Hardening Wireless in the Law Firm Environment

by Faith M. Heikkila of Pivot Group

The managing partners have come to you to discuss the installation and deployment of wireless in your organization. How do you respond? This article outlines the basic issues you need to consider and address prior to deploying wireless at your firm. As a priority, consider some of the risks involved with a wireless environment.

Step 1: Identify Wireless Threats and Vulnerabilities. There are a number of security threats associated with deploying wireless connectivity. These threats include dictionary attacks, (any word in the dictionary is searched against passwords), man-in-the-middle attacks (hackers spoof an organization's logins and capture keystrokes containing passwords) or soft Access Points (AP) conversions (a laptop or desktop is converted into an AP). Incorrectly configured devices and wireless networks can also be security threats even if you do not have wireless in your office. When you use someone else's wireless network, the connection bypasses your firm's firewalls, IDS and other protection technologies. Connecting to a rogue AP, such as a wireless network from another office within your building, creates a backdoor for hackers. Hackers can sit in parking lots, create rogue APs from their cars and then attempt attacks using cracking tools. They can also use big directional antennas to pick up a weak signal from extremely long distances.

Step 2: Determine Your Mobile and Wireless Risk. The firm's management committee should provide guidance as to whether guests such as experts and clients are allowed wireless access. Some of the things you need to consider prior to implementing wireless are whether you should:

- Exclude wireless altogether from the firm environment
- Allow guest access to only the Internet from your firm
- Allow guest access to the firm's internal network while at your firm
- Provide a wireless access point as a convenience to guests of the firm

Identify and assess the existing wireless networks within range of your law firm. Perform a site survey to identify the potential sources of interference and signal strength from various offices within your office building. This will help you ensure there is adequate coverage for deploying wireless.

Step 3: Design and Set Up Best Practices for Visitors and Employees. Prepare written security policies and procedures that describe the types of wireless data networks that are allowed and those that are not allowed. For example, wireless access may be allowed for guests but discouraged for employees. Rogue WLANs also would be prohibited. The security policy should describe the purpose for wireless data networks and identify the security requirements for each network. Defining security policies and procedures, as well as training employees how to follow the policies, is crucial in order to make sure that everyone is aware of what is expected of them when using company computers and networks.

A captive portal is highly recommended for guest wireless. This portal does not permit traffic until login authentication is received from the Web browser. This is similar to the design of most "hotspots." A VLAN should be integrated into this network design so that VLAN technology can be used to segment the wireless traffic from the internal traffic on switches or physically separate the traffic on separate network devices for more security.

Strong authentication such as EAP-TTLS, PEAP, or the strongest option of EAP-TLS, works well in the enterprise environment. Strong encryption includes:

- AES
- TKIP
- WPA = trimmed down 802.11i
- WPA2 = 802.11i
- WPA requires TKIP with AES optional
- WPA2 requires both TKIP and AES

Use strong encryption, such as WPA or WPA2 when setting up the wireless access points. Do not use Wire Equivalent Protection (WEP) because it is vulnerable to passive and active network attacks.

When naming the SSID, don't use the name of your firm. Using a nondescript name for the SSID prevents tipping hackers as to who owns the wireless network. Disable SSID broadcasts as well.

MAC addresses and IP addresses are transmitted in clear text and are trivial to capture or copy. MAC filtering and static IP addresses can be an administrative nightmare, so choose these options wisely to ensure they fit the needs of your organization.

Remove automatic connection to available networks from wireless network connection properties. Unassociated wireless networks are ticking time bombs because a user can accidentally log on to an unsecured wireless network

connection if it is left in the properties. Also, make sure to "turn off" wireless cards when not in use. Wireless card firmware/driver flaws allow compromise without association to access points. Keep firmware/driver software up to date.

The obvious best practice is to disallow all wireless access to the firm network. In reality, however, there may be times when you need to provide Internet access to guests. Whether the firm chooses to do so through a wireless connection is a matter for the management committee to decide. When guest access is required, it is best to have the guest log in on a network and Internet access point or WLAN separate from the firm network. If the guest, such as an expert witness, needs access to the firm's network, set them up to go through a VPN unrelated to your internal network.

Step 4: Wireless Network Monitoring Tools. Determine the right tools for your firm by investigating open source and commercial tools such as fat access points, network admission control and wireless survey or assessment tools. One example is CoovaChilli, a.k.a. ChilliSpot, an open-source captive portal or wireless LAN access point controller. It is used for authenticating users of a wireless LAN. It supports Web-based login which is today's standard for public hotspots. Authentication, authorization and accounting are handled by your favorite radius server.

In order to verify that there is no wireless access in your environment, you need a tool that listens to the wireless space to ensure no one has set up a rogue AP. The following are some wireless network monitoring tools to consider:

- AirDefense – wireless monitoring and IDS tool
- AirMagnet – wireless survey tool
- NetStumbler – detects WLANs using 802.11a, b and g
- Kismet – wireless packet capture

NetStumbler was one of the first freeware discovery applications available and is the most widely used. MiniStumbler runs on handheld devices. This tool provides the following feedback:

- Signal strength
- Channels being used
- Encryption method (WEP, WPA)
- MAC addresses
- Real-time signal and noise information
- SSID
- Type of network (IEEE 802.11a/b/g/pre-n)

These tools can be employed to test your own wireless network and show you what a hacker may see when attempting to penetrate your firm's wireless network.

Step 5: Regular Risk Assessments
When you perform your annual risk assessments, conducted internally or by a qualified independent third party, include a wireless assessment. Because of the ever-changing threat environment, it is a security best practice to assess your risks associated with critical assets. Identifying where your wireless environment is vulnerable will help you mitigate those risks.

About our author :: :: ::

Faith Heikkila is Pivot Group's Regional Security Services Manager for the Great Lakes and has more than 18 years of paralegal and IT project management experience. She is currently a PhD candidate in information systems, specializing in information assurance, at Nova Southeastern University. Faith is a member of the ACM, the Association of Information Technology Professionals (AITP), the Computer Security Institute (CSI), the IEEE, InfraGard, the Information Systems Security Association (ISSA) and the Great Lakes Interactive Marketing Association-Southwest. She can be reached at fheikkila@pivotgroup.net.

This article was first published in International Legal Technology Association's November, 2007 Peer to Peer - The Quarterly Magazine of ILTA and is reprinted here with permission. For more information about ILTA, visit their website at www.iltanet.org.