

WLAN Security Challenges

by: Josh Glenn, 08/03/2005

<http://www.securitydocs.com/library/3534>

Executive Summary

Organizations are eager to migrate to wireless LANs (WLANs). Users want the any-time/anywhere network access WLANs provide; administrators can't resist the easy, flexible installation and demonstrate long-term savings. New technologies enabling WLANs to operate at Ethernet speed have only intensified demand.

However, security has been a challenge for wireless equipment manufacturers, and consequently a barrier to widespread WLAN adoption. It hasn't helped that an early implementation of the most recent de facto WLAN security standard, WEP, was a spectacular public failure; one team of academics provided how a WEP WLAN might be infiltrated - and the network server compromised - in just 15 minutes.

The latest WLAN specification, 802.1x, provides a roadmap for implementing improved WLAN security. Not surprisingly, an authentication server - long a cornerstone of remote access security - plays a pivotal role in securing an 802.1x WLAN. And, new 802.1x security methods provide strong authentication and data privacy techniques to fully secure WLAN access. This paper:

- Outlines the specific issues which characterize WLAN security, and describes how 802.1x addresses them
- Describes the role of an authentication server and 802.1x security methods in securing WLANs
- Demonstrates some tools out in the wild that are available for use on WLANs

The Benefits and Drawbacks of Wireless LANs

The demand for WLAN access has surged dramatically over the past year. Users are clamoring for WLAN access because it allows them to access their network and the Internet from anywhere in the workplace, without having to "plug in." Administrators are attracted to WLANs because they're easier to install (no cable to pull through walls and ceilings), they're flexible (they can be installed in places that wired LANs can't, and don't require rewiring when seating or office plans change), and, in part owing to this flexibility, they're less expensive to maintain over the long-term.

For these reasons, experts expect the WLAN market to grow steadily, even in the face of an economic downturn. Cahners projects that WLAN revenues will grow to \$4.6 billion by 2005; WLANs have already made significant penetration into the education, hospitality, healthcare and financial industries, and continually decreasing equipment prices should help drive adoption in other industries. Even owners of public meeting places - now known in the industry as hotspots are trying to get into the act. Coffee shops, airline lounges and libraries are just a few of the venues offering WLAN access to their patrons, enabling their customers to make better use of what used to be mandatory unconnected time.

WLAN Architecture and Security Challenges

As with any technology shift, migrating users to WLANs has its drawbacks. The initial investment in hardware may be significant and somewhat irksome: Organizations will have to deploy multiple wireless access points, and outfit every user with wireless network cards when most will already have perfectly good NIC cards for the wired LAN.

But the chief concern in migrating to WLAN access is security. Physical wires turn out to be one of the primary obstacles to attackers looking to hack their way onto a LAN. It's unlikely that a stranger plugging into a corporate network would go unchallenged, either by network security that's already in place, or by surrounding workers.

On a WLAN, of course this obstacle disappears. Instead user credentials and data are broadcast from both the client and the wireless access point (AP) in a radius which may reach 300 feet or more.

Of course, the fact that data is being broadcast via radio waves rather than transmitted over a wire introduces security challenges namely:

- How can you prevent user credentials from being hijacked during authentication negotiation?
- Once authentication is complete, how can you protect the privacy of the data being transmitted between client and access point?
- How can you make sure the authorized user connects to the right network?

We'll discuss each of these challenges in turn.

Authentication

Most password-based protocols in use today rely on a hash of the password with a random challenge. Thus, the server issues a challenge, the client hashes that challenge with the password and forwards a response to the server, and the server validates that response against the user's password retrieved from its database. This general approach describes CHAP, MS-CHAP, MS-CHAP-V2, EAP/MD5-Challenge, and EAP/One-Time Password.

The problem with such an approach is that an eavesdropper that observes both challenge and response can mount a dictionary attack, in which random passwords are tested against the known challenge to attempt to find one which results in the known response. Because passwords typically have low entropy, such attacks can in practice easily discover many passwords.

While this vulnerability has long been understood, it has not been of great concern in environments where eavesdropping attacks are unlikely in practice. For example, users with wired or dial-up connections to their service providers have not been concerned that such connections may be monitored. Users have also been willing to entrust their passwords to their service providers, or at least to allow their service providers to view challenges and hashed responses which are then forwarded to their home authentication servers, using for example, proxy RADIUS, without fear that the service provider will mount dictionary attacks on the observed credentials. Because a user typically has a relationship with a single service provider, such trust is entirely manageable.

With the advent of wireless connectivity, however, the situation changes dramatically. Legacy password protocols are easily subjected to eavesdropping and man-in-the-middle attacks. An eavesdropping attacker can easily mount a dictionary attack against such password protocols. A man-in-the-middle attacker can pass through the entire authentication, then hijack the connection and act as the user.

Data Privacy

Another concern is the security of the wireless data connection between the client and access point subsequent to authentication. While client and access point could easily negotiate keys subsequent to authentication, if the keys are not cryptographically related to the prior authentication the data session would be subject to a man-in-the-middle attack. For example, Diffie-Hellman key exchange is not secure against such an attack unless the public keys that are exchanged are themselves authenticated. Therefore it is incumbent upon the authentication negotiation to result in keys that may be distributed to both client and access point to allow the subsequent data connection to be encrypted.

