Microsoft Solutions for Security

Choosing a Strategy for Wireless LAN Security

Microsoft®

Choosing a Strategy for Wireless LAN Security

Introduction

Wireless Local Area Network (WLAN) technology is a controversial topic. Organizations that have deployed WLANs are concerned about whether they are secure; those that have not deployed them are worried about missing out on user productivity benefits and lower ownership costs. There is still a good deal of confusion about whether a WLAN is safe to use for corporate computing.

Ever since weaknesses in first generation WLAN security were discovered, analysts and network security firms have strived to resolve these problems. Some of these efforts have contributed significantly to the cause of wireless security. Others have had their share of flaws: some introduce a different set of security vulnerabilities; some require costly proprietary hardware; and others avoid the question of WLAN security altogether by layering on another, potentially complex security technology such as virtual private networks (VPN).

In parallel, the Institute of Electrical and Electronic Engineers (IEEE), along with other standards bodies and consortia, have been diligently redefining and improving wireless security standards to enable WLANs to stand up to the hostile security environment of the early twenty–first century. Thanks to the efforts of standards bodies and industry leaders, "WLAN security" is no longer an oxymoron. WLANs can be deployed and used today with a high level of confidence in their security.

This document introduces two WLAN security solutions from Microsoft® and answers the questions about whether WLANs can be secure and which is the best way of securing them.

Overview of Wireless Solutions

The main objective of this document is to help you decide on the most suitable method of securing WLANs in your organization. To do this, the document deals with four main areas:

- The arguments for wireless LANs (and the security concerns associated with them)
- Using secure WLAN standards
- Alternative strategies such as VPN and Internet Protocol security (IPsec)
- Selecting the right WLAN options

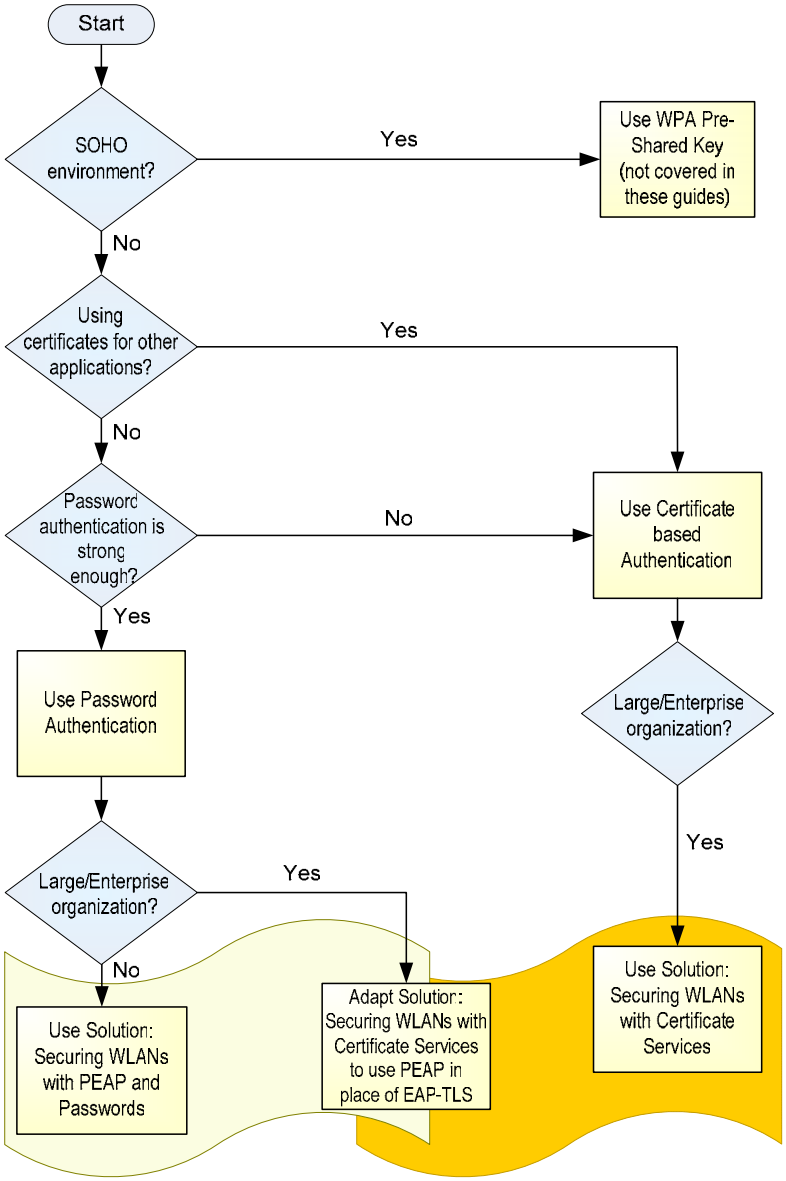
Microsoft has produced two WLAN solutions, based on open standards from bodies such as the IEEE, the Internet Engineering Task Force (IETF), and the Wi–Fi Alliance. The two solutions are titled *Securing Wireless LANs—A Windows Server 2003 Certificate Services Solution* and *Securing Wireless LANs with PEAP and Passwords*. As the names suggest, the former uses public key certificates to authenticate users and computers to the WLAN whereas the latter uses simple user names and passwords. However, the basic architecture of the two solutions is very similar. Both are based on Microsoft Windows® Server™ 2003 infrastructure and Microsoft Windows XP and Microsoft Pocket PC 2003 clients.

Although not apparent from the titles, the intended audiences for these solutions are different. The *Securing Wireless LANs—A Windows Server 2003 Certificate Services Solution* is aimed primarily at large organizations with relatively complex information technology (IT) environments; *Securing Wireless LANs with PEAP and Passwords* is significantly simpler and can be deployed easily by much smaller organizations.

This does not imply that password authentication is not usable by large organizations (or that certificate authentication is not suitable for smaller organizations), it simply reflects the type of organization where that particular technology is more likely to be used. The following figure shows a simple decision tree to help you select the solution appropriate for your organization. The three main options available are:

- Wi–Fi Protected Access (WPA) Pre–shared Key (PSK) for very small businesses and home offices.
- Password–based WLAN security for organizations that do not use and do not need certificates.
- Certificate–based WLAN security for organizations that need and can deploy certificates.

