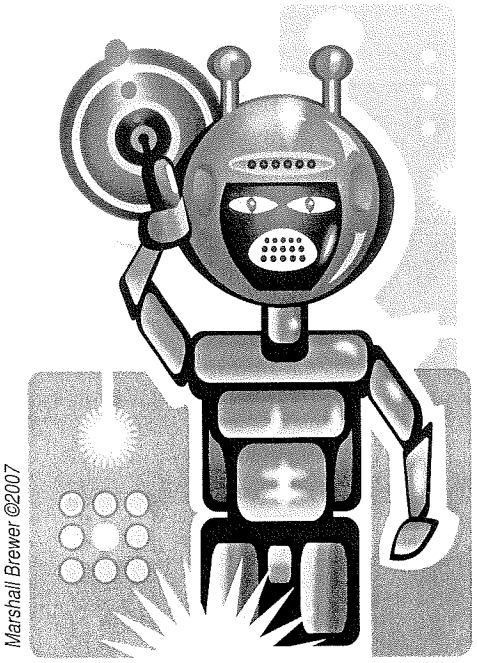

Marshall Brewer ©2007

YOU CAN HEAR ME NOW!

Cell phone technology: curse or lifesaver?

By Kent L. Colby

Gingrich and Hilton, Strange Bedfellows

Ask any passerby with a cell phone in his or her ear what a cell phone, Newt Gingrich and Paris Hilton share in common. Most likely the conversation will turn to security. Cell phone security, that is. A few years back, someone just happened to have a scanner, with a recorder, and Newt happened to drive by right when he was saying the darndest things. Last year, Ms. Hilton's phone, or rather the database, was compromised by a couple of teenyboppers who immediately shared the misbegotten information about her high-roller friends with the world.

There is no evidence that Mr. Gingrich's name was in Hilton's database, nor that Newt was talking about or to Paris. The common sheet in these two separate and unrelated scenarios is that ubiquitous cell phone. The cell phone that has become one of the world's fastest-selling electronic gadgets.

Technology Has Come a Long Way

Odds are when the former Speaker of the House (Gingrich) found his conversation being shared with the world, he was talking on a brick or similar device. It probably transmitted analog in plain old FM, and anyone with an inexpensive police scanner in range of cell phones at the time could have eavesdropped. Lots of voyeurs got their kicks scanning the cell phone frequencies to hear what they could hear. The architects of today's more robust technology make it much more difficult to casually listen in.

Digital phones generally operate at lower power levels than the analog phones of yesteryear and the few remaining today. It is also almost impossible to latch on to a conversation of a phone passing in proximity. The employment of new encryption secures both the phone and the conversation. Encryption keys rotate between the cell phone and the cell head end equipment. Incidently, cell phone scanners were made illegal by the Federal Communications Commission (FCC) several years ago. But, just on the odd chance a person with a scanner finds a channel and the time slice of a cell phone within proximity, they would also have to match the encryption code to decode the signal. The encryption also prevents the cloning of cell phones by encrypting the cell phone number and related information, as well as the voice.

Sometimes It's the People

After all the hoopla about Paris' escapades that allegedly led up to the compromising of her Who's Who address book, it turned out not to be the device. The young innocent's address book contained not only addresses, but also e-mail addresses, nude photos, and correspondence. Her device was the Sidekick II from T-Mobile and fits into the smart phone category. In this case, the database was part of the carrier's service, and the hacker apparently gained the password to the account by schmoozing someone in the office. Perhaps it was that her secret question was just too easy.

Major Concerns of Cell Phone Users

Cell phones are getting smarter and smarter. The little device takes up little more space than the "little black book" of a bygone generation. But it contains so much more information. How secure is that information? Personal information–including contacts, bank and credit card information, schedules and even sensitive business info–is all right there in the palm of the user's hand. It is one thing if the device–whether a phone, Palm or Blackberry–is lost or stolen. But is all that information at risk every time the user powers up?

Cell phones are by their very nature more vulnerable than their wired counterpart. The two biggest perceived vulnerabilities are eavesdropping and fraudulent billing.

Eavesdropping comes in two forms. The first requires no technology or special equipment. Sometimes the casual eavesdropper is hard-pressed to not listen to one half of the conversation. There is not much that can be said in a technology piece to fix that problem. Engineers in labs are working to afford better protection against scoundrel eavesdroppers.

If these bottom feeders do hack into a phone conversation, it is not only the intimacies or business secrets they can pirate, but also the phone's Electronic Serial Number (ESN) and Mobile Identification Number (MIN). This amounts to the equivalent of a stolen calling card. Cornell University's Web site makes the following recommendations:

