Cell Phone Vulnerabilities

Be Aware! Your cell phone 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 your 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.

Vulnerability to Monitoring

All cell phones are 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 – YOU. Opportunistic hobbyists sometimes sell their best "finds" – YOU. There are also criminal syndicates in several major U.S. metropolitan areas that maintain extensive cell phone monitoring operations. It is easy for an eavesdropper to determine a target's – YOU, cell phone number, because transmissions are going back and forth to the cell 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 – YOU, to leave his or her home or office and start the car. The scanner immediately picks up the initial transmission to the cellular site to register the active system. The number can be entered automatically into a file of numbers for continuous monitoring.

Real World

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 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

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 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 $250,000.00 for each offense.

Vulnerability to being used as a microphone

A cell telephone can be turned into microphone and transmitter for the purpose of listening to conversations in the vicinity of the phone. This is done by transmitting a maintenance command on the control channel to the cell phone. The command places the cell phone 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 al nearby sounds until he or she tries to place a call. Then, before the cell phone can be used to place calls, the unit has to be cycled off the back on again.

This threat is the reason why cell telephones are prohibited is areas where classified or sensitive discussions are held.

Vulnerability to cloning.

Cell phone thieves don't steal phones 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 be 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 these numbers into another phone 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 and 800 arrests for the cloning offense. Each day more unsuspecting people are being victimized by cell phone thieves. In one case, more than 1,500 telephone calls were placed in a single day by cell phone thieves using the number of an 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 cell telephone to a cell site and stores the information into its memory. What makes this possible is the fact that each time your cell phone 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, airport, shopping malls, concert halls, sports events, 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.

Cell Phone Security Measures

The best defense against these three major vulnerabilities is very simple.

1. Do not use a cell phone.

2. If you must use a cell phone, you can reduce the risk by following the following guidelines:
    - Because a cell phone can be turned into a microphone without your knowledge, do not carry a cell phone into any classified discussion area or other area where sensitive discussions are held.
    - Turn your cell phone 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 cell phone.
    - Do not discus sensitive information on a cell phone.
    - When you call someone from your cell phone, consider advising them that 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 cell phone unattended.
    - Avoid using your cell phone within several miles of the airport, stadium, mall or other heavy traffic locations. These are areas where scanners most often used for monitoring.
    - If your cell phone has the capability to utilize personal identification numbers (PIN) consider using one.

A $26,000.00 cell phone bill

The following happened to three consumers in California:

- A resident in San Francisco received a $26,000.00 bill after her phone was unknowingly stolen before she left for an overseas vacation. Cingular held the individual responsible for the charges incurred after the phone was taken, up to the time the individual discovered the theft and notified the carrier. The individual was able to prove via airline and passport documents they were out of the country and couldn't have possibly have made the unauthorized calls from San Francisco during the time period stated. Cingular still held the cell pone owner responsible for the charges. To add insult to injury Cingular advise the individual that if they could not pay the bill they should consider filing for bankruptcy!
- Another individual had their cell phone stolen on their vacation. They reported it to police, filed a report and contacted their carrier, Sprint, immediately, but then received a bill of almost $16,000. Sprint claimed they never received the call from the individual reporting the stolen phone. The individual was able to submit proof from landline records that they had indeed called Sprint customer service. However late fees continued to accrue as the situation remained unresolved for months.
- Another individual had their cell phone stolen which they reported the next day. However by that time $1,800 in unauthorized charges had been charged. Due to the suspicious nature of the fraudulent charges this individual was interviewed by the FBI and cleared of all responsibility. However T-Mobile continued to insist for payment of the outstanding charges plus late fees and interest.

This year more than 600,000 cell phones will be reported lost of stolen. The following ten tips may help you from becoming a static.

1. Guard your cell phone like your wallet and be careful of the information that you store in your cell phone.
2. Password protect your device. This may buy you some time until you have discovered your loss and have reported it.
3. Don't be fooled by cell phone insurance. They protect against the loss of the unit, not any unauthorized charges for calls.
4. Call your cell phone provider as soon as you discover the loss. Keep records of the call, date and time your discovered the loss, date and time you called your network provider, the name and ID number of the individual with whom you spoke at your provider when you reported the loss and what you were told. Also note the state or region of their call center plus the extension number you called. Finally ask for confirmation in writing that your phone has been disabled.
5. File a police report. This may not help get your phone back but it does provide an official record of the crime. Some carriers may require a copy of this when provide them notification of the loss. Open an investigation with your carrier if necessary. If you find you are not getting anywhere by working directly with your cell phone company, don't waste a minute start going up the chain of command and follow up in writing. Requesting an investigation may give you a better chance of preventing any formal collection actions and also may delay any reporting to the credit bureaus. Advise your carrier that you will be filing a complaint with the FCC, your state's attorney general's office and your state's public utility commission and follow through. Your carrier is more likely to pay closer attention to you when they know that you are an informed consumer.
6. Open an investigation with your carrier if necessary.
7. Contact the FCC. The FCC will forward your complaint to your service provider requiring a response from them in 30 days.
8. Contact your state's attorney general's office.
9. Contact your state's PUC. Each state has a government agency that is usually called the public utility commission that oversees telephone companies.
10. When all else fails, contact the media. Wireless companies are particularly adverse to negative media. So when all else fails go public. This is what happen to the three cases previously mentioned and they were all resolved in favor of the individual but the companies had to be forced to do the right thing.

This information is from the Cell Phone Vulnerabilities Powerpoint by the North American Aerospace Defense Command and the United State Northern Command