

Enterprise Wireless LAN Security: Making Sense of the Options

Don't let the paranoia freeze you. It's less secure to do nothing.

No two concepts seem at such odds as wireless LANs (WLANs) and security. While visions of war drivers dance in your head, the reality is that WLANs can have security equal to, if not better than, wired networks.

Securing your WLAN requires a multilayer defense to ensure data privacy and protect against attackers who might launch man-in-the-middle and denial-of-service (DoS) attacks. It requires not only secure authentication and strong encryption but also radio frequency (RF) planning and rogue access point (AP) detection. Deploying an enterprise WLAN with confidence requires you to understand key deployment issues, including a multitude of encryption options, and then developing a security strategy appropriate to the risks in your environment.

Wireless Security: Solving a Big Problem

Understanding the security risks unique to WLANs is a critical first step. IT managers typically have four major concerns with WLAN security:

What if data isn't protected? Ensuring data privacy not only makes good business sense, but failing to protect privacy leaves corporations vulnerable to financial and legal liabilities. As one example, healthcare organizations now face the additional challenge of complying with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulation.

Because physical access to the Ethernet jacks or wire itself is required to tap into communications over wired networks, this first level of basic physical security keeps most network managers from feeling the need to encrypt these wired communications. But with wireless, physical security is not an option since the RF signal propagates throughout a given area with little discretion. Instead, the communications must be encrypted. The bad news is that the industry's initial, most widely used solution for wireless encryption used static keys shared amongst all users—a solution that has since been proven to be easily breakable by hackers.

What about rogues? Unapproved or rogue APs are another WLAN security challenge for IT managers. An unknown AP may have come from a well-meaning but misguided employee or it may have been placed by an attacker.

Executive Summary

Access control and encryption are vital to ensuring data privacy and preventing attacks on wireless LANs. The discredited static WEP has been replaced by an overwhelming multitude of options for encryption, leaving IT managers to sort out the best strategy and migration plan for their organizations. Careful planning and design of the WLAN, as well as tools for rogue detection, are essential to building a secure enterprise WLAN.

This white paper will help IT staffers understand:

- Options for building a progressively secure wireless LAN
- How to weight your choices for encryption
- How wireless LAN planning and rogue detection help you build a strong line of defense



An employee can buy an AP at from any consumer electronics retailer and plug it into an Ethernet wall jack, conveniently providing WLAN service for himself and neighboring co-workers. To hide the AP he can simply throw a jacket over it or put it in a desk drawer and an IT manager will need a specialized handheld RF scanner to spot the unapproved device. This do-it-yourself employee has unintentionally opened up a security hole through which a malicious hacker can launch a man-in-the-middle or DoS attack on the corporate network.

What about IT's control over clients? Wireless is being embedded in virtually every laptop, handheld and converged PDA/phone, and employees bring those devices from home into the office. An employee can set up an ad hoc network by putting his wireless laptop in peer-to-peer mode so he can more easily share files with co-workers or play games during lunch. Despite the employee's harmless intentions, he has created a security risk for IT. His system can be easily accessed and can itself become a launch pad into the rest of the wired network.

What about RF signal propagation? Unintended signal propagation is another challenge for IT managers. By nature, RF signals spread—even as far as the parking lot, where an enterprising attacker with access to a Pringles can, glue, and some copper wire could be eavesdropping.

What's an IT Manager to Do?

With IT managers and budgets stretched tighter than ever, the prospect of securing WLANs causes some CIOs to run screaming, dismissing their users and the 802.11 community as lacking a fundamental grasp of security and the value of proprietary corporate data. In such corporations, WLANs are off-limits. IT managers patrol the corridors with handheld wireless scanners in a thankless attempt to locate unapproved APs that employees have installed. Other companies may go so far as to install an overlay wireless detection system that identifies ad hoc and rogue APs—at very nearly the price of a fully functional WLAN system.

Ignoring wireless and preventing its entry into the enterprise actually diminishes IT's control over the network and security. Corporate edicts notwithstanding, employees will bring wireless into the enterprise. With Intel permeating the laptop market with the Centrino WLAN chip, it's harder to buy a laptop without wireless than with it. Users are demanding wireless access in their conference rooms, classrooms, or at their patients' bedsides. Executives spend more time away from their desks but they still need their corporate resources. Users want access to their critical information anytime, anywhere. Realistically, wireless can't be ignored.

