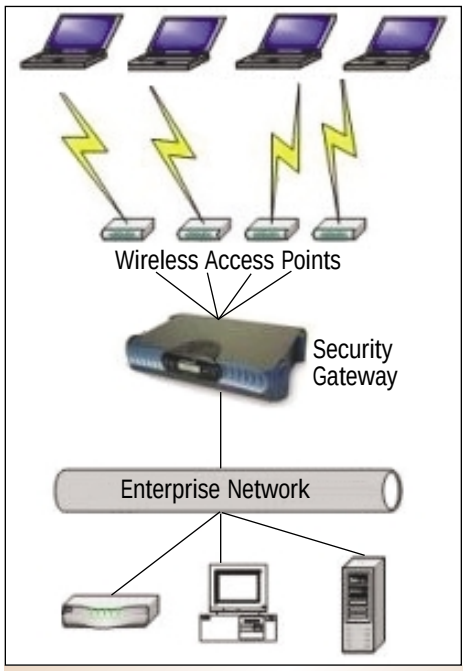
Wi-Fi usage can open "back doors" to networks

By RANDY BARRETT

The biggest threat to wireless network security walks through your front door every day. Sometimes the worst offender is the Big Boss himself.

The problem: Wi-fi enabled laptop computers and personal digital assistants which, if configured improperly, broadcast open invitations to anyone who might want to steal your bandwidth – or attack your network.

"Nearly every organization has left [wireless] doors open so it hardly matters what locks they are using on the doors that are closed," says Rich Mironov, vice president of marketing for **AirMagnet Inc.**, of Sunnyvale, CA. The company sells a line of scanners that can locate all wireless devices in a local area and determine whether they are properly secured. Most of the time, the offending machines have inadvertently been left open to the airwaves. But sometimes, employees know full well what they're doing. Such "rogue" wireless devices installed by workers are the bane of IT departments around the country, Mironov says.



Some Wi-Fi suppliers are offering security gateways that provide authentication, management & access capabilities

While many organizations now have strict policies forbidding the installation of personal wireless networks in the office, AirMagnet's scanners often lead directly to the CEO suite. "It's always the execs [who have them]," Mironov says. "The rest of the employees feel like they have to follow the company policy."

By all accounts, Wi-Fi enabled gear is pervasive and more is hitting the streets every day. The industry generated $1.7 billion in revenues last year, a 140 percent increase over 2002, according to the market research company **In-Stat/ MDR**. The firm projects that 35 million Wi-Fi units will be built and sold in 2005.

That's a staggering number of potentially open doors. Silicon Valley venture capitalists have been busy funding a broad array of new vendors who aim to keep your wireless airspace clear, safe and secure. In addition to scanning- and intrusion-detection companies like AirMagnet and Alpharetta, GA-based **AirDefense**, a number of companies offer secure gateways to protect wireless transmission.

BlueSocket Inc., of Burlingon, MA, sells standalone gateways that funnel wireless communication into secured channels. The hardware sits in front of the enterprise network and blocks out rogue users. The system provides authentication, priority bandwidth management and role-based access.

"You can't secure the [wireless] device, you authenticate the user," says Patrick Rafter, vice president of communications for BlueSocket. "Once you've authenticated somebody you can add [user] policies."

The system use IP SEC and PPTP encryption algorithms to protect data transmission. Pricing ranges from about $3,000 for a small office to $25,000 for an organization with more than 1,000 users.

The City of St. Cloud, FL, is installing a BlueSocket gateway platform to create a "hot spot" in a new, 590-acre residential development. In addition to providing free wireless access for its citizens, the town also plans to override the system during an emergency and give the network over to first responders.

"We'll give public safety officials priority access at all times," said Jonathan Baltuch, a contractor who is integrating the system for St. Cloud.

BlueFire Security Technologies Inc., of Baltimore, MD, has a different solution to the wireless problem. The company develops firewall software for individual mobile devices. "We protect the end point," says Tom Goodman, vice president of business development for the company. The software handles authentication, security management and allows centralized control of

More on Page 35