Kinds of Cell Phones

There are many different kinds of cell phones, each with a different security profile. Before you can understand the security of your cell phone, you need to know what kind of cell phone you have.

Analog Cell Phones, also called **AMPS** (Advanced Mobile Phone System). These were the first cellular telephones. Developed in the 1970s and deployed in the 1980s and still used today. These phones transmit voice as an analog signal without any encryption of scrambling. As a result, they can be eavesdropped upon using handheld scanners sold at places like Radio Shack. Analog systems are widely deployed throughout the US, especially in rural areas. Although analog cell phones are still sold but not a good deal, as analog providers generally charge a lot of money, the phones do not have good battery life, and the sound quality is generally poor. The big advantage of analog cell phones is that they have the best nation-wide coverage, but that's changing fast. If you have an analog cell phone, you probably want to get a new one. (Note: many "dual-mode" digital phones support have analog for roaming in remote areas; roaming fees are sometimes included in a one's monthly plan, but other times they are extra.)

GSM (Global System Mobile, recently renamed Global System for Mobile Communications) is the cell phone system used by most of the world, and increasingly by carriers in the United States. GSM phones usually have a "chip" in them that contains your account number and other information. GSM phones use digital, encrypted communication between your phone and the cellular telephone base station. At the base station your voice is decrypted and sent over the telephone network. Like all digital systems, GSM phones provide substantially more voice privacy than analog systems, but they can still be eavesdropped upon by either the cellular telephone company, the government, or any organization that has access to the telephone network's switching equipment. The GSM encryption algorithm (called A5) can also be cracked by a suitably motivated attacker.

TDMA (Time Division Multiple Access) is the digital telephone standard that was deployed by AT&T in the 1990s. AT&T's telephones had a "voice privacy" or "voice security" setting which enables encryption. Unfortunately, if your turned this feature on, your phone won't work with AT&T's network, because AT&T never enabled the encryption feature in their base stations. As a result, TDMA phones can be eavesdropped upon using a some kinds of digital scanners and "soft radios." In practice, this equipment is not generally available. AT&T is migrating its network to GSM; if you buy an AT&T phone today, you're running GSM.

CDMA (Code Division Multiple Access) is the digital telephone standard that was developed by Qualcomm and deployed by Sprint PCS and by Verizon. CDMA used RC4 encryption but the protocol doesn't keep the keys secret, so in practice CDMA communications can be eavesdropped by a motivated attacker. In practice, though, it's must easier to wiretap a CDMA telephone on the provider's network. Today CDMA is used by the Sprint part of Sprint/Nextel and by Verizon.

iDEN (Integrated Digital Enhanced Network) is a technology developed by Motorola for multiplexing fleet radio systems in the 1980s. This technology was adopted by Fleet Call which renamed itself Nextel. Besides providing digital telephone communications, iDEN has a "push-to-talk" feature that allows the units to be used as if they were a walkie-talkie. It's used by the Nextel part of the Sprint/Nextel network.

Privacy Risks with Cell Phones

There are many privacy risks inherent in using cell phone technology.

Risks of Eavesdropping. The primary risk that privacy activists focus on is eavesdropping --- that is, someone being able to "listen in" on the phone call without the knowledge of those on the line. There are many locations that an attacker can eavesdrop on a cellular telephone phone call:

- **Loud people.** Many people speak loudly when they are on a cell phone. It is not uncommon to hear people conducting business and discussing extremely confidential materials in restaurants, on trains, or on the street. These individuals have a significant risk of being overheard.
- **Environmental microphones.** Your telephone call can be monitored by someone who places a microphone in your room.
- **Intercepting the wireless link.** The wireless link between the phone and the cell can be monitored by a third party. Digital links are less susceptible to interception than analog links; encrypted links offer better security still.
- **Interception at the cell site.** The cell sites provide an ideal location for monitoring the communications of all individuals who are using it.
- **Interception at the telephone switch.** Cell sites of a provider are connected by leased-lines to a telephone switch. Law enforcement agencies typically place court-ordered wiretaps at telephone switches.
- **Interception on the leased-lines.** The leased lines that connect base stations to the telephone switches can be monitored as well. These "lines" can be physical wires, channels of a fiber optic cable, channels of a microwave link, or even virtual circuits within an ATM network. Indeed, a typical "leased-line" will often travel through multiple different transport layers as it travels from the cell site to the telephone switch: each of these locations provides an opportunity for monitoring.

