

Managing Wireless Network Security

New measures and standards greatly improve security for wireless networks

Much has been made of the relatively weak security inherent in the Wi-Fi standard, which has led some potential adopters to hold off on installing it. But wireless network equipment vendors and standards bodies have been working feverishly to build more security into wireless networks.

Hotel and restaurant operators face a real challenge when it comes to wireless security decisions. Making the log-on experience in their public access network fast and simple means avoiding extra steps—the very thing that may be necessary to make that user's online experience more secure.

Security for a wireless network starts with the same basic measures and security that protects wired networks. It may be obvious, but it warrants repeating. Access should be controlled by user log in and password for all functions other than public access to the Internet as well as firewalls and virus protection.

Current Wi-Fi systems already have some security features in place. The Wired Equivalent Privacy (WEP) system allows users to set up either 64 or 128-bit encryption keys. Such encryption is probably enough to keep most prying eyes out of network systems, but the current system still has significant holes in it.

WPA: Administering a work in progress

Providers of public access Wi-Fi will most likely employ WPA and 802.11i only for their internal, operational use of the wireless network, says Frank Hanzlik, managing director of the Wi-Fi Alliance. Most public access Internet hotspots turn off security measures to make access easier for users. The same infrastructure can be used for both public and operational use if the access points support "mixed mode" operation and additional network traffic management technology is deployed, he explains.

The Wi-Fi Alliance (formerly known as the Wireless Ethernet Compatibility Alliance) is an organization of wireless companies formed to certify 802.11a, b and g products to ensure interoperability. Rather than

Case Study: A Network Home Run

Wireless technology is a hit at the Great American Ball Park

Fans of the Cincinnati Reds can order a round of beer for their friends, or a ton of hotdogs with all the toppings, or even a hardy salad dripping with their favorite dressing—without leaving their seats once.

How so you ask? Because premium seats at the new Great American Ball Park, which opened in March 2003 to replace Cinergy Field, come with in-seat food service, thanks to a wireless POS solution from MICROS. The system, which was installed by Brolin Retail Systems of Ohio, is part of Great American Ball Park's MICROS 9700 HMS hospitality management solution.

Throughout the design and construction phases, the Reds incorporated many of the best features from some of the other newly built Major League ballparks. But the best feature, according to Joseph Sims, general manager of sports service, Concessionaire for Delaware North, which services the Great American Ball Park, is the wire-



For More Information

There are numerous sources for additional information about wireless technology and wireless networks.

Visit the following websites to learn more:

Bluetooth Special Interest Group (SIG)

www.bluetooth.com

The Institute of Electrical and Electronics Engineers

www.ieee.org

The Open Mobile Alliance

www.wapforum.com

The Wi-Fi Alliance

www.wi-fi.org

The Wireless LAN (Local Area Network) Association

www.wlana.org

Wireless LAN Weblog

www.wireless-lan.com

wait for the slow moving IEEE, the Wi-Fi Alliance has developed WPA (Wi-Fi Protected Access) as an interim stop-gap security measure.

“WPA is the step in the right direction,” insists William Clark of Gartner

Dataquest. “And, now that it has been blessed and certified, hospitality companies don’t have to standardize on a proprietary system.” WPA was designed to close up some of Wi-Fi’s security holes in data protection and access control in 802.11b networks before the next full security release, 802.11i. Existing 802.11b equipment can be upgraded to WPA compliance via a firmware change.

Managing the security risk

Due out late this year or in early 2004, 802.11i will include everything in WPA plus one additional encryption standard and two authentication measures.

There is always risk inherent in a network, wired or not. Users of public networks assume their own risk when it comes to security. According to Wi-Fi Alliance, many hotspot providers and Wi-Fi manufacturers are implementing improved security technologies to protect Wi-Fi users against interception and eavesdropping in public hotspots. In the meantime, these are steps you can take to protect your guests from unwanted hackers:

- ▶ **Set up a VPN or VLAN:** Make sure your network is compatible with the most widely used virtual private networks or even a virtual local area network for groups of users. These technologies set up a temporary secure access for a single user or a group of users on a common network, protecting them from each other and outside access.
- ▶ **Authentication techniques:** These help ensure only authorized users are using the network access you’re providing.
- ▶ **Use additional encryption:** Consider offering dongles—external hardware devices that guests add to their laptops to encrypt the data.
- ▶ **Ask your vendor:** Many Wi-Fi vendors and solution providers may offer additional security and access control measures that ride on top of the network, such as ensuring that two users on a network cannot see each other’s traffic.
- ▶ **Set up firewalls:** Firewalls are essential to protect your hotel or restaurant’s network from public access. ■

less concession service that allows fans to order menu items from their seats.

“Fans think its cool”

“I think it’s great,” said Sims.

“Anytime you try something new you’re a little leery. I just knew this thing was going to break down all the time. But it hasn’t given us any problems, the fans think it’s cool, and we can provide a lot of services that were not offered at Cinergy.”



Great American Ball Park installed the Mobile MICROS hand-held solution that allows waiters and waitresses to use a handheld device to take orders in the seating bowl, print receipts and even swipe credit cards. Once a fan places his order, a wireless signal is sent to one of two access points, called boosters, which boost the order to the correct kitchen. The order is then prepared and delivered to the fan in less than five minutes.

“These handhelds allow us to do things we can’t do at the concession stand because we don’t have the space or the capability, such as serve salads, roll sandwiches, and certain types of ice cream,” said Sims. “Now we can utilize the back kitchen and serve more elaborate dishes and drinks, like eventually, mixed drinks, pasta and pita bowls.”

The wireless premium

All this luxury, however, comes with a small price. Those who want premium service have to pay for premium seats that are closer to the field and the players. The cost for these 3300 premium seats is between \$50 and \$80, whereas most seats range from about \$16 to \$30.

“Right now about 60% of premium seat guests are using the in-seat service,” says Sims. “Some people order just to show off to their friends and show them how fast the food comes. Others order because the person in front of them ordered something with their credit card and they realize they can use one too. Some hardcore fans use it because they don’t want to miss a second of the game. Overall, we get more incremental sales and it makes us the envy of some of our peers in the business.” ■