To find the right WLAN security system, you must understand what level of security is appropriate for your corporate environment and which WLAN system will deliver on the enterprise requirements for security. An enterprise WLAN system must:

- Authenticate users
- Solve the data encryption problem
- Identify rogue APs
- Detect ad hoc or rogue users
- Allow guest access
- Plan and manage RF coverage
- Locate the source of DoS and man-in-the-middle attacks

What Level of Protection Do You Need?

Authentication and encryption are fundamental requirements of WLAN security. First, a sender must be authenticated, so you know the user is allowed on the network. Second, you must ensure message integrity, so you can prove that the message came from that user to prevent a man-in-the-middle attack where a session is hijacked. Third, the data must be encrypted, so an intervening device cannot read clear text.

The industry has rallied around 802.1X as the standard for strong authentication of users. As testament to the dominance of 802.1X, Microsoft has provided updates to its operating systems all the way back to the Windows 98 release to add support for 802.1X, marking the first time Microsoft has updated such dated releases to add a feature.

While 802.1X is widely accepted as the solution for authentication on a WLAN, multiple options remain for wireless encryption. They include dynamic Wired Equivalent Privacy (WEP) with rolling keys; Wi-Fi Protected Access (WPA) 1.0, which uses 802.1X and the Temporal Key Integrity Protocol (TKIP); WPA 2.0, which uses 802.1X and the Advanced Encryption Standard (AES); and IPsec virtual private networks (VPNs), which may be deployed as a standard VPN solution or as an ultra secure Federal Information Processing Standard (FIPS) 140-2 Level 1 or Level 2 solution, particularly for government deployments. The IEEE is expected to finalize the 802.11i standard in 2004, which defines both TKIP and AES.

To determine the right level of encryption for your environment, think of securing your corporate facilities as if you were securing your house using the following options:

Lock your doors, leave the key under the mat. Static WEP is the equivalent of locking the corporate front door, but then leaving the key under the welcome mat. Anyone can—and will—find the key and get inside. Unless you're securing the wireless connection to your printers, static WEP deserves its bad reputation.

Lock your doors, take the key with you. 802.1X with dynamic WEP is the equivalent of taking the key with you after you've locked the door. Given plenty of time, a lock can be picked, but the average thief won't be able to enter the house. Most people find this level of security sufficient.

Lock your doors, turn on the alarm. For WLANs, this is the equivalent of deploying WPA 1.0 with TKIP encryption. If someone attempts to break in to your house, the alarm system will alert you and the proper authorities. TKIP will do the same—upon detecting an attack, TKIP will invalidate the keying material to thwart admission to the network and alert the administrator that it has taken this counter-measure.

Build a safe room. The totally risk averse homeowner can build a safe room in the basement. If this is you, then WPA 2.0 or 802.11i with AES, the strongest encryption possible for non-military use, is right for you. With AES, you can be absolutely confident in your security.

Sell the house and move. Head for the hills and build a subterranean bunker with reinforced concrete walls. Produce your own clean air and fresh water, and have a year's supply of ready-to-eat meals. That's the home security equivalent to IPsec VPNs with the super-secure FIPS 140-2 Level 2 or greater certification, which may be required to do business with some agencies in the U.S. and Canadian governments.

But let's keep things in perspective. An attacker can show up at your door impersonating a deliveryman with package in hand, and gain access to your facilities. Any of the above strategies can be defeated by an adversary who is intent on wrongdoing. There is no such thing as perfect security. Security is a systemwide issue, and there will always be weak links. The challenge is to strike a reasonable balance between protection and service.

Making Sense of Encryption Options

Dynamic WEP Good, Static WEP Bad

Don't confuse dynamic WEP with static WEP—they are very different. WEP with dynamically generated keys offers vastly improved security—it's easy to deploy and it makes for a great interim solution. Also, the majority of deployed wireless clients support only WEP for encryption, so organizations will need dynamic WEP for a long time.

