

Secure Authentication, Access Control, and Data Privacy on Wireless LANs

White Paper

November 2002



Funk Software, Inc.
222 Third Street
Cambridge, MA 02142
(617) 497-6339
<http://www.funk.com>

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 demonstrable 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 proved 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 such as EAP-TTLS in securing WLANs
- ♦ Demonstrates how Odyssey and Steel-Belted Radius, Funk Software's WLAN security solutions based on 802.1X, meet the functional and performance requirements for a secure WLAN environment

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.¹ 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 the 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.

¹ *Wild on Wireless Networking: WLAN Market Young, Energetic, and Growing* (Abstract), Cahners, March 2000.

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 easily 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 reuse 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 within 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.² A more recent study by AT&T Labs outlines a modification of this technique that enables retrieval

² Borisov, N., Goldberg, I., and Wagner, D. “Intercepting Mobile Communications: The Insecurity of 802.11; 2001.

of the network key – hence, unrestricted access to the network's resources – *in fifteen minutes or less.*³

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 vendor-developed "EAP authentication types", which may protect credentials, data privacy, or both.

EAP Authentication Types

Because WLAN security is essential – and EAP authentication types provide the means of securing the WLAN connection – vendors are rapidly developing and adding EAP authentication types to their WLAN access points. Some of the commonly deployed EAP authentication types include:

- ♦ *EAP-TTLS*. Funk Software and Certicom have jointly developed *EAP-TTLS* (Tunneled Transport Layer Security). EAP-TTLS offers the dual benefits of extremely strong security over the wireless link, while also being very easy to set up and manage. EAP-TTLS is an extension of EAP-TLS which provides for certificate-based, mutual authentication of the client and network. Unlike EAP-TLS, however, EAP-TTLS requires only server-side certificates, eliminating the need to configure certificates for each WLAN client. In addition, it supports legacy password protocols, so you can deploy it against your existing

³ Stubblefield, A., Ioannidis, J., Rubin, A. D. "Using the Fluhrer, Martin, and Shamir Attack to Break WEP:" AT&T Labs, August 21, 2001.

authentication system (such as tokens or Active Directories). It securely tunnels client authentication within TLS records, ensuring that the user remains anonymous to eavesdroppers on the wireless link and the entire network to the RADIUS server

- ♦ *EAP-TLS* (Transport Layer Security). EAP-TLS – the security method used in the 802.1X client in Windows XP – provides very strong security, but requires that each WLAN user be running a client certificate. It is generally appropriate for enterprises who have already deployed a PKI infrastructure. EAP-TLS provides for certificate-based, mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication; dynamically generated user- and session-based WEP keys are distributed to secure the connection. Windows XP includes an EAP-TLS client.
- ♦ *EAP-Cisco Wireless*. Also called *LEAP* (Lightweight Extensible Authentication Protocol), this EAP authentication type is used primarily in Cisco WLAN APs, including the Aironet Series. While easy to set up and manage, LEAP does not provide strong credential security over the wireless link, leaving password credentials vulnerable to dictionary attack. It encrypts data transmission using dynamically generated WEP keys, and supports mutual authentication.
- ♦ *EAP-MD-5 Challenge*. The earliest EAP authentication type, this essentially duplicates CHAP password protection on a WLAN. EAP-MD5 represents a kind of base-level EAP support among 802.1X devices. Because of significant security vulnerabilities, the use of MD-5 is not recommended for security-conscious enterprises.

It is likely that this list of EAP authentication types will grow as more and more vendors enter the WLAN security market, and until the market chooses a standard. (For example, Cisco and Microsoft will be introducing WLAN solutions based on EAP-PEAP, a strong WLAN protocol which offers a subset of the functionality found in EAP-TTLS.)

