

Chapter 2

TYPES OF WIRELESS NETWORK SECURITY TECHNOLOGY

1. INTRODUCTION

Wireless networks are too inexpensive to ignore. But, security has stymied many network managers looking to bring wireless into the corporate fold. There's a lot of information and misinformation out there about types of wireless network security technologies. This chapter will help to clear up some of that confusion, and present some common types of wireless network security technologies to help guide your path.

The first thing you have to do is educate yourself. The Internet has a lot of data and opinions on wireless security technologies, but it's difficult to get a perspective on things without a good background primer (like this book). You need to put this into the context of corporate security. What threats are you worried about? How sensitive are the data on the wireless- local area network (LAN) or wide area network (WAN)? What vulnerabilities do you need to guard against? Sniffing? Denial of service? Freeloading? Impersonation? You'll never establish an appropriate 802.11 security policy for your corporate network if you don't think about these technologies now.

Second, you must do something to get started. Wired Equivalent Privacy (WEP) is still an awful technique to use. It's like giving everyone in the company the same password and never changing it. But, that doesn't mean you shouldn't use it. The theoretical attacks on WEP exploited by various tools are blocked by modern firmware. In some recent testing, using current releases of 10 different enterprise-class access points and eight different

client cards, Initialization Vector-based attacks on WEP were no longer effective.

Third, you should arm yourself with wireless security tools. Most wireless security tools are fabulous for enterprise network managers. If you only have a few access points to worry about, a laptop with some public domain tools is a fine start. But, without at least some tools, you'll be left completely in the dark about the wireless data speeds that are beginning to surround your network [10].

Fourth, you should prepare your wireless security strategy. Today, the 802.1X-based authentication is up-and-running technology to help resolve basic wireless security problems. Or, you can go down the virtual private network (VPN) path and treat wireless users the same way you treat remote access VPN clients. Either works fine with off-the-shelf hardware [11].

Over the long run, the Institute of Electrical and Electronics Engineers (IEEE) 802.11i standard will lay out a path to higher security for wireless networks that combines 802.1X authentication with better key management than is available on WEP. But that standard is still being cooked, and it will be a year or more before things completely settle.

So, with the preceding in mind, many wireless networks are not properly secured or-even worse-are completely unsecured. Naturally, security is a top concern among those interested in deploying wireless networks. Fortunately, both user knowledge about security and the solutions offered by technology vendors are improving. Today's wireless networks feature comprehensive security capabilities and, when these networks are properly protected, enterprises can confidently take advantage of the benefits they offer. This first part of the chapter will help you gain a better understanding of wireless LAN security elements and best practices that can go a long way toward enabling you to reap the benefits of wireless networking. And, you get peace of mind, knowing your enterprise's data is secure.

2. WIRELESS NETWORK SECURITY TECHNOLOGIES

Vendors are doing a good job of improving security features, and users are getting an understanding of wireless security. "But, all threats are still considered important, and vendors continually need to address the lingering perception that wireless LANs are insecure.

Indeed, security is the biggest barrier to the adoption of wireless LANs. And, it's not just a big-enterprise worry. When it comes to wireless

networking, security is still the number one concern for enterprises across all sizes.

Gaining a better understanding of wireless LAN security elements and employing some best practices can go a long way toward enabling you to reap the benefits of wireless networking. And, you get peace of mind, knowing your enterprise's data is secure.

2.1 Elements Of Wireless Security

Intentionally or not, enterprises and individuals may set up wireless networks with no security at all. That happens because most wireless access points come from the factory in open access mode by default, meaning that all security features are turned off. It's the buyer's responsibility to turn them on.

Three actions can help to secure a wireless network:

- Discouraging unauthorized users through authentication
- Preventing unofficial connections through the elimination of rogue access points
- Protecting data while it's being transmitted through encryption [3]

Not coincidentally, these are also important issues to companies.

The number one wireless LAN security concern is users from outside the company (illicitly or maliciously accessing the enterprise wireless LAN. Number two is internal rogue access points, and number three is encryption.

2.1.1 Using Authentication

When you want to make sure that the individuals who use a wireless network are authorized to do so, use authentication (sometimes called access control). Unique logins and passwords are the basis of authentication, but additional tools can make authentication more secure and reliable. The best authentication is per-user, per-session mutual authentication between the user and the authentication source.

2.1.2 Checking For Rogue Access Points

A well-meaning employee who enjoys a wireless network at home might want to enjoy the same freedom at work. He or she might purchase a cheap access point and plug it into a network jack without asking permission. These are known as rogue access points, and the majority of these are installed by employees—not malicious intruders. Even company-sanctioned access points, when configured improperly, can be security risks.

Checking for rogue access points isn't difficult. There are tools that can help, and checking can be done with a wireless laptop and software in a small building or by using a management appliance collecting data from your access points.

You can have technical personnel scan for new wireless access points. And, if they do a daily scan, they can pick these things up early.

2.1.3 Using Encryption

To make sure that data can't be read, and to protect data from being altered as it's transmitted between an access point and a wireless device, use encryption. In a basic sense, encryption is like secret code: It translates your data into gibberish that only the intended recipient understands. Encryption requires that both the sender and receiver have a key to decode the transmitted data. The most secured encryption uses very complicated keys, or algorithms, that change regularly to protect data.

2.2 Available Solutions For Wireless Security

Three solutions are available for secure wireless LAN encryption and authentication:

- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access 2 (WPA2)
- Virtual private networking (VPN) [3]

The solution you select is specific to the type of wireless LAN you're accessing and the level of data encryption required.

2.2.1 WPA and WPA2 Standards-Based Security Certifications

WPA and WPA2 are standards-based security certifications from the Wi-Fi Alliance for enterprise, SMB, and small office/home office wireless LANs that provide mutual authentication to verify individual users and advanced encryption. WPA provides enterprise-class encryption and WPA2. These are the next generation of WiFi security, which supports government-grade encryption.