Risks of Recording. In addition to these locations, there are other ways that an attacker might be able to record a cellular telephone conversation:

- **Answering machines.** It is not uncommon for telephone conversations to be inadvertently recorded by answering machines. This risk applies to both wired telephones and to wireless ones.
- **Handset voice recorders.** As the memory in cell phones increases, it is expected that cellular telephones themselves will increasingly be equipped with the capability to record "voice memos" or to record even record entire telephone conversations.

Traffic Analysis. Even if the conversation itself is not recorded, other confidential information can be disclosed, including:

- **Call detail information.** Cell phone providers typically record the **time, date, duration, calling number, called number,** and **location of the cell phone** for every phone call placed on their network. Some (but not all) of this information is presented to subscribers on their telephone bill. Both the records in provider's computers and the printed (or downloaded) bill could disclose a caller's relationship or location without their knowledge.
- **Call history.** Cell phones will record call detail information and store this information in the phone itself as a "history" of recently placed, received, or unanswered calls. This information can be disclosed to anyone who is holding a telephone.
- **Phone book.** Just as the call history can contain confidential information, so can a telephone's phone book.

Geolocation. In order to function properly, the telephone network needs to know where the phone is located. It's been widely reported that some telephone providers keep this location information on file for extended periods of time. This information can be made available to the police or other organizations under certain circumstances.

- **GPS.** As a result of the US E911 regulations, many phones sold in the US are now also equipped with a Global Positioning System receiver. This makes it even easier for the provider to establish the cell phone's position.
- **Tracking.** If you don't want your positioned tracked, *turn off your cell phone!*

Some phones allow themselves to be locked. If locked, both the phone's call history and the phone book cannot be accessed unless the phone is unlocked. Be aware, however: all phones

have “administrative codes” that allow them to be unlocked in the event that the subscriber forgets the password they used to lock the phone.

Other Cell Phone Security Risks

Cell phones have additional security risks because they are, fundamentally, general purpose computers.

- **Downloaded code.** Many of today’s cell phones allow code to be download and run. The code can be downloaded by the phone’s user or it can be “pushed” by the provider. This code could change the behavior of the cell phone. For example, it has been widely reported in England that the police have downloaded “wiretapping” code to certain cell phones. This code turns on the microphone whenever the police want, allowing them to use the phone to bug a room. The only way to protect yourself against this kind of threat is to remove the battery.
- **Recovery of deleted messages**. Just like any other computer system, phones do a poor job of actually overwriting the data when a user tries to delete a message. In practice, this means that SMS messages, call logs, and even the list of cell towers that your phone has touched can be retrieved by a forensic expert.
- **Targeting of Missiles.** Cell Phones emit radiation. This radiation can be used for targeting weapons. HARM (High-Speed Anti-Radiation) missiles, in particular, can use the radiation emitted from a cell phone as a homing beacon.

Cell Phone Financial Risks

- If your phone is stolen and you do not report the theft, you may be liable for calls that are made with the stolen phone.
- If you use an analog phone, your phone’s Mobile Serial Number (MSN) can be “cloned,” allowing someone to make phone calls on your account as if they were using your phone.
- You can be roaming on another provider’s network without your knowledge. In this case, you may incur a bill of hundreds or thousands of dollars and be responsible for paying it.
- If you have a GSM phone, someone can steal your chip without your knowledge. Your phone will no longer work, but you may not notice this for several hours. In the meantime, the thief can make phone calls on your account without your permission. The thief can also intercept calls that are destined for you—or just look at the caller ID to see who is calling.