

White Paper



Wireless Network Security

Secure Your Network As You Would
Protect Your Home

7 July 2004, Rev. B

System administrators who deploy wireless networks without implementing the proper security measures are risking a lot more than stolen credit card numbers; they might be putting your company on the line. Sometimes protecting your wireless network is as easy as flipping a switch—sometimes it's not—but it's always worth your effort.

Wireless Network Security

Secure Your Network As You Would Protect Your Home

7 July 2004, Rev. B

System administrators who deploy wireless networks without implementing the proper security measures are risking a lot more than stolen credit card numbers; they might be putting your company on the line. Sometimes protecting your wireless network is as easy as flipping a switch—sometimes it's not—but it's always worth your effort.

Wireless security

Protecting data. Controlling access.

Most hackers enter wireless networks at will because the doors are unlocked and the sentries were never called to post.

The typical system administrator simply plugs in the access point right out of the box and doesn't give a single glance to the default settings.

About 30 percent of the market uses security appropriately.

Imagine your home, filled with the people you love and all your prized possessions. You open the Windows, unlock the doors, and then stand on the front stoop, bullhorn in hand, to announce to the world that your domain is wide open. According to many computer security analysts, this is essentially what you're doing when you fail to activate the wireless security features included with systems today.

One common misconception about computer security—wireless or otherwise—is that intruders gain access to systems only after working feverishly through the night to defeat whatever digital sentry stands in their way. The reality, however, is quite sobering: Most hackers enter wireless networks at will because the doors are unlocked and the sentries were never called to post. In fact, that's the number-one issue with WLAN security: System administrators aren't turning it on. The typical system administrator simply plugs in the access point right out of the box and doesn't give a single glance to the default settings. Or—just as common—he or she doesn't understand the basics of network security, becomes frustrated trying to set it up, and simply switches it off.

Current trends show that about 30 percent of the market uses security appropriately. The hope is that with just a little information, and a list of good resources, that number will soon rise. And perhaps—just perhaps—within a short time, effective wireless network security will be the norm, and hackers *will* work late into the night to defeat the digital sentries standing guard over their well-protected wireless charges.

Evaluating Risk

How Much Security is Enough Security?

Anyone with a wireless device can potentially connect to your Wireless LAN.

In a traditional local area network (LAN) environment, every device connected to the system is hard-wired. A typical system consists of a network server—a LAN backbone with drop-lines to device locations—and an Ethernet protocol adapter in each connected device. This kind of system provides excellent security—if you are not capable of physically connecting to the network, you are unable to access system resources.

Although data is sometimes valuable to hackers, in many cases, they are hoping to use your system as a stepping stone to a larger target.

With a typical wireless LAN, the drop-lines and Ethernet adapters are substituted with radio access points and radio cards in the end devices; this system lacks physical connections. Anyone with a wireless device can potentially connect to your system. Hackers can intercept and decode the radio signals transmitted by your WLAN—an activity called sniffing—to try to break into your network by presenting themselves as valid users—an activity called spoofing.

Two objectives motivate a typical hacker: information and access. Although data is sometimes valuable to hackers, in many cases, they are hoping to use your system as a stepping stone to a larger target. Analyzing these two spheres of motivation will help you determine the level of security that will keep the hackers at bay.

If your firm works with government agencies such as the U.S. Department of Defense, you would certainly want to deploy a security system of the highest standards.

Data

What type of data does your company manage? If the fact that you have four cases of paper towels in stock, or that perhaps Jane Worker punched in 10 minutes late this morning, is your most valued data, then expending resources to implement a state-of-the-art firewall or other security measures on your WLAN is likely unnecessary; a basic security system may suffice. However, if your firm handles and stores customer credit card information or personal health records, protecting that data may be critical to your company's continued existence. Or if, even more critically, your firm works with government agencies such as the U.S. Department of Defense, you would certainly want to deploy a security system of the highest standards.

Your data may not be worth much to anyone outside your business; but your connections to the Internet, or more importantly, to other firms, may be a very lucrative prize.

Access

For hackers, access is the goal. In your particular situation, your data may not be worth much to anyone outside your business; but your connections to the Internet, or more importantly, to other firms, may be a very lucrative prize. For example, if your company maintains an open Internet connection to the networks of subcontractors or suppliers, you may be an enticing target, particularly if the subcontractor maintains an Internet connection to a major financial institution. A frontal assault on a financial institution's network might be too daunting for some hackers. However, strolling casually through a backdoor—via your wireless network connection—might prove to be irresistible. You must protect yourself against this type of attack. And with the wide spectrum of WLAN security available today, you can.

The Deadbolt

Basic Wireless LAN Security

WEP 128 generates secret encryption keys shared by an information source and the destination station, enabling both to protect the information from eavesdroppers.

SSID serves as a simple password for network access and provides minimal security.

ACL enables wireless networks to grant access to only those devices included on the MAC address list.

Revisiting the unlocked-house metaphor, the first thing you would do to secure your home is close the windows and lock the doors. Then you would throw away the bullhorn. This is an equivalent to the basic security standard for wireless networks as established by the Institute of Electrical and Electronic Engineers (IEEE), a United States-based standards organization.