It is recommended that WPA or WPA2 be used for enterprise and SMB wireless LAN deployments. WPA and WPA2 provide secure access control, strong data encryption; and, they protect the network from passive and active attacks.

2.2.2 Using VPN

VPN provides effective security for users wirelessly accessing the network while on the road or away from the office. With VPN, users create a secure tunnel between two or more points on a network using encryption, even if the encrypted data is transmitted over unsecured networks such as the public Internet. Home-based teleworkers with dial-up or broadband connections can also use VPN.

2.3 Policies For Wireless Security

In some cases, you may have different security settings for different users, or groups of users, on your network. These security settings can be established using a virtual LAN (VLAN) on the access point. For example, you can set up different security policies for distinct user groups within your enterprise such as finance, legal, manufacturing, or human resources. You can also set up separate security policies for customers, partners, or visitors accessing your wireless LAN. This allows you to cost effectively use a single access point to support multiple user groups with different security settings and security requirements—all while keeping your network secure and protected.

It is also important to consider wireless network security in the context of overall network security and network management. The majority of enterprises that deploy, or will deploy, wireless LANs want to do it in a way that complements the wired LAN. They want it integrated with common management.

A common management system increases efficiency for network administrators. Resource-strapped SMBs can use management tools to simplify and automate many repetitive and time-consuming administrative tasks.

Wireless LAN security (even when integrated with overall network management) only works if it's turned on and used consistently across the entire wireless LAN. That's why user policies are also an important part of good security practices. Resist the temptation to overact when setting a wireless LAN security policy. The first policy is often 'no wireless. The problem with that is, there are so many massive gains from having wireless in place.

The challenge is to devise a wireless LAN user policy that's simple enough that people will abide by it, but secure enough to protect the network. Today that's an easier balance to strike because WPA and WPA2 are built into WiFi certified access points and client devices.

Your wireless LAN security policy should also cover when and how employees can use public hot spots, the use of personal devices on the enterprise wireless network, the forbidding of rogue devices, and a strong password policy.

2.4 Taking Practical Steps

The first step in security a wireless network is to turn on the security features inherent in your access points and interface cards. This is usually done by running a software program that came with your wireless equipment.

The same program that turns on your wireless security features will probably also show what *firmware* version your access points use [3]. Check the device manufacturer's Web site for the most current firmware version, and update your access point if it's not current. Updated firmware will make your wireless network more secure and reliable. Also check to see what security resources your hardware vendor offers.

Note: Firmware is software used by devices such as access points or routers.

Not everyone who wants the benefits wireless networking is capable of, or interested in, deploying and maintaining a secure wireless LAN. In such cases, value-added resellers, network implementers, or other suppliers of wireless networking gear can often help with these tasks.

Some SMBs choose to enlist the aid of an outsourced managed security service, many of which have wireless security offerings. According to Jupiter Research [4], a small but considerable segment of enterprises (13%), would outsource wireless security; compared to the 18% that would outsource their overall network management [3].

No matter how you proceed, do it in an organized fashion. Security is definitely something that has to be planned for, just like managing the network, providing coverage and access, and so forth. But, it shouldn't be a barrier to the deployment of a wireless LAN.

3. WIRELESS NETWORK SECURITY TECHNOLOGY PERSPECTIVES

Today, many enterprises are embracing wireless networking technologies to enhance productivity, provide better customer service, and even offer

Internet access to partners and on-site visitors. The emergence of new technologies, widespread cellular-data service, and an increasing number of wireless access points are making it easier for users to access information they need, when and where they need it.

With wireless hotspots available in coffee shops, airports, and restaurants, business travelers can work easily no matter where they are. In addition, many users are enjoying the convenience of wireless fidelity (Wi-Fi) connections in their hotel rooms and homes.

While providing users wireless access to file shares, applications, and other network resources offers many benefits, doing so can present security and manageability challenges. The multiplicity of connectivity options—cellular, local area networks (LANs), wireless local area networks (WLANs), and WiFi—can be difficult for IT departments to manage.

Because users need to access resources from both IT-managed devices such as corporate laptops and from unmanaged devices such as personal digital assistants (PDAs), many existing remote access solutions leave the network open to security threats from viruses, malware, and Trojan horses. In addition, the lack of interoperability among wireless vendors, an ever-evolving security framework for WLANs, and issues related to Internet and firewall traversal present further challenges [7].

3.1 Using SSL VPNs In Secure Wireless Networking

Enterprises are embracing wireless technologies to increase productivity, provide more flexible work arrangements for their employees, and work more closely with their business partners. Wireless technologies include both local area and wide area systems. However, the multiplicity of networking options as well as computing platforms creates significant security issues, including:

- An evolving security framework for WLANs and interoperability issues between vendors.
- Different native security options for wireless local area networks (WLANs) than cellular networks.
- Employees using both managed devices and unmanaged devices, such as home computers and public terminals.
- Internet traversal for many wireless remote-access solutions.
- Outdated WLAN equipment that is insecure.
- The danger of rogue access points [1].

The security architecture that addresses all these issues is an SSL virtual private network (VPN). SSL VPNs provide a means of protecting every node, whether internal or external to the enterprise, leading to the concept of an inverted security model that does not depend on a hardened perimeter. By

taking advantage of installed browsers and the associated SSL security layer, enterprises can not only provide access through computers that have no VPN client software installed, but can also provide additional communications flexibility for systems with dynamically installed software.

3.1.1 Wireless Networks Prevalence

As previously explained, many enterprises are embracing wireless networking technologies to enhance the productivity of their workers, to improve customer service, and even to provide Internet access to visitors. Business travelers are taking advantage of wireless hotspots in public locations such as airports and restaurants, as well as enjoying the convenience of Wi-Fi in their hotel rooms and homes. They are also using cellular networks for communications from almost anywhere.