In general, you may wish to evaluate any EAP authentication type you're considering deploying based on the following functionality:

- ♦ *Does it provide adequate credential security?* Secure exchange of user information during the authentication process prevents stolen credentials and protects a user's locational privacy.
- ♦ *Does it permit mutual authentication of the client and the network?* Mutual authentication prevents an intrusion onto the network by an unauthorized user, and ensures that the client is connecting to the right network.
- ♦ *Does it require dynamic encryption keys?* Dynamically generated encryption keys that are different for every user and session significantly improve the security of users' data transmissions.
- ♦ *Does it support re-keying?* Re-keying – the generation of new keys at set intervals during a WLAN client's session – makes it virtually impossible for a would-be eavesdropper to break in on and decrypt a connection.
- ♦ *Is it easy to manage?* Ease of set-up and management is critical, particularly if you're deploying WLAN access to hundreds or thousands of users. For example, EAP-TLS requires client-side certificates – which you'll have to separately

configure and maintain for each WLAN client – while EAP-TTLS requires no client-side certificate configuration.

- ♦ *Can you easily implement it on your network?* Being able to deploy WLAN security against your existing infrastructure permits speedy roll-out of the new technology, and allows users to connect to a WLAN in their usual manner. For example, EAP-TTLS allows you to safely authenticate WLAN users against your existing Windows authentication databases.

WEP in 802.1X Environments

Note that 802.1X does not fix WEP. It makes no provisions or recommendations for an improved method of ensuring data privacy; in fact, WEP keys still form the basis of most WLAN connection encryption.

However, most of the EAP authentication types listed above – including EAP-TTLS – eliminate the problems introduced by the use of static WEP keys. When these EAP authentication types are in use, stolen or lost laptops no longer present a serious security problem. Instead, each user is issued a new key as part of the authentication process each time he connects; in addition, new keys may also be re-generated at set intervals (say, every 10 minutes) during a user's session. In practice, this rapid re-keying of WEP keys cures the problems with WEP. New encryption techniques will be introduced in the future which will cure WEP – in practice and in theory.

How RADIUS Works in the 802.1X Environment

In the most common 802.1X WLAN environments, the APs defer to the RADIUS server to authenticate users and to support particular EAP authentication types. The RADIUS server handles these functions, and provides crucial authentication and data protection capabilities according to the requirements of the EAP authentication type in use. Although some details will vary across EAP authentication types, the following steps provide a basic framework for how the transaction between the WLAN client and RADIUS server works to set up a secure WLAN connection:

1. The WLAN Client (called the “Supplicant” in IEEE documents) tries to access network. [EAPoL]
2. The AP (the “Authenticator”) responds to requests, and will ask client for identity. [EAPoL]
3. Client responds with identity to AP [EAPoL]
4. AP will forward Access-Request to RADIUS server with the user's identity. [RADIUS]
5. RADIUS server will respond with a challenge to AP. The Challenge will indicate the EAP authentication-type requested by the server [RADIUS]
6. AP forwards challenge to client [EAPoL]
7. If Client agrees to EAP-type, then negotiation will continue; if not, client will NAK request and suggest an alternative method. [EAPoL]

8. AP forwards response to RADIUS server. [RADIUS]
9. If these credentials are correct, the RADIUS server accepts the user. If not, the user is rejected. An Access-Accept or Reject is sent. [RADIUS]
10. If authentication succeeds, AP connects client to the network.

Because the RADIUS server plays such a central role in WLAN security – brokering client and AP authentication, and providing and enforcing any other security measures specified by the EAP authentication type – organizations looking to maximize the return on their WLAN investment should seek a RADIUS server that:

- ◆ Supports all existing EAP authentication types
- ◆ Supports multiple vendors' equipment, on a single WLAN, so that the organization can grow its WLAN by adding whatever equipment meets its requirements (instead of being tied to solutions provided by a particular vendor)
- ◆ Offers the performance and transaction capacity to support large-scale migration to WLAN, as well as increased transactions that accompany additional security techniques such as re-authentication.

