



The Security Division of EMC

White paper

# Securing WLANs with Two-factor Authentication



# “What are the security issues wireless LANs create?”

Wireless Local Area Networks (WLANs) offer the promise of tremendous workplace flexibility – but they also potentially pose risks to enterprise information. Anytime, anywhere access to enterprise applications and data throughout headquarters or regional offices extends the IT infrastructure to cover the entire work area of an organization.

WLANs present a particularly vulnerable point of attack – one that is surprisingly easy to compromise if WLANs are not properly implemented. Improperly designed WLANs leave organizations exposed to the risk of unauthorized access, and protecting WLANs is key to the successful deployment of wireless

infrastructure. Organizations should identify and address key security issues so they can safely support the inevitable movement to wireless computing while protecting the data that flows through WLANs.

Strong, two-factor authentication allows organizations to easily secure WLANs while granting secure access to authorized users. This white paper discusses the explosion of enterprise WLANs and reviews enterprise needs to protect information in transit over wireless networks. It reviews the standards-based security protocols available, explains the limitations of passwords and discusses the importance of strong, two-factor authentication to secure enterprise WLANs.

---

## Contents

---

Managing the Explosive Growth of LANs	page 1
Drivers for WLAN Implementations	page 1
The Need for WLAN Security	page 2
Securing WLANs	page 2
Implementing Strong Two-factor Authentication for WLANs	page 4
Integrating WLAN and Wired Authentication	page 6
Conclusion	page 6

---

## Managing the Explosive Growth of LANs

---

In just a few short years, enterprise networks have swiftly deployed wireless technology to improve employee access to information. Employees expect – and may even demand – wireless networks that provide them with the freedom to do their jobs no matter where they are located throughout the enterprise.

Many employees are familiar with Wireless Local Area Networks (WLANs) from having deployed them at home to provide wireless connectivity throughout the household. WLAN products are available through retail channels and can be easily installed to allow households to share Internet access, files and peripherals. A user can just install a wireless Access Point (AP) to a router or to a cable or DSL modem, install a wireless access card into a PC or laptop, set a few configurations and create a WLAN.

But residential users generally do not have the same security concerns that face enterprise networks. Residential WLANs are generally configured with only minimal security – or no security at all. But enterprise networks are only as safe as their weakest link, and a non-secure WLAN can have catastrophic effects on network security. Enterprise networks that offer WLAN access must be secured against hackers, and they must be protected to ensure the enterprise maintains an ongoing audit trail of user access to important applications and information. Organizations deploying WLANs need to be able to mitigate against the risk of unauthorized users gaining access to the enterprise network.

But this can be done efficiently and cost effectively by relying on standard WLAN security protocols and strong, two-factor authentication, which combines something you know – a Personal Identification Number (PIN) – and something you have – the constantly changing code on a hardware or software token. Users can be granted secure WLAN access to the same information they can access from a wired connection to their desktops, and the enterprise can safely deploy wireless connectivity to authorized users. Secure WLAN access allows organizations to:

- Increase productivity: Employees can be productive wherever they are within the enterprise. They can use their laptops in a conference room or in a cafeteria, and create ad-hoc meetings wherever the space is available.

- Reduce networking costs: Organizations no longer need to hard-wire every desktop with Ethernet cable. They can avoid the costs and delays of running Category 5 cabling to the desktop by providing WLAN access to workers in both headquarters and remote office locations.
- Ensure compliance: Audit trails and strong, two-factor authentication provide the reporting needed to document security and comply with regulatory requirements.
- Process automation: Many manual tasks can be automated by the use of WLANs. For example, medical offices can have patients fill out records at an online kiosk, or a warehouse can be automated to support real-time inventory management.

---

## Drivers for WLAN Implementations

---

Investigating the drivers of the WLAN phenomenon reveals several good reasons why Information Technology (IT) departments are rapidly deploying WLANs:

- Prices for WLAN gear have been dropping sharply and hardware vendors are increasingly embedding wireless capabilities directly into off-the-shelf products.
- Deploying WLANs is far cheaper than setting up wired LANs, and a lot easier too. There is no need to fish wires through and around walls, and no need to move individual workers to make room for the cabling. Thus, WLANs have a relatively low total cost of ownership.
- New hardware is making the mobile computing experience more compelling and productive than ever before, fueling demand at the most fundamental, grass roots user levels. Once users experience the freedom of anywhere/anytime computing, they do not want to return to the fully tethered desktop world.
- iWireless standards and protocols governing bandwidth, security and other aspects of WLAN operations are emerging quickly.

