



What You Need to Know about WLAN Security



At the turn of the millennium, the security mechanisms available for wireless LANs were insufficient for the privacy needs of a corporate enterprise. This became all-too clear when cryptography experts exposed the vulnerabilities of an early encryption standard called WEP (Wired Equivalent Privacy) in 2001, and many enterprises decided, wisely, that WLANs were not yet safe. Today the wireless industry offers security mechanisms that can, if configured correctly, render a wireless LAN even safer than a wired network. In lieu of WEP there is WPA2 (Wi-Fi Protected Access). Based on the IEEE 802.11i security standard, it uses algorithms based on AES (the advanced encryption standard), and it provides highly advanced key encryption.

However, securing a wireless network requires much, much more than a checklist of encryption acronyms.

The sad fact is that as security mechanisms have advanced, so too have the methods of attacking a wireless network. Today's wireless hackers include sophisticated international crime rings that stand to make billions of dollars by stealing private data from vulnerable corporations. If there is a way to exploit a network, these criminals will find it. And their methods involve more than technical hacks – their methods also involve tricking employees into giving up private information.

Hackers are great at their jobs. To that end, any company that deals with private data must employ a wireless LAN security system that's great at its job – or else risk losing millions of dollars in damages and network downtime. There's no such thing as "good enough" security.

Security is, and should be a tremendous concern for any company running a wireless LAN, because the network perimeter doesn't stop at the four walls of the office. Rather, it extends right into the lap of any given hacker in the parking lot, sitting there with a "Pringles cantenna," sniffing out poorly secured wireless networks whose signals bleed outside of the building. (A "cantenna" is a jerry-rigged antenna made from coax cables, a connector, copper and an empty potato chip can; it costs about \$10 to create. Any mischievous teenager can make one. But all too often hackers are not teenagers but rather

bonafide criminals on a reconnaissance mission, looking for gaps in your defense system, and working from there to infiltrate your network. A great wireless LAN security system includes superior encryption mechanisms for sure, but also a 24X7 intrusion detection, protection and alert system; centralized management and authentication; consistent policies for network clients; audit logging of all network activity; and a firewall that detects all wireless activity.

Moreover, the system needs to be relatively easy to operate, for obvious reasons: if a system isn't configured properly it won't work properly, and a system that takes weeks to configure could equal weeks of hacking attempts. And ideally the entire system comes from the same vendor, in order to maintain seamless operations and avoid the pitfalls of a "bolted-on" solution. (You wouldn't want Frankenstein protecting your network.)

Investing in a gap-free wireless security system means maintaining customer confidence and, consequently, retaining those customers. Furthermore, catching unauthorized devices before they do any damage to the network will mitigate the likelihood of network downtime. Investing in a reliable wireless LAN security toolset now will save you a lot of money and headaches in the long run.

Hindsight Is Costly

It's not easy for a company to calculate the return on investment of installing an effective wireless LAN security system. After all, only the criminals know who their next target is. But suffice it to say that if you're the victim of a network attack, the cost of securing a network is miniscule compared with the cost of not securing it.

According to the technology consultancy Gartner Group, "a company with at least 100,000 accounts to protect can spend, in the first year, as little as \$6 per customer account for just data encryption or as much as \$16 per customer account for data encryption, host-based intrusion prevention and strong security audits combined."¹ On the other hand, the cost of paying for a data breach – including investigation fees, written apologies, data recovery, fines,

lawsuits, and severe loss of customer confidence – can amount to \$300 per breached account. And the numbers add up fast. You may have heard of the infamous case in which an international crime ring hacked into the insufficiently-secured wireless networks of several major retail stores for several months between 2005 and 2006, stealing more than 40 million credit and debit card numbers before their actions were discovered.

And it's not an isolated case. According to the Identity Theft Resource Center, there were 656 reported identity data breaches in 2008, including information such as customers' credit card and social security numbers. This marks an increase of 47% over the 2007 total of 446 breaches.²

Within those 656 breaches last year, 35,691,255 customer records were exposed. And these were only the breaches that the victims knew about and reported; the cleverest criminals might break into and lurk on a company's network for years without being detected at all.

