

Five Steps to Stamp Out Unsafe Wi-Fi use

Lisa Phifer

06.07.2006

In its recently published [Wireless Threat Index](#), security vendor Network Chemistry analyzed events collected from RFprotect Endpoint users. By publishing these real-world statistics, the company hoped to dispel [several misconceptions](#) about Wi-Fi usage. Specifically, after evaluating more than 700,000 laptop Wi-Fi connections attempted during 1Q06, Network Chemistry found that:

- **Users *do* connect to wireless and wired networks simultaneously.**
(37% of the endpoints analyzed had network bridging enabled.)
- **Users with VPNs do not always use them to protect traffic.**
(68% had experienced violations of VPN policy.)
- **Ad hoc networks are used *frequently*.**
(63% had ad hoc enabled or tried to connect to an ad hoc peer.)
- **Wireless connections are often made to unknown networks.**
(87% of the endpoints had connected to an unknown AP.)

Companies can discourage these risky behaviors by educating the workforce about Wi-Fi threats and enforcing Wi-Fi security policies that prevent unsafe connections.

1. Disable network bridging

Any device that is simultaneously connected to more than one network has the potential to relay traffic between those networks. Windows Internet Connection Sharing (ICS) actually facilitates this -- for example, letting a Wi-Fi ad hoc peer share your laptop's Ethernet LAN connection. Companies may counsel users to disable unused connections, but, frankly, many users either forget or cannot be bothered.

One way to discourage bridging is to define Windows hardware profiles that enable just one interface. For example, boot with an "office" profile that enables a laptop's Ethernet connection but disables Wi-Fi, or boot with a "hotspot" profile that enables that laptop's Wi-Fi connection but disables Ethernet. Hardware profiles can be inconvenient, and they don't stop users from manually enabling connections. But they are simple to configure, easy to select, and available on every Windows laptop.

Another approach is to define interface rules that can be enforced by mobile security agents on laptops and PDAs. Just a few examples include [Senforce](#) Endpoint Security Suite, [Trust Digital](#) Mobile Edge Device Security, and [Credant](#) Mobile Guardian. These agents do much more than permit or deny use of Wi-Fi, Ethernet, Bluetooth and 3G interfaces. But the concept is simple: use a client-side agent to enforce a centrally configured security policy when mobile devices are used outside the office.

2. Mandate VPN usage

Companies have no control over the security measures used to protect Wi-Fi traffic in home networks or public hotspots. The only way to ensure over-the-air business data protection, independent of access method, is to require VPN or application layer security. Mandating VPN use is not difficult when employees access the corporate network. The hard part is mandating VPN use for everything else -- preventing NetBIOS broadcasts from leaking onto a hotspot, or browsing the public Internet "in the clear."

One way to mandate VPN use is to launch a VPN client at start-up, require administrative privilege to stop the VPN client, and define VPN rules that prevent split tunneling (i.e., force all traffic to any destination through the VPN tunnel). But users may not appreciate this approach, in part because of difficulty using the Internet in hotels, airports, business centers and other public access venues that require Web login before a VPN tunnel can be launched. Some VPN clients support login exceptions or scripts to work around this problem.

Another approach is to bind your VPN client to your remote access client, using policies to launch the VPN client as soon as network login is complete, automatically ending the connection if the VPN client or tunnel fails. Many remote access or Wi-Fi connection managers can be linked to VPN clients in this fashion -- examples include [iPass](#) Connect, [Fiberlink](#) Extend360 and the [PCTEL](#) Roaming Client used by hotspot providers such as T-Mobile and Boingo. Here again, central policy management provides the foundation for on-the-road enforcement.

3. Prevent ad hoc connections

Most users would be surprised to learn that they have engaged in ad hoc peer-to-peer connections. Some ad hoc connections are

intentional -- to share files between colleagues, for example -- but most are not. Windows XP promotes ad hoc usage in two ways. First, defaults used by XP's Wireless Zero Configuration service allow clients to connect to any available wireless network, ad hoc or access point (AP). Second, if an XP client has previously associated to an AP with a given network name (SSID), it will try to re-associate to any device with that SSID -- even an ad hoc peer pretending to be "linksys" or another common home/hotspot SSID.

More information

[Read about the top five myths of wireless security in this article](#)

One easy way to stop ad hoc connections is to reconfigure XP (or any Wi-Fi connection manager that you use instead of WZC) to associate only to Infrastructure Mode SSIDs. In companies that use Windows Active Directory for laptop/desktop administration, this change can be applied to WZC-related registry keys using [Windows Group Policy Objects](#). Companies that don't use WZC may use third-party Wi-Fi connection manager "policy generation" tools to accomplish this.

Although this may not stop users from expressly enabling ad hoc mode, it will avoid all those unintentional ad hoc connections.

4. Control WLAN associations

When it comes to finding free Internet access, users can be surprisingly open-minded. Here again, common defaults tend to promote association with any SSID (known or otherwise). Worse, connections managers such as WZC do not differentiate between APs -- they associate to any AP offering a given SSID unless further steps are taken. This makes it hard for users to know whether they've associated with the desired AP or a phony look-alike AP or [evil twin](#).

One step is to require 802.1X authentication of the RADIUS server inside the target WLAN. When a client associates to an AP that uses 802.1X with an Extensible Authentication Protocol (EAP) that supports mutual authentication, the user has the opportunity to verify the RADIUS server's digital certificate. Clients should be configured to associate only with known/configured SSIDs and to validate the server's certificate when using 802.1X-capable SSIDs. 802.1X is most appropriate in enterprise WLANs, but some hot spots do support 802.1X (e.g., [iBAHN](#)), and there are even SOHO 802.1X services (e.g., [Witopia](#)).

5. Deploy Wi-Fi endpoint security

Of course, using a variety of solutions to address threats individually does not provide comprehensive security monitoring or enforcement for Wi-Fi endpoints. To fill that gap, several vendors offer host-resident wireless intrusion detection/prevention agents that watch, analyze and even block Wi-Fi client activities. Examples include [AirTight Networks](#) SAFE, [AirDefense](#) Personal, [Highwall](#) EndPoint, and [Network Chemistry](#) RFprotect Endpoint (the data source behind the Wireless Threat Index). Some Wi-Fi endpoint agents can be used in standalone mode by individuals and small businesses. Some can be integrated with enterprise wireless intrusion prevention systems to create a single point of control over on-site and off-site Wi-Fi use. Monitoring Wi-Fi activity isn't a substitute for securely configuring those clients in the first place, but it can help you spot unsafe connections -- and take timely action to stop them.

About the author: *Lisa Phifer owns Core Competence Inc., a consulting firm specializing in network security and management technology. She has been involved in the design, implementation and evaluation of networking, security and management products for more than 20 years. Phifer has written extensively about network infrastructure and security technologies for numerous publications, including SearchNetworking.com, SearchMobileComputing.com, SearchSecurity.com, Wi-Fi Planet, ISP-Planet, Business Communications Review and Information Security.*