Vertical applications of WLAN technology are increasing, as many industries find major opportunities to reduce network operating costs, improve productivity and automate workflows. For example, manufacturing, warehousing and logistics businesses have used WLANs for years to improve order processing and to deliver self-service tools to the plant floor. In addition, new markets – including healthcare, finance, retail and education – are aggressively introducing wireless applications.

In healthcare, a sector under extreme pressure to control costs, WLANs allow caregivers to access real-time patient information and clinical records without third-party intervention. Financial markets are exploiting WLAN technologies in bank and brokerage offices, giving employees mobility that greatly improves service to customers. WLANs also support the business continuity and disaster recovery initiatives of financial services institutions by enabling fast network setup in a new location if needed.

The retail sector is seeing the value of easily deploying checkout registers throughout a store using wireless technology. WLANs also allow for the instant tracking of products on store shelves with real-time updating of inventory data. And on college campuses, WLANs can give students and educators access to the network from any classroom, lab, dorm or library. The practical applications of WLANs are exciting, but they are fraught with potential security risks that must be carefully managed to enable safe and secure WLAN access.

---

## The Need for WLAN Security

---

With users realizing major benefits and with WLAN equipment vendors responding with more affordable pricing, it is easy to gain a glorified view of this hot sector of the IT market. However, it is actually one of the most attractive features of WLANs – their ease of deployment – that is causing the greatest concern with security-conscious managers.

For very little expense and without any significant technical expertise, departmental users can set up WLANs that can potentially expose the enterprise network. Enterprises continue to battle the installation of these unauthorized or “rogue” WLAN APs on corporate networks. Departmental employees likely install the increasingly inexpensive APs in well-intentioned efforts to support departmental mobility, but they usually do not focus on the potential security risks.

Security experts and IT managers universally agree that companies need to institute strong security policies that are designed to guarantee that only authorized users are granted access to information. The reality today is that unauthorized users can and do access unprotected or poorly protected WLANs. In fact, well-intentioned users may even “borrow” access to a WLAN to surf the web, send email or access their own corporate network.

The massive growth of public “hotspots” means there are a great many mobile users accustomed to seeking Internet access throughout their workday. Near these hotspots are significant numbers of unprotected business networks that are clearly not hotspots but still offer access to those who might accidentally or intentionally connect to them. This has added a new and disturbing dimension to the wireless security problem; the massive growth of hotspots for mobile users means that there are large numbers of mobile users who are frequently seeking connections throughout their travels. This introduces an even greater threat to regular business users of wireless networks who are operating them with little or no security. Fueled by the availability and profusion of hotspots, mobile users expect to find wireless networks – and know how to connect to them.

Organizations also have to be wary of fake, temporary hotspots, designed to attract connections and steal login, username and password details. A hacker can easily set up a bogus, temporary WLAN near an office to capture this critical login information, since unsuspecting users will likely enter the requested information on the assumption that it is being demanded by the enterprise network.

A network breach can have major impact on an organization. It can result in:

- Direct and indirect financial loss
- Loss of customer confidence
- A decline in brand value and corporate reputation
- Litigation
- Loss of revenue
- Government regulatory action should the breach involve data the organization is obligated to protect, such as patient information that must be protected by healthcare organizations

It is prudent for organizations to establish security policies to protect end-to-end access to information, and to protect WLANs against intrusion by unauthorized users.

---

## Securing WLANs

---

In the simplest terms, securing data in wireless networks focuses on two aspects:

- The encryption of the data itself
- The authentication of network users

### A Study of WLAN Security

RSA Security recently conducted its annual survey of wireless networking technology adoption and wireless security in London, New York, San Francisco and Frankfurt. Frankfurt had the best security level, since 66 % of its corporate networks had some level of security. A close look at just one of the cities sampled offers some startling statistical insights. In San Francisco, over a third of all business networks discovered were found to be unsecured, 28% of all APs were found to be displaying default values and 31% of the APs discovered in San Francisco were unprotected by encryption.

Wireless users want the same kind of access to business-critical data they can get from a traditional hard-wired environment. Getting that data to the right person securely is the challenge at hand. There are emerging standards and protocols that characterize efforts to help make WLANs more secure and implementers have several choices. They include the following:

#### Simple 802.11 – Wireless LANs Without Security

The 802.11 IEEE standard defines how devices communicate with one another in a wireless environment. In its simplest form, 802.11 handles the sending and receiving of unencrypted data over the air. Most APs come preconfigured in this manner as a default. This is an open invitation for anyone with an 802.11 compatible wireless client device to drive by and view your data as it travels the airwaves, or to hop onto an enterprise network and browse around.