Any organization with valuable information is a likely target of a data breach, even the U.S. Government. The U.S. Government Reform Committee reports that all 19 government departments and agencies reported at least one loss of personally identifiable information since Jan. 2003.³

New Regulations Require Superior Wireless Security

Avoiding a financial nightmare and saving face are sufficient reasons to secure your wireless network soundly. But if your company is involved in retail, healthcare, or government operations, then chances are that federal and industry regulations require you to maintain a secure wireless LAN – or else face a stiff penalty.

Many corporate networks are subject to various government regulations and industry policies that require companies to protect customer data. New regulations pop up on a regular basis, and they keep getting stricter. Common regulations include the Payment Card Industry standard (PCI-DSS), the Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Processing Standard (FIPS) 140-2, and the Department of Defense's wireless directive 8100-2.

PCI-DSS: Established in 2005 by a group of major credit card companies, the Payment Card Industry Data Security Standard (PCI-DSS) comprises a set of security guidelines designed to help retailers prevent credit card fraud and identity theft. In a nutshell, any company that processes, stores, or transmits credit card numbers must comply with the PCI DSS standard. The standard encompasses several rules specifically for companies that operate wireless LANs – including the encryption of any necessary wireless transmission of cardholder data using Wi-Fi Protected Access (WPA and WPA2) technology, and the implementation of a reliable network intrusion detection system. It is important to note that in the aforementioned 2007 retail hack, the victims had not implemented WPA or WPA2, relying instead on the outdated and insufficient WEP standard.

HIPAA: The Health Insurance Portability and Accountability Act, enacted by the U.S. Congress of 1996, requires the security and privacy of medical patient records. The strict security provisions in HIPAA include administrative, physical, and technical safeguards. These include rules for access control, auditing, data integrity and transmission, and user authentication – all of which must be addressed with regard to a wireless LAN.

FIPS 140-2: FIPS 140-2 is the Federal Information Processing Standard for encrypting unclassified U.S. Government data. Any company with U.S. Government clients – or even clients who partner with U.S. Government contractors – is likely required to adhere to the rules of FIPS 140-2. In terms of wireless technology, FIPS 140-2 requires data be encrypted with the Advanced Encryption Standard (AES), which is included in the aforementioned WPA2.

DOD 8100-2: In April 2004 the Department of Defense issued this directive, which assigns policies for the use of wireless devices within the DoD's Global Information Grid. In addition to mandating encryption of wireless data and authentication of wireless users, the directive requires 24X7 intrusion detection. That mandate includes the ability to track devices and detect when otherwise authorized devices enter unauthorized areas.

There Are Many Ways To Infiltrate A Network Wirelessly

Hacking into a wired network is generally a matter of thwarting Internet Protocol Security (IPSec.) Wireless is a different animal. Criminals generally take a layered approach to infiltrating a wireless network, starting from the outside and working their way in. To that end securing a wireless network requires a seamless layered approach. Let's look at some of the tricks of the trade:

Masquerading as a hotspot: This common attack is aimed at business travelers who log on to the corporate network from a public wireless "hotspot" in a coffee shop or hotel lobby hundreds of miles from the office. Hackers will set up an "evil twin," which is a wireless network signal that masquerades as a legitimate hotspot with a feasible-sounding SSID, such as "Hotel Hotspot!" In reality, the evil twin exists for the purpose of stealing information from the user. In fact, the Internet offers a bevy of free tools that help hackers create such a ruse.

Companies can avoid the pitfalls of an evil twin by requiring employees to install VPN software, which creates a tunnel between the employee's laptop (or other wireless device) and the corporate network.

War driving is a basic reconnaissance mission in which potential hackers travel around shopping malls and office parks looking for poorly secured wireless networks whose signals bleed outside of the building. To detect these networks hackers generally use handheld computers equipped with war driving software that "sniffs" the radio signals of unsecured networks. There are several tools readily available on the Internet to help war drivers do their bidding. Such products – including Netstumbler, Kismet, Aircnort, Cowpatty, and Wireshark – help war drivers in their quest to beat insufficient encryption mechanisms, intercept communications, and even associate as a rogue AP.

If a company has not employed advanced encryption methods, it's fairly easy for a hacker to sniff out network keys and gain access to private information. In fact, the gigantic identity breaches of 2007 began with war driving. ⁴ Once inside the network, the criminals were able to capture card numbers, passwords and account information without ever entering a building.