- **Limit roaming:** *Review which phones have roaming enabled and limit these as much as practical. Roaming usually defeats the use of Personal Identification Numbers (PINs). Cloners prefer roaming phones for this reason and they target airport parking lots, airport access roads and rural interstates. Roaming also makes it more difficult for some cellular carriers to use fraud-detection programs to monitor an account and shut it down when fraud is detected.*
- **Turn the phone off:** *Cell phones poll the cellular base station with the strongest signal every few second. This is how the system knows which base station to route calls through. However, this polling exposes the phone to interception and cloning.*
- **Review all bills** *and report every erroneous call to the service provider. There are two types of cloning:*
  - Outright theft of the phone's ESN/MIN is most common. A bill will reflect hundreds, even thousands of bogus calls.
  - The other type of cloning is called tumbling, where a cloned phone uses a different ESN/MIN for each call. A bill might have only one bogus call this month, none next month, but three calls the month after that. The phone has still been cloned and fraud is occurring.
- **Prefer hands-off vehicle-mounted phones to handhelds:** *The boxes used to capture ESN/MIN have a limited range; cloners will follow an individual they know is using a phone. Recent news reports reflect the chances of an accident increase substantially if a driver is operating a vehicle and a cellular phone simultaneously.*

Alaska's ASC is well aware of security issues, noting in the company's Business Solutions promotion that, "Our signal is encrypted with approximately 4.4 trillion codes. That means phone calls will always be private and secure."

"The company's Mobile Manager Service, once contacted, will remotely lockdown a phone, erase all its data, and trigger it to emit a blood-curdling scream to scare the bejesus out of the thief."
–Software Company Synchronica Web Site

Cell Phone Hot Buttons (Risks), Points to Consider

Whom Do You Trust?

When signing up for cellular service, you are committing your mobile information to that carrier. If you rely on a phone company to keep data secure, confirm the company's security policy and perhaps not store valuable or personal information there.

Beware the Virus

That mini or simplified computer is one of many out there and is an attractive market for the burgeoning world of attackers. (To date, attacks on cell phones are nothing compared to attacks the PC. Some say it is only a matter of time, however.)

Don't innocently believe that the threat is not real. Known viruses released for cell phones do everything from kill batteries to send pricey SMS messages and place expensive calls. Recently "CommWarrior" has hit Symbian, the OS on Nokia Series 60 handsets. This virus sends messages via Bluetooth wireless connections. Another virus, Cabir, attacks MMS and can spread itself around the world in a matter of hours.

The avoidance is simple and the thunder from the same old drum: Do NOT install illegal software. Do NOT open attachments.

New Technology Problems

Technology in cell phones is changing, and fast. Look at all the little perks that are being added to this, once simple, communications tool: MP3 players, cameras, text, TV, GPS; and, can we say, Blackberry, Treo, Razr, iPhone (not currently available in Alaska)? Like all perks in the computer world, they do not come without some potentially nasty side effects.

Caution: Do not trust personal

information (photos, contact lists) new, glitzy, untested algorithms.

Privacy

Treat your mobile phone conversations as if your spouse, mother, big brother, or the FBI is listening. It may be difficult to hack into the two-way conversation; yet passive listening is easy. Passwords, account numbers, sales information–all are too routinely discussed within earshot of multitudes. Be careful what you let slip out.

VoIP, Caller ID and Voice Mail

Set and use a PIN on all voice mail accounts and verify that callers are who they say they are. Remember Voice over IP (VoIP) has security issues and VoIP phones can be tricked into passing fake information, such as a fake caller ID or bypassing security checks.

Wi-Fi and Phones

Wi-Fi networks are the least secure and the technology to make VoIP calls is not without risk. These networks are easily monitored and frequently attacked. Keep your guard up and verify your security is in order before connecting to a Wireless Local Area Network (WLAN) and be cautious of the information you share.

Bluetooth

Consider a world without wires and with cell phones so small that you forget it is in your pocket or purse, all the while emanating a mini network cloud that connects the user to a headset permanently affixed to the ear. That same cloud, if not correctly applied, leaves the information on the phone wide open to attackers retrieving personal information and spreading viruses.

Leave the Bluetooth component disabled when not in use.

Lost/Stolen Phone

Rarely are cell phones password protected and, when lost or stolen, the finder will have instant access to all personal information on the phone.

Software company Synchronica suggests you scream for your phone if it is lost or stolen. According to their Web site, "The company's Mobile Manager Service, once contacted, will remotely lockdown a phone, erase all its data, and trigger it to emit a blood-curdling scream to scare the bejesus out of the thief."

Homeland Security or Big Brother

If the news this past year about shared phone usage lists doesn't scare you enough, think about this: The 911 service can locate an emergency caller wherever they are located. What is to keep some rouge hacker from tracking a caller with similar soft and hardware?

My favorites: Cell Phone Radiation, Driving and Manners

These may not be security issues, but there are dangers associated with cell phones.

These little rascals emit energy when transmitting, which they do whenever you have a connection and are holding the phone to your ear–right next to your brain. It's called radiation.

Who hasn't complained of the precarious driving of someone with a cell phone to his or her ear? Who reading this article has not done it? There is a plethora of accessories to eliminate the dangers of holding a phone up to your ear while driving.

We alluded to manners earlier. Cell phone manners, or lack there of, can well be a security issue as well. Not just security from someone listening in on your conversation, but the callers well being. If you are the target of nasty comments, angry stares and insults, it could turn physical. As a flight attendant on a recent flight so apply put it, "If you use your cell phone while we are in flight, you will be on the wing for our feature film: Gone with the Wind."

Paranoid Yet?

Viruses and privacy should be of paramount concern. As on your home PC, implement the basic cell phone security controls. If this piece has put your paranoia over the edge, then perhaps it is best to turn off your phone, remove the battery, and lock it into a lead-lined safe. ❑