While everyone knows static WEP is flawed, it's important to understand why. Static WEP suffers from a weak initialization vector (IV) and offers only a rudimentary way to check the message integrity. The IV is supposed to help make the encryption key more random. However, with static WEP, the IV is only 24 bits long, so the IV is guaranteed to repeat after 16 million packets. It doesn't take a network very long to produce 16 million packets. In practice, the IV values are likely to repeat much more frequently. An attacker that has two identical IVs and the corresponding ciphertext can begin to decode the static WEP key, putting your network at risk.

Some IVs are inherently weak. An attacker that sees one of these weak IVs can exploit it to help decode the static WEP key. There's no real fix here, although a larger key size (104 bits vs. 40 bits) helps, because a longer WEP key takes longer to decode. Changing the keys frequently is the best solution.

WEP with dynamic keying solves the weak IV problem. By rotating the keys frequently, dynamic WEP can make it much more difficult to crack the password, keeping data secure. If the keys are changed every 15-30 minutes for each user session, an attacker would have less than a half hour to decode the key before it changed again. That's pretty good.

Dynamic WEP uses different keys for unicast traffic and broadcast traffic. The unicast key, which is unique to each user's session, is dynamically generated and changed, or rolled, frequently. It's also changed every time the user roams to a new AP or logs out and logs back in. A separate key is used for broadcast and multicast traffic. The broadcast/multicast key must be the same for all users on a particular VLAN/subnet and radio because users sharing the same VLAN and radio should see the same broadcasts. These keys should be rolled frequently—ideally every 15-30 minutes.

Ask your prospective WLAN system vendors how they handle key generation. Frequently rolling the keys can affect performance if you have a large enterprise or heavily loaded RADIUS server. Most AP vendors rely on the RADIUS server to generate keys for all wireless users.

A more scalable approach is to offload the key generation function to WLAN or mobility switches, instead of relying on the RADIUS server. Offloading the RADIUS server better distributes and scales crypto processing, since any given WLAN switch may need to perform crypto services for only 100 to 200 users, while a RADIUS server would have to scale to thousands of users. Also many wireless switches use hardware acceleration for encryption processing rather than relying on crypto software running on a server.

Although dynamic WEP overcomes the weak IV problem of static WEP, it offers only a basic message integrity check (MIC) to prove that a message has not been altered. WEP is susceptible to DoS attacks because it uses a cyclical redundancy check (CRC) for the MIC. CRCs are not cryptographically secure; they are relatively easy to defeat. This approach carries some risk, but be mindful that traditional wired intranets face similar risks. Most Ethernet jacks in employees' cubes are not as well protected from DoS attacks as the external Internet connections to the corporate network.

A major advantage of using dynamic WEP is its straightforward deployment. You can deploy dynamic WEP without upgrading your client OS drivers or AP firmware. Deploying dynamic WEP is a no-cost, minimal-effort undertaking. It's easy—and that's a big advantage.

Although dynamic WEP is not in the WLAN limelight, it offers adequate protection. By rolling the keys frequently, it overcomes static WEP's weaknesses. Dynamic WEP keys are much harder to crack, and data privacy is reasonably assured. However, dynamic WEP is at minimal risk to DoS attacks.

Some corporations, satisfied with the security level provided by dynamic WEP with rolling keys, will skip the upgrade step of moving to TKIP and simply wait to move to AES. Other organizations may find that the interim upgrade to TKIP is worthwhile. Regardless, AES remains the holy grail of WLAN encryption.

WPA 1.0 with TKIP

The Wi-Fi Alliance created WPA, which is 802.1X port-based authentication combined with TKIP encryption, as an interim solution until the 802.11i standard is ratified in 2004. TKIP is essentially a wrapper around the same encryption engine used by static and dynamic WEP. TKIP has several advantages.

TKIP uses a longer key—a true 128-bit key, while WEP uses a maximum 104-bit key. With TKIP, the key and the IV are changed with every packet, which eliminates the weak IV problem entirely. Cracking TKIP is much more difficult.