Companies who want to thwart war drivers should ensure that their networks are configured with a layered set of wireless defenses – WPA2 Enterprise with AES encryption and 802.1x authentication, along with 24x7 wireless monitoring and intrusion prevention. Additionally, companies should implement an Intrusion Detection System (IDS) that can detect excessive failed authentication failures and indicate an active attempt to attack the network.

Deploying rogue access points and smuggling unauthorized devices in an office can thwart a seemingly secured network. Even if a company maintains a high level of security on its own switches and access points, its network may still fall victim to a rogue. Rogue wireless access points are connected to a company's wired network even though they are not authorized to be there. Sometimes rogues are installed by an employee or contractor who doesn't know any better. Sometimes they are installed with malicious intent. At any rate, rogue access points are generally installed without any security mechanisms enabled; unfortunately, the "plug and play" nature of many access points does not require security mechanisms in order to broadcast a signal. Hence, these unsecured rogue access points provide hackers with a wide-open back door into the corporate network.

To a hacker, gaining access to a rogue device is essentially the same as gaining access to an Ethernet port. Rogues give hackers the ability to perform a "man in the middle attack" – infiltrating communication between two authorized devices on a network, often without being detected. By the same token, hackers can and will try to take advantage of any unsecured Wi-Fi-enabled handheld devices. And because people who receive Wi-Fi-enabled smartphones like to show them off to their cubicle mates the next day, chances are pretty good that there are some unsecured Wi-Fi-enabled devices in the office.

In another scenario, a hacker might steal administrative rights on the access point and (via MAC address filtering) block all access to the network – except access for the hacker. In that scenario, a company would have to deal with a financial double whammy: the cost of network downtime and the cost of recovering stolen information.

To mitigate rogues, companies should employ a wireless intrusion protection system that can monitor the network constantly and send alerts when something is amiss, as well as physically locate the rogues so that IT managers can eventually physically remove them. An effective rogue containment solution can accurately classify innocent neighboring devices from actual rogue threats that are connected to the network – and automatically block them, either over the air or by denying their access to the wired network.

Sneaking past the firewall at Layer 2: The computer network architecture is arranged in seven layers. The seventh layer lies closest to the end user, and each successive layer lies further into the network. Starting with #7, the layers are:

- (#7) application layer
- (#6) presentation layer
- (#5) session layer
- (#4) transport layer
- (#3) network layer
- (#2) data link layer
- (#1) physical layer.

Here's the problem, which can endanger both wired and wireless networks: most firewalls set up to allow or deny traffic on specific ports at Layer 3 – and only Layer 3. Most firewalls do not detect activity on layer #2, which happens to be where wireless LAN activity takes place. Therefore, it behooves network operators to seek out and deploy a firewall that can detect Layer 2 activity.

Good old-fashioned robbery: It's important to remember that protecting a network requires more than preventing technical hacks. For sure, technical hacks of a poorly encrypted network are all too common. But even more common are physical thefts of portable computers, drives and disks, or unauthorized use of data by employees. Of the 656 data breach incidents reported to the Identity Theft Resource Center in 2008, 11.7 percent of them were a result of mere hacking. 20.2 percent were a result of "data on the move" – i.e. lost or stolen notebook computers, thumb drives, or handheld computers containing would-be private data. 13.5 percent were due to a subcontractor either stealing or losing the data.

Most disturbingly, 15.8 percent of data breaches in 2008 were due to a deliberate theft by someone inside the company. That's compared with 6 percent of the breaches in 2007, indicating that the problem of insider theft has more than doubled in the course of a year.⁵

Social engineering: Popularized by the infamous hacker Kevin Mitnick, "social engineering" is a fancy term for "conning." In short, it means persuading or tricking people into divulging information, such as passwords, credit card numbers, or encryption keys. According to Mitnick, social engineering is actually the most popular method of gaining illegal network access. ⁶ Social engineering is especially dangerous in cases where all the clients and access points on a network share the same encryption key for network access, because smart criminals will often use their wily ways to obtain the pre-shared key.

Sometimes a criminal will pull off a social engineering exploit by pretending to be an angry bigwig who demands network access. Sometimes the social engineer is a sweet old lady who calls the IT department, claiming to be a scatterbrained receptionist who misplaced her password. Sometimes social engineering is simply a matter of surreptitiously watching someone type in an access code. (The technical name for this technique is "shoulder surfing.")

