Intermec

White
Paper

Intermec

WLAN SECURITY IS JUST LIKE YOUR HOUSE

Imagine your home, filled with the people you love and your prized possessions. You open all the windows and unlock all the doors. Then you place a man with a bull-horn outside announcing to the world that your domain is wide open, and invite them to come on in and go through your things, any time they want. According to many industry analysts, this is essentially what you are doing by not turning on the available wireless security that comes with systems today. In fact, the biggest problem with wireless local area network (WLAN) security today is that it is not being used. The issue is not that hackers (burglars) can break security measures, but that they can walk right in and take what they want. This happens because people just plug in the access point right out of the box and don't change the default settings. Or, users don't understand security, become frustrated trying to set up and turn it off. As the graphic below shows, only about 30% of the market is using security appropriately.

Using Security
Appropriately

Didn't Turn
Security On

Turned Security
Off - Lack of
Understanding
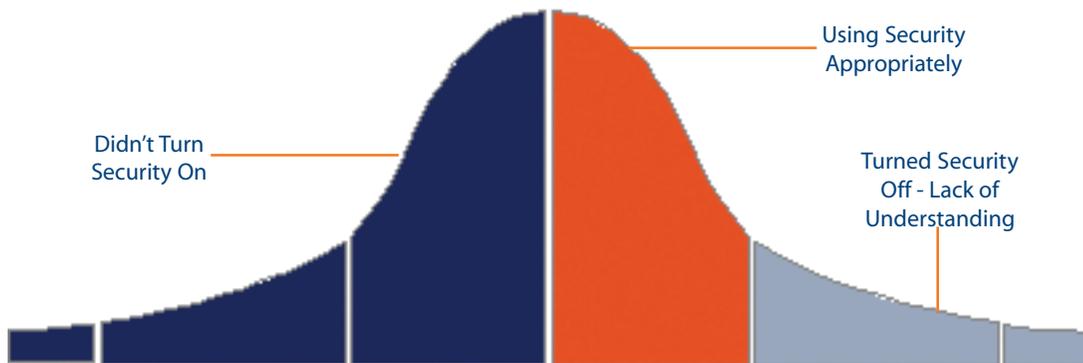
The purpose of this white paper is to give you an overview of WLAN security in the simplest terms possible. We will start by helping you begin to assess your needs, and then talk about what types and levels of security are available today.

HOW MUCH SECURITY DO YOU NEED?

In a wired local area network (LAN) environment, every device that is connected to the system is "hard-wired". The system consists of a network server, a LAN backbone with drop-lines to device locations, and an Ethernet protocol adapter in each device that is to be attached. This provides some very good security–if you are not allowed to be physically attached, you are not connected.

On a wireless LAN, the drop-lines and Ethernet adapters are replaced with radio access points and a radio card in the end devices. There are no physical connections. Anyone with a radio that can receive WLAN radio signals (called sniffing) can potentially connect to your system. Hackers gain access by intercepting signals carrying specific information about your WLAN, manipulate that information to present himself or herself as a valid participant of your network (called spoofing), and use that information to break in. There are two things in which hackers have interest: data and access. Depending upon your situation, analyzing each of these areas will help you determine the level of security you need so you don't get hacked.

Data

What types of information does your company manage? If four cases of paper towels on isle 5 or that one of your employees punched in 10 minutes late is your most important piece of data, then you may not need to expend the funds for extremely tight and aggressive WLAN security. Basic or active security may suffice (more on this later).

But, if your firm handles customer credit card information or personal health records, protecting that data may be critical to your company's very existence. In addition, if your firm works with a government agency, such as the U.S. Department of Defense, hardened security that follows very stringent standards may need to be employed. In many cases, hackers are not interested in your company's data, but in the access your firm gives them to somewhere else in your supply chain.