To prevent forgeries and other active attacks such as fragmentation attacks, bit-flipping attacks and iterative guessing against the key, TKIP adds a true, keyed MIC, called "Michael." Michael is a keyed hash, making it cryptographically secure. Michael is 64 bits, which is twice the size of WEP's CRC. If you're running TKIP and

someone tampers with the packet, the packet will be discarded. If someone tampers with two or more packets within one minute, TKIP instructs the AP to regenerate keying material, resulting in the AP refusing end user connections for a short time (about one minute) in an attempt to dampen the potential attack.

Thus in solving the message integrity issue, TKIP created another challenge: It can be used as the source of a DoS attack itself. If TKIP sees two bad MICs within one minute, it assumes it is an attack and kicks all users off the AP and invalidates all key material. If the attacker is a man-in-the-middle, the AP invalidates everyone's keys. In an attempt to be ever vigilant about security, TKIP ends up encouraging simple DoS attacks.

While TKIP doesn't require new WLAN hardware, it does require some effort to support. Client operating systems must be upgraded to the latest versions of Windows XP or MacOS. Wireless card drivers must be updated. How the AP supports TKIP will vary by vendor; it may require a firmware update. Only Windows XP supports TKIP, so if your organization is pre-XP, you'll need a third-party solution to run TKIP on other Windows platforms. And don't forget to turn off WEP in the client to run TKIP; the two can't operate simultaneously since they share the same encryption engine.

WPA 2.0 with AES

AES, the U.S. government approved successor to the Triple Data Encryption Standard (3DES), is the ultimate in wireless encryption. AES eliminates all the vulnerabilities of WEP, including the potential for DoS attacks. AES is the result of a four year effort involving cooperation between the U.S. government, private industry and academia around the world. It's the strongest encryption available for non-military application, and it can be exported outside the United States. AES is also known as FIPS 197.

To give you an idea of AES's quality, the National Institute of Standards and Technology (NIST) describes it this way: While no one can predict how long any encryption algorithm will remain secure, it took 20 years to crack DES. But if you could build a machine that could recover a DES key in a second, it would take that machine 149 trillion years to crack a 128-bit AES key. To put this in perspective, the universe is believed to be less than 20 billion years old.

AES appears to be more cost-effective than TKIP. In addition, AES is very computationally efficient and requires less processing power than 3DES. While AES will be a part of 802.11i, that IEEE standard is not yet complete. Windows XP is capable of supporting AES, and pre-standard AES cards and drivers have begun appearing in the market as of summer 2003.

802.11i allows AES to be implemented in software, so adapter cards, clients and APs can support AES through new drivers or firmware. Be aware that many platforms, particularly APs, rely on hardware in the radio chips to perform encryption and so do not include enough processing power for encryption. Ask your WLAN system vendor whether the AP they sell you today can migrate via software to support AES tomorrow.

FIPS 140 and IPsec VPNs

If you're doing business with the U.S. or Canadian governments, your RFPs will likely call for FIPS 140 Level 1 or Level 2 certification. The FIPS 140 certification program, run by NIST, is an extensive documentation and testing process that demonstrates end-to-end secure computing. Employing IPsec VPNs with a public-key infrastructure (PKI) and static IP addresses can provide FIPS 140 certification when used on a FIPS approved platform. FIPS approved platforms may be employed alongside Trapeze Networks equipment, and users and administrators can still benefit from the advanced features of the Trapeze Networks Mobility System Software™ (MSS™).

To compensate for the weakness of static WEP, some organizations that don't have these government requirements chose to implement VPNs for access and subnet mobility on WLANs. Given the emergence of 802.1X and dynamic WEP with rolling keys, the VPN approach is rarely needed outside of FIPS environments. In fact, some organizations that perceive VPNs as providing tight security take shortcuts in the VPN deployment that actually reduce security. Using 802.1X authentication can plug the security holes in this approach.

Let's examine how 802.1X can improve WLAN security if you are using IPsec VPNs. Normally IPsec VPNs are deployed in point-to-point network topologies, like dial remote access for example. However, 802.11 networks are Layer 2 broadcast domains—much like the early days of Ethernet on shared hubs. Anywhere there is an access point you have a Layer 2 broadcast domain. This opens up lots of security issues at Layer 2.

