Gilmore Commission Calls for Independent Center to Coordinate Terrorism Intelligence

continued from page 4

able to terrorism, but actual threats from terrorists need to be defined, the commission found. Several dual-use actions can be taken to protect the agricultural sector and food supply from terrorist attacks and naturally occurring disease outbreaks, including increasing laboratory capacity, education and training to deal with foreign animal diseases.

- Improving the Protection of Critical Infrastructure: The Gilmore Commission recommended creation of an independent commission to suggest strategies for protection of the nation's critical infrastructure, and urged that the Department of Homeland Security elevate the priority of other aspects of critical infrastructure protection.

Vulnerability of Wireless Local Area Networks to Interception

By David C. Jenn and
Navy Lt. Paul Sumagaysay
For Homeland Defense Journal

A wide variety of wireless systems are used in both the civilian and military sectors. Many organizations have chosen wireless local area networks (WLANs) over hardwired networks because of their convenience and flexibility. One challenge in deploying systems that radiate in free space is the possibility of the signal being intercepted by unauthorized users. For example, portable computers with client adapter antennas could be placed covertly so as to intercept the WLAN microwave transmission signal.

Even though the power levels involved are very low, a person just outside of a building or in a lobby could conceivably receive and record signals for analysis at a later time. There are unique propagation conditions that occur inside of buildings and in "urban canyons" that could enhance signal detection under certain circumstances. Thus, the WLAN is vulnerable to uninvited intruders who could collect sensitive information or possibly even disrupt the computer network by injecting deceptive signals.

According to K. Pahlavan's article "Trends in Local Wireless Networks," which was published in the March 1995 issue of IEEE Communications Magazine, several security measures have been incorporated into the WLAN standards. For example, authentication and encryption would provide data security. And, networks with media access control (MAC) contain address-based access lists on access points registers and recognize MAC addresses that are allowed to join the network. Radius server-based authentication would provide security for the network by assuring that users are authenticated against a centralized radius server that is based on the MAC address or the username and password.

Encryption between the wireless adapter and the access point would provide security with the network. Wired equivalent privacy is an algorithm designed to provide privacy for data transmitted between the wireless client and the access point. It utilizes data encryption with 40-bit or 128-bit keys that are hidden from users, according to Sandeep Singhal's "The Seven Deadly Sins of Wireless LANS," available at www.reefedge.com.

Although complex encryption techniques would make it difficult for the average person to penetrate the system, the algorithms built into the network software have been defeated by knowledgeable hackers. The first step in the hacking process would be gaining unauthorized access to network traffic. In many cases this is most easily accomplished by intercepting wireless signals. Thus, predicting and subsequently con

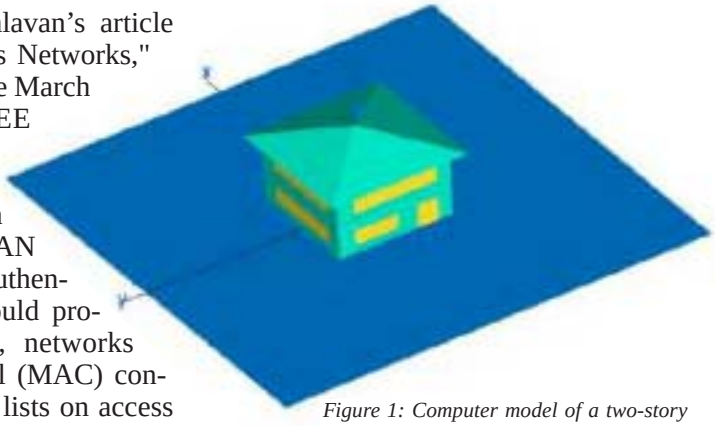

Figure 1: Computer model of a two-story office building

trolling the electromagnetic radiation is an effective means of securing the network.

In general, the approach to providing effective WLAN access for users is to position hubs to cover the desired area adequately, most often by trial and error. Electromagnetic wave propagation modeling in indoor and urban environments is difficult because of the interactions between a large number of scattering objects such as walls and furniture. Modern buildings and furnishings use many materials that affect propagation by attenuation, reflection, and diffraction. Building walls, floors, landscape, and even adjacent buildings affect the manner in which these signals propagate.

The underlying electromagnetic theory is well understood, and accurate propagation simulations are achievable with sufficient computational resources, such as CPU time and memory, and high-fidelity building models. Often, the lack of knowledge of the materials enclosed in a wall limits the accuracy of a simulation, not a shortcoming in the electromagnetic analysis.

continued on page 7

Vulnerability of Wireless Local Area Networks to Interception

continued from page 6

Research at the Naval Postgraduate School, sponsored by the Department of Justice, has examined the vulnerability of WLANs to interception and provided some simple steps that can be taken to improve security. Science Application International Corp.'s Urbana Wireless Toolset was used to predict signal levels in complex environments such as the inside of a building. The propagation model is essentially a 3-D ray tracing process that predicts the local mean power received at any given point. The model includes the effects of wave polarization, material properties, and antenna patterns. The simulations provided contours of power levels that could predict the maximum detection distance of the wireless signals.