Access

With hackers, access is king. In your particular situation, your data may not be worth anything to anyone other than you and your customers. But, your connections to the Internet, or more importantly, with other firms, may be the real target. For example, let's say your company is a sub-contractor to Company B and that you have an open Internet connection to their network. And it turns out Company B has an Internet connection to a major banking institution. A hacker may not want to attack the bank head on, but sneak in their backdoor through your company. You need to protect yourself against this type of attack as well. You can protect both data and access. There is a spectrum of WLAN security available today that will address the level of security your enterprise requires.

TYPES OF SECURITY AVAILABLE

For the sake of organization, WLAN security will be categorized into three types: Basic, Active and Hardened.
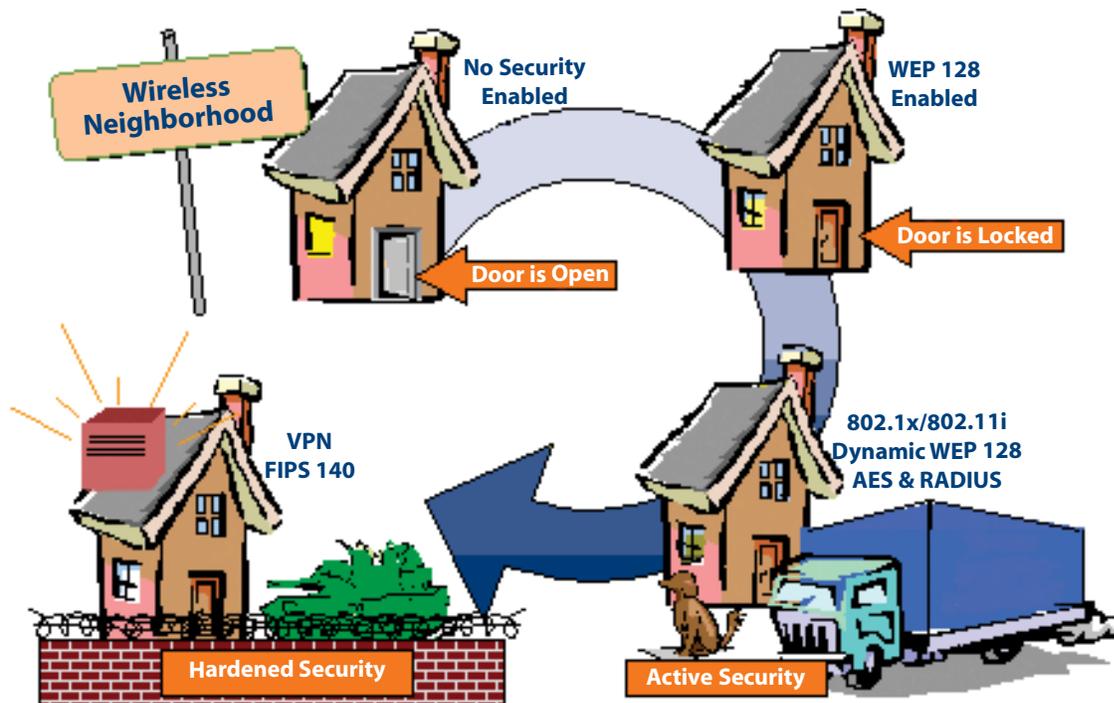

Basic Security - Lock Your Doors

Getting back to our open house analogy, the first thing you would do to secure your home is close the windows and doors and lock them. Next, you would fire that guy out on your front lawn with the bullhorn. This is equivalent to the basic security standard established by the Institute of Electrical and Electronic Engineers (IEEE).

IEEE is a United States-based standards organization participating in the development of standards for data transmission systems. IEEE has made significant progress in the establishment of standards for LANs, namely the IEEE 802 series of standards. The section of standards specific to wireless LANs is known as 802.11. One of the first task groups under the IEEE 802.11 focused on bringing the equivalent level of security found in a wired network to the wireless world. The result was the Wired-Equivalent-Protocol standard or WEP 128.