IPsec VPNs offer good security at Layer 3 but come with their own set of challenges. First, to protect against Layer 2 broadcast domain problems, VPNs require client software or personal firewalls that are a nightmare to deploy and manage. Moreover, because Dynamic Host Control Protocol (DHCP)-based IPsec VPNs require an IP address before encryption can begin, an attacker can easily get an IP address and launch an attack on other users associated with the same AP.

Even if static IP addressing is used, attackers can assign themselves an unused IP address in a given subnet and execute attacks against other users connected to the same AP. If your IPsec VPN uses RADIUS for user authentication then you probably use the IPsec XAUTH shim. XAUTH requires a secret shared by all, negating the mutual authentication provided by Internet key exchange (IKE). XAUTH is vulnerable to man-in-the-middle attacks, and carries known plain text of name and password prompts as encrypted payload.

Perhaps the most significant VPN detractor is the significant complexity and difficulty of scaling a VPN deployment across a large user population. As WLANs proliferate and support more users, maintaining VPNs for security quickly leads to an expensive overlay of VPN tunnel servers.

Furthermore, IPsec does not have a standard way to support multicast key distribution, so you'll have to unicast the streaming video of the CEO's monthly address where every one of the large enterprise's 40,000 employees is tuning in for a private broadcast from his or her office, home office, satellite office or local coffee shop—a significant increase in network traffic.

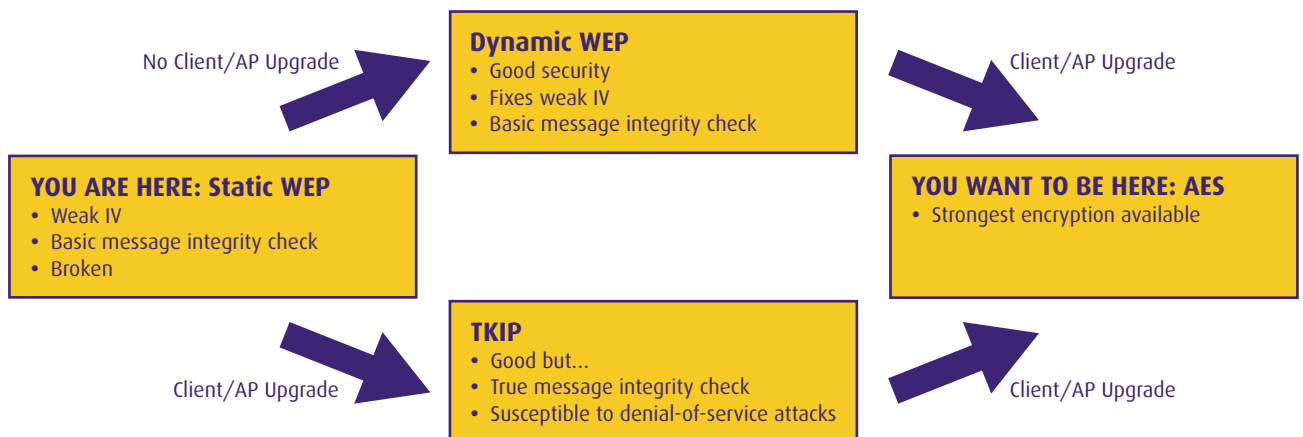
You can deploy both IPsec and 802.1X security to ensure the strongest possible authentication, encryption and communication. 802.1X will give you Layer 2 protection that cannot be provided by today's IPsec Layer 3 VPNs.

If FIPS 140 Level 2 security is needed, a strong implementation of IPsec with a public key infrastructure (PKI) is usually required. This approach is quite secure and usually quite expensive. But it is still a valid option and is totally transparent to 802.1X and Layer 2. This option may be added on to an existing 802.1X WLAN when needed.

What's the Best Deployment Course?

Don't let security paranoia stop you in your tracks. It's actually less secure to do nothing now while waiting for 802.11i and AES to be finalized. The best way to secure your WLAN is to identify your security goals. Most corporate enterprises want to give wireless users security that is at least equal to the security for wired users.

For many organizations, dynamic WEP will provide the strongest security with the easiest deployment that fits their WLAN clients' needs. Many are looking at upgrading to WPA 1.0 with TKIP, and the industry widely agrees that AES is the ultimate security answer.