Although most wireless-data usage has been with Wi-Fi (based on the IEEE 802.11 family of standards), enterprises are increasingly using cellular-data services, which now offer a near-broadband experience over wide geographic areas. Cellular-data usage includes smartphones, PDAs and laptops with PC Card modems, and laptops using phones as modems by means of a cable or Bluetooth connection. Cellular-data networks encompass multiple technologies, the most prevalent of which today include Enhanced Data Rates for GSM Evolution (EDGE), Wideband CDMA (WCDMA), and the CDMA2000 group of technologies. Despite the alphabet soup of names, they all have a common capability—the ability to support IP-based packet communications from almost anywhere [1].

Emerging technologies such as WiMAX promise even higher performance over the wide area. Whereas cellular-data networks offer rates approaching 1 Mbps, WiMAX vendors are hoping to provide higher throughput rates [1].

Many professionals use a combination of Wi-Fi and cellular data networks. Wireless networking not only increases productivity, but it also enhances personal lifestyles—employees can telecommute not just from home but from practically anywhere.

The multiplicity of connectivity options, however, raises significant security challenges for your enterprise, which needs to secure these connections while accommodating a wide variety of mobile computing platforms, providing a simplified user experience, and limiting access to specific resources, all within a system that can be managed easily.

3.1.2 Wireless Connectivity Security Challenges

The number one concern expressed by IT managers regarding wireless networking is security. This is justifiable, because radio signals are inherently subject to eavesdropping due to their extended propagation.

Fortunately, there are many effective approaches for securing both Wi-Fi and cellular-data connections. To understand the benefits and limitations of the various approaches, you need to first consider the security issues in greater detail.

3.1.2.1 Issues For Wi-Fi Security

Initial implementations of Wi-Fi security, called Wired Equivalency Protocol (WEP), were completely inadequate, allowing any determined attacker to easily monitor connections or access the network. A new Wi-Fi security standard, IEEE 802.11i, addresses the security problems of WEP. This standard has come in two iterations: Wi-Fi Protected Access (WPA), which addresses all the deficiencies of WEP, and WPA2, which bolsters encryption by using the Advanced Encryption Standard (AES). IEEE 802.11i is based on IEEE 802.1X, a port-based security architecture where authentication is handled by using Extensible Authentication Protocol (EAP) methods in conjunction with authentication systems such as RADIUS. Most new equipment supports WPA or WPA2, both of which are considered reasonably secure [1].

A number of issues exist, however, for organizations using IEEE 802.11i for Wi-Fi security. First, IEEE 802.11i does not accommodate older deployed equipment; second, it applies only to access equipment in the organization's control; and third, the complexity of IEEE 802.11i-based security solutions is already raising interoperability concerns among different vendors' equipment.

To fill the Wi-Fi security gap, many Wi-Fi vendors have implemented security enhancements in their equipment. Many of these enhancements have required customers to buy cards and access points from the same vendor. This vendor dependence also applies to new WLAN architectures that employ centralized controllers to coordinate and manage access points. These controllers often include security functions, such as detecting rogue access points and providing VPN tunnel end points. However, any security benefits from these architectures apply only to the directly connected WLAN nodes and do not extend to other connections, such as Ethernet, or to WLAN connections in public places or employee homes.

3.1.2.2 Issues For Cellular-Data

With cellular-data connections, the security issues are somewhat different than for Wi-Fi. For example, whereas Wi-Fi attackers can use normal Wi-Fi hardware for their attacks, cellular-network attackers require specialized equipment to receive and decode the radio signal. The cost of such specialized equipment by itself, however, is not a sufficient deterrent. As a result, some (but not all) cellular networks encrypt the radio link. The general trend of cellular networks is for 3G technologies, with the most current generation of these technologies designed to offer strong encryption based on algorithms such as Kasumi and AES. Even after these next-generation networks are widely available, though, they are still likely to rely on previous-generation technology for coverage in less densely populated areas, where encryption is not always provided. And even if your home operator encrypts the link, you may roam onto a partner network that does not. The bottom line is that you cannot depend on the protection of the radio link.

Cellular-data connections share a common issue with Wi-Fi hotspots. Both primarily offer connectivity to the Internet, and even when they encrypt the radio signal, the IP traffic over the Internet portion remains unprotected. As an option, some cellular operators offer more secure back-end connectivity options to connect from the operator's core network to the customer network, including dedicated frame relay circuits or IPsec-based, network-to-network VPN connections. However, these arrangements incur additional costs, both through initial networking setup fees and then through recurring monthly fees.

3.1.2.3 Connections And Platforms Multiplicity

Although it is possible for you to implement specific security solutions for Wi-Fi and for cellular-data connections, each solution will be unique, and managing both is probably not practical. Another concern is that employees may use a variety of computing devices, including portable computers, smartphones, PDAs, home computers, and public systems. IT will have control over some, but not all, of these devices. Unmanaged devices, including home systems and public workstations may leave the network open to security risks.

3.1.3 Wireless Security Architecture Recommendations

There is a clear need for a security solution that embraces the world of mobile and wireless computing—with an approach that addresses all forms of connectivity, including Wi-Fi on premises, Wi-Fi off premises, cellular

data, public kiosks, home access, and whatever else may become available. But before you can specify an effective security architecture, there are other important security features that you will probably need, including the ability to:

- Allow conformance with government regulations that protect items such as financial and medical information.
- Have control over the end-point node to check for proper software configuration such as virus protection, to scan the system for dangerous code, and to clear caches.
- Provide granular control to resources, rather than just providing access to a network.
- Support both managed and unmanaged nodes as well as accommodate a wide range of device types, including desktops, portable computers, PDAs, and smartphones [1].

The security architecture that meets all of these needs is an SSL-based VPN. SSL VPNs take advantage of the browsers and the SSL security layer that are available for nearly all computing platforms, including notebook platforms, PDAs, and smartphones. Fig. 2-1 shows an SSL appliance securing all forms of wireless access and shows how IP traffic is redirected into an SSL tunnel [1].