WEP generates secret shared encryption keys that both the information source and destination stations can use to alter frame bits (pieces of data) to avoid disclosure to eavesdroppers. This is like closing your doors and windows and locking them. Then giving a key only to those you want to allow access to your house.
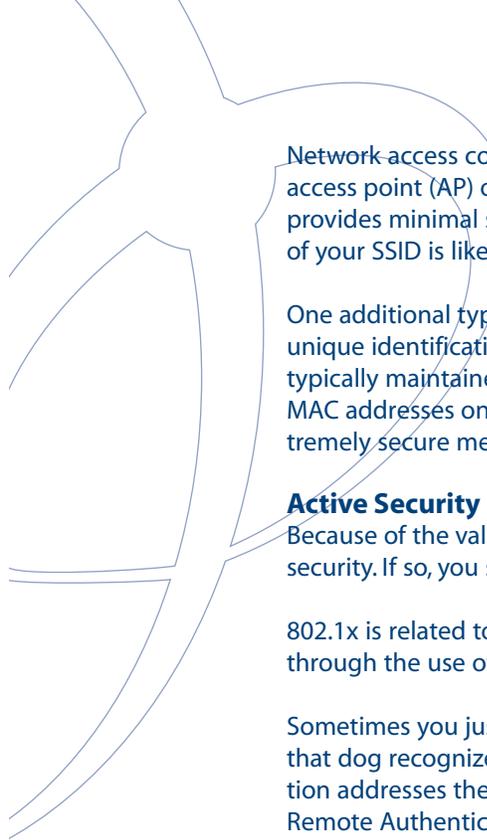
Network access control is implemented by using a Service Set Identifier (SSID) associated with an access point (AP) or group of APs. The SSID acts as a simple password for network access and provides minimal security since wireless clients can share it. Turning off the broadcast default setting of your SSID is like getting rid of the guy with the bullhorn outside your house.

One additional type of security is known as an Access Control List (ACL). Each wireless device has a unique identification, known as a media access control (MAC-layer) address. A MAC address list is typically maintained in the access point or a server for all access points in the network. Only those MAC addresses on the list are allowed onto the wireless network. An ACL is not viewed as an extremely secure method to security because MAC addresses can be stolen and replicated (spoofed).

Active Security

Because of the value of items in your home, you may choose to employ a more active level of security. If so, you should consider implementing the IEEE 802.1x security standard.

802.1x is related to the 802.11 standards and covers two distinct areas: network access restriction through the use of authentication, and data integrity through WEP key rotation.

Sometimes you just want a good watchdog in your yard… say a Doberman or a Rottweiler. Unless that dog recognizes the person wanting access to your house, they aren't getting inside! Authentication addresses the 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. That request is constructed and wrapped in a very specific way based upon the EAP/TLS standard. TLS protocol allows applications to communicate in a way that is designed to prevent eavesdropping, tampering or message forgery. It requires both sides of a communication transaction to have a "certificate" issued by a trusted third-party that proves their identity. This is similar to having to show your ID when cashing a check. An extension of this standard is called Tunneled Transport Layer Security (TTLS). It is very similar to the method used when you buy items with your credit card over the Internet.

802.1x implementations also improve data encryption through rotation of the WEP 128 key. Think of this as having your own personal locksmith periodically show up at your home and change all the locks on your doors and windows. You dictate how often the key should be changed. Just when a hacker thinks they have enough information to "steal" a key, you change the locks.

The IEEE is working on improving some of the remaining weaknesses in the WEP 128 encryption key. A new standard called Temporal Key Integrity Protocol (TKIP), adds message source and destination authentication (proof of who your are), protection against a specific denial of service (DoS) attack and other improvements. The DoS protection prevents simple replay of frames (packet of information) into the wired backbone. TKIP will be complemented by an initiative, from Microsoft and an industry consortium, called Simple Security Network (SSN). It will speed implementation of TKIP in the market place. They 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 test compatible with these standards receive the "Wi-Fi" (Wireless Fidelity) logo from WECA.