The Ideal Wireless LAN System

After you have determined the right encryption for your environment, examine how different WLAN systems meet enterprise security requirements. The ideal WLAN system supports multiple encryption types and distributes cryptography processing across WLAN mobility switches and APs, offloading the RADIUS server.

Support for multiple types of encryption lets you fine-tune security to your business need. You should be able to use different types of encryption for different users or groups. For instance, you may want to use 802.1X authentication with AES encryption for engineering users while the marketing department gets dynamic WEP. Also, while laptops and PDAs have sufficient processing power to handle rotating keys, digital phones and other such devices will likely require the use of static WEP.

Any WLAN system you consider should enforce per-user dynamic keying and change the keys every 15-30 minutes transparently to the client to avoid the weak IV problem in static WEP. With per-user dynamic keying, you can set the encryption types by the user's identity. In addition to supporting dynamic WEP, your WLAN system should be TKIP- and AES-ready as those standards are finalized.

Your enterprise WLAN system should be able to offload key generation from the RADIUS server and distribute it to the WLAN mobility switches. Distributing cryptographic processing to mobility switches offloads the RADIUS server, which would be hard pressed to handle key generation for hundreds or thousands of users. For added scalability, look for WLAN mobility switches that offer hardware acceleration for cryptography. This feature is common in the new generation of mobility switches, but it is not available in RADIUS servers.

Also examine the functionality of the AP when considering WLAN system architectures. The current crop of "thin" APs are cheap but totally emaciated and bereft of any useful security capabilities. Then there are the "fat" APs advocated by incumbent vendors in a desperate attempt to protect their installed base of old, outdated legacy equipment. Containing sensitive access and routing information, fat APs represent the most serious security breach because they are placed on ceilings and walls in plain view of potential hackers and thieves.

So called "integrated" or "hybrid" APs that retain enough intelligence to handle encryption give you the most cryptographic scaling at a minimum cost. Encryption algorithms are part of the radio chipset on the AP, so you don't have to pay extra for centralized encryption as you do in a switch or VPN appliance. A June 2003 report by Forrester Research states that a hybrid "contains elements of both thin and fat access points and distributes work where it makes sense. It is likely that this approach will be refined, improved, and followed by other vendors and become even more sophisticated."

Once you've resolved your encryption strategy, you must deal with the RF nature of WLANs.

Planning for Signal Propagation

Wireless LAN security doesn't usually conjure up images of network planning, but planning is a critical element of WLAN security. Cabling provides the most basic line of defense for wired networks. Not so for RF networks with propagating signals. Building a WLAN involves more than installing APs every 40-70 feet. Carefully planning a WLAN in advance of actual deployment lets you control where the RF signal propagates.

RF planning and management tools offer that control and you should not attempt to install an enterprise-class WLAN system without them. Automated planning tools let you create what-if scenarios that show where you want RF coverage—and where you don't want it. You don't want to blast RF signals into the parking lot or neighboring businesses, but you might want coverage, for example, in your company's outdoor eating area. With these tools, you'll see where RF signals propagate before deploying a single AP.

Locating and Identifying Rogues

Authentication and encryption mitigate the risk of rogues because all users must be authenticated to gain access to the WLAN, and once authorized, all communication is encrypted. Although an attacker that manages to get access cannot steal or corrupt any data, it's still critical to detect and locate rogue APs because they are the main source of man-in-the-middle and DoS attacks.

Look for RF planning tools that also provide air-aware management. These kinds of tools are a key defense for detecting and locating rogues. For instance, there are WLAN management tools that verify received RF signals after deployment, making it easy to pinpoint an unknown or unapproved user or AP, because it knows who the approved users and APs are—and where they are located. Then through regular scanning of the entire network, the WLAN management tool can detect and locate rogues.

You should also look for WLAN management tools that can identify and locate rogue APs or ad hoc clients on either 802.11a or 802.11b networks. Some APs can actually participate in network scanning across all channels, allowing a thorough and complete scan. Conversely, some APs only scan active channels, which allows rogues to hide.

