Secure Connections

The proliferation of wireless technology makes a comprehensive security solution all the more important.
The popularity of wireless technology is indisputable. In less than a decade, wireless has evolved from an emerging novelty to a mainstream solution that’s used by educational institutions and government.

Today, Wi-Fi hot spots are nearly ubiquitous and a growing number of organizations are using wireless systems to address key needs: providing guest access to the Internet, setting up temporary networks at job sites, and providing remote access to servers for road warriors at airports, hotels and hot spots.

There’s no question that wireless technology offers enormous productivity gains. Putting data in the hands of workers — where and when they need it — allows an organization to streamline processes and avoid bottlenecks and delays. In some instances, such as a university campus, it also eliminates the need for costly infrastructure and wiring.

Yet, all the gain doesn’t come without some issues. Wireless technology also creates significant security challenges. Without the right protections in place, an organization can find its data lost, missing or stolen.

Safeguarding the Network

Locking down a wireless network is no simple task, however. “A growing array of devices and network configurations exist, and the technology is constantly changing,” says Victoria Fodale, an industry analyst for market research and consulting firm In-Stat, located in Scottsdale, Ariz.

“With mobile and wireless tools now in widespread use, it is important to protect devices and secure the network. The threats are increasing and the risks of a breach are significant.”

Indeed, organizations must remain vigilant on a number of fronts: device authentication, file encryption, maintaining secure connections via a Virtual Private Network (VPN), managing access points, network administration through consoles that display where and how resources are used, and remote device management.

It’s also vital that employees understand the risks of using wireless technology and that they take the appropriate safeguards and precautions.

“Today, the same information that’s available at the desktop is accessible via wireless devices,” states Pravhat Agarwal, manager of information security solutions at Input, a Reston, Va., consulting firm. “There’s a need to introduce stringent security procedures at the network level as well as with all the devices that connect to servers and systems.”

Protection Schemes

What makes wireless systems so appealing — and worrisome — is that they extend the network from within the four walls of the organization to virtually anyplace that receives a wireless signal.

“It takes only one weak link in the wireless network for a breakdown to occur,” Agarwal points out. “It’s essential to understand the risks as well as the environment and systems you’re trying to protect.”

Two of the primary concerns are the possibility of intrusions and the viewing of unauthorized files. While many of the same concerns exist for conventional wired networks, the need to authenticate users is essential in the wireless environment and managing access points and network connectivity is paramount.

Ultimately, an organization must ensure that any transmission is available only to the intended recipients (no eavesdropping or interception takes place), a message originates from the person claiming to send it, no modifications to files or messages has taken place and the network is resistant to Denial-of-Service (DoS) attacks and other hacking problems.

Since data transmitted over a wireless network is available over the airwaves rather than an Ethernet port controlled by the organization, data encryption is at the foundation of an effective wireless security strategy.

Data Encryption

Unfortunately, the original encryption standard, Wireless Equivalent Privacy (WEP), isn’t adequate; a hacker can break through a WEP-protected network using brute force techniques in a matter of minutes or hours. “It’s simply not strong enough for government,” says Fodale.

Instead, organizations should use Wi-Fi Protected Access (WPA) or WPA2, also known as 802.11i. The latter uses the AES-CCMP algorithm and Extensible Authentication Protocol (EAP) with Research and Development for Image Understanding Systems (RADIUS) servers and Pre-Shared Key (PSK) based security.

As a result, WPA2 is extremely difficult to crack. Combined with an intrusion prevention system (IPS) that identifies suspicious packets and activity, it’s possible to know when an outsider has gained access to the wireless network and take steps to thwart the attack.

A Sense of Security

Encryption is only part of an effective wireless defense strategy. For those accessing data from an offsite location or a Wi-Fi hot spot, it’s important to rely on high-grade authentication and, in some cases, VPN.

High-grade authentication limits access to only those authorized to use the network and VPN encrypts data transmissions so that hackers and thieves cannot view any portion of the data as it is sent back and forth over local networks and the Internet.