Rogue Access Points

A final security challenge results from the possibility that someone could install a WLAN access point and network and fool your user into doing work on that network. Such a scenario is not entirely far fetched, and mutual authentication techniques - wherein the WLAN client authenticates the network he's connecting to - must be in place to guard against such practices.

Early WLAN Implementations

The first WLAN implementations - designed primarily for home use - did little to address these security issues. 802.11b, published in 1999, was the first IEEE draft outlining specifications and protocols for WLAN connections with LAN-equivalent speed and security. More popularly known as Wi-Fi (wireless fidelity), 802.11b provides for wireless transmission rates of 11Mbps.

In 802.11b WLAN solutions, user authentication happened in the clear, via the WLAN device's unique Media Access Control (MAC) address. Each AP contained a database of each authorized client's MAC address; if the client's MAC address was present in the AP's database, the user was granted access to the network. Of course, this left a user's MAC address exposed; anyone sniffing the network could see a valid MAC address being broadcast (and re-set his own device to that address). Plus, if the user's client device was stolen, the thief would have all the credentials he or she needed to access the network (without having to know or guess a username and password).

In addition to the security problems this method introduced, it also didn't scale well. The MAC address for each user must be stored on each AP on the wireless LAN, creating a cumbersome management scenario and increasing the possibility of security breaches due to administrative oversight.

Data privacy was provided for via a sub-protocol called wired equivalent privacy, or WEP, intended to provide the same level of security found in a wired LAN. As it turned out, first generation implementations of WEP did not provide this level of security. In fact numerous published reports, the latest prepared by AT&T, demonstrated convincingly that WEP was easily cracked, seriously breaching the privacy of any wireless data transmission.

The problem with WEP

In WEP, both the client and the AP have the same 40-bit encryption key - a "shared secret" between them. When the client attempts to authenticate, the AP issues a random challenge, which the client returns, encrypted with the key and a 24-bit initialization vector (IV) intended to randomize part of the key, using the RC4 PRNG encryption algorithm. The AP decrypts this encrypted challenge and, if it matches the original challenge, the client is authenticated.

The chief vulnerability of WEP results from the constant encryption key, the small IV, and the high speed of the connection. Theoretically, at the maximum transmission speed of 11Mbps, the system will be forced to refuse an IV within five hours; in practice, regardless of slower speeds resulting from heavy traffic and overhead, the system is still guaranteed to reuse any encryption key within 24 hours. Because the encryption key never varies, this means that in a maximum of one day an attacker can collect two packets encrypted with the same key, which the attacker can subsequently reverse-engineer to derive the encryption key.

Early attacks developed by the University of California at Berkeley and the University of Maryland took between eight hours and several days. A more recent study by the AT&T Labs outlines a modification of this technique that enables retrieval of the network key - hence, unrestricted access to the network's resources - in fifteen minutes or less.

The 802.1x Solution

802.1x is a next-generation draft of IEEE WLAN specifications and protocols written to address the security and management pitfalls of 802.11b. The 802.1x protocol provides subprotocols and methods for better protecting authentication and data transmission, including:

- An authentication process - such as a RADIUS server or access point-based authentication - to manage WLAN user authentication, connection attributes, and other matters related to setting up and securing the WLAN connection. While the 802.1x protocol does not recommend one authentication process over another, the market has overwhelmingly adopted RADIUS as the preferred authentication process on WLANs for several compelling reasons:
 - With RADIUS authentication is user-based rather than device based, so for example, a stolen laptop does not necessarily imply a serious security breach.

- RADIUS eliminates the need to store and manage authentication data on every AP on the WLAN, making security considerably easier to manage and scale.
- RADIUS has already been widely deployed for other types of authentication on the network.
- Extensible Authentication Protocol (EAP), and EAPoL (EAP over LAN) - EAPoL is the transport protocol used to negotiate the WLAN user's secure connection to the network. Security is handled by the vendor-developed "EAP authentication types", which may protect credentials, data privacy, or both.

Tools Available for use on WLANs

Radiate 802.11b frame handling (capturing, creation, injection) for use on Linux/BSD operating systems.

<http://www.packetfactory.net/projects/radiate/>

ApSniff is a wireless (802.11) access point sniffer for Windows 2000. It enables you to list all access points broadcasting beacon signals at your location. Useful for helping you set new access points making sure you do not have interfering APs, and helping you set-up wireless clients by providing you with the client configuration information. Requires WLAN cards of Prism 2 chipset. It works with a DLINK DWL-650 and linksys WPC11.

OS: Microsoft Windows 2000

<http://www.bretmounet.com/ApSniff>

Kismet is a 802.11b wireless network sniffer. It is capable of sniffing using almost any wireless card supported in Linux, which currently divide into cards handled by libpcap and the Linux-Wireless extensions (such as Cisco Aironet), and cards supported by the Wlan-NG project which use the Prism/2 chipset (such as Linksys, Dlink, and Zoom). Features Multiple packet capture sources, Runtime network sorting by AP MAC address (bssid), IP block detection via ARP and DHCP packet dissection, Cisco product detection via CDP, Ethereal and tcpdump compatible file logging, Airtsnort-compatible "interesting" (cryptographically weak) logging, and Secure SUID behavior.

<http://www.kismetwireless.net>

<http://www.nerv-un.net/~dragorn/kismet/>

© By: [Josh Glenn](#)