Wireless Perils

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

When wireless telephone handsets (ordinary phones useful for short-range wandering around the house and garden, not cellular telephones) were introduced into the home market years ago, teenagers very quickly discovered that it was the handset that controlled connection to the public switched (telephone) network (PSN). In other words, putting the handset down on the cradle or picking it up had nothing to do with whether the phone could connect to the PSN. Kids began walking around their neighborhoods with their parents’ wireless handsets turned on; after a few hundred feet from home base, they would lose the dial tone. If they kept the handset on, though, sometimes they’d get another dial tone – this one from a compatible wireless phone in a neighbor’s house. The kids could then place long-distance or other chargeable calls at someone else’s expense with little chance of discovery. Sometimes they’d hear a conversation in progress and eavesdrop for a while.

These no-security phones thus suffered from several design problems: (1) Phones from different manufacturers nonetheless had considerable interoperability; (2) The transmissions were unencrypted; (3) It was difficult to detect an intrusion while it was happening. Manufacturers scrambled to fix the problems by introducing a wider range of frequencies (so that the handset and the base station could communicate but other phones would be less likely to hit the same frequency) and some simple encryption methods. Even so, I remember warning corporate clients never to allow a wireless handset into their offices for confidential communications. And as for the idea of using those wireless handsets in airline clubs – ptooie: never use one of those to talk about sensitive details. You never know who might be listening.[1]

Cellular (mobile) phones are relatively secure today. Nevertheless, some security experts routinely answer calls on these devices with, “Hi, this is <name>. This line is not secure.”[2]

Similar problems of excessive transparency occurred in the 1980s when the wireless local area networks (LANs) began arriving into the world of IEEE 802.3 Ethernet communications. Early wireless LANs offered dramatically lower installation costs for existing buildings (retrofitting LAN cable into an existing ceiling or wall is a dusty, tiresome and expensive job), but they had no encryption at all. People worried even then about the safety of using such systems for any kind of sensitive or critical application.

A similar set of problems has developed with wireless communications using the newer protocols that allow access to the Internet as well as to intranets. For those who want a six-page overview of wireless LAN security, I recommend Christopher Klaus’ excellent FAQ.[3] For those even more interested in detail, see Matthew Gast’s new book from O’Reilly.[4]

In my next column, I’ll look at mobile phones that are designed for industrial espionage.

* * *

References
http://www.spybusters.com/wireless_phone_alert.html

http://www.tinhat.com/cell_phone/mobile_phone_security.html

http://www.iss.net/wireless/WLAN_FAQ.php


* * *
A Master’s degree in the management of information assurance in 18 months of online study from Norwich University – see < http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2005 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.