These options are explained later in this document, as is the possibility of merging the features of the last two options to produce a hybrid solution.



a. ***Figure 1: Decision Tree for Microsoft Wireless LAN Solutions***

The Argument for Wireless Networking

It is easy to understand the appeal of WLANs for businesses today. WLAN technology has been around in one form or another for nearly a decade, but it has singularly failed to hit the mark until relatively recently. Only when reliable, standardized, and low cost technology met the growing desire for more flexible ways of working and ever more pervasive connectivity, did WLAN adoption really start to take off. The rapid adoption of this technology, though, has also brought to light a number of serious security weaknesses with the first generation WLANs. This section looks at both the pros (the functionality) and cons (security) of WLANs.

Benefits of Wireless LANs

The benefits of WLAN technology fall into two main categories: core business benefits and operational benefits. Core business benefits include improved employee productivity, quicker and more efficient business processes, and greater potential for creating entirely new business functions. Operational benefits include lower costs of management and lower capital expenditure.

Core Business Benefits

The core business benefits of WLANs arise from the increase in flexibility and mobility of your workforce.

People are freed from their desks and can easily move around the office without losing connection to the network. It is helpful to look at some examples of how increased mobility and network flexibility can benefit businesses.

- Mobile workers moving between offices and telecommuters coming into the office, save time and heartache with transparent access to the corporate local area network (LAN). Connection is near–instantaneous and available from any physical location with wireless coverage and there is no need to hunt for network ports, cables, or IT staff to help connect you to network.
- Knowledge workers can stay in touch wherever they are in the building. Using e–mail, electronic calendars, and chat technologies, your staff can remain online even while in meetings or working away from their desks.
- Online information is always available. Meetings no longer need come to a standstill while someone dashes out to retrieve the report of last month's figures or get an update of a presentation. This can significantly improve the quality and productivity of meetings.
- Organizational flexibility is also enhanced. As teams and project structures change, quick and easy desk moves, or even whole office moves, become possible because people are no longer wired to their desks.
- Integration of new devices and applications into the corporate IT environment improves significantly. Devices like personal digital assistants (PDAs) and Tablet PCs, until recently were often executive playthings on the margins of corporate IT;.these can become far more integrated and useful when organizations are wireless–enabled. Workers and business processes that were previously untouched by IT can benefit from the provision of wireless computers, devices, and applications into formerly network–free areas, such as manufacturing shop floors, hospital wards, stores, and restaurants.

Different organizations will experience different benefits; which of these are relevant to your organization depends on many factors such as the nature of your business and the size and geographic distribution of the workforce.

Operational Benefits

The main operational benefits of WLAN technology are lower capital and operational costs and can be summarized as follows:

- The cost of provisioning network access to buildings is substantially lowered. Although most office space is cabled for networks, many other workspaces such as factory floors, warehouses, and stores are not. Networks can also be provisioned at locations where wired networks would be impractical, for example, outdoors, at sea, or even in a battlefield.

- The network can be easily scaled to respond to different levels of demand as the organization changes, even from day–to–day, if required; it is far easier to deploy a higher concentration of wireless access points (APs) at a given location than to increase the number of wired network ports.
- Capital no longer needs to be tied into building infrastructure; wireless network infrastructure can be moved to a new building relatively easily, whereas wiring is usually a permanent fixture.

Security Concerns with Wireless LANs

Despite all these benefits, a number of security concerns with WLANs have limited their adoption; particularly in security–conscious sectors such as finance and government. Though the risks of broadcasting unprotected network data to anyone in the vicinity might seem evident, a surprising number of WLANs are installed without any security features enabled. The majority of businesses have implemented some form of wireless security, however, it is usually only in the form of basic, first generation features, which offer inadequate protection by today's standards.

When the first IEEE 802.11 WLAN standards were being written, security was nowhere near as big a concern as it is today. The level and sophistication of threats was much lower and the adoption of wireless technology was in its infancy. It is against this background that the first generation WLAN security scheme, known as Wired Equivalent Privacy (WEP), emerged. WEP underestimated the measures needed to make the security of the air “equivalent” to the security of a wire. In contrast, modern WLAN security methods are designed to work in a hostile environment like the air where there are no clear physical or network perimeters.

It is important to distinguish between first generation static WEP (which uses a shared password to protect the network) and security schemes that use WEP encryption coupled with a strong authentication and encryption key management. The former is a complete security scheme including authentication and data protection and is referred to in this document as "Static WEP". Dynamic WEP, on the other hand, defines only the data encryption and integrity method used as part of more secure solutions described later in the document.

Security weaknesses discovered in static WEP means that WLANs protected by it are vulnerable to several types of threats. Freely available "audit" tools like Airsnort and WEPCrack make breaking into static WEP–protected wireless networks a trivial task. Unsecured WLANs are obviously exposed to these same threats as well; the difference being that less expertise, time, and resources are required to carry out the attacks.

Before looking at how modern WLANs security solutions work, it is worth reviewing the principal threats to WLANs. These threats are summarized in the following table.

Table 1: Main Security Threats for WLANs

Threat	Threat Description
Eavesdropping (disclosure of data)	Eavesdropping on network transmissions can result in disclosure of confidential data, disclosure of unprotected user credentials, and the potential for identity theft. It also allows sophisticated intruders to collect information about your IT environment, which can be used to mount an attack on other systems or data that might not otherwise be vulnerable.
Interception and modification of transmitted data	If an attacker can gain access to the network, he or she can insert a rogue computer to intercept and modify network data communicated between two legitimate parties.

Threat	Threat Description
Spoofing	Ready access to an internal network allows an intruder to forge apparently legitimate data in ways that would not be possible from outside the network, for example, a spoofed e–mail message. People, including system administrators, tend to trust items that originate internally far more than something that originates outside the corporate network.
Denial of service (DoS)	A determined assailant may trigger a DoS attack in a variety of ways. For example, radio–level signal disruption can be triggered using something as low–tech as a microwave oven. There are more sophisticated attacks that target the low–level wireless protocols themselves, and less sophisticated attacks that target networks by simply flooding the WLAN with random traffic.
Free–loading (or resource theft)	An intruder may want nothing more sinister than to use your network as free point of access to the Internet. Though not as damaging as some of the other threats, this will, at the very least, not only lower the available level of service for your legitimate users but may also introduce viruses and other threats.
Accidental threats	Some features of WLANs make unintentional threats more real. For example, a legitimate visitor may start up a portable computer with no intention of connecting to your network but then is automatically connected to your WLAN. The visitor's portable computer is now a potential entry point for viruses onto your network. This kind of threat is only a problem in unsecured WLANs.
Rogue WLANs	If your company officially has no WLAN you may still be at threat from unmanaged WLANs springing up on your network. Low priced WLAN hardware bought by enthusiastic employees can open unintended vulnerabilities in your network.