Unfortunately, many network administrators fail to change the default name, IP addresses and access levels on the network interface cards used to connect to a wireless local area network (WLAN). This, combined with a desire to maximize wireless access (and not limit the availability of the network beyond a predefined perimeter), complicates the authentication process.

Although basic password protection that’s built into Windows and other operating systems provides some defense, it’s not enough to stop hackers and thieves.

Basic Input Output System (BIOS) level protection, which requires authentication before gaining access to the operating system, makes it far more difficult to hack or steal a password and gain entry. Computer manufacturers, such as HP, are increasingly offering systems with built in BIOS-level protection.

At a minimum, organizations should require individuals accessing the network to use strong passwords, which rely on a long, random or otherwise nonreproducible string of characters. Most strong passwords consist of at least 10 characters and a combination of letters, numbers and symbols. ▶
Many organizations are also turning to smart cards and Universal Serial Bus (USB) authentication tokens for mobile and wireless devices. These systems provide so-called two-factor authentication. A user holds the card to a reader or plugs the device into the computer port, enters a password and only then gains access to the system, application or network. Without both the token and the password, access is denied.

**Rogue Access**

Another potential vulnerability is unauthorized access points used within a WLAN. “You can have your entire wireless network locked down using encryption and a RADIUS server for authentication. But if an employee plugs an unsecured access point into an open port on the wired portion of the network, it creates a gaping hole in the entire network,” says Michael S. Scott, technical media manager for D-Link.

In some cases, the intent may be innocent. For example, an employee may only be looking to extend wireless coverage to a particular area. However, a thief may be looking to intercept data and steal information, including passwords, files and confidential records.

According to Input’s Agarwal, it’s essential to deploy a network administration control panel that automatically detects and shuts down rogue access points, tracks the user IDs and Media Access Control (MAC) addresses on computers and PDAs, and matches them to a database of registered devices and users.

It is also important to utilize a Service Set Identification (SSID) system to enforce policies at the port level (thus protecting against peer-to-peer software and other illicit activities). Some organizations are taking a close look at the access points themselves. Many are migrating from older thick access points to thin models that simplify network administration.

**Locking Down Devices**

Protecting a wireless network also means securing wireless devices, including notebook computers, PDAs, smartphones and other devices. A computer that is lost or stolen (and lacks adequate protection) can serve as an entry point into a network.

“Many security problems are due to human errors,” In-Stat’s Fodale says. “People leave computers in places they can be stolen, or they don’t use an encryption tool because it slows them down, or they step away from their computer for a few minutes while they’re still logged in.”

A growing number of personal computer manufacturers are adding BIOS-level protection through a number of security tools.

For example, HP’s line of business computers and handheld devices rely on several features, including a power-on password that provides access to the BIOS; drive locks that prevent access to the hard drive without the correct password;

**THE DANGER ZONE**

According to the SANS Institute, here are some of the most common WLAN vulnerabilities:

