



Lobby trot shows issues with Hub's wi-fi security

At the request of *Mass High Tech*, we conducted an informal survey of wi-fi-enabled network security in Hub businesses.

After picking up coffee at the Dunkin' Donuts on State Street in downtown Boston, we walked to a nearby office building to begin the first of our lobby surveys. We made ourselves comfortable in the welcoming lobby chairs, opened our laptops and made it seem as if we were killing a few minutes waiting for another person to join our group before taking the elevator upstairs to a meeting. In less than five

minutes, our laptops and hand-held wireless scanner quietly delivered a list of five, six, seven, ... eventually 12 wireless networks of businesses located on the lower floors of the building.

We lobby-surveyed two more nearby buildings, returned to our car, and headed west on the Mass Pike to check on a few Route 128 office-building locations. The survey results hardly varied as

we moved from one lobby to another, whether in downtown Boston or along Route 128. In all cases, we discovered that one out of three wireless signals were readily available to lobby visitors, coming from businesses whose wireless networks were open for public access.

We wondered why people were paying for Starbucks coffee in order to gain wireless Internet access when Boston-area lobbies with soft chairs offer plenty of high-speed wireless "hotspots" to choose from.

Our surveys found wireless signals emanating from numerous businesses that had secured their wireless networks. But well more than half of the secure networks are providing their owners with

a false sense of security because they've employed WEP (wired equivalent privacy), an outdated wireless security technique for handling 64- or 128-bit encrypted data packets. WEP security is easily cracked with inexpensive or free software readily available over the Internet. In the wrong hands, these tools can be used to break WEP's wireless encryption keys and gain access to these secure networks.

Other businesses had secured their wireless networks by not broadcasting their network SSID (Service Set Identifier) or using MAC address filtering to keep out intruders. Hopefully, the owners of these networks realize these steps provide very limited security benefits.

Securing wireless networks using these techniques should no longer be relied on for achieving wireless network security. Since WEP wireless security was easily cracked, WPA (Wi-Fi Protected Access) was developed to better secure wireless networks. WPA overcomes the serious weaknesses that were uncovered in WEP by researchers and hackers. It comes in two flavors: WPA and WPA2. WPA was to be an intermediate solution that would replace WEP until the 802.11i security standard was finalized. It was designed to work with all wireless network interface cards, but not necessarily first-generation wireless access points (or routers). WPA2 implements the full 802.11i standard, but doesn't necessarily work with older network cards. The best approach to strong wireless security today is WPA.

By upgrading to the more secure WPA or WPA2, businesses networks can avoid having their wireless networks being used as free wireless "hotspots." Without taking this step to improve their security, many businesses will leave a back door open to their entire network.

Do's and Don'ts with Wireless Networks

Do:

- Implement either WPA or WPA2 security on all of your wireless networks
- Replace any wi-fi equipment that does not support WPA
- Change default passwords on all wi-fi equipment
- Have a third party audit your wi-fi networks for security risks
- Keep drivers and firmware for all wi-fi equipment up to date
- Document your wi-fi security policy and communicate the policy with your users
- If your organization manages more than 5 wi-fi access points, consider an enterprise-class centralized management system to manage firmware updates and security
- Separate "guest" or semipublic wi-fi traffic from your wired network using firewalls or other security techniques, and place limits on the amount of bandwidth that your "guest" network can use

Don't:

- Rely on WEP to secure your wi-fi communications — it is too easy to hack with freely available tools
- Rely exclusively on MAC filtering to secure wi-fi communications — spoofing a valid MAC address is trivial and will allow a hacker to gain access to your wi-fi network
- Rely on disabling the broadcast of the SSID to secure wi-fi communications — passive sniffing of the wireless traffic will rapidly reveal the SSID
- Try to meet all user whims, but keep your wi-fi networks as simple and secure as possible
- Allow "rogue" access points to be installed by non-IT staff — all wi-fi equipment should be under the direct control of your organization's IT department

GUEST COLUMN



Harry J. Segal

Founded in 1985, Networks Unlimited, Inc. serves the information security needs of mid-market organizations across a variety of industries, including financial, healthcare, manufacturing, and legal. Networks Unlimited performs security audits and deploys information security systems that protect computer networks and help customers avoid business disruptions, loss of confidential information, and the other detrimental effects of security breaches.

Networks Unlimited, a privately-held company headquartered in Hudson, Massachusetts, with a satellite office in Austin, Texas, is recognized as one of the nation's foremost information technology consulting firms specializing in information security. The company has been featured editorially in influential *Computerworld*, *IT Week*, *Financial Executive* and *Network World* articles. Further information is available at their web site: www.networksunlimited.com.

Harry J. Segal, President & Founder, Networks Unlimited
Prior to founding Networks Unlimited, Harry Segal was vice president of Micro-com, a manufacturer of modems that was best known for its invention of the error-correcting protocol still used in today's dial-up modems. His career in the computer industry began over 30 years ago, after receiving a bachelor's degree in information and computer science from Georgia Tech. He can be contacted at harry.segal@networksunlimited.com.

Shawn Bernard, Senior Security Engineer for Networks Unlimited, contributed to this article.