1.

Security concerns with WLANs, focused on static WEP, have received a great deal of attention in the media. Despite the fact that good security solutions exist to combat these threats, organizations of all sizes remain wary of WLANs; many have halted deployment of WLAN technology or even banned its use altogether. Some of the key factors contributing to this confusion and the popular misconception that WLANs and network insecurity go hand–in–hand include:

- Widespread uncertainty exists over which WLAN technology is secure and which is not. Businesses are suspicious of all WLAN security measures after a succession of flaws were discovered in static WEP. The bewildering list of official standards and proprietary solutions claiming to resolve the problems has done little to clear up the confusion.
- Wireless is invisible; for network security administrators this is not just psychologically unsettling, this poses a real security management problem. Whereas you can actually *see* an intruder plugging a cable into your wired network, intrusion into WLANs is much less tangible. The traditional physical security defenses of walls and doors that help guard your wired network are no protection from a "wireless" attacker.
- There is now much greater consciousness of the need for information security. Businesses demand much higher levels of security in their systems and are mistrustful of any technologies that may bring security vulnerabilities with them.

- As a corollary to this increasing security awareness, legislative and regulatory requirements that govern data security are appearing in a growing number of countries and industry sectors. One of the best known examples of this phenomenon is the US government's Health Insurance Portability and Accountability Act of 1996 (HIPAA), which governs the handling of personal healthcare data.

How to (Really) Secure Your WLAN

Since the discovery of the security weaknesses of WLANs, described earlier, leading network vendors, standards bodies, and analysts have focused a great deal of effort on finding remedies for these vulnerabilities. This has yielded a number of responses to the concerns over WLAN security. The principal alternatives are:

- Not to deploy WLAN technology
- Stick with 802.11 static WEP security
- Use VPN to protect data on the WLAN
- Use IPsec to protect WLAN traffic
- Use 802.1X authentication and data encryption to protect the WLAN

These strategies are listed in order of the least to the most satisfactory based on a combination of security, functionality, and usability; although this is a subjective judgment to an extent. The option favored by Microsoft is the last of these alternatives: using 802.1X authentication and WLAN encryption. This approach is discussed in the following section and is then gauged against the list of major WLAN threats identified earlier (Table 1). The principal advantages and disadvantages of the other approaches are also discussed later in the document, following this section.

Protecting the WLAN with 802.1X Authentication and Data Encryption

This approach has many good points to recommend it (although its title and array of obscure terminology are not among them). Before discussing the advantages of solutions based on this approach, it is important to clarify some of the terminology and explain how such a solution works.

Understanding WLAN Security

Protecting a WLAN involves three major elements:

- Authenticating the person (or device) connecting to the network so that you have a high degree of confidence that you know who or what is trying to connect.
- Authorizing the person or device to use the WLAN so that you control who has access to it.
- Protecting the data transmitted on the network so that it is safe from eavesdropping and unauthorized modification.

You may require an auditing function as well in addition to these items, though auditing is primarily a means to check and reinforce these other three elements.

Network Authentication and Authorization

Static WEP security relies on a simple shared secret (password or key) for authentication to the WLAN. Anyone possessing this secret key can access the WLAN. The original WEP standard does not provide for a method for automating the update or distribution of

these keys, therefore it is extremely difficult to change them regularly. Cryptographic flaws in WEP mean that an attacker can discover static WEP keys using simple tools.

To provide a much stronger method of authentication and authorization, Microsoft and a number of other vendors proposed a WLAN security framework using the 802.1X protocol. 802.1X is an IEEE standard for authenticating access to a network and, optionally, for managing keys used to protect traffic. Its use is not limited to wireless networks; it is also implemented in many high–end wired LAN switches.

The 802.1X protocol involves the network user, a network access (or gateway) device such as a wireless AP, and an authentication and authorization service in the form of a RADIUS (Remote Authentication Dial-In User Service) server. The RADIUS server performs the job of authenticating the users' credentials and authorizing the users' access to the WLAN.

802.1X relies on an IETF protocol called Extensible Authentication Protocol (EAP) to carry the authentication conversation between the client and the RADIUS server (relayed by the AP). EAP is a general protocol for authentication that supports multiple authentication methods, based on passwords, digital certificates, or other types of credential.

Because EAP is a pluggable authentication method, there is no one EAP standard authentication type to be used. Different EAP methods, using different credential types and authentication protocols, may be appropriate for different circumstances. The use of EAP methods in WLAN authentication is discussed in a later section.

WLAN Data Protection

802.1X authentication and network access are only a part of the solution. The other significant component is the protection of the wireless network traffic.

The flaws in WEP data encryption described earlier might have been ameliorated if static WEP has included a method to automatically update the encryption keys regularly. Tools for cracking static WEP need to collect between one and ten million packets encrypted with the same key. Because static WEP keys often remain unchanged for weeks or months it is usually easy for an attacker to collect this amount of data. As all computers on a WLAN share the same static key, data transmissions from all computers on the WLAN can be harvested to help discover the key.

Using a solution based on 802.1X allows the encryption keys to be changed frequently. As part of the 802.1X secure authentication process, EAP method generates an encryption key that is unique to each client. To prevent the WEP cracking attacks (described earlier), the RADIUS server regularly forces the generation of new encryption keys. This allows WEP encryption algorithms (found in most current WLAN hardware) to be used in a much more secure way.

WPA and 802.11i

Although WEP with 802.1X dynamic re–keying is secure for most practical purposes, there are a few lingering problems including:

- WEP uses a separate static key for global transmissions like broadcast packets. Unlike the per–user keys, the global key is not renewed regularly. Although confidential data is unlikely to be transmitted using broadcast, using a static key for global transmission gives attackers the potential to discover information about the network such as IP addresses and computer and user names.
- WEP protected network frames have poor integrity protection. Using cryptographic techniques, an attacker can modify information in the WLAN frame and update the frame's integrity check value without the receiver detecting it.

