Summary

There is a range of effective solutions available to supplement native 802.11 security mechanisms and protect against the spectrum of nontargeted and targeted attacks. Enterprises have strong reasons to begin deployment of 802.1X authentication solutions today to both supplement existing WEP-based security, and migrate toward network-wide Wi-Fi Protected Access.

Wi-Fi Protected Access will provide standards-based, native security mechanisms that effectively address all known WEP vulnerabilities. It will provide a strong deterrent against non-targeted and targeted attacks. WPA1 will be forward compatible with the full implementation of 802.11i, tentatively called Wi-Fi Protected Access 2. Mandatory Wi-Fi Alliance compliance testing will support Wi-Fi Protected Access offerings from the majority of manufacturers by mid-year, 2003.

VIII. WLAN Security Best Practices

To protect your wireless LAN network from attack, the following best practices are recommended:

1. Educate employees about WLAN risks, with focus on threats from
   - Unauthorized attachment of APs (rogue APs)
   - Use of WLAN cards in ad hoc mode, especially when in public areas or any building with perimeter less than the WLAN broadcast range
   - Connect only to known APs; masquerading APs are more likely in unregulated public spaces
2. Deploy personal firewalls on all mobile machines. Use corporate network security policy to enforce their continuous use
3. Actively and regularly scan for rogue APs on the corporate network, using available WLAN management tools, such as NetStumbler, AirMagnet, or AirDefense
4. Change default management passwords on APs
5. Change the default SSID on all APs, and allow the APs to broadcast their SSIDs. This enables users to easily identify the AP to which they are connecting and only present the necessary credentials
6. Turn on and use WEP. It provides basic-level protection against the drive by snooper or unintentional visitor. WEP should always be used with other measures in a corporate environment
7. When deploying 802.1X infrastructure to implement dynamic WEP, configure the session key update for at least once per hour to minimize the chance of key repetition

8. Avoid placing APs against exterior walls or windows
9. Reduce the broadcast strength of the AP when possible to keep it within the necessary area of coverage, and avoid coverage of unintended areas such as parking lots
10. When planning network design, use 802.1X-based port authentication for wired switches and hubs to inhibit future addition of unauthorized, user-attached APs
11. When using a VPN/firewall solution to protect campus WLANs, use IPsec-based VPNs with secondary authentication