Figure 1 shows a model of a two-story building that might be occupied by a small business. The building footprint is a square, 40 feet on a side. A WLAN access point antenna, located on the first floor at the + symbol, was considered to be transmitting. The signal levels were calculated at points inside and outside of the building using *Urbana.*

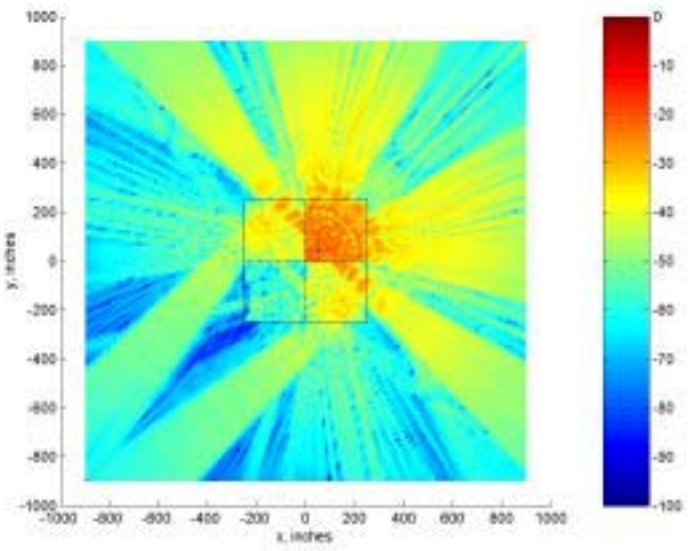

Figure 2: Power levels for a building with metal composite walls and standard glass windows. Units are decibels relative to a milliwatt (dBm). Strong signals passing through the windows are evident.

Figure 2 shows the power levels for a transmitter power of 100 milliwatts, which is the highest power allowed. The building walls are a metal composite, and standard glass windows are used.

The receiver sensitivity is the minimum power required for maintaining the link. WLAN sensitivities range from –94 dBm for 1 Mbps to –85 dBm for 11 Mbps, where dBm is a decibel relative to a milliwatt reference, according to www.cisco.com. Although the strongest signals are confined to the interior of the building, significant levels are transmitted through the walls and windows. No interception would be possible in the dark blue areas. Note that at the lowest data rate, interception is possible over most of the computational grid that is 1800 inches (150 feet) on a side.

In Figure 3 the standard glass windows are replaced by tinted glass. There has been a significant reduction in the power outside of the building. A further reduction in power can be achieved by moving the transmit antenna to the second floor, as evident in Figure 4.

The fact that the WLAN is contained inside a closed building gives a false

continued on page 8

Vulnerability of Wireless Local Area Networks to Interception

continued from page 7

sense of security. Many small businesses use WLANs, yet system administrators are not aware of the susceptibility of these systems to interception, or feel that they do not have the resources to tighten security. However, some steps could reduce the probability of interception, including:

1. locate access points in the most interior building spaces
2. close all exterior doors and windows
3. use metal blinds or tinting on exterior windows
4. use directive or sectored access point antennas to confine the direction of strong radiation
5. use the lowest possible power settings
6. buildings with metal exterior walls are preferred over those with wood

These simple measures can deny terrorists access to the information they need to inflict damage.

Dr. David C. Jenn is an associate professor in the Department of Electrical & Computer Engineering at the Naval Postgraduate School. Paul Sumagaysay is a lieutenant in the U.S. Navy, and recently graduated from the Information Warfare program at the Naval Postgraduate School.

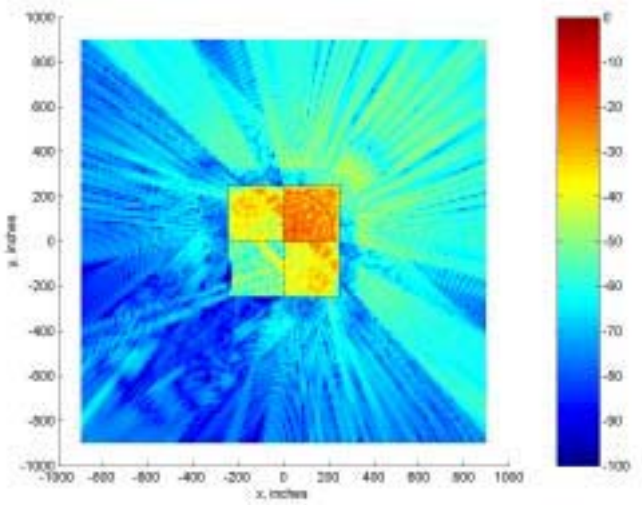

Figure 3: Outside power levels are reduced using tinted glass, which reflects signals back into the building.

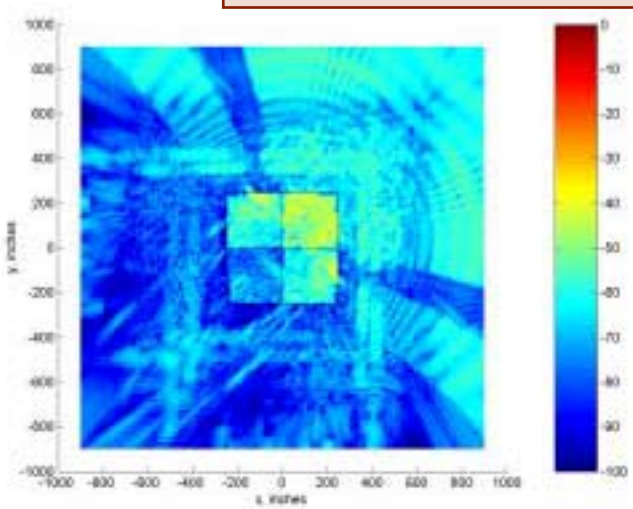

Figure 4: Outside power levels are reduced further after moving the access point antenna to the second floor.