- As WLAN transmission speed improves and computational power and cryptanalytic techniques improve, WEP keys will have to be renewed with greater frequency. This may place an unacceptable load on the RADIUS servers.

To address these problems, the IEEE is working on a new WLAN security standard called 802.11i; also known as Robust Security Network (RSN). The Wi–Fi Alliance, a consortium of the leading Wi–Fi vendors, has taken, what is essentially an early release of 802.11i and published it in an industry standard known as WPA (Wi–Fi Protected Access). WPA includes a large subset of features of 802.11i. By publishing WPA, Wi–Fi Alliance has been able to mandate adherence to WPA for all equipment bearing the Wi–Fi logo and allowed Wi–Fi network hardware vendors to offer a standardized high security option in advance of the publication of 802.11i. WPA brings together a set of security features that are widely regarded as the most secure techniques currently available for securing WLANs.

WPA includes two modes; one using 802.1X and RADIUS authentication (simply known as WPA) and another simpler scheme for SOHO environments using a pre–shared key (known as WPA PSK). WPA couples robust encryption with the strong authentication and authorization mechanism of 802.1X. WPA data protection eliminates the known vulnerabilities of WEP by:

- Using a unique encryption key for each packet
- Using a much longer initialization vector, effectively doubling the key space by adding an additional 128 bits of keying material
- Adding a signed message integrity check value that is not vulnerable to tampering or spoofing
- Incorporating an encrypted frame counter to thwart replay attacks

However, because WPA uses cryptographic algorithms similar to those used by WEP, it can be implemented on existing hardware with a simple firmware upgrade.

The PSK mode of WPA also allows small organizations and home workers to use a shared key WLAN without any of the vulnerabilities of static WEP (provided the chosen pre–shared key is strong enough to avoid simple password–guessing attacks). Like the RADIUS–based WPA and dynamic WEP, individual encryption keys are generated for each wireless client. The pre–shared key is used as an authentication credential; if you possess the key, then you are authorized to use the WLAN and receive a unique encryption key to protect the data.

802.11i (RSN) will bring even higher levels of security to WLANs, including better protection against DoS attacks, and is expected to be released in mid–2004.

EAP Authentication Methods

EAP, as the "Extensible" in its name implies, supports many authentication methods. These methods can use different authentication protocols such as Kerberos, Transport Layer Security (TLS), and Microsoft–Challenge Handshake Authentication Protocol (MS–CHAP) using a range of credential types such as passwords, certificates one–time password tokens and biometrics. Although any EAP method can, theoretically, be used with 802.1X, not all are suitable for use with WLANs; in particular, the method used must be suitable for use in an unprotected environment and be able to generate encryption keys.

The principal EAP methods in use for WLANs are EAP–TLS, Protected EAP (PEAP), Tunneled TLS (TTLS), and Lightweight EAP (LEAP). Of these, PEAP and EAP–TLS are supported by Microsoft.

EAP–TLS

EAP–TLS is an IETF standard (RFC 2716) and is probably the most widely supported, on both wireless clients and RADIUS servers. It uses public key certificates to authenticate both the wireless clients and the RADIUS servers by establishing an encrypted TLS session between the two.

PEAP

PEAP is a two stage authentication method. The first stage establishes a TLS session to the server and allows the client to authenticate the server using the server's digital certificate. The second stage requires a second EAP method tunneled inside the PEAP session to authenticate the client to the RADIUS server. This allows PEAP to use a variety of client authentication methods including passwords with the MS–CHAP version 2 (MS–CHAP v2) protocol and certificates using EAP–TLS tunneled inside PEAP. EAP types such as MS–CHAP v2 are not secure enough to be used without the PEAP protection because they would be vulnerable to offline dictionary attacks. Support for PEAP is widespread in the industry and Microsoft Windows XP SP1 and Pocket PC 2003 have built–in support for PEAP.

TTLS

TTLS is a two stage protocol similar to PEAP that uses a TLS session to protect a tunneled client authentication. Besides tunneling EAP methods, TTLS can also use non–EAP versions of authentication protocols such as CHAP, MS–CHAP, and others. Microsoft and Cisco do not support TTLS, although TTLS clients for a number of platforms are available from other vendors.

LEAP

LEAP is a proprietary EAP method developed by Cisco, which uses passwords to authenticate clients. Although popular, LEAP only works with hardware and software from Cisco and a few other vendors. LEAP also has several published security vulnerabilities such as susceptibility to offline dictionary attacks (which may allow attackers to discover users' passwords) and man–in–the–middle attacks. In a domain environment, LEAP can only authenticate the *user* to the WLAN, not the *computer.* Without computer authentication, machine group policies will not execute correctly, software installation settings, roaming profiles, and logon scripts may all fail, and it will not be possible for users to change expired passwords.

There are WLAN security solutions that use 802.1X with other EAP methods. Some of these EAP methods, such as EAP–MD5, have significant security weaknesses when used in a WLAN environment and should never be used. There are others supporting the use of one–time password tokens and other authentication protocols such as Kerberos. These have yet to make any significant impact in the WLAN market.

Benefits of 802.1X with WLAN Data Protection

The key benefits of an 802.1X solution are summarized in the following list:

- **High security:** It is a high security authentication scheme because it can use client certificates or user names and passwords.
- **Stronger encryption:** It allows high strength encryption of network data.
- **Transparent:** It provides transparent authentication and connection to the WLAN.
- **User and computer authentication:** It allows separate authentication of user and computer. Separate authentication of computer allows the computer to be managed even when no user is logged on.
- **Low cost:** Low cost of network hardware.

- **High performance:** Because encryption is performed in WLAN hardware and not by client computer CPU, WLAN encryption has no impact on the performance level of the client computer.

There also are some caveats to an 802.1X solution.

- Although 802.1X has near universal acceptance, the use of different EAP methods means that interoperability is not always guaranteed.
- WPA is still in early stages of adoption and may not be available on older hardware.
- Next generation RSN (802.11i) is yet to be ratified and will require deployment of hardware and software updates (network hardware will typically need a firmware update).

However, these are relatively minor issues and are easily outweighed by the benefits; particularly when weighed against the serious shortcomings of the alternative approaches discussed later.