The next generation of data encryption is being developed under the IEEE 802.11i task group. It is called the Advanced Encryption Standard (AES). AES uses an entirely different set of mathematical algorithms that are much more complex and difficult to crack. Firms that manage even more sensitive data or access connections may want to adopt this standard after it is approved.

Hardened Security

A small number of enterprises manage data and access to other trading partners that could be "Top Secret" in nature. These firms may need wireless security that is much more difficult to crack, similar to having an alarm system and armed guards patrolling the grounds.

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 are a private connection between two machines or networks over a shared or public network (Internet). VPN technology allows an organization to securely extend its networking services over the Internet to remote users, branch offices, and partner companies, allowing access only through user ID and password. VPNs always include encryption of some type. Sometimes that encryption solution is FIPS 140.

But, VPNs and FIPS 140 are not one in the same thing. 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 for network security–the firewall needs to protect the Enterprise from intruders. The AP's become vulnerable on the outside of the firewall.

VPNs can also provide gaps in security when the end node is connected to secondary networks. For example, say someone is connected to their corporate network via VPN dial-up or Internet from their home. In their home they have a wireless network with no security in place. A hacker outside that house could connect to the PC via an unsecured connection, and share the VPN tunnel without the worker's knowledge. This is referred to as the "split tunnel" vulnerability.
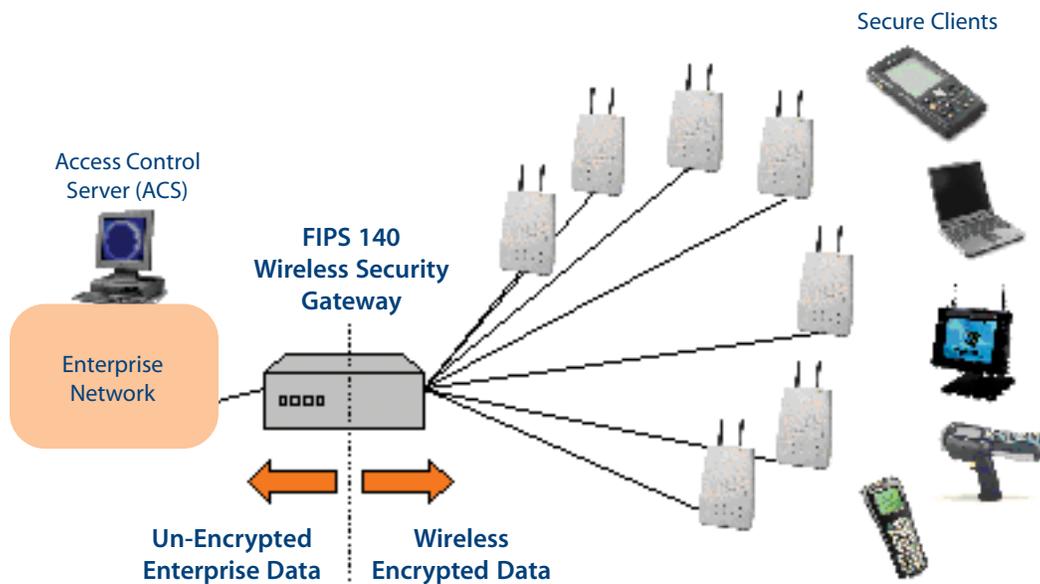
FIPS 140 provides data payload security (encryption), but not network security without firewall isolation and use of a VPN. FIPS 140 allows a number of encryption methodologies to be employed such as Advanced Encryption Standard (AES) or Triple Des (3Des). Some experts say that 3Des could not be broken by a supercomputer in 1,000 years. This is a much different data security approach than WEP and does not require key rotation.

Vendors in this market may offer just a VPN or FIPS capability, or some combination or sub-set of the two combined in one solution. Understanding what each can offer against your security require-ments is essential.
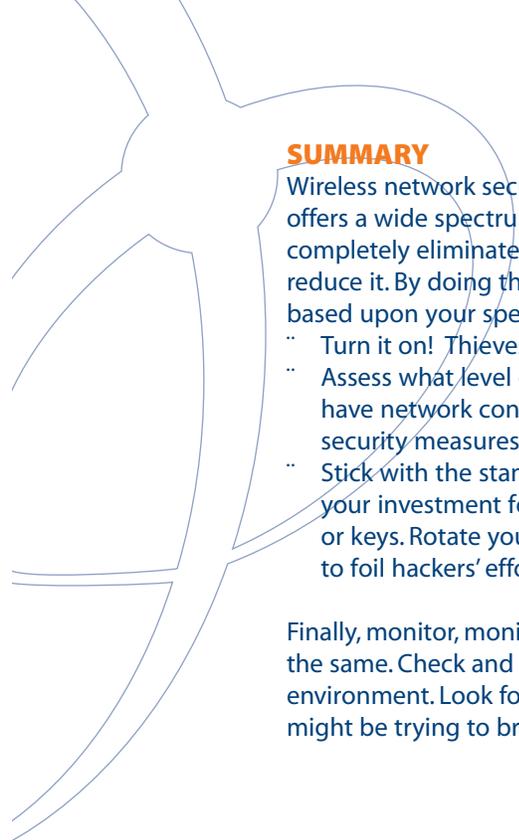
SUMMARY

Wireless network security is a complex issue, but one that can be tackled easily. Seek a vendor that offers a wide spectrum of security solutions because your needs will change. It may be impossible to completely eliminate the risk that someone will hack into your system, but you can significantly reduce it. By doing the following three things you can provide a reasonable level of network security based upon your specific situation:

- Turn it on! Thieves like unlocked doors and will pass by locked areas for the easy pickings
- Assess what level of security you really need. How important or confidential is your data? Do you have network connections with trading partners that have even more sensitive data? Implement security measures in proportion to your needs.
- Stick with the standards. Standards not only ensure others have tested the waters, but protect your investment for future changes and expansion. Don't use default settings, 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, monitor, monitor!! Do not just turn your network on and assume it will always stay the same. Check and sniff your own network for APs you don't know about. Be aware of your physical environment. Look for any unfamiliar cars in the parking lot with someone just sitting in them? They might be trying to break into your house!

WIRELESS SECURITY: IT'S LIKE SECURING YOUR HOME

North America
Corporate Headquarters
6001 36th Avenue West
Everett, Washington 98203
tel: 425.348.2600
fax: 425.355.9551

Systems & Solutions
550 2nd Street S.E.
Cedar Rapids, Iowa 52401
tel: 319.369.3100
fax: 319.369.3453

Media Supplies
9290 Le Saint Drive
Fairfield, Ohio 45014
tel: 513.874.5882
fax: 513.874.8487

Europe/ Middle East & Africa
Headquarters
Sovereign House
Vastern Road
Reading, Berkshire RG1 8BT
United Kingdom
tel: +44.118.987.9400
fax: +44.118.987.9401

Asia
Hong Kong
2602 Convention Plaza
Office Tower
1 Harbor Road
Wanchai, Hong Kong
tel: 852.2574.9777
fax: 852.2574.9725

Singapore
25-16 International Plaza
10 Anson Road, 079903
tel: 65.324.8391
fax: 65.324.8393

Australia
Level 7, 200 Pacific Highway
Crows Nest NSW 2065
Australia
tel: 61.2.9492.4400
fax: 61.2.9954.6300

South America & Mexico
Latin America Headquarters
17921 B Skypark Circle
Irvine, California 92614
tel: 949.442.9393
fax: 949.757.1687

Mexico
Tamulipas 141, Primero Piso
06140 Mexico, D.F.
tel: 525.55.211.1919
fax: 525.55.211.8121

Worldwide Fax Document Retrieval Service
800.755.5505
(North America Only)
tel: 650.556.8447

Internet
www.intermec.com

Sales
800.347.2636
(toll free in N.A.)
tel: 425.348.2726

Service and Support
800.755.5505
(toll free in N.A.)
tel: 425.356.1799