It's important to employ a system that can recognize not only unauthorized users, but also any unauthorized activity on the network – including the location of network devices.

Motorola Offers A Layered Approach To Gap-free Wireless Security

Hackers take a multi-layered approach to infiltrating wireless networks. To that end, protecting the wireless network requires a multi-layered approach, as well. Motorola offers the tools necessary for a multi-layered approach to protecting your wireless LAN – protecting and monitoring the network from both the outside and the inside, and managing it from the center.

Compared with other leading wireless network equipment providers, Motorola has the strongest and most efficient wireless security portfolio on the market. Motorola integrates key features directly into the switches and APs to provide superior access control and network defense.

Because threats really exist at the edge of the wireless network, Motorola has created the strongest and most comprehensive wireless edge security offering. In fact, every AP includes on-board AAA, stateful firewall and VPN, which secures traffic without gaps. Combined with the Motorola AirDefense Wireless Intrusion Protection System (described below,) this is the most secure wireless edge defense available. This entire security architecture can be managed from a single console, and offers regulatory compliance with the highest levels of security validation in the wireless industry, from the aforementioned FIPS to Common Criteria Level 4.

For authentication and encryption Motorola also has the best offerings on the market, with four-factor access control right in the AP; this allows companies to control access based on the user's ID or role in the company; policy compliance via NAC (network access control), and geofencing – which is a means to control access by a user's location using the system's RTLS (real-time locationing system) application.

All of Motorola's **access points** support the highest available levels of encryption, including IEEE 802.11i (WPA and WPA2) and well as 3DES IPsec encryption. On Motorola dual radio APs (the AP-5131, which supports 802.11 a/b/g and AP-7131, which supports 802.11 a/b/g/n), one radio can be dedicated to network access and the other can act as a sensor that monitors the airwaves for rogue devices 24 hours a day.

Motorola's Authentication, Authorization and Accounting (AAA) features include:

- Internal and external RADIUS (Remote Authentication Dial In User Service) capabilities that support EAP (Extensible Authentication Protocol), providing an extra layer of security beyond WPA2 with a strong encrypted mutual authentication that thwarts man-in-the-middle attacks.

- RADIUS accounting, which keeps a log of not only which users are authenticated by the network, but which access point authenticated them, whether they roamed from one AP to another, and how long they remained connected to the network.
- Lightweight Directory Access Protocol (LDAP) or Active Directory integration, providing authentication against a common user database so as to ensure that those people who gain secure access to the network are really authorized to be there.
- Features that authorize not only who is authorized to use the WLAN, but when and how and on which access point each individual user is allowed to be there – assigning specific permission guidelines based on individual identity.
- Sophisticated role-based firewall features that dynamically apply admission rules to employees and guests based on the Extended Service Set ID and which AP they are using,

Wireless intrusion prevention or WIPS is the eyes and ears of the RF network. The Motorola AirDefense WIPS solution can detect more than 200 current and lethal attacks and threats in real-time – as opposed to the dated on-board WIPS systems that can't see much more than 20 attacks. Furthermore, the Motorola 24x7 wireless intrusion prevention system can reside alongside a WLAN radio on a single AP. The ability to transport packets and detect intruders on the same AP is not only extremely cost-effective, it's extremely secure. WIPS sensors are solely dedicated to detecting and preventing intruders. This is important to note: many other WLAN systems on the market use a far less effective approach called "time-slicing," in which the radio on an access point spends some time broadcasting network traffic and some time scanning the network for intruders. Unfortunately, these time-slicing solutions end up spending only about 4 minutes per day scanning for intruders. You don't have to be a math genius to know that 24 hours a day is better than four minutes a day! In addition, the AirDefense WIPS is not band-locked – meaning it can monitor both 2.4 and 5 gigahertz bands simultaneously. This is important for any network that utilizes both the 802.11b/g and 802.11a standards.

Understanding that rogue access points are a major threat to wireless networks today, Motorola offers the industry's most effective and manageable rogue mitigation solution. Network managers can instantly detect and locate a rogue, determine its current and historic threat level, and choose either to monitor or immediately sever it from the network. The ability to perform this function is a critical requirement for adhering to industry regulations such as PCI and HIPAA..

Network managers often don't realize the prevalence of rogue APs. It should be noted that many Motorola customers find that after installing WIPS alongside their existing rogue detection system, they find at least one rogue associated to the network per week.

