Browser-based wireless security

For some companies, "wireless security" is more about access control than privacy. In that case, standard security measures like wired equivalent privacy (WEP) just aren't useful. For example, in a conference center or public hot spot, the primary security application boils down to tracking how long individuals are on the network in order for the proprietor to charge them correctly. Moving this technology into the corporation typically requires less emphasis on charging and more emphasis on simply blocking access to unauthorized individuals.

To illustrate this example, the iLabs team built a wireless network that required users to authenticate to the network using only a browser.

Vernier Networks, Reef Edge, Colubris and Blue Socket have stepped up to provide browser-based authentication for enterprise networks. With browser-based authentication, the user must authenticate with a username and password (or other authentication technique, such as a one-time password token) through a typically encrypted browser window before their system can access to the network. Of course, these products are susceptible to a number of different attacks, such as system masquerading, where someone assumes the Ethernet media access control address of a legitimate user and takes over their session. But where the goal is general access control, not absolute secrecy or accuracy, this technique is useful.

Our test network for this technology was based on Vernier's product line. With proper configuration, this worked great: The Vernier box intercepted DNS requests and Web requests, and pretty much boxed us into authenticating before we could move on.

One of the more useful extensions to this technique is something Vernier calls 802.1X sniffing. With 802.1X sniffing, the access manager — which would block access to the internal network — sits between a wireless access point and the rest of the world. The goal of this dual-mode configuration is to support 802.1X and non-1X clients.

The iLabs team showed this concept, linking Cisco and Karlnet access points, a Vernier Access Manager, and Microsoft's .Net authentication server, all connected using a Macintosh client.

In this environment, 802.1X-enabled clients authenticate and are placed onto the secure site of the network, with WEP encryption enabled. This authentication dialog is "sniffed" by the inline access manager, so when users successfully authenticate using 802.1X, they have access without any further logon process. If users don't have 802.1X software, they connect to the wireless network and see the browser-based authentication window. When users authenticate using their browser, they're connected to the "guest" virtual LAN.

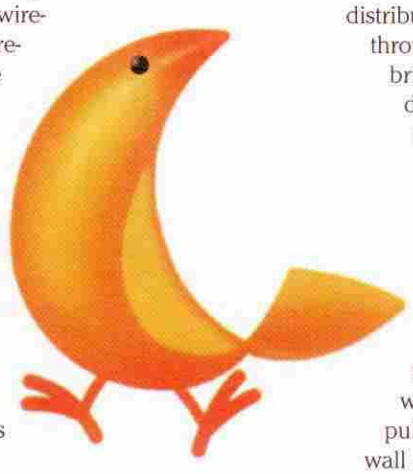
While a company could easily require its own employees to have 802.1X software and configuration on mobile systems, it might not have the same requirement for guest users. The idea is to maintain a single wireless infrastructure, with trusted users given access inside the corporate firewall, and guests and visitors placed outside.

— Joel Snyder

Wireless IPSec

For many companies, wireless networks have the same low-level security afforded on the Internet: not controlled, not authenticated and not trusted. So why not treat wireless LAN users like Internet users and bring them in from outside the firewall via VPN technologies?

The strategy is simple: Put your wireless network outside the corporate firewall, and give wireless users the same client tools as Internet users, including a VPN client and some authentication information. Because IP Security (IPSec) has one of the strongest security models available in networking, using it to secure wireless networks gives even stronger security than offered by wireless security tools like 802.1X. In addition, where VPN access via the Internet is common, most users will already have the necessary client software installed on their laptops, so the transition from home use to wireless use in the office is smooth and seamless (see diagram, right).



The iLabs team built a wireless network where access to the corporate LAN was controlled by a Nokia VPN/firewall device. We used smart cards from Schlumberger, which give a strong two-factor authentication. In this case, the access point was an SMC 802.11a (54M bit/sec) model.

If you consider using this strategy, keep in mind some important issues. One main difference between 802.1X and IPSec products is that 802.1X is a link-layer authentication system, while IPSec is a network-layer VPN technology. In the IPSec case, this means that anyone who wants to use the wireless network as a carrier, without going onto the corporate LAN, can do so without restrictions.

It's only when the packets try to leave the wireless environment that the IPSec security gateway blocks access. At the same time, only IP is supported by IPSec. In iLabs testing, that wasn't a problem, but we didn't care about services such as IP multicast. If you do, or if you have IPX or Appletalk, IPSec is not the right solution.

Another issue with this strategy relates to distribution. Wireless LANs can be spread throughout a corporate campus, and bringing the entire LAN back to the data center, where the VPN concentrator is located, can be a complex undertaking. Virtual LANs, an obvious option, must be used with care. Virtual LAN switches are not designed as security devices, and packets can and do hop virtual LAN boundaries. Without virtual LANs, though, the question of running an entire second network infrastructure just to pull wireless outside the firewall can increase costs dramatically.

VPN concentrators also can be a stumbling block. A concentrator sized for a moderate number of users connecting via dial-in or DSL service might not be able to handle the encryption load of wireless users connecting at LAN speeds directly to the corporate network.

— Joel Snyder

Putting IPSec rules to wireless security