In Summary

When developing your WLAN security strategy, it's important to assess the risks—and then develop a reasonable defense. It's easy to be caught in the maelstrom of security paranoia and whipped around by the seeming complexity of encryption choices. Once you've developed a plan, evaluate how the WLAN system vendors ensure a secure infrastructure.

AES has the strongest encryption available outside the U.S. military, and corporate customers will welcome 802.11i with AES encryption when the standard is ratified. In the meantime, dynamic WEP with rolling keys and TKIP, provide very strong security.

When choosing a WLAN system provider, examine the authentication and encryption support, as well as RF planning, verification and rogue detection tools, which are critical pieces in securing the WLAN.

Many vendors lay claim to meeting enterprise requirements for wireless security. But only a few actually solve the strong authentication and data encryption problem. Ideally, your WLAN should support and be ready for multiple types of encryption—dynamic WEP, TKIP and AES—so you can select the appropriate encryption by the user's identity or group association. Insist on a WLAN system that enables authentication and encryption to scale by offloading cryptography processing from RADIUS servers and distributing it throughout the WLAN infrastructure.

With the right suite of planning, deployment and management tools, IT can design a secure WLAN before deploying a single AP or mobility switch. RF planning and management tools let you deal swiftly and decisively with rogues. By planning RF coverage, you can tune your RF signal propagation to minimize coverage spilled into the parking lot or to neighboring businesses.

With knowledge of users' identities and locations, the right set of management tools can enable IT to identify rogue APs as well as ad hoc or rogue users. By pinpointing rogue locations, these management tools can be quite effective in preventing DoS and man-in-the-middle attacks.

Recommended Reading

For additional information on deploying a secure WLAN, read the following whitepapers from Trapeze Networks:

- Detecting Rogue Users and APs in a Wireless LAN
- Secure Mobility for Wireless LANs
- AP architecture impact on the WLAN, Part 1: Security and Management

Table 1. Comparing Encryption Options

	Strengths	Weaknesses	Deployment	Availability
IPsec VPNs	Early method of deploying secure wireless access before 802.1X and other secure subnet mobility approaches were available.	IPsec VPNs leave you exposed at Layer 2. Shortcuts such as DHCP or XAUTH weaken the security, leaving you exposed to attacks. Requires client software or personal firewalls, which are an IT administrative nightmare. Streaming media support is difficult.	Appropriate to environments needing to meet FIPS-level security.	Available now.
Static WEP		Weak IV. Key can be cracked in a matter of hours. Authentication mechanism fatally flawed. Using CRC for rudimentary message integrity check makes it subject to message alteration attacks.	Don't use it unless you have to.	Available now.
Dynamic WEP	Provides rolling keys and fixes weak IV problem of static WEP. Uses different keys for unicast and broadcast/multicast.	A CRC as a rudimentary message integrity check makes it subject to message alteration attacks.	Deploys easily with no changes to clients or APs.	Available now.
WPA with TKIP	Changes and cryptographically mixes WEP key and IV for every packet to eliminate weak IV problem. Uses a true message integrity check. 128-bit encryption key. Uses different keys for encryption and message integrity checking.	Vulnerable to simple DoS attacks. If TKIP sees two bad MICs in one minute, it kicks all users off the AP.	Requires a software upgrade to the client drivers and APs.	Emerging. Wi-Fi Alliance certifies products as compliant and interoperable. Mandatory certification as of August 2003.
WPA with AES	Strongest encryption available outside the U.S. military.	None known.	Requires a software or firmware upgrade to clients and APs.	AES standard complete. AES supported as part of 802.11i, which is expected to be ratified in 2004.



5753 W. Las Positas Blvd., Pleasanton, CA 94588 Phone 925.474.2200 Fax 925.251.0642

Trapeze Networks, the Trapeze Networks logo, the Trapeze Networks flyer icon, Mobility System, Mobility Exchange, MX, Mobility Point, MP, Mobility System Software, MSS, RingMaster, Trapeze Access Point Access Protocol and TAPA are trademarks of Trapeze Networks, Inc. Trapeze Networks SafetyNet is a service mark of Trapeze Networks, Inc. All other products and services are trademarks, registered trademarks, service marks or registered service marks of their respective owners. © 2003 Trapeze Networks, Inc. All rights reserved.