It's also important to note that WIPS provides a graphical map of the network, providing the ability to distinguish a true rogue access point from an access point that belongs to a nearby business. This capability is especially helpful in shopping malls and office parks, where wireless signals tend to bleed between walls.

WIPS also logs the activity of every wireless device on the network, more than 300 wireless statistics per device per minute, using a detailed wireless forensic database. It can log activity for months, as well as offer instant analysis with an easy-to-use forensic wizard, enabling it to notice unusual network activity – a weird increase in traffic on a particular access point, for example. This is an invaluable tool for detecting the nefarious activity of a social engineer or a disgruntled employee.

As mentioned previously, a wireless network has a layer two architecture with its own collection of threats such as MAC spoofing, man-in-the-middle, DoS, and network injection attacks that are invisible to the layer three defenses – which are fine for wired networks but insufficient to protect a wireless network. In addition, in true wireless mesh networks, which are common on corporate campuses with multiple buildings, network traffic can enter and exit without backhauling through a central chokepoint. With that in mind, Motorola has introduced the industry's most extensive yet easy-to-use wireless firewall that enforces layer two policy right in the AP, at the network edge.

The fact that Motorola's wireless firewall *guards Layer 2* (as well as Layers 3 through 7) helps to prevent attacks such as ARP cache poisoning and

DHCP spoofing, both of which are popular attacks in the Layer 2 domain – and which are virtually invisible to wired network firewalls. The wireless firewall also provides a clean separation between wireless and wired networks, which happens to be one of the requirements of the aforementioned PCI-DSS.

As mentioned previously, adherence to PCI-DSS and HIPAA is extremely important in retail and healthcare environments, respectively. In fact, virtually every industry in every country must be mindful of and compliant with at least one Federal regulation. (Sarbanes-Oxley compliance, for instance, is required of most large companies in the United States.) Motorola has created the optimal solution: the promise of regulatory compliance as well as the promise of the industry's best gap-free security system. Motorola provides methodologies and provisions to monitor, report and assure compliance, and also going beyond those regulatory requirements to provide the most secure wireless network operation. After all, simply being compliant with an industry regulation does not necessarily ensure total security.

Another scary reality is that criminals seem to keep improving their skills, continually breaking what was once thought to be secure. First WEP was broken, then WPA-TKIP is broken. Breaking WPA2 may just be a matter of time. To that end, Motorola AirDefense offers cloaking software, which creates fake network data traffic and encryption keys meant to fool hackers and to quickly protect legacy technologies against hackers.

Of course, no network is completely autonomous, and security alerts can't be fully effective if there is not an organized way to receive and manage. A system in which an IT manager has to monitor multiple consoles in multiple locations is not only ineffective – it's exhausting!

Fortunately, Motorola's **RF Management Suite** provides a **centralized console** for monitoring every event on the network – working in conjunction with the **WIPS** to consolidate alarms and present critical events via a graphical interface – on a single console.

Motorola's layered approach to wireless security provides the capability to thwart every known hacker threat – including social engineering. To that end, a Motorola WLAN protects your company's network and your peace of mind. And it meets all the security requirements of all major industry regulations.

¹ Pescatore, John, "Defending Your Privacy in a Wireless World," Gartner, Inc. 2008

² Identity Theft Resource Center (http://www.idtheftcenter.org/artman2/publish/iib_survey/ITRC_2008_Breach_List.shtml)

³ Identity Theft Resource Center (http://www.idtheftcenter.org/artman2/publish/m_facts/Facts_and_Statistics_printer.shtml)

⁴ <http://www.usdoj.gov/opa/pr/2008/August/08-ag-689.html>

⁵ Identity Theft Resource Center (http://www.idtheftcenter.org/artman2/publish/m_press/2008_Data_Breach_Totals_Soar.shtml)

⁶ <http://www.zdnet.com.au/insight/security/soa/Kevin-Mitnick-Social-engineering-101/0,139023764,339290739,00.htm>



MOTOROLA

motorola.com

Part number WP-GAP-SECURITY. Printed in USA 03/09. MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners. ©Motorola, Inc. 2009. All rights reserved. For system, product or services availability and specific information within your country, please contact your local Motorola office or Business Partner. Specifications are subject to change without notice.