Resilience of 802.1X Solution to Security Threats

The principal security threats to WLANs were described earlier in the document (in Table 1). These threats are re–assessed in the following table against a solution based on 802.1X and WLAN data protection.

Table 2: Security Threats Assessed Against the Proposed Solution

Threat	Mitigation
Eavesdropping (disclosure of data)	Dynamically assigning and changing encryption keys at frequent intervals and the fact that keys are unique to each user session means that as long as the key refresh is sufficiently frequent, discovering the keys and accessing data is not possible by any currently known means. WPA brings greater security by changing encryption keys per packet. Global key (protecting broadcast traffic) is re–keyed per packet.
Interception and modification of transmitted data	Enforcing data integrity and strong data encryption between the wireless client and the wireless AP ensures that it is infeasible for a malicious user to intercept and modify data in transit. Mutual authentication between the client, the RADIUS server, and the wireless AP makes it difficult for any of these to be impersonated by an attacker. WPA improves data integrity with Michael protocol.
Spoofing	Secure authentication to the network prevents unauthorized individuals from connecting to the network and introducing spoofed data from the inside.
DoS	Data–flooding and other DoS attacks at network level are prevented by controlling access to the WLAN using 802.1X. There is no defense against low level 802.11 DoS attacks in either dynamic WEP or WPA. This is being addressed by the 802.11i standard. However, even this new standard will not be immune to physical layer (radio–level) disruption of networks. These vulnerabilities are a feature of current 802.11 WLANs

Threat	Mitigation
	and common to all the other options discussed later in this document.
Free—loading (resource theft)	Unauthorized use of the network is prevented by the requirement for strong authentication.
Accidental threats	Accidental connection to the WLAN is prevented by the requirement for secure authentication.
Rogue WLANs	Although the solution does nothing directly to deal with rogue wireless APs, implementing a secure wireless solution such as this largely takes away the motivation for setting up unofficial WLANs . However, you should plan on creating and publishing a clear policy prohibiting the use of unapproved WLANs. You can enforce the policy by using software tools that scan the network for wireless AP hardware addresses and by using handheld WLAN detection equipment.

2.

Other Approaches to WLAN Security

The previous section discussed 802.1X authentication with WLAN data protection in some detail. This section details the other four alternatives to WLAN security listed earlier (in the beginning of the "How to (Really) Secure Your WLAN" section).

The four other approaches listed were:

- Not to deploy WLAN technology
- Stick with 802.11 static WEP security
- Use VPN to protect data on the WLAN
- Use IPsec to protect WLAN traffic

The key differentiators between these approaches and an 802.1X–based solution are summarized in the following table (although the “No WLAN” option is not included since it is not directly comparable with the others). These options are covered in greater detail in subsequent sections.

Table 3: Comparison of WLAN Security Approaches

Feature	802.1X WLAN	Static WEP	VPN	IPsec
Strong authentication (1)	Yes	No	Yes, but not VPNs using shared key authentication	Yes, if using certificate or Kerberos authentication
Strong data encryption	Yes	No	Yes	Yes
Transparent connection and reconnection to WLAN	Yes	Yes	No	Yes
User authentication	Yes	No	Yes	Yes
Computer authentication(2)	Yes	Yes	No	Yes

Feature	802.1X WLAN	Static WEP	VPN	IPsec
Broadcast and multicast traffic protected	Yes	Yes	Yes	No
Additional network devices required	RADIUS servers	No	VPN servers, RADIUS servers	No
Secures access to the WLAN itself	Yes	Yes	No	No

3.

(1) Many VPN implementations that use IPsec tunnel mode employ a weak, shared key authentication scheme known as XAuth.

(2) Computer authentication means that the computer will stay connected to the WLAN and the corporate network even when no user is logged on to the computer. This capability is needed for the following Windows domain features to work properly:

- Roaming user profiles
- Computer Group Policy settings (particularly startup scripts and deployed software)
- User logon scripts and software deployed using Group Policy

Alternative 1—Not Deploying WLAN Technology

Perhaps the most obvious way of dealing with WLAN security threats is to avoid them altogether by not deploying any WLANs. Besides having to forego the benefits of WLANs outlined earlier in this document, this strategy is not free of pitfalls. Organization taking this approach must deal with what the META Group calls the "Price of Postponement," which is more than just an opportunity cost. The META Group study based its findings on an analysis of the unmanaged way in which the use of wired LANs grew in many organizations over a decade ago. In most cases, central IT departments were forced to step in and take control of the LAN deployment reactively. Typically, the cost of re–engineering the multitude of independent and often incompatible departmental LANs was huge. For more information, see the article "How Do I Limit My Exposure Against the Wireless LAN Security Threat? The New Realities of Protecting Corporate Information" published by META Group on 12/18/2002.

This same threat has resurfaced with WLANs, especially in larger organizations where it is impossible to physically see what is happening in each location. Unmanaged grassroots deployment of WLANs, made possible by the extremely low cost of the components, is potentially the worst scenario. This exposes the organization to all the security threats outlined earlier but without the central IT group knowing anything about it or being able to take steps to combat the threats.

This implies that if your strategy is not to adopt WLAN technology, you need to pursue this strategy in an active rather than a passive way. You should back up this decision with a clear, published policy and ensure that all employees are aware of it, and of the consequences of violating it. You may also want to consider using scanning equipment and network packet monitors to detect the use of unauthorized wireless equipment on your network.

Alternative 2—Use 802.11 Basic Security (Static WEP)

Basic 802.11 security (static WEP) uses a shared key to control access to the network and uses the same key to encrypt the wireless traffic. This simple authorization model is often supplemented by the use of port filtering based on WLAN card hardware

addresses, although this is not a part of 802.11 security as such. The main attraction of this approach is its simplicity. Although it provides some level of security over an unsecured WLAN, this approach has serious management as well as security drawbacks, particularly for larger organizations.

The drawbacks of using WEP include the following:

- Static WEP keys can be discovered in a matter of hours on a busy network using a PC with a WLAN adapter and hacking tools such as Airsnort or WEPCrack.
- The most serious weakness of WEP is that there is no mechanism for dynamically assigning or updating the network encryption key. Without 802.1X and EAP to enforce regular key updates, encryption algorithm used by WEP is vulnerable to the key recovery attacks as described earlier.
- The static keys can be changed, but the process for doing this on the APs and wireless clients is usually manual and always time consuming. To make matters worse, the key updates must be done on clients and APs simultaneous to prevent clients' connectivity from breaking. In practice, this is so difficult that the keys are usually left unchanged.
- The static key needs to be shared between all users of the WLAN and all wireless APs. A secret shared between a large number of people and devices is unlikely to remain a secret for long.