Funk Software Solutions for Secure WLANs

Funk Software's RADIUS servers – Odyssey and Steel-Belted Radius – are uniquely suited to providing secure WLAN access. Depending on your requirements, you may find that a combination of Odyssey and Steel-Belted Radius presents the most functional and cost-effective solution.

- ◆ **Odyssey Server** – Odyssey Server is a RADIUS server specially designed to handle WLAN access control and security. It is ideally suited to smaller organizations or autonomous networks in larger organizations where network access is governed by Windows user names and passwords. Beyond being able to safely authenticate WLAN users against a Windows database and set up their secure connections, Odyssey Server can communicate with Steel-Belted Radius to authenticate WLAN users in branch offices or distributed departments against a central security infrastructure which may or may not be based on Windows.
- ◆ **Steel-Belted Radius/Enterprise Edition** – Steel-Belted Radius/Enterprise Edition is Funk Software's market-leading RADIUS server, and is uniquely capable of managing both remote and WLAN access and security. It provides the same high level of WLAN security that Odyssey provides, and extends that capability to remote users as well, ensuring that only authorized users can connect – whether they're connecting via VPN, dial, or firewall – and that they receive the appropriate level of access. Plus, Steel-Belted Radius lets you authenticate your remote and WLAN users against a wider variety of back-end authentication systems, including token systems and LDAP-based user name and password stores. Finally, Steel-Belted Radius fully supports RADIUS accounting, so you can easily track and document remote and WLAN user access.

- ♦ **Steel-Belted Radius/Global Enterprise Edition (GEE)** – Steel-Belted Radius/GEE extends the capabilities of Steel-Belted Radius/Enterprise Edition to meet the security management needs of global enterprises who are managing thousands of remote and WLAN users across multiple sites. In addition to offering all the capabilities of Steel-Belted Radius/Enterprise Edition, Steel-Belted Radius/GEE permits sophisticated distribution of authentication and accounting requests – to easily handle centralized management of far-flung users, and seamlessly integrate new users acquired, for example, as a result of a merger. Plus, it supports the advanced reliability features you need to ensure 99.999% uptime, and is easily managed from an SNMP-based network monitoring system.

Whatever Funk Software RADIUS server is appropriate to your network, you'll find that each offers:

- ♦ **Support for EAP and strong EAP authentication types** – and support for new protocols as they emerge. Odyssey Server and Steel-Belted Radius support EAP, and the EAP-TTLS, EAP-TLS, and EAP-Cisco Wireless (LEAP) authentication types.
- ♦ **Broad multi-vendor support.** Odyssey and Steel-Belted Radius reflect the broad multi-vendor support that has always been the hallmark of Funk Software's RADIUS products. Odyssey Server and Steel-Belted Radius support all 802.1X-compatible access points, including Cisco Aironet Series 340/350, Agere's AP 2000, and Enterasys access points.

And, Odyssey Server and Steel-Belted Radius support a wide variety of WLAN environments, and are compatible with other 802.1X solutions. For example, Odyssey Server can manage connections from Microsoft or Cisco 802.1X clients you may have already deployed.

- ♦ **Support for multiple EAP authentication types on a single WLAN.** Odyssey and Steel-Belted Radius allow different sets of users to use different EAP authentication types, on the same WLAN. This gives the WLAN administrator the flexibility to vary equipment based on the security needs of individual users – and build out the WLAN in whatever way best meets overall security, performance, and budgetary goals.

In addition, when EAP-TTLS is in use, Odyssey and Steel-Belted Radius provide compelling management benefits, making it the easiest 802.1X security solution to deploy across your enterprise.

- ♦ **Unsurpassed security.** Odyssey and Steel-Belted Radius employ advanced security techniques, both during user authentication and for the session duration to prevent unauthorized access to your network, and eavesdropping on the connection.

EAP-TTLS allows users to be authenticated onto WLANs with their existing password credentials, and, using strong public/private key cryptography, to protect those password credentials against eavesdropping and other attacks that are suddenly made possible by the advent of wireless communications.

