Wireless Security: 802.11, Bluetooth and Handheld Devices

Dr. Tom Karygiannis, NIST

Abstract: Wireless Security: 802.11, Bluetooth, and Handheld Devices Wireless local area networks (WLAN) provide the mobile workforce with access to enterprise computing resources without confining them to their office space and without the need for cables and wires. Less wiring means greater flexibility, increased efficiency and reduced wiring costs. Ad hoc networks, such as those enabled by Bluetooth, eliminate the need for cables for printers and other peripheral device connections. Handheld devices, such as Personal Digital Assistants (PDA) and cell phones, allow remote users to synchronize personal databases, as well as provide access to network services such as wireless e-mail, web browsing, and Internet access. These technologies can offer dramatic cost savings and added capabilities to diverse applications ranging from retail settings to manufacturing shop floors to first responders. Risks are, however, inherent, in any wireless technology. Some of these risks are similar to those of wired networks; some are exacerbated by wireless connectivity; some are new. Perhaps the most significant difference from wired networks and the main source of these risks is that with wireless networks the technology's underlying communications medium, the airwave, is openly exposed to intruders, making it the logical equivalent of placing an Ethernet port in the parking lot. This presentation will provide a brief overview of these wireless technologies, their risks, and associated countermeasures. For more detailed guidance on wireless security, NIST Special Publication 800-48 can be downloaded from **http://csrc.nist.gov**.