WEP gives WLANs a very limited access control mechanism based on knowledge of the WEP key. If you discover the name of the network, which is easy, as well as the WEP key, you can connect to the network.

One way of improving this is by configuring the wireless APs to allow only a predefined set of client network adapter addresses. This is commonly known as media access control (MAC) address filtering; the MAC layer refers to the low–level firmware of the network adapter.

Network adapter address filtering for access control comes with its own set of issues:

- Manageability is extremely poor. Maintaining a list of hardware addresses for anything but a small number of clients is difficult. Also, distributing this list to, and synchronizing it across, all your APs is a significant challenge.
- Scalability is poor. APs have a finite filter table size limit, thus restricting the number of clients that you can support.
- There is no way to associate a MAC address with a user name, so you can only authenticate by computer identity and not user identity.
- An intruder could spoof an “allowed” MAC address. If a legitimate MAC address is discovered, it is easy for an intruder to use this address instead of the predefined address burned onto the adapter.

Pre–shared key solutions are only practical for small numbers of users and APs due to the difficulty in managing key updates across multiple locations. Cryptographic flaws with WEP mean that its usefulness is extremely questionable even in very small environments.

WPA's pre–shared key mode, however, does bring a good level of security with a very low infrastructure overhead for small organizations. A wide range of hardware supports WPA PSK, and WLAN clients can be configured manually. This should be considered the configuration of choice for SOHO environments.

Alternative 3—Virtual Private Networks

VPNs are probably the most popular form of network encryption; a lot of people rely on the tried and trusted VPN technologies to protect the confidentiality of data sent over the Internet. When the vulnerabilities of static WEP were discovered, VPN was quickly proposed as *the* way to secure data traveling over a WLAN. This approach was endorsed by analysts such as the Gartner Group and, unsurprisingly, was enthusiastically promoted by vendors of VPN solutions.

VPN is an excellent solution to securely traverse a hostile network such as the Internet (although the quality of VPN implementations varies). However, it is not necessarily the best solution for securing internal WLANs. For this kind of application, a VPN offers little or no additional security compared with 802.1X solutions while significantly increasing complexity and costs, reducing usability, and rendering important pieces of functionality inoperable.

Note: This is distinct from using VPNs to secure traffic over public wireless LAN hotspots. Protecting the network data of users connecting over hostile remote networks is a legitimate use of VPNs. In this kind of scenario users expect secure connectivity to be more intrusive and less functional than a LAN connection; something that they do not expect when inside the company's own premises.

The advantages of using VPNs to protect WLANs include the following:

- Most organizations already have a VPN solution deployed so users and IT staff will be familiar with the solution.
- VPN data protection normally uses software encryption allowing algorithms to be changed and upgraded more easily than hardware–based encryption.
- You may be able to use relatively less expensive hardware because VPN protection is independent of WLAN hardware (although the price premium of 802.1X capable network hardware has all but vanished).

The disadvantages of using VPNs in place of native WLAN security include:

- VPN lacks user transparency. VPN clients usually require the user to manually initiate a connection to the VPN server; therefore, the connection will never be as transparent as a wired LAN connection. Non–Microsoft VPN clients may also prompt for logon credentials at connection in addition to the standard network or domain logon. If the VPN disconnects, because of a poor WLAN signal or because the user is roaming between APs, the user has to reconnect.
- Because the VPN connection is only user–initiated, an idle, logged–off computer will not be connected to the VPN (and thus the corporate LAN). Therefore, a computer cannot be remotely managed or monitored unless a user is logged on. Certain computer Group Policy object (GPO) settings, such as startup scripts and computer assigned software will never be applied.
- Roaming profiles, logon scripts, and software deployed to the user using GPO may not work as expected. Unless the user chooses to log on using the VPN connection from the Windows logon prompt, the computer will not connect to the corporate LAN until after the user has logged on and initiated the VPN connection. Attempts to access the secure network before this will fail. With a non–Microsoft VPN client, it may be impossible to do a full domain logon over the VPN connection.
- Resuming from standby or hibernation does not automatically re–establish the VPN connection; the user has to do this manually.

- Although the data inside the VPN tunnel is protected, the VPN offers no protection for the WLAN itself. An intruder can still attach to the WLAN and attempt to probe or attack any devices attached to the WLAN.
- The VPN server(s) can become a bottleneck. All WLAN client access to the corporate LAN is channeled through the VPN server. VPN devices traditionally service a large number of relatively low speed remote clients; hence, most VPN gateways will be unable to cope with tens or hundreds of clients running at full LAN speed.
- The cost of additional hardware and ongoing management of the VPN devices is likely to be much higher than a native WLAN solution. Each site will typically need its own VPN server in addition to WLAN APs.
- VPN sessions are more prone to disconnection when clients roam between APs. Although applications will often tolerate a momentary disconnection when switching wireless APs, VPN sessions will often be broken requiring the user to manually reconnect.
- The cost of VPN server and client software licenses, as well as the cost of deploying the software, may be an issue with non–Microsoft VPN solutions. You may also have concerns with the VPN client software compatibility because non–Microsoft clients often replace core Windows functionality.
- Many analysts and vendors make an unstated assumption that VPN security is always better than that of WLANs. Though this may be true for static WEP, it is not necessarily the case for the 802.1X EAP based solutions described in this document. VPN authentication methods, in particular, are often far *less* secure and, at best are unlikely to be significantly stronger. For example, the WLAN solutions supported by Microsoft use exactly the same EAP authentication methods as its VPN solutions (EAP–TLS and MS–CHAP v2). Many VPN implementations, especially those based on IPsec tunnel mode, use pre–shared key authentication (a group password). This has been widely discredited and shown to have serious security vulnerabilities, ironically, sharing some of these vulnerabilities with static WEP.
- A VPN does nothing to secure the WLAN itself. Though the data inside the VPN tunnels is secure, anyone can still attach to the WLAN and attempt to attack legitimate wireless clients and other devices on the WLAN.