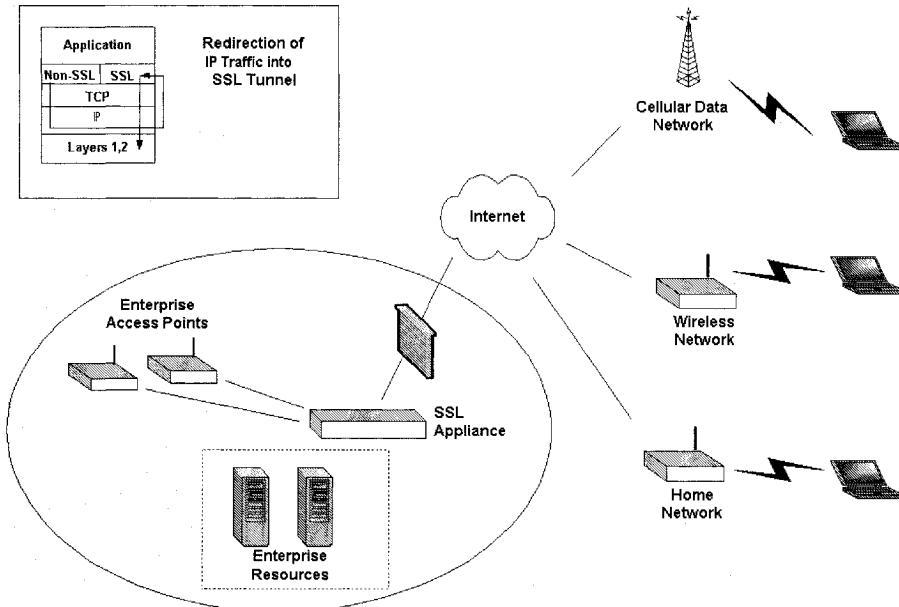


Figure 2-1. An SSL VPN can secure both external remote access and internal access.

3.1.3.1 The Inverted Security Model

Traditional security architectures are based on the concept of a perimeter, where firewalls mediate between nontrusted external networks and trusted internal networks. However, this model breaks down when a significant portion of your employees reside on public networks. The perimeter model also falls short when your network needs to allow select access by contractors, business partners, and customers.

The inverted security model assumes that you trust no node, whether internal or external. It shifts the emphasis to granular identity and access management. SSL VPNs enable this model by providing strong control of end points, strong user authentication, access to predefined resources, data integrity, nonrepudiation, and detailed auditing. By restricting access at the application layer, SSL VPNs shift security management from the network domain to the user domain.

3.1.3.2 Other Approaches Compared To VPN

According to Forrester Research [2], SSL VPNs are becoming the dominant remote access solution: By breathing new life into secure mobility and remote access, SSL VPNs will experience significant growth as both vendors and service providers mature their offerings. This growth will continue; and, Forrester expects SSL VPNs will enjoy dominant market share by 2009. Meanwhile, wireless connections are becoming the favored form of remote access.

The reasons for using SSL VPNs are clear. SSL VPNs provide trusted and proven data confidentiality, multiple user authentication methods, control over accessed applications, the greatest flexibility in platform types, and the ability to secure any connection, whether external or internal, thus fully protecting against the security risks of wireless networking.

IPSec-based VPNs will continue to be used, but have a better fit for network-to-network connections. As for other wireless security approaches, there are a variety of secure application-specific solutions, such as the RIM Blackberry. These are highly optimized for specific applications such as push e-mail and calendar synchronization, with some support for synchronization of other mobile data. They are not, however, general-purpose networking solutions like SSL VPNs. In some cases, your SSL VPN can obviate other mobile platform security solutions, whereas in other cases, you might want to use both approaches. Table 2-1 summarizes the aspects of different security approaches [1].

Table 2-1. Summary of Pros and Cons of Different Security Approaches

Type of Security Solution	Pros	Cons
IEEE 802.11i Security Standard	Comprehensive security framework for Wi-Fi security.	Available only in corporate settings. Does not address other wireless connections such as cellular. Does not support outdated hardware. Vendor interoperability issues.
Cellular Data Security Mechanisms	Primarily designed to protect operator from fraudulent use. Many networks, but not all, encrypt the radio link.	Only a partial security solution, and only if operator offers data encryption. Normal configuration has data passing the Internet in the clear. Does not address other wireless connections such as Wi-Fi.
IPSec VPN	Mature and available from multiple vendors.	Requires client code. Not necessarily available for all mobile platforms. Optimal for network access, not application level access.
Wireless-specific VPN	Efficient for wireless networking.	Specific to wireless networking and not necessarily applicable as a comprehensive enterprise security framework.
Application Specific Solutions (Wireless Email)	Efficient for wireless networking. Limits access to specific resources.	Requires client code Limited to small application base such as email, calendar synchronization, and contact databases. Not a general-purpose, remote-access solution.
SSL VPN	Efficient for wireless networking. Enhanced features such as persistent sessions can address wireless challenges. Secures all forms of connections, whether WLAN, cellular, or other.	Not yet as widely adopted as IPSec VPNs. Market still evolving.

	Provides the greatest degree of control over access to resources. Greatest client flexibility between browser, browser with agent code, and full client version.	
--	---	--

Next, serious flaws have emerged in the basic Bluetooth specification and the Advanced Encryption Standard (AES). Now, let's look at the details on both of these vulnerabilities, as part of the wireless network security (WNS) technology perspectives; as well as, a look at the rest of the latest security threats out there. It's been a bad year for encryption all around—even when encryption technology wasn't in effect.

3.2 Wireless Network Security Encryption

Apparently, all of Bluetooth is divided at the core, according to Israeli security specialists who have recently reportedly found a serious core vulnerability in the basic Bluetooth specification. According to NewScientist.com (<http://www.newscientist.com/home.ns>), researchers have discovered a cryptographic flaw (the worst kind of flaw) in the Bluetooth standard that renders all Bluetooth implementations vulnerable to a fairly simple attack, making those implementations completely insecure.

Bluetooth is a short-range (about a 300-foot maximum) radio standard used by networks to feed data to printers, portable phones, laptops, and other electronic devices. The newly discovered decryption technique makes all Bluetooth communications insecure—even when the user has enabled all of the security features to the maximum levels.

