DEFENSE SECURITY SERVICE
INDUSTRIAL SECURITY FIELD OFFICE (S41PA)
283 S. LAKE AVENUE, SUITE 202
PASADENA, CA 91101-3105

CELLULAR PHONE VULNERABILITY!

Be Aware! Your cellular telephone has three major vulnerabilities

1. Vulnerability to monitoring of your conversations while using the phone.

2. Vulnerability of your phone being turned into a microphone to monitor conversations in the vicinity of your phone while the phone is inactive.

3. Vulnerability to "cloning," or the use of your phone number by others to make calls that are charged to your account.

Before discussing the vulnerabilities, a brief tutorial is provided on how cellular phones function.

- They send radio frequency transmissions through the air on two distinct channels, one for voice communications and the other for control signals. When a cellular telephone is first turned on, it emits a control signal that identifies itself to a cell site by broadcasting its mobile identification number (MIN) and electronic serial number (ESN), commonly known as the "pair."

- When the cell site receives the pair signal, it determines if the requester is a legitimate registered user by comparing the requestor's pair to a cellular subscriber list. Once the cellular telephone's pair has been recognized, the cell site emits a control signal to permit the subscriber to place calls at will. This process, known as anonymous registration, is carried out each time the telephone is turned on or picked up by a new cell site.

VULNERABILITY TO MONITORING:

All cellular telephones are basically radio transceivers. Your voice is transmitted through the air on radio waves. Radio waves are not directional -- they disperse in all directions so that anyone with the right kind of radio receiver can listen in. Although the law provides penalties for the interception of cellular telephone calls, it is easily accomplished and impossible to detect. Radio hobbyists have web sites where they exchange cell phone numbers of "interesting" targets. Opportunistic hobbyists sometimes sell their best "finds." Criminal syndicates in several major U.S. metropolitan areas maintain extensive cell phone monitoring operations.

If the cellular system uses analog technology, one can program a phone number, or a watch list of phone numbers, into a cell-monitoring device that automatically turns on a voice-activated tape recorder whenever one of the watch listed numbers is in use. Computer assisted, automatic monitoring allows monitoring a specific phone 24 hours a day, as the target moves from cell to cell, without any human assistance. If the cellular system uses newer digital technology, it is possible, for a price affordable by most radio hobbyists, to buy a digital data interpreter that connects between a scanner radio and a personal computer. The digital data interpreter reads all the digital data transmitted between the cellular site and the cellular phone and feeds this information into the computer.

It is easy for an eavesdropper to determine a target's cellular 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. Therefore, the eavesdropper simply waits for the target to leave his or her 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 can be entered automatically into a file of numbers for continuous monitoring.

One of the most highly publicized cases of cellular phone monitoring concerned former Speaker of the House of Representatives Newt Gingrich. A conference call between Gingrich and other Republican leaders was "accidentally" overheard and then taped. The conversation concerned Republican strategy for responding to Speaker Gingrich's pending admission of ethics violations being investigated by the House Ethics Committee. The intercepted conversation was reported in the New York Times and other newspapers.

Pagers have similar vulnerabilities. In 1997, police arrested officials of a small New Jersey company, Breaking News Network, that was monitoring pager messages to New York City leaders, police, fire, and court officials, including messages considered too sensitive to send over the police radio. They were selling the information to newspaper and television reporters. The offenses carry a penalty of up to five years in prison and fines of $250,000 for each offense.

VULNERABILITY TO BEING USED AS A MICROPHONE:

A cellular telephone can be turned into a microphone and transmitter for the purpose of listening to conversations in the vicinity of the phone. This is done by transmitting to the cell phone a maintenance command on the control channel. This command places the cellular telephone in the "diagnostic mode." When this is done, conversations in the immediate area of the telephone can be monitored over the voice channel. The user doesn't know the telephone is in the diagnostic mode and transmitting all nearby sounds until he or she tries to place a call. Then, before the cellular telephone can be used to place calls, the unit has to be cycled off and then back on again. This threat is the reason why cellular telephones are often prohibited in areas where classified or sensitive discussions are held.

VULNERABILITY TO CLONING

Cellular telephone thieves don't steal cellular telephones in the usual sense of breaking into a car and taking the telephone hardware. Instead, they monitor the radio frequency spectrum and steal the cell phone pair as it is being anonymously registered with a cell site.

Cloning is the process whereby a thief intercepts the electronic serial number (ESN) and mobile identification number (MIN) and programs those numbers into another telephone to make it identical to yours. Once cloned, the thief can place calls on the reprogrammed telephone as though he were the legitimate subscriber.

Cloning resulted in approximately $650 million dollars worth of fraudulent phone calls in 1996. Police made 800 arrests that year for this offense.

Each day more unsuspecting people are being victimized by cellular telephone thieves. In one case, more than 1,500 telephone calls were placed in a single day by cellular phone thieves using the number of a single unsuspecting owner. The ESN and MIN can be obtained easily by an ESN reader, which is like a cellular telephone receiver designed to monitor the control channel. The ESN reader captures the pair as it is being broadcast from a cellular telephone to a cell site and stores the information into its memory. What makes this possible is the fact that each time your cellular telephone is turned on or used, it transmits the pair to the local cellular site and establishes a talk channel. It also transmits the pair when it is relocated from one cell site to another.

Cloning occurs most frequently in areas of high cell phone usage -- valet parking lots, airports, shopping malls, concert halls, sports stadiums, and high-congestion traffic areas in metropolitan cities. No one is immune to cloning, but you can take steps to reduce the likelihood of being the next victim.

CELLULAR PHONE SECURITY MEASURES:

The best defense against these three major vulnerabilities of cell phones is very simple:

Do not use a cell phone. If you must use a cell phone, you can reduce the risk by following these guidelines: Because a cellular phone can be turned into a microphone without your knowledge, do not carry a cellular phone into any classified area or other area where sensitive discussions are held.

Turn your cellular telephone on only when you need to place a call. Turn it off after placing the call.

Ask your friends and associates to page you if they need to talk with you. You can then return the page by using your cellular telephone.

Do not discuss sensitive information on a cellular phone. When you call someone from your cell phone, consider advising them you are calling from a cell phone that is vulnerable to monitoring, and that you will be speaking generally and not get into sensitive matters.

Do not leave your cellular telephone unattended. If your cell phone is vehicle-mounted, turn it off before permitting valet parking attendants to park the car, even if the telephone automatically locks when the car's ignition is turned off.

Avoid using your cellular telephone within several miles of the airport, stadium, mall, or other heavy traffic locations. These are areas where radio hobbyists use scanners for random monitoring. If they come across an interesting conversation, your number may be marked for regular selective monitoring.

If your cellular service company offers personal identification numbers (PIN), consider using one. Although cellular PIN services are cumbersome and require that you input your PIN for every call, they are an effective means of thwarting cloning.

Article compiled from various references.