VPN is ideally suited to securing traffic passing over hostile networks, whether the user is connecting over a home broadband connection or from a wireless hotspot. However, VPN was never designed to secure network traffic on internal networks. For most organizations, VPN in this role will be too cumbersome and functionally limiting for the user and too costly and complex for the IT department to maintain.

In exceptional cases where higher security for a particular connection or traffic type is needed, this can be provided by a VPN tunnel or IPsec transport mode *in addition to* the native WLAN protection. This is a more sensible use of network resources.

Alternative 4—IP Security

IPsec allows two network peers to securely authenticate each other and authenticate or encrypt individual network packets. IPsec can be used either to securely tunnel one network over another or simply to protect IP packets being transmitted between two computers.

IPsec tunneling is typically used in client access or site–to–site VPN connections. IPsec tunnel mode is a form of VPN and works by encapsulating a whole IP packet within a protected IPsec packet. This adds an overhead to the communication, like other VPN solutions, which is not really needed for communication between systems on the same

network. The pros and cons of IPsec tunnel mode were covered in the discussion on VPN in the previous section.

IPsec can also secure end–to–end traffic between two computers (without tunneling) using IPsec *transport mode*. Like VPN, IPsec is an excellent solution in many circumstances, although, as will come clear in this section, it is not a replacement for native WLAN protection implemented at the hardware layer.

Some of the advantages of IPsec transport mode protection are:

- It is transparent to users. Unlike VPNs, no special logon procedure is required.
- IPsec protection is independent of WLAN hardware. It only requires an open, unauthenticated WLAN. Unlike VPN, no additional servers or devices are required because the security is negotiated directly between the computers at each end of the communication.
- Use of cryptographic algorithms is not constrained by the WLAN hardware.

Disadvantages of using IPsec in place of native WLAN security include the following:

- IPsec uses computer–level authentication only; there is no way to implement a user–based authentication scheme along with it. For many organizations, this will not be a problem but it does allow *unauthorized* users to connect to other IPsec protected computers on the network if they manage to log on to an *authorized* computer.

Note: Some IPsec implementations on non–Windows platforms use user–only authentication. However, as with the VPN solution, the computer will not be connected to the network when the user is not logged in, thereby, preventing certain management operations and disabling user settings functionality.

- Managing IPsec policies can be complex for a large organization. Attempts to enforce general IP traffic protection may interfere with more specialized uses of IPsec where end–to–end protection is required.
- Full security requires encrypting all end–to–end traffic, but some devices may not be IPsec–capable. This will force traffic to these devices to be transmitted unencrypted. IPsec will provide no protection to these devices, which will be exposed to anyone who connects to the WLAN.
- Because IPsec protection occurs at the network level rather than at the MAC layer, it is not fully transparent to network devices such as firewalls. Some IPsec implementations will not work across a network address translation (NAT) device.
- End–to–end IPsec cannot protect broadcast or multicast traffic because IPsec relies on two parties mutually authenticating and exchanging keys.
- Although the data inside the IPsec packets is protected, the WLAN itself is not protected. An intruder can still attach to the WLAN and attempt to probe or attack any devices attached to the WLAN or listen to any traffic not protected by IPsec.
- IPsec network traffic encryption and decryption loads the computer's CPU. This can overload heavily used servers. Although this processing overhead can be offloaded to specialized network cards, they are usually not fitted by default.

Like VPN, IPsec is an excellent solution for many security scenarios but does not address WLAN security as well as native WLAN protection.

Selecting the Right WLAN Options

From the preceding discussion, it should be apparent that an 802.1X WLAN solution is by far the best of the available alternatives. However, as discussed in the “Understanding WLAN Security” section, once you have decided to use an 802.1X solution you then have to choose from a number of options that go to make up the solution.

The two key choices are:

- Whether to use passwords or certificates to authenticate your users and computers.
- Whether to use dynamic WEP or WPA WLAN data protection.

These two items are independent of each other.

As discussed earlier in the document, Microsoft has two WLAN security solution guides; one using password authentication and the other using certificate authentication. These solutions work with either dynamic WEP or WPA.

Deciding on the Right WLAN Security Solution

The following flowchart summarizes the choice between the two WLAN security solutions.