This is not the same vulnerability that exists when Bluetooth devices initially negotiate their connection, which is a well-known threat that's rather difficult to exploit. Instead, the new threat lets attackers penetrate a Bluetooth network at any time and take over the connection, perhaps establishing a connection allowing unlimited long distance calls. Basically, the researchers have found a way to force Bluetooth devices into the initial pairing mode and thus decrypt the 128-bit key in well under a second, even using older PCs.

In addition, one basic design flaw in Advanced Encryption Standard (AES) allows a timing attack to recover AES keys from a remote server

using OpenSSL AES. To make matters worse, this basic design flaw in AES is not limited to any particular implementation.

3.2.1 Serious Applicability Risk Level

The Bluetooth flaw affects any and all Bluetooth networks, and the AES vulnerability affects any and all AES encryption. Because these new vulnerabilities affect the overall technology rather than a specific implementation, the risk level is serious for both flaws.

With regards to the preceding, the FBI recently demonstrated how easily someone can break Wired Equivalent Privacy (WEP) encryption and gain access to a secured network. This part of the chapter examines the critical role that security plays in wireless technology and offers some suggestions for locking down your wireless network.

3.3 WEP Woes

As previously mentioned, the Federal Bureau of Investigation recently were able to conclusively demonstrate how insecure the majority of wireless networks really are. In addition, the agency announced that even 802.11b wireless access with Wired Equivalent Privacy (WEP) encryption (widely touted as the secure replacement for the 802.11a standard) is just as insecure.

Anyway, it took the FBI literally four minutes to demonstrate how to break WEP encryption and gain access to a secured network. The FBI's findings should serve as a warning to enterprises currently using wireless access, and it might prevent some enterprises from using wireless networks entirely. Regardless, enterprises need to be more aware of the critical role that security plays in wireless networks.

Whatever comes of the FBI demonstration, it's important that enterprises fully understand this concept: Unless you've deployed end-to-end data encryption, communication is never really secure, no matter how well-secured the wireless network. Despite advances in wireless technology, the security of a wireless network will never equal that of a wired network.

Unfortunately, most enterprises that have already deployed wireless access chose usability over security, just like most software enterprises. In addition, many enterprises don't consider the fact that wireless access doesn't really offer any advantages over wired access in many cases.

In fact, it can actually introduce new problems. Numerous 802.11b wireless network problems have been caused entirely by the use of 2.4-GHz wireless phones, often from wireless PBX systems.

Wireless networks are now in the enterprise environment, and enterprise deployments are increasing. However, it is strongly recommended that

enterprises use this strategy when deciding whether to go wireless: Use wireless networking only in cases where wired access is impossible, not just as a simple or trendy alternative.

And, while security should be a primary factor in this decision, keep in mind that there are more than just security-related reasons for staying wired. For example, wired networks can handle significantly higher bandwidth, as well as offer better security, because they don't broadcast packets of information.

But, if bandwidth isn't a concern, and the powers-that-be are convinced that wireless is the way to go, rest assured that it is possible to make wireless access much more secure without depending on WEP. Two methods for accomplishing this include using protocols such as Point-to-Point Tunneling Protocol (PPTP) or Layer Two Tunneling Protocol (L2TP) and enforcing access controls with usernames and passwords or some other authentication method. Add IPSec to the mix, and you've got both access control and end-to-end encryption that's more secure than wired network access. But, keep in mind that this solution is still prone to interference.

Of course, some people will argue that 802.11i features all of this security provided by Wi-Fi Protected Access (WPA) (WEP's expected replacement); as well as, better interference control. While this is great news, 802.11i is no use to anyone until there are plans to replace all existing wireless networking equipment or upgrade the firmware, if that's even possible.

In addition, remember that no matter what security technologies or standards emerge, there will always be someone out there trying to break it—and that includes WPA. In any event, you can deploy Gigabit Ethernet access at a lower cost, so it can provide both superior security and bandwidth irrespective of data encryption.

If wireless access is your only alternative, explore the use of PPTP/L2TP and IPSec on your existing infrastructure before deciding to replace or upgrade existing 802.11a and 802.11b equipment. While it's not pretty from a technological point of view, it's quite functional, and it just might prove to be more secure than 802.11i [1].

Even with the heightened awareness of the security risks posed by wireless networks, some IT pros continue to overlook some of the essential safeguards the systems require. This next part of the chapter presents five practices you should avoid so that you can ensure the best protection for your wireless network.

4. WIRELESS NETWORKS AT RISK: ASSESSING VULNERABILITIES

Wireless networks require the same security measures as conventional networks, and then some. The issues that concern you in the wired realm should still concern you with wireless networks and devices: Keep the encryption strong, keep the certificates in place, and keep focused on security. Wireless security isn't a matter of *different* security, it's a matter of *more* security. Here are the most common security oversights and how you can avoid them.

- Don't breach your own
- Don't spurn MAC
- Don't spurn WEP or WPA
- Don't allow unauthorized access points
- Don't permit ad-hoc laptop communications [5]

4.1 Don't Breach Your Own Firewall

You've firewalled the network, wireless or not, and rightly so. However, you've done yourself no good if your configuration doesn't place your wireless system's access points outside the firewall. Make sure it does—otherwise, you're not only failing to create a necessary barrier, you're creating a convenient tunnel through one that was already there.

4.2 Don't Spurn MAC

Media Access Control (MAC) is often ignored because it's not spoof-proof. But it is another brick in the wall. It's essentially another address filter, and it clogs up the works for the potential hacker by limiting network access to registered devices you identify on address-based access control rosters. MAC also lets you turn the tables on the potential intruder.

Consider that the intruder must knock on the door before being denied. If you have MAC in place, the intruder will bump into it before realizing it's there and then must regroup to get past it. And, now your network knows what the intruder looks like. So think of your MAC list as creating three classes of visitors:

- Entities that aren't on the list but are known because they've tried to get in before, uninvited, and are now instantly identifiable if they approach again
- Friendly entities that are on the MAC list
- Unknown entities that aren't on the list and that knock by mistake [5]

In short, if you monitor your wireless network and watch for multiple attempts at access by entities not on the MAC list, you've spotted a potential intruder. And, he or she won't know you've seen him or her.