#### 802.11 with Wired Equivalent Privacy

The 802.11 standard also includes a provision to send and receive encrypted data. The Wired Equivalent Privacy (WEP) is an optional method for two wireless devices to share a secret key that is used by an algorithm to encrypt and decrypt data. While turning on the WEP feature is better than no encryption at all, there are functional and operational limitations that should be understood before doing so. Because WEP uses a shared secret, each client and AP must be manually configured, placing a burden on the network administrator. Due to their static nature and the

fact they are generally used for extended periods, shared secrets provide hackers with a relatively easy opportunity to capture, analyze and eventually decrypt packets. WEP is insufficient for protecting enterprise networks, since it offers limited device authentication – and does not offer user authentication.

#### 802.1x and Extensible Authentication Protocol

Recognizing the limitations of 802.11 and WEP, the IEEE developed a new standard. This new protocol, which has been adopted by many well-recognized providers of wireless technology including Microsoft®, Cisco®, Juniper Networks® and others, is called 802.1x and it relies on the Extensible Authentication Protocol (EAP) to provide both user authentication and a stronger method of implementing shared keys for encryption.

EAP significantly enhances user authentication in a wireless network by providing a method to challenge the user for identification. Unlike WEP, it provides for user authentication and does not rely on the shared secret to prove identity. The EAP protocol makes provisions for various forms of user authentication including password, tokens and digital certificates. There are several implementations of EAP, including:

**Lightweight EAP (LEAP).** This proprietary implementation is used in the Cisco® Aironet® solution. It provides for fixed password user authentication and supports dynamic WEP key generation.

**Protected EAP (PEAP).** This was co-developed by Cisco, Microsoft and RSA Security. PEAP makes it possible to authenticate WLAN clients without requiring them to have certificates, thereby simplifying the architecture of secure WLANs. It also supports dynamic WEP key generation and provides options for password, token or digital certificate based user authentication.

**EAP Tunneled Transport Layer Security (EAP-TTLS).** This protocol was developed by Juniper Networks and is a competing standard very similar to PEAP. It also supports password, token or certificate-side user authentication.

When 802.1x is deployed, the wireless client must first authenticate against an authentication server, such as a Remote Authentication Dial-In User Service (RADIUS) server. If the enterprise has opted for strong, two-factor authentication, the user can fill in his/her PIN and the code on an RSA SecurID® token at that moment, and the RADIUS server will proxy the authentication request off to the RSA® Authentication Manager.

Once authenticated successfully, the AP will allow access to the network and permit other types of communication to be transmitted. EAP/TTLS and PEAP both support token authentication and the RSA SecurID solution is designed to work out of the box with the Cisco Secure Access Control Server® and with the Juniper Networks Steel-Belted Radius® authentication servers.

EAP also makes provisions for dynamic encryption key generation that goes a long way toward solving the problems associated with shared key distribution. With EAP, the keys are dynamically generated and shared after the user has been authenticated. In spite of many security improvements, 802.1x and EAP still have drawbacks that should be carefully considered before moving forward. The major concern is the requirement to install software on every client's desktop.

Deploying software in a large user environment can be an unwieldy and expensive proposition. To help with this problem, some of the leading operating system vendors are including or planning to include wireless client software with their offerings, but IT departments and users must be sure that it will be compatible with the version of EAP deployed to authenticate users. Enterprise networks are best served by deploying a configuration that includes 802.1x and EAP with a strong, two-factor authentication solution that only provides access to WLANs to authorized users.

---

## Implementing Strong Two-factor Authentication for WLANs

---

Passwords are easily forgotten and simple to steal – particularly over wireless networks where they can be “sniffed” out. Good passwords are comprised of complicated combinations of letters, numbers and special characters that make them difficult to guess – and difficult to remember. An effective password policy requires a user to change passwords on a regularly scheduled basis, but the combination of numerous, hard to remember passwords and strict password policies puts a strain on the end user and causes an ever-increasing number of password-related calls to the help desk.

The deployment of strong, two-factor authentication with WLANs that support EAP protocols allows the enterprise to secure WLANs. Organizations can deploy RSA SecurID tokens to users that provide a constantly changing passcode that a user enters with his-or-her PIN to gain network access.

### A Brief Look at the 802.11 Protocols

IEEE 802.11 refers to a family of specifications developed by the IEEE for wireless technology. 802.11 specifies an over-the-air communication between wireless units (client/AP, AP/AP, client/client). The IEEE first accepted the specification in 1997, and there are currently several components of the 802.11 specification:

- 802.11 applies to WLANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band.
- 802.11a is an extension to 802.11 that provides up to 54 Mbps in the 5 GHz band.
- 802.11b is an extension to 802.11 that provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band.
- 802.11d is a wireless communications specification for use in countries where systems using other standards in the 802.11 family are not allowed to operate. It is well-suited for the systems that want to provide global roaming because although it is like 802.11b in many aspects, the MAC layer configuration allows it to comply with the rules of the country in which the network is being used.
- 802.11e is a proposed enhancement to the 11a/b specifications to offer Quality of Service (QoS) through prioritization of protocols used for voice, video and data communications.
- 802.11g provides 20+ Mbps in the 2.4 GHz band, and is the most popular protocol. It is being deployed widely today throughout the world.
- 802.11i provides improved encryption for networks that use the 11a, b and g standards at present. The new protocols, namely the Temporal Key Integrity Protocol (TKIP) and the Advanced Encryption Standard (AES), are required in any such 11i implementation.

Each user is provided a hardware-based token small enough to attach to a key chain, and it displays a new access code every 60 seconds. The user just needs to key in the access code and his-or-her PIN to gain secure WLAN access. Organizations can also distribute software-based tokens that can allow wireless devices such as smart phones or personal digital assistants to authenticate. There are two implementation options for strong, two-factor authentication to WLANs:

- Virtual Private Network (VPN) WLAN access
- Native WLAN access

Both of these implementations rely on strong authentication, but the VPN implementation requires client software loaded on PCs to create a secure, encrypted tunnel while the native implementation relies on the Wi-Fi Protected Access (WPA) protocol, a new standard for wireless networks that is included with the 802.1x protocols and is much more secure than WEP.

#### VPN WLAN Access with Two-factor Authentication

For many organizations, installing a VPN solution over the wireless network is ideal. This option is particularly attractive for organizations that have already implemented VPNs with two-factor authentication for remote access because it allows users to access the WLAN similarly to how they would access the enterprise network while working from home or traveling.

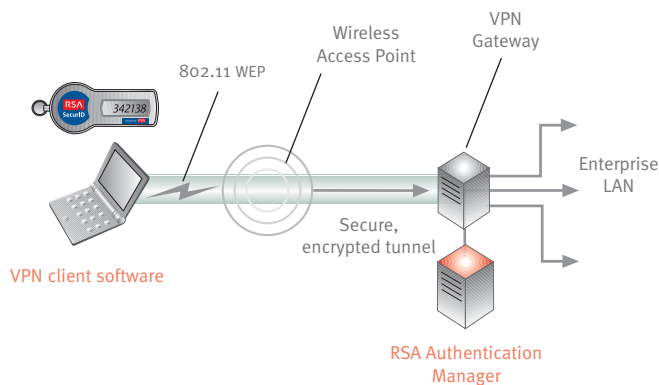


Figure 1: Wireless users can access the VPN gateway through a wireless access point, which passes along the authentication request to the RSA Authentication Manager. Authorized users are granted access to enterprise LANs via wireless connections.

VPNs provide a strongly encrypted connection between two end points over an insecure network. They are routinely used to secure data as it travels between remote users and a corporate server via the Internet, and they offer the additional function of ensuring that the data has not been tampered with during transit by providing a checksum function that compares “what was sent” to “what was received” to detect any differences.

In a wireless network configured in this manner, the client device – the “supplicant” in wireless terminology – would make a connection to the wireless AP that would connect the user to the VPN gateway, which would initiate an authentication request to an RSA Authentication Manager. The current version of the RSA Authentication Manager includes a limited edition RADIUS server based on Juniper Steel-Belted Radius, so organizations can authenticate users via the 802.1x-compatible RADIUS server that comes packaged with RSA Authentication Manager. Alternatively, they can use a separate, standalone RADIUS server if needed, such as in environments supporting very large numbers of WLAN users that require multiple authentication methods.

Once the authentication is successfully completed, the VPN would pass the session encryption key to the user. All communication between the network and the user would pass through the gateway and be encrypted/decrypted using the shared secret.