The IEEE has made significant progress in the establishment of standards for LANs. Its most notable creation—the IEEE 802 series of standards—includes a group of wireless LAN specifications known as 802.11. One of the first task groups created under 802.11 focused on developing a level of security for wireless devices that would equal the standards found in wired networks. The result was the Wired-Equivalent-Protocol standard or WEP 128. This protocol generates secret encryption keys that are shared by an information source and the destination station, enabling both to alter frame bits—pieces of data—to protect the information from eavesdroppers. Returning once more to the house metaphor, after you lock up, WEP 128 is the key you share with those whom you wish to grant access to your home.

Network access control is implemented by using a Service Set Identifier (SSID) associated with a single or group of access points (APs). The SSID serves as a simple password for network access and provides minimal security—minimal because those who possess it can share it. Turning off the broadcast default setting of your SSID is like throwing away your bullhorn.

Another form of wireless security is known as an Access Control List (ACL). Every wireless device has a unique identifier, known as a media access control (MAC) address. A MAC address list is typically maintained in the access point or on a server that controls all access points in the network. ACL enables wireless networks to grant access to only those devices included on the MAC address list. An ACL is not viewed as an extremely secure method of security because MAC addresses can be stolen and spoofed.

The Watchdog Active Wireless LAN Security

With a good watchdog, unless the animal recognizes someone trying to get into your house, that person is going to remain outside.

A RADIUS server requires a user to login with a user name and password.

Temporal Key Integrity Protocol adds message source and destination authentication, protection against a specific denial of service attack, and other improvements.

802.1x implementations also improve data encryption through rotation of the WEP 128 key. This would be like periodically calling a locksmith to change your home's locks.

If you possess a number of valuables in your home, you may choose to employ a more active level of security—like a watchdog. You can the same for your wireless network by implementing the IEEE 802.1x security standard. 802.1x is related to the 802.11 standards and governs two areas: network access restriction through the use of authentication; and data integrity through WEP key rotation. With a good watchdog, unless the animal recognizes someone trying to get into your house, that person is going to remain outside.

Authentication addresses a well as answer an encryption key question simple question, “Who are you?” The 802.1x standard recommends the use of a Remote Authentication Dial-In User Service (RADIUS) server in conjunction with two data communication protocols: Extensible Authentication Protocol (EAP) and Transport Layer Security (TLS). A RADIUS server requires a user to login with a user name and password as well as answer an encryption key question—a request constructed and wrapped according to the EAP/TLS standard. The TLS protocol allows applications to communicate via a method designed to prevent eavesdropping, tampering, or message forgery. The protocol requires both sides of a transaction to present an identification certificate issued by a trusted third-party. An extension of this standard is called Tunneled Transport Layer Security (TTLS)—a method similar to those used to purchase items with a credit card over the Internet.

802.1x implementations also improve data encryption through rotation of the WEP 128 key. This would be like periodically calling a locksmith to change your home's locks. The user dictates how often the key is changed. The hope is that when a hacker thinks they have enough information to steal a key, you change the locks.

A new standard called Temporal Key Integrity Protocol (TKIP) adds message source and destination authentication (proof of identity), protection against a specific denial of service (DoS) attack, and other improvements. The DoS protection prevents the replaying of frames (packets of information) into the wired backbone. When launched, TKIP will be complemented by an industry initiative called Simple Security Network (SSN)—an effort that should speed the implementation of TKIP within the market place. The backers of the initiative are currently working with the Wireless Ethernet Compatibility Association (WECA) to enlist their endorsement for testing and standardization. (WECA is a membership organization founded in 1999 to promote the direct sequence (DS) version of the 802.11 wireless Ethernet technology (IEEE 802.11b High Rate). Products that prove to be compatible with these standards receive the “Wi-Fi” (Wireless Fidelity) logo from WECA.)

The IEEE 802.11i task group is developing the next generation of data encryption. Called the Advanced Encryption Standard (AES), the standard uses a set of mathematical algorithms that are extremely complex and much more difficult to crack. Firms that manage highly sensitive data or access connections may want to adopt this standard after it is approved.

The Security Guard

Hardened Wireless LAN Security

A small number of enterprises manage data that is top secret in nature—or they might maintain access to trading partners who possess such data. These companies need wireless security that is extraordinarily difficult to crack.

FIPS 140 allows a number of encryption methodologies to be employed such as Advanced Encryption Standard (AES) or Triple Des (3Des). Some believe that 3Des could not be broken by a supercomputer in a millennium.

A small number of enterprises manage data that is top secret in nature—or they might maintain access to trading partners who possess such data. These companies need wireless security that is extraordinarily difficult to crack, similar to having an alarm system and armed guards patrolling the grounds of your home. Many of these firms may need to employ a security solution that is Federal Information Protection Standard 1.40 (FIPS 140) certified. Products in this category provide point-to-point security for wireless network communications and include offerings such as AirFortress and IPSec Virtual Private Networks (VPNs). VPNs provide private connections between two machines or networks over a shared or public network such as the Internet. VPN technology allows organizations to extend secure network services over the Internet to remote users, branch offices, and partner companies, and provide access through the verification of a user ID and password. VPNs always include encryption—sometimes at the level of FIPS 140, sometimes not.

It is important to note that, according to Fortress and others, even IPSec VPNs are open to privacy invasions and denial of service attacks—besides being fairly problematic to manage. VPNs do not provide network security—the firewall needs to protect the enterprise from intruders—because APs become vulnerable when they set up on the outside of the firewall. VPNs can also provide gaps in security when the end node is connected to secondary networks. For example, if someone is connected to his or her corporate network via VPN dial-up from their home—where they have a wireless network with no security in place—a hacker could connect to the PC via an unsecured connection, thereby sharing the VPN tunnel without the worker's knowledge. This is referred to as a "split tunnel" vulnerability. FIPS 140 provides data payload security (encryption), but not network security without firewall isolation and use of a VPN. FIPS 140 allows a number of encryption methodologies to be employed such as Advanced Encryption Standard (AES) or Triple Des (3Des). Some believe that 3Des could not be broken by a supercomputer in a millennium. This is a much different data security approach than WEP and does not require key rotation.

Vendors of security products may offer just a VPN or FIPS capability, or perhaps some combination or sub-set of the two combined into one solution. Understanding what each offers to meet your security requirements is essential.

And Finally... Just Remember the Basics

Eliminating the risk that someone will hack into your system is a difficult task, but you can significantly reduce your vulnerability.

Don't simply turn on your system and assume it will always remain secure. Check and sniff your own network for hidden access points.

Although wireless network security is a complex issue, it can be easily tackled. Find a vendor that offers a wide spectrum of security solutions that will well serve you even as your security needs change. Eliminating the risk that someone will hack into your system is a difficult task, but you can significantly reduce your vulnerability. Remember the following, however, and you can provide the level of security your needs and network require:

- Turn on your security features! Hackers and thieves will pass by locked areas for the thousands of unsecured doors they can find elsewhere.
- Properly assess the level of security you need, and then implement measures in proportion to your requirements. How important or confidential is your data? Do you have network connections with trading partners who possess sensitive data?
- Go with the standards. Standards ensure effectiveness while protecting your investment for future changes and expansion. Don't use default settings, or obvious passwords or keys. Rotate your WEP keys often—at least once per day or every 10,000 packets of information—to foil hackers' efforts.
- Finally, monitor your network. Don't simply turn on your system and assume it will always remain secure. Check and sniff your own network for hidden access points.

Company Overview

Allied Telesyn: It's Our Network, Too.

A global company with nearly two decades of continuous profitability.

Allied Telesyn focuses entirely on end-to-end, purpose-built Ethernet applications.

A world-class engineering and support organization spanning five continents and more than 30 countries.

The ideal choice for cost-conscious IT professionals who are looking for high-quality, feature-rich network solutions.

Founded in 1987 with the goal of producing feature-rich, reliable, standards-based networking products, Allied Telesyn has a proven track record in bridging the gap left by other Ethernet networking manufacturers, whose solutions are often limited in scope or cost-prohibitive.

By taking cues directly from our customers and leveraging our global manufacturing competencies, we've evolved a market-focused approach to system development that is geared entirely to applications, rather than individual components. And by concentrating on battle-tested, end-to-end solutions for vertical market applications we avoid the scattershot, company-focused approach common in the industry. Our tagline: "It's our Network, too" is a testament to our high-level of accountability and to our investment in our customers' bottom line success.

Allied Telesyn focuses entirely on end-to-end, purpose-built Ethernet and IP applications; with a complete line of networking products that includes Layer 2 switches, Layer 3 switches, carrier class fiber/copper Multiservice Access Platforms, wireless access points, wireless adapter cards, and residential gateways. No other networking vendor can match Allied Telesyn's breadth and depth of Ethernet products—we are the leading manufacturer of media converters, unmanaged Fast Ethernet switches and hubs, fiber optic network adapters and other feature-rich interconnectivity products, worldwide. Additionally, Allied Telesyn has developed a world class systems engineering and support organization that ensures networks are designed and implemented to handle the stress of providing voice, video and data services.

With engineering, manufacturing, sales, and distribution divisions strategically located throughout the Americas, Europe, Asia and Japan, Allied Telesyn is able to deploy solutions anywhere in the world, quickly and efficiently. And by rigorously testing products in design and support centers and leveraging our design and manufacturing competencies, Allied Telesyn is able to offer solutions for the access edge that are both customized and plug-and-play. This ideal combination helps our customers keep costs low, speed network deployment and maximize network uptime.

Our customer-driven approach—combined with a pragmatic, value-based pricing scheme and a superlative service organization—has made Allied Telesyn a global networking leader, with more than 17 years of continuous profitability and products deployed in more than 50,000 companies in 30 countries and five continents. Allied Telesyn: the ideal choice for cost-conscious IT professionals who are looking for high-quality, feature-rich network solutions at a lower price.

www.alliedtelesyn.com

This white paper was adapted with permission from Intermec's published paper: "Wireless Security".