4.3 Don't Spurn WEP Or WPA

Wired Equivalent Privacy (WEP) is a protocol specific to wireless security, conforming to the 802.11b standard. It encrypts data as it goes wireless, over and above anything else you're using. Use it. But remember that it is key-based, so don't stay with the default key. You may even wish to create a unique WEP key for individual users when they first access the system. Don't rely on WEP alone. Even multiple layers of encryption don't make you hack-proof, so use WEP in combination with other wireless-specific security measures.

And, don't overlook WiFi Protected Access (WPA2), which addresses header weakness issues in WEP and is readily available to Windows XP users. WPA2 can be configured to rekey your encryption and is actually easier to use than WEP.

4.4 Don't Allow Unauthorized Access Points

Access points are incredibly easy to set up, and an over-burdened IT department might loosen the rules to allow them to be set up on an as-needed basis by anyone smart enough to run a VCR. But, don't succumb to this temptation. The access point is a primary target for an intruder. Implement a deployment strategy and procedure and stick to them. Carefully outline the correct guidelines for positioning an access point and be certain that anyone deploying an AP has those guidelines on hand. Then, put a procedure in place for noting the presence of the AP in your wireless network configuration for future reference and for appropriately distributing or making available the revised configuration. Regardless of who sets up the AP, have another person double-check the installation as soon as it's convenient. Is this a lot of trouble to go to? Yes. And, security penetrations due to rogue or leaky APs are even more trouble.

4.5 Don't Permit Ad-Hoc Laptop Communications

This is a tough one to enforce in any enterprise. Ad-hoc mode lets WiFi clients link directly to another nearby laptop, which is so darned convenient; you just can't imagine not using it. As part of the 802.11 standard, ad hoc mode permits your laptop's network interface card to operate in an

independent basic service set configuration. This means that it can go peer-to-peer with another laptop via RF. When you're in ad hoc mode, you can spontaneously form a wireless LAN with other laptops.

At face value, this is such a cool trick that no one can resist trying it out. But, it permits access to the entire hard drive of the laptop. If you enable it and forget that it's enabled, your fly is open for all the world to see. And, the danger isn't only to your open machine. An intruder can also use the networked laptop as a doorway into the network itself. If you leave your machine in ad hoc mode and somebody sneaks in, you've exposed the entire network. Avoid this risky habit by never letting it develop in the first place. Just accept that it isn't worth the risk [5].

Finally, let's look at end point security control. This final part of the chapter explains the range of features that increase IT control and data protection by giving users access that's finely tuned to the risks of their environment.

5. END POINT SECURITY CONTROL

The widespread use of SSL VPNs for remote access enables more users to gain access to your network from far more places than they would if they were using a traditional IPSec VPN. Clearly, that enhances productivity; at the same time, security threats for both the end user and IT increase substantially as access extends to places that IT cannot possibly control. To effectively control these risks, managing access by user identity alone is no longer enough. You also need to focus on the safety of that user's environment.

For example, your enterprise needs to deliver secure anywhere access to network resources from the most dangerous places (New Orleans, from airport kiosks, employee-owned PCs, wireless hot spots, and unmanaged PDAs) without sacrificing the integrity of the enterprise network. In other words, your IT administrators should be able to differentiate a remote access policy based on end point security. Here's what you should be able to offer:

- Security anywhere access from multiple environments
- Policy Zones rather than an "access" policy
- Device Interrogation
- Control and ease of administration [6]

5.1 Security Anywhere Access From Multiple Environments

An executive might work remotely using a enterprise-issued laptop PC, then log into the network in the afternoon to check e-mail from a tradeshow kiosk. Later that day, she might update a presentation from her home PC. End point security control should be able to secure all these end points as appropriate based on the security policy you set. For example, this would mean limiting her access to certain applications or requiring advanced data protection on riskier end points.

5.2 Policy Zones Rather Than An Access Policy:

You want to deliver as much access as possible to your users, without compromising security. To do that, you need more options than simply allow access or don't allow access. If an end point is semi-trusted, for example, you want to create three more Policy Zones, for example trusted, semi-trusted, and non-trusted. This allows IT to offer users some degree of centrally managed access even if an untrusted environment doesn't warrant full access rights.

5.3 Device Interrogation:

You should be able to detect what is or isn't on an endpoint machine. For example, you should be able to automatically launch an agent prior to authentication, so login can be stopped if any malicious software (malware) is discovered. Based on what applications are found on the end point (for example, a predefined personal firewall or anti-virus application), you should be able to automatically classify the end point into one of the Policy Zones, so that the level of access granted is appropriate both to the user and the level of risk of the end point.

5.4 Control And Ease Of Administration

Your object-based policy model should be able to administer SSL VPN. This provides the ability to easily enforce policies from a single point to deliver access with maximum security.

5.5 User Authentication Focused Security

In the past, enterprises relied on VPN access from the relative safety of the enterprise laptop. The immobility of traditional client VPN technologies actually reduced IT fears of security risks such as malware damaging the network. IPSec clients could not be planted on a kiosk and were unlikely to be deployed on a home network. Because of these limitations, IT had little concern about non-enterprise machines and presumed that employees gained access solely from enterprise owned and-managed machines. Non-employees generally were not given any access, or enterprises risked giving them the same full access that their own employees had.

As a result of this model, IT security concerns focused solely on user authentication-identifying users as strongly as possible. Many large enterprises invested in two-factor authentication systems to identify users. These enterprises believed that if users always accessed the network from the same trusted location, the key issue centered on ensuring that the users were who they said they were.

5.6 Mobility Boosts Risk And Productivity

SSL VPNs from enterprises, provide anywhere access that increases employee productivity. In addition, SSL VPNs provide security benefits such as SSL encryption, protection from direct network access, full authentication support, and granular access control. However, some types of risks for end users and IT substantially increase as users demand access from places that IT cannot control. Today, the issue focuses not only on who the user is, but also how trustworthy the remote access environment is. An SSL VPN user can gain access from a range of end devices, all posing different levels of security threats. For instance, home PCs, PDAs, and tradeshow kiosks have a higher risk of hosting malware that could infect the network with viruses or Trojan horses, capture passwords for later reuse, or cache confidential information.

5.7 IT Must Address User Identity And Risk

IT managers dearly have concerns about their ability to protect enterprise assets when access can occur from any desktop or device. In addition to accessing the enterprise network via unauditable entry points, users may inadvertently leave behind information at a kiosk or hotel business center if downloaded files, viewed e-mail attachments, Web pages, and passwords are cached on the hard drive. For the user, the issue transcends security policy

and the integrity of the corporate network; it becomes an issue of personal privacy [8].

As SSL VPN access becomes widespread, remote access policies will undergo scrutiny and must address the concerns of end users, auditors, business stakeholders, and IT. With recent press reports on incidents in which information was secretly captured via keystroke logging at public kiosks, this pressing security issue is just beginning to get public attention.

But, what can IT realistically do to overcome these threats? A few written IT policies ban kiosk access, but in practice it is a very hard policy to enforce. Plus, that type of restriction significantly reduces some of the productivity gains that SSL VPNs offer. So far, few enterprises have clearly thought out how to handle this concern.

End point security control enables IT to manage the risk of Web-based access. Now enterprises *will* no longer have to ban mobile access to enterprise assets or accept a high degree of risk in return for providing greater user productivity [6].

5.8 So What Is End Point Control?

End point security control is the ability to enforce policy based upon the level of trust that IT has for the user and his or her environment. IT organizations can establish and define Policy Zones, including untrusted machines such as kiosks, semi-trusted machines such as home PCs, and trusted enterprise assets like laptops. With, end point security control, they can then appropriately manage those zones with a simple set of parameters. In other words, end point security control provides a very high degree of granularity, so IT can reduce risk, provide access from more places at a lower cost to the enterprise, and control access by user location.

5.9 How To Deliver End Point Security Control

End point security control delivers unprecedented capability for enterprises to provide exactly the type of remote access they want. You can ensure secure access to resources by using three essential components:

- Device Interrogation
- Policy Zones
- Enhanced data protection and remediation [6]

5.9.1 Device Interrogation

End point security control automatically interrogates the end point when the user accesses the enterprise's SSL VPN in order to determine what is and what is not on the machine. You need to ensure that the access point is free of malware like keystroke loggers and Trojan horses. This happens prior to authentication so login can be stopped if any malware is discovered.

5.9.2 Policy Zones

Device interrogation looks for certain applications or watermarks on the end point. For example, if a specified antivirus product or a personal firewall is present, device interrogation may instantly classify the end point into one of the predetermined Policy Zones-such as trusted, semi-trusted, and non-trusted. Each zone enables a different level of access, appropriate to its level of risk.

5.9.3 Enhanced Data Protection And Remediation

The most flexible remote access options should be required in the semi-trusted zone. And, in a non-trusted zone such as kiosk access, ASD could be required for remediation.

5.10 Policy Zones Grant Access By Trust Level

Many enterprises want to support multiple access environments, but would like to differentiate that access for less trusted end points. This is where end point security control comes in. End point security control provides extensive access control and policy management flexibility, so administrators can plan ahead for any remote access scenario. Other SSL VPN solutions offer access/no access models, but that approach simply isn't sufficient to support today's broad range of access scenarios. By using the SSL VPN, you can easily define multiple Policy Zones that limit access to resources and ensure that sensitive information is not left behind. Unlike competitors' products, which associate data protection with group membership, **Policy Zones** give administrators highly granular access control over users and their remote access environments, such as:

- IT-managed laptops
- Home PCs
- Kiosks [6]

Essentially, having more zones makes your network more secure. For instance, IT-managed laptops have the highest level of trust and get

complete access, because they are owned and provisioned by your enterprise and have predefined characteristics such as a personal firewall, virus checker, and a digital certificate. But, a category of devices with a lower trust level could be classified as semi-trusted. This Policy Zone includes devices like home PCs that are not owned and provisioned by IT. Users in this zone would be able to access only a subset of the privileges they get in the trusted zone. A third category of non-trusted devices includes kiosks found at hotels, airports, and convention centers. Users in this zone may have even more limited access, such as access only to e-mail. Defining different Policy Zones for each access scenario makes it easy to support this broad range of use cases.

5.10.1 Defining Policy Zones

Policy Zones are created by specifying one or more device profiles and indicating the level of data protection for the zone. Administrators can create up to 10 zones.

5.10.1.1 What Is A Device Profile?

A device profile is a set of characteristics that must be present on a device to assign zone classification. Attributes might include:

- Application /process
- Directory/file name
- Registry key (can be used to specify an antivirus signature update or an O/S Patch Level)
- Antivirus program
- Personal firewall
- Windows domain membership [6]

For example, an administrator could define a profile that would authenticate a device as trusted only after the access point meets designated conditions: such as having the appropriate antivirus solution, the appropriate personal firewall, and membership in the correct Windows domain (one device profile can include multiple domains to check against). So for greater flexibility, administrators can specify one or more device profiles for each Policy Zone, which can match more than one profile with an OR condition. Thus, a device with either the Business Partner device profile OR the Home PC device profile can be classified into a semi-trusted zone, which makes it extremely easy to organize a small number of zones to cover multiple access scenarios.

5.10.1.2 What Is Data Protection?

SSL VPN technology enables you to tie the level of data protection directly to the Policy Zone. For example, with an *IT* managed device, you might not require data protection; whereas, with a semi-trusted home PC, you might want to protect against the loss of sensitive information. Likewise, if a device or environment is considered risky, such as a kiosk, end point security control helps remediate the situation by increasing the level of data protection through encryption and deletion of confidential data on the endpoint machine.

