Rogue Access Points

"Rogue" wireless access points are another pressing concern. Employees may install them in order to facilitate intra-office mobility with their laptops. But lurking in the parking lot could be laptop-equipped "sniffers," using such access points to gain entry into the entire network. DHS policy prohibits any use of these devices without the written permission of the system accreditor.

A similar security breach can happen when an employee sets up a wireless local area network (LAN) at home. Many wireless LAN switches currently offer rogue-access-point detection, however. The small physical size of wireless devices also opens up major potential security vulnerabilities, by increasing the risk of loss, theft, and tampering.

Countermeasures

- Never store or process classified information on a wireless device.
- Turn off and power down the device and remove the battery before entering a classified or sensitive processing area. For other than collateral material, these devices are prohibited altogether from such areas.
- Maintain a three-meter separation between your wireless device and any classified processing equipment.
- Enable an alphanumeric password that is at least eight (8) characters long.
- Maintain physical control over your wireless device at all times.
- If you think your device has been tampered with, discontinue its use.
- Lock your device when not in use.
- Do not download e-mail attachments or files from the Internet, unless you are sure of the content.
- Do not use or rely on wireless devices for emergency notification or continuity of operations.
- Never connect or cradle a wireless device to a classified computer or system, and turn wireless function off before attaching to a sensitive computer or system.

International Travel

When traveling, especially internationally, a wireless device may leave the possession of its owner during security or customs inspections, opening a door of opportunity for foreign adversaries to collect information.

Before entering such checkpoints, consider removing the battery and SIM card (if applicable). Place these pieces in a physically different location, such as a bag or coat pocket.

As an alternate, the device may be placed in a clear, tamper-evident bag.

Wireless Technology

Friend or Foe?

U.S. Department of Homeland Security
Office of Security
Washington, D.C. 25208
Phone: 202-447-5010

Homeland Security

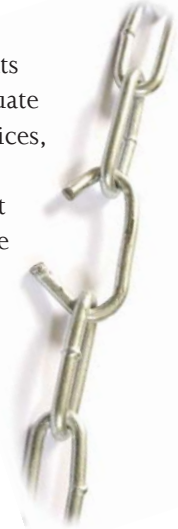
Introduction

Wireless technologies are increasingly relied upon to transmit voice, data, and video in support of national security and emergency preparedness operations. It is imperative that we understand the vulnerabilities and risks associated with using wireless technology to afford proper protection to our national security information.

What is Wireless Technology?

Wireless technology is a complex system of software, hardware, and firmware that provides its user with unparalleled connectivity. If these devices are used or handled improperly, they can provide an adversary unparalleled access to a user's data and other sensitive information.

Vulnerabilities

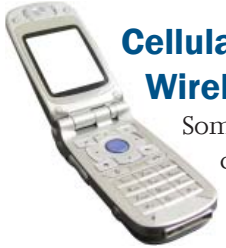


Known vulnerabilities and related threats include but are not limited to - inadequate encryption, improperly configured devices, inadequate physical security, protocol vulnerabilities, inadequate management of passwords and keys, and convergence of wireless and data communications, resulting in interception.

Wireless technology applies to all commercial wireless devices, services, and technology.

Wireless vulnerabilities are not generally applicable to receiver-only pagers, Global Positioning System receivers, hearing aids, pacemakers, and other implanted medical devices or personal life support systems.

Wireless transmissions may be intercepted and, if encrypted or unencrypted under a flawed protocol, their contents made known.



Cellular Phones and Other Wireless Devices

Some cell phones and other wireless devices that operate on radio frequencies can be monitored by radio frequency scanners.

Even while devices such as mobile phones, or even your vehicle's diagnostics system, are "off" or on "standby," the device sends transmissions to the local tower, providing a stream of data that enables the tracking of the person's movements. These are capable of being recorded, used, and analyzed.

It is easy for an adversary to program a watch list of phone numbers into a computer that automatically picks out all calls to or from those numbers and records the conversations. In addition to being simple, this is nearly impossible to detect.

An eavesdropper can effortlessly determine a target's cell phone number, because transmissions are going back and forth to the cellular site whenever the cell phone has battery power and is able to receive a call.

For a car phone, this generally happens as soon as the ignition is turned on. All an eavesdropper has to do, then, is to simply wait for the target to leave his home or office and start the car. The initial transmission to the cellular site to register the active system is picked up immediately by the scanner, and the number is entered automatically into a file of numbers for continuous monitoring.

The simplest way to ensure your conversations are not being monitored or recorded is to prohibit them in secure facilities. Removing the battery is another way of disabling the phone.

Many of the technological advances designed for our convenience can easily be used against us. As mentioned, cellular telephones are especially vulnerable, but cordless phones, e-mail, answering machines, and voice mail can all be exploited in various ways.

Bluetooth

Bluetooth technology is technology that's built into various wireless devices. As with other wireless devices such as headphones, keyboards, digital cameras, cellular phones, etc., Bluetooth capability can also be remotely enabled without the user's knowledge.

Portable Electronic Devices (PEDs)

PEDs are extremely useful in managing appointments and contacts, reviewing documents, corresponding via e-mail, delivering presentations, and accessing corporate data. And because of their relatively low cost, they are becoming a commonplace fixture within office environments.

Imagine how the lost or theft of a PED can be devastating to the user and a gold mine to the adversary.

Memory Sticks or Flash Drives

The USB Memory Stick, or Flash Drive, generally hold up to four or more gigabytes of data. These devices plug into most PCs and laptops and instantly become another hard drive. Because they are handy and cheap to buy, Memory Sticks have essentially replaced floppy disks and CDs when it comes to moving data around. Many times, these devices are lost or left in the office, which makes them susceptible to anyone looking for an easy target. Because these devices can be as small as a finger, they are easy to conceal.

This poses a security officer's worst nightmare, because in most cases, the owner doesn't immediately miss the Flash Drive or remember exactly what type of data was stored on the device.