- **Systems that aren’t configured for security or are poorly configured.** Many organizations do not use basic encryption and authentication; a large number don’t change default SSIDs and passwords. Also, some Windows XP systems may search out and connect to an undesirable access point.
- **No set physical boundaries.** In some instances, a wireless network may enter another user’s airspace and provide undesired access.
- **Physically insecure locations.** Access points must be mounted in locations where they cannot be removed and tampered with.
- **Untrained users setting up unauthorized networks.** Those who lack knowledge about security policies and procedures are unlikely to configure devices correctly, and they may program systems to conflict with existing procedures.
- **Rogue access points.** Employees, contractors and others may set up their own access points for innocent or nefarious purposes.
- **Lack of network monitoring.** Without intrusion detection or more sophisticated intrusion protection systems, hackers can install rogue access points and other threats.
- **Insufficient network performance.** A network that isn’t designed with adequate capacity can underperform and open the door to security problems.
- **MAC address filtering.** Too heavy of a reliance on MAC addresses can lead to identity theft, commonly referred to as MAC spoofing.
- **Inadequate encryption.** WEP isn’t strong enough for widespread organizational use, yet many organizations continue using it. It’s essential to use WPA or WPA2.
- **Off-hours traffic/war driving.** A common tactic among hackers is sitting in a parking lot and attempting to break into a wireless network after hours. In some cases, war drivers head from one location to another in search of a vulnerable network.
- **Unauthorized data rates.** If an access point accepts data at a rate that’s slower than the 802.11b/g/n standard, an intruder may be attempting to access data.
- **Man-in-the-middle attacks.** An external rogue access point can attract legitimate network traffic and a hacker can gather authentication information from a legitimate computer. At that point, it’s possible for the hacker to access a VPN and other network systems.
- **Unsecured holes.** A hacker circumvents firewalls and obtains access to key systems or provides access to others.
- **DoS attacks.** Unauthorized rogue access points can lead to DoS attacks, in which the network is flooded with packets. The resulting performance declines can wreak havoc on productivity.
an administrator password that allows a computer to boot but restricts access to
the BIOS so that someone can’t change settings; and a biometric fingerprint reader
that replaces passwords.

Networking equipment manufacturers, such as Cisco Systems, are also adding
protection. Its Unified Wireless Network offers a wired and wireless solution
that addresses WLAN security, deployment, management and control issues that
an organization faces. It can create multiple wireless networks for employees,
guests and contractors, while monitoring for rogue access points and those
lacking encryption.

Meanwhile, Cisco’s Mobility Express solution offers configuration tools, highly
scalable access points and application-based mobility. “It’s essential to build a solid
security foundation up front in order to avoid additional costs and problems down
the line,” says Jeff Barnes, systems engineer for strategic markets at Cisco.

Other manufacturers are also ratcheting up features. 3Com’s Unified Wireless
Switch provides advanced wired and wireless management, including detection of
rogue access points, peer-to-peer applications, ad hoc systems and DoS attacks.

Meanwhile, its access points offer the latest security features, including VPN pass
throughs and support for Virtual Local Area Networks (VLANs). 3Com describes
its access points as “fit” rather than “thin,” according to Rohit Mehra, director of
enterprise wireless for 3Com.

An organization can auto configure access points across the network rather than
address each unit. “There is a great deal more intelligence built into the wireless
network,” he says.

D-Link’s xStack 3200 series of switches offer sophisticated security features,
including centralized management and real-time monitoring for rogue access points.
In fact, it is able to jam signals from unauthorized WLAN nodes. And it includes
WPA and WPA2 encryption.

According to D-Link’s Scott, the ability to manage the entire wireless network from
a central location, using a single switch, goes a long way toward boosting security
and creating a manageable security framework.

Security Strategies
Yet, success is more than the sum of equipment. IT must reevaluate the wireless
network and infrastructure periodically, and conduct regular security audits. If
a breach occurs, employees should know what to do and who to contact, and
every organization should have a policy in place for notifying the appropriate law
enforcement agency.

Best practice organizations develop distinct mobile computing policies and
procedures to reflect their unique needs. These policies typically cover everything,
from the types of devices that are allowed and where they can be used, to
acceptable software and required security measures and practices.

IT must approach wireless security as a complex and multifaceted task. A single
layer of defense cannot provide an adequate level of protection.

In the end, best practice organizations make sure that security systems and defense
policies intertwine in order to create a more holistic and targeted strategy. Says In-
Stat’s Fodale: “Today, as wireless networking has become an essential part of the
enterprise, security has emerged as a key consideration.”

- Never leave a wireless device on the default settings.
- At a minimum, use WPA for encryption. Better yet, use WPA2.
- Rotate WPA pass phrase keys on a regular basis.
- Implement 802.11x for RADIUS authentication.
- Use rogue access point detection and mitigation.
- Create a second public wireless network for guests.
- Always use the highest level of security possible.