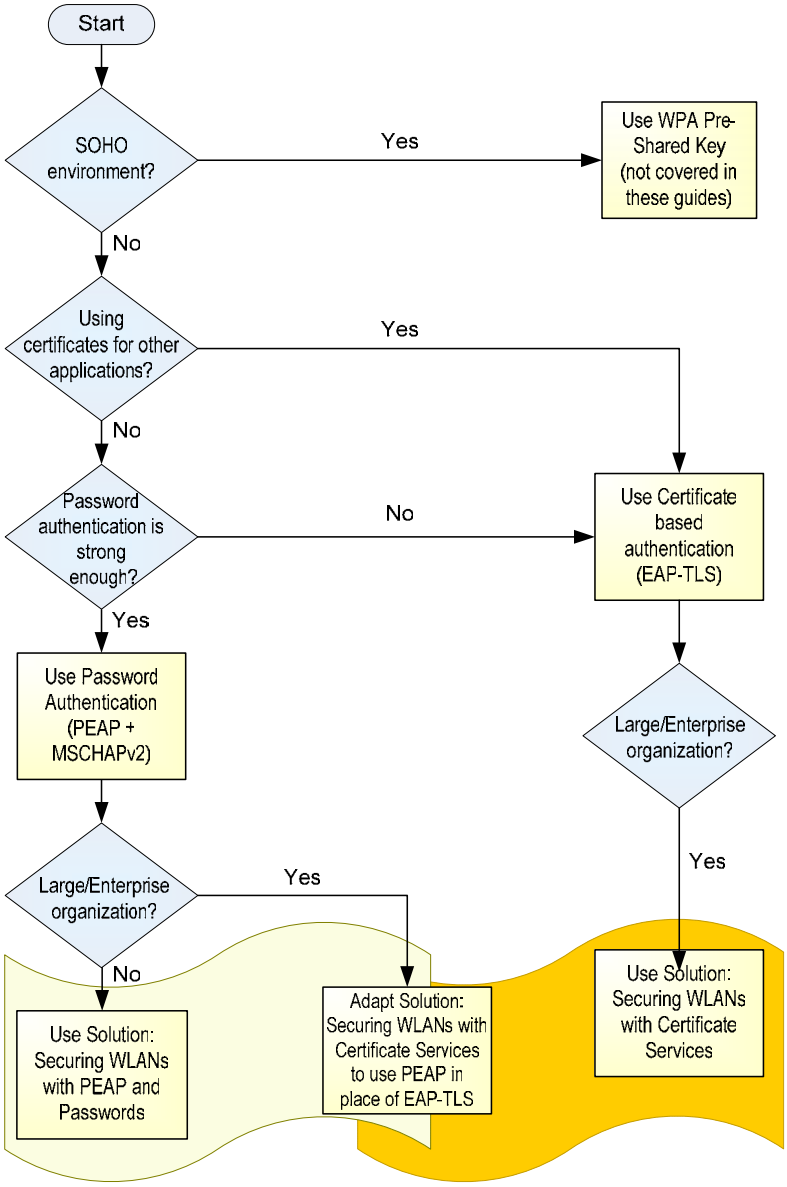


Figure 2: Decision Tree for WLAN Security Solution

The outcome of this decision tree depends on the size and specific security requirements of your organization. Most organizations will be able to use one or the other of the Microsoft WLAN solutions without any modification. For example, most small–to–medium organizations will choose the simpler password–based authentication solution described in the *Securing WLANs with PEAP and Passwords* solution guide. Larger organizations are more likely to move towards using the digital certificate–based *Securing Wireless LANs—A Windows Server 2003 Certificate Services Solution*.

Although each solution was written with these audiences in mind there is a good deal of latitude with each solution. *Securing Wireless LANs with PEAP and Passwords* can be deployed by organizations with a few tens of users to organizations with many thousands of users. *Securing Wireless LANs—A Windows Server 2003 Certificate Services Solution* is applicable to organizations with a few hundred or tens of thousands of users (organizations with fewer than five hundred users normally do not have sufficient IT resources to deploy and maintain certification authorities).

One common case that isn't directly covered by either of the guides is large organizations deploying a password–based WLAN solution. Although the technical detail in the *Securing Wireless LANs with PEAP and Passwords* solution is equally applicable to large and small businesses, much of the design, planning, and operational detail required by larger organizations has been omitted in the interest of simplicity. Fortunately, the similarity between the architecture and technical components used in both solutions allows you to mix–and–match parts of the solutions relatively easily. The *Securing Wireless LANs with PEAP and Passwords* solution has an appendix that gives you some guidance on which parts from each solution are relevant.

Choosing between Dynamic WEP and WPA

WEP data protection, when combined with the strong authentication and dynamic key update brought by 802.1X and EAP, gives a level of security that is more than adequate for most organizations. However, the WPA standard improves upon this and provides even better levels of security.

The differences between using WPA and a dynamic WEP in either of the solutions are minimal, and migrating from a dynamic WEP environment to a WPA environment is very simple. The key changes moving from dynamic WEP to WPA are:

- If your network hardware (wireless APs and wireless network adapters) does not currently support WPA, you must obtain and deploy firmware updates for these. Firmware updates for wireless network adapters are often included in network driver updates.
- You must enable WPA on your wireless APs.
- The WLAN client configuration must be changed to negotiate WPA instead of WEP security.
- The session time–out on the IAS (Internet Authentication Service) remote access policy, which is used to force WEP key refresh, should be increased to reduce the load on the IAS server.

Note: IAS is the Microsoft RADIUS server implementation and is included in Windows Server 2003 but not installed by default.

WPA should be your first choice, if it is available to you. However, you should consider whether any of the following issues will make using WPA more problematic:

- Your network hardware may not yet support WPA (this is unlikely with new devices but you may have a large installed base of pre–WPA hardware).
- Support for GPO controlled settings is available only in SP1 of Windows Server 2003 (due in H2 of 2004); prior versions do not have this support and WPA settings must be configured manually on Windows XP clients.
- WPA may not be supported on all your clients; for example, Windows 2000 and earlier and Pocket PC currently have no built–in support for WPA.

If you decide that you are not yet in a position to deploy WPA, you should deploy a dynamic WEP solution and plan to migrate to WPA when circumstances permit.

Summary

This document should have given you the information you need to work out your strategy for wireless LAN security. The first part of the document explored the business advantages of wireless networks and also the security threats to poorly protected

WLANs. The middle section looked at how wireless LAN security based on 802.1X, EAP, and strong data protection works to combat these threats. The relative merits of alternatives such as VPNs, IPsec, and static WEP security were also discussed. The final section included guidance on which WLAN security options to select and which of the Microsoft WLAN security solutions would best suit your organization.

References

This section provides references to important supplementary information and other background material relevant to this document.

- The Microsoft solution for *Securing Wireless LANs with PEAP and Passwords* is available at the following URL:
  http://go.microsoft.com/fwlink/?LinkId=23459
- The Microsoft solution for *Securing Wireless LANs—A Windows Server 2003 Certificate Services Solution* is available at the following URL:
  http://go.microsoft.com/fwlink/?LinkId=14843
- For more detailed technical information about IEEE 802.11 and related technologies, see the "802.11 Wireless" section of the Windows Server 2003 Technical Reference available at the following URL:
  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/techref/w2k3tr_wir_intro.asp
- For more information about 802.11, see the IEEE 802.11 Web page at the following URL:
  http://www.ieee802.org/11/
- For more information about 802.1X, see the IEEE 802.1X Web page at the following URL:
  http://www.ieee802.org/1/pages/802.1x.html
- For more information about the EAP standard, see RFC 2284 at the following URL:
  http://www.ietf.org/rfc/rfc2284.txt?number=2284
- For an overview of the Wi–Fi Alliance WPA standard, see the following URL:
  http://www.wi-fialliance.org/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf
- For more information about wireless networking, see the Microsoft wireless networking site at the following URL:
  http://www.microsoft.com/wifi
- For a detailed discussion of PEAP and how it compares with LEAP (and also EAP–TLS and EAP–MD5), see "The Advantages of Protected Extensible Authentication Protocol (PEAP): A Standard Approach to User Authentication for IEEE 802.11 Wireless Network," article at the following URL:
  http://www.microsoft.com/windowsserver2003/techinfo/overview/peap.mspx
- The META Group article "How Do I Limit My Exposure Against the Wireless LAN Security Threat? The New Realities of Protecting Corporate Information" is available at the following URL: