

Finding security in a wireless world

By Marcus Shields

Special to *Globe & Mail*, Toronto

The cost-effectiveness and flexibility of wireless ("Wi-Fi") LANs — or WLANs — offer a seemingly ideal solution to mobile workers.

WLANs allow access to real-time information and corporate resources almost anywhere a mobile worker may be located. With the growing popularity of wireless "hotspots," mobile workers can now connect to the Internet at airports, hotels, restaurants and other public places.

However, as WLANs continue to rapidly proliferate, the technology is scarcely discussed without mention of security concerns. If your organization is planning to deploy a WLAN — or has already done so — you should know the facts surrounding wireless networks so you can use your WLAN in a secure manner.

Here are some guidelines that can help:

- Do a Threat/Risk Analysis (TRA): Review your organization's real business and technical security requirements. Know what resources are most likely to be attacked. Without undertaking this crucial step, you may be over-securing low-sensitivity resources, while under-securing critical resources.
- Architect a secure wireless solution: Design an appropriate, secure wireless scheme that meets your users' needs. A system which leaves important functions unaddressed, such as access to home-based wireless networks, may be bypassed by end users — resulting in no security at all.
- Authentication is the key: The most significant vulnerability of wireless LANs is they enable access to anyone — authorized or not — within a WLAN access point's radius of useful signal strength. Providing robust authentication security for use of wireless access points will instantly stop 80 per cent of intrusion attacks.
- Turn down the volume: Many Wi-Fi access points can be manually configured to reduce the signal strength they emit, thus reducing the area of coverage within which potential attackers can attempt to access them. No legitimate user within your building needs to connect to an access point from a parking lot three blocks away. Therefore, turn down your wireless volume and make it harder for remote attackers to "listen in." Also ensure wireless access points aren't located too close to windows so the signal has to travel farther (thereby becoming weaker) before it gets outside your building.
- Use WEP... but don't expect miracles of it: The Wired Equivalent Privacy (or WEP) authentication and encryption protocol is not perfect; however,

using it is far preferable to having no wireless encryption protection at all. Enable it for all the access points that support it. By not using WEP (or its successor, WPA), you make the task of intrusion immensely easier, just as you would be by not placing a lock of any kind on your home's front door.

- Roaming: Propose an effective roaming solution that extends the network beyond the office. Wireless LANs are here to stay; attempts to prohibit or to ignore them are likely to be futile.
- End-run WEP problems with RADIUS: An excellent, industrial-strength solution to the WLAN authentication issues is an authentication infrastructure that implements a RADIUS client/server architecture. RADIUS, an IETF standard security management protocol first used for dial-up access to Internet Service Provider modem pools, enables control over the users that can connect to your network and the resources they can access. Wireless-optimized extensions to RADIUS can enable wireless users to be strongly authenticated at access points using X.509 digital certificates as well as other strong authentication mechanisms.
- Install, configure and test: Build and configure WLAN authentication servers using best security practices. Install, configure and test hardware and software. Don't assume security equipment and software actually does what it claims to do.
- The problem can start at home: From the perspective of an attacker, unsecured, home-based WLAN access points may be considerably more attractive targets than the likely better-protected assets at an enterprise's business offices. There may be little your organization can do to prevent or restrict how employees use their computers at home. But there are ways to mitigate this risk, from both wireless and conventional remote access perspectives.

Another thing to keep in mind is that the IT department needs to insist on sophisticated multi-factor methods of user authentication beyond usernames and passwords for access either to employee home computers or corporate resources.

If possible, implement a VPN (Virtual Private Network) system to secure the data stream between remote client PCs and central enterprise data resources.

Provide tools for good security practices on home computers. Among these are software firewalls, anti-virus software and anti-spyware software.

Provide at least some security-related education for all employees — particularly those who may be using, or considering using, wireless networking at home.

Keep in mind that attackers may want your bandwidth, not your data. Not all attacks against enterprise WLANs may involve the usual security threats such as data interception or password compromises. For example, attackers may want

access to your organization's infrastructure for more mundane but still inappropriate purposes: trading illegally copied media items (songs and movies) or software, creating a launching point for mass "spam" mail blasts, storing pornography or simply free Web surfing.

Review your WLAN support options to meet the needs of your internal customers. Adjust these options to take into account changing needs, especially at the residential and home networking levels. The easier it is for users to access your support resources to get answers to security-related concerns, the more likely it will be that your users will adhere to whatever wireless security policy your organization has decided upon.

Wireless LANs are neither the inherently insecure demon that their detractors depict, nor are they inherently secure enough to be implemented in exactly the same way as conventional wireline LANs would be. As this technology continues to gain momentum from a consumer acceptance perspective, it is imperative that your organization rolls out its WLAN(s) in a secure fashion. The results will benefit users of both wireless and wireline infrastructures ... and improve your organization's productivity as well.

Start the security process now - before your WLAN starts to broadcast things you don't want the public to hear.

© Reproduced by kind permission of the *Globe & Mail*, Toronto, Canada. 2005.
All rights reserved.