And, Odyssey and Steel-Belted Radius generate dynamic per-session keys to encrypt the wireless connection and protect data privacy. Odyssey and Steel-

Belted Radius can be configured to re-authenticate and thus re-key at any interval; frequent re-keying thwarts known attacks against the encryption method used in wireless communications (WEP).

- ♦ **Easiest deployment, with no client certificates required.** Odyssey and Steel-Belted Radius let you avoid the substantial administrative burden in operating a certificate authority to distribute, revoke, and otherwise manage user certificates that 802.1X solutions based on EAP-TLS require. Instead, Odyssey and Steel-Belted Radius provide extremely strong security, while allowing users to connect with their usual usernames and passwords.

Safe deployment against any authentication database. Odyssey and Steel-Belted Radius offer different options for where you authenticate your WLAN users.

Choose Odyssey if you need to authenticate WLAN users against a Windows authentication database (Windows XP or Windows 2000 Native Domain, Windows NT Domains).

Choose Steel-Belted Radius if you need to authenticate WLAN and remote users against Windows, as well as databases based on SQL/LDAP, token systems such as RSA Security's ACE/Server, TACACS+, NIS/NIS+ (if running on Solaris), and a native database.

Odyssey can also forward WLAN user authentication requests to Steel-Belted Radius for authentication against any of the back-end databases Steel-Belted Radius supports. This feature is important for two reasons:

- ♦ **Performance** – WLAN security is computationally intensive. To enhance performance, you can add Odyssey Servers to handle the security computations, while optionally have them forward to Steel-Belted Radius for user authentication.
- ♦ **Cost** – Odyssey costs less than Steel-Belted Radius. So, you may wish to deploy Odyssey Server on distributed WLANs around your enterprise, and have them communicate with Steel-Belted Radius at the central site.
- ♦ **Multi-platform.** Odyssey Server runs on Windows XP/2000 (Server and Professional); Steel-Belted Radius runs on XP/2000/NT and Solaris, for compatibility in your network environment.

Odyssey Client

The final component of Funk Software's suite of WLAN security products is Odyssey Client. Odyssey Client runs on a wireless device and lets the user securely connect to the WLAN. It:

- ♦ **Supports strong EAP authentication methods for maximum security** – including EAP-TTLS and/or EAP-TLS.
- ♦ **Is easy to deploy and manage** – Odyssey Client provides unsurpassed multi-platform and multi-vendor support of 802.1x-compliant WLAN adapter cards. It

also offers numerous auto-configuration tools so you can streamline large-scale deployments of WLAN access and mandate enterprise-level security.

- ♦ **Protects confidentiality of user credentials** – Odyssey Client fully protects users' identities between the client node and the trusted network, to protect their locational privacy against surveillance, undesired acquisition of marketing information, and other intrusions from monitoring and eavesdropping.
- ♦ **Provides multi-platform compatibility** – Odyssey Client runs on Windows XP, 2000, 98, and ME, for compatibility in your network environment.

Conclusion

Organizations who deferred migrating to WLANs because of security can now safely do so by implementing 802.1X WLANs which implement advanced security techniques and which are managed by a RADIUS server.

Funk Software's Odyssey and Steel-Belted Radius are ideally suited to this role. They support the innovative and advanced EAP-TTLS authentication type, providing extremely secure WLAN access that's easily managed. And, Both products reflect the high quality, multi-vendor support, and scalability that have been the hallmarks of Funk Software's RADIUS/AAA products since 1996. These characteristics help ensure a maximum return from an organization's WLAN investment.

For more information on Odyssey or Steel-Belted Radius, contact Funk Software at 1-800-828-4146 (US/Canada) or 1-617-497-6339.



Funk Software, Inc.
222 Third Street
Cambridge, MA 02142 USA
(617) 497-6339
www.funk.com