5.11 Object-Based Model Promotes Granular Control

Based on the same security and management principles that underlie leading firewalls, you can gain a single view of all access control rules, which is far simpler and ultimately more secure than the typical flat policy management approach used by other vendors' products. Unlike those models, which become increasingly complex as you add groups and resources, access control rules should match users/groups to defined resources, which can then be made dependent upon the specified *Policy Zones*. In a single step, you can make object changes [6].

You now have the option of defining all users/groups, resources, and Policy Zones; and, combining them to create extremely granular access control rules. Resources, which include client/server and Web resources, as well as file shares are defined once, and are then related to multiple rules. A defined resource can relate to a single application or to all applications that exist within a domain, subnet, or IP range.

For greater security, Web resources can also be defined as aliases, so users cannot view private URLs. This is ideal for enterprises that grant access to specific resources to someone outside the enterprise, such as a business partner or customer [6].

Finally, for very granular access control, you can create advanced policy variables such as time of day. For example, you can limit a contract employee's network access to a specific application only from a trusted zone during standard business hours. Rules are checked sequentially for policy matches, similar to the way that policy models work in other perimeter security solutions, such as firewalls and content security products.

6. SUMMARY AND CONCLUSIONS

Although Wi-Fi technologies have significantly improved their security capabilities, many of the features and abilities are available only in newer

equipment for IT-managed infrastructure. Meanwhile, cellular data networks rely on a completely separate security architecture that emphasizes protection of the radio link and does not provide end-to-end encryption.

By using an SSL VPN, you can secure all forms of wireless communication, both externally and internally. Moreover, this approach accommodates a wide range of user equipment [1].

Nevertheless, it's too soon to tell whether WNS encryption problems will turn out to be a tempest in a teapot or seriously exploited vulnerabilities. However, they do point out that you shouldn't rely too heavily on encryption or any other security technologies—you never know when a new discovery will compromise what was otherwise a relatively secure platform (see sidebar, “Tales From The Encrypt”).

Tales From The Encrypt

Is merely possessing encryption software evidence of criminal intent? Apparently so: An appeals court has recently ruled that the judge in a criminal case was correct in permitting the prosecution to argue that the mere presence of PGP software on a computer implied criminal intent. Now, that's really scary! The guy on trial was in a really deep hole to begin with, and there was little he could offer in his own defense, and his lawyers created a side issue in his case. But that doesn't detract from the fact that a court has ruled the mere presence of PGP can be evidence of a guilty mind.

After all of the recent stories about various schools' carelessness with personal data, it's comforting to know that banks are more interested in protecting their customers' privacy—yeah, right! Citigroup, the world's largest bank, is blaming United Parcel Service for the loss of 4.1 million personal banking records stored on computer tapes. Even better, it took 29 days before anybody realized the tapes were missing.

While Citigroup appears to be placing all of the blame on UPS, the actual tapes were unencrypted, a fact that will be hard to pin on the shipping company. Can you say dumbest move ever by a big financial institution? And, this just months after Bank of America lost its own tapes, resulting in more than a 2 million missing records. It must have cost Citigroup far more to mail out

notices to all those customers than it would have to encrypt everything a dozen times over.

Of course, the biggest problems occur when black hats find a way to crack encryption that a company has used to protect data in long-term storage [9]. They can then go back and dig out the data the organization thought it had securely protected [1].

Finally, how do you fix these new problems in Bluetooth or AES? Just don't use the technology.

7. REFERENCES

- [1] Peter Rysavy, "Secure Wireless Networking Using SSL VPNs," Rysavy Research, [© 2005 Aventail Corp. All rights reserved. Aventail Corporation, 808 Howell St., Second Floor, Seattle, WA 98101], Rysavy Research, PO Box 680, Hood River, OR 97031 U.S.A., 2005
- [2] Robert Whiteley, Stan Schatt and Benjamin Gray. "SSL Is The Future Of Remote Access VPNs," © 1997-2005, Forrester Research, Inc. All rights reserved. Forrester Research, Inc., 400 Technology Square, Cambridge, MA 02139, USA), June, 2004.
- [3] Fred Sandmark, "Securing Wireless Networks," Copyright © 2005 Cisco Systems, Inc. All rights reserved. Cisco Systems, Inc., 170 West Tasman Dr., San Jose, CA 95134, USA [iQ Magazine (vil. VI, No. 1), 2005.
- [4] Jupitermedia Headquarters, Jupiter Research, 23 Old Kings Highway South, Darien, CT 06820, 2005.
- [5] Scott Robinson, "Strengthen Your Wireless Security By Avoiding These Missteps," Copyright ©2005 CNET Networks, Inc. All rights reserved. TechRepublic, 235 Second Street, San Francisco, CA 94105, 2005.
- [6] "End Point Control: Secure Anywhere Access With Reduced Risk And Increased IT Control," © 2004 Aventail Corp. All rights reserved. Aventail Corporation, 808 Howell St., Second Floor, Seattle, WA 98101, 2004.
- [7] John R. Vacca, *Firewalls : Jumpstart for Network and Systems Administrators*, Digital Press, 2004.
- [8] John R. Vacca, *Net Privacy: A Guide to Developing and Implementing an Ironclad ebusiness Privacy Plan*, McGraw-Hill, 2001.
- [9] John R. Vacca, *The Essential Guide To Storage Area Networks*, Prentice Hall, 2002.
- [10] John R. Vacca, *Wireless Data Demystified (Mcgraw-Hill Demystified Series) (Paperback)s*, McGraw-Hill Professional, 2003.
- [11] "Securing The Wireless LAN," Network World, Network World, Inc., 118 Turnpike Road, Southborough, MA 01772 Copyright, 1994-2005 Network World, Inc. All rights reserved. August 12, 2002.



<http://www.springer.com/978-0-387-95425-7>

Guide to Wireless Network Security

Vacca, J.R.

2006, XXIII, 848 p., Hardcover

ISBN: 978-0-387-95425-7