In this environment, user authentication is critical. Recognizing this, most of the leading VPN gateway vendors have made provisions within their products to accommodate two-factor authentication such as that provided by the RSA SecurID authentication solution. For example, leading companies such as Juniper, Check Point and Cisco have completed the RSA Secured® program to help ensure their products interoperate with RSA SecurID solutions.

#### Native WLAN Access with Two-factor Authentication

While VPNs provide an attractive alternative to securing WLAN access, they should not be installed without giving serious consideration to the overhead imposed by VPNs. Advances in standardized security protocols allow the enterprise to benefit from secure, native WLAN access without the need to distribute and manage client-side VPN software.

WPA is a newer protocol that was developed as a replacement for the less-secure WEP standard, and it was designed for use with an 802.1x authentication server. WPA addresses many of WEP's security and privacy concerns, significantly increasing the level of data protection and access control for WLANs. Unlike WEP, WPA is a dynamic encryption system that uses rekeying and per-station keys, making it much more difficult for hackers to grab packets and decipher keys. It also improves data encryption by incorporating the Temporal Key Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and adds integrity-checking features to ensure that keys have not been tampered with during transmission.

Organizations can avoid the overhead of VPNs and allow users to prove their identities via strong, two-factor authentication. When a user attempts to access the WLAN, a wireless client communicates over an EAP variant to the AP, which either requests authorization from the RSA Authentication Manager and its on-board RADIUS server, or through a standalone RADIUS server to the RSA Authentication Manager.

The RSA SecurID authenticator combines a unique seed record with the current time-of-day to generate a pseudo-random token code. When prompted for a token code, a user simply enters the PIN followed by the code displayed on the token. The two factors – the PIN and the token code – combine to enable two-factor authentication.

The RSA Authentication Manager identifies the user and runs the same algorithm using the user's unique seed record and the current time-of-day to perform a comparison and either grant or deny access. Authorized users are provided with secure wireless connectivity and allowed to access the same enterprise resources they could access as if they were logged in through a wired connection.

## Integrating WLAN and Wired Authentication

The RSA SecurID solution can be deployed to support both WLAN and wired authentication at the same time. RSA SecurID hardware and software tokens can be used for wired, wireless and remote access, and RSA Authentication Manager can authenticate users whether they are attempting to connect via the Ethernet LAN, the WLAN or the Internet. A single token can provide an authorized user with flexible access to the network, and organizations can centrally manage policy-based, secure authentication for WLAN, wired and remote users.

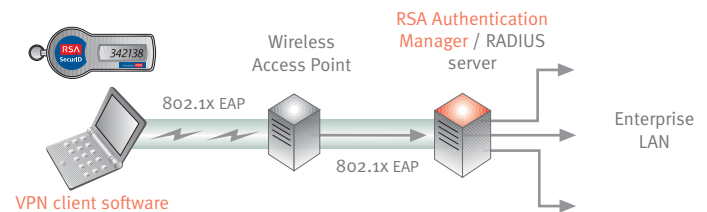


Figure 2: Enterprise networks can leverage advances in EAP with two-factor authentication to simplify WLAN security and streamline network operations.

## Conclusion

While advances in wireless protocols have made major improvements in enabling WLAN security, two-factor authentication is crucial to protecting wireless networks from intrusion. Organizations can deploy wireless VPNs or can offer native WLAN access without the need to deploy and manage VPN client software, and they can implement two-factor authentication to deliver the easy-to-use security necessary to drive widespread adoption of WLANs. The combination of 802.1x standards, the EAP standards, WPA and RSA SecurID solutions allow organizations to deliver secure access to critical corporate assets while protecting data during transit in a wireless world.

### About RSA

RSA, The Security Division of EMC, is the expert in information-centric security, enabling the protection of information throughout its lifecycle. RSA enables customers to cost-effectively secure critical information assets and online identities wherever they live and at every step of the way, and manage security information and events to ease the burden of compliance.

RSA offers industry-leading solutions in identity assurance & access control, encryption & key management, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit [www.RSA.com](http://www.RSA.com) and [www.EMC.com](http://www.EMC.com).



RSA Security Inc.  
RSA Security Ireland Limited  
[www.rsa.com](http://www.rsa.com)

The Security Division of EMC

RSA, the RSA logo and SecurID are registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC is a registered trademark of EMC Corporation. All other products or services mentioned are trademarks of their respective owners. ©2006-2007 RSA Security Inc. All rights reserved. WLAN WP 0607