SERVICE PROVIDERS HAVE LARGELY SOLVED THE CLONING PROBLEM, BUT EAVESDROPPING IS STILL AN ISSUE, AND E-COMMERCE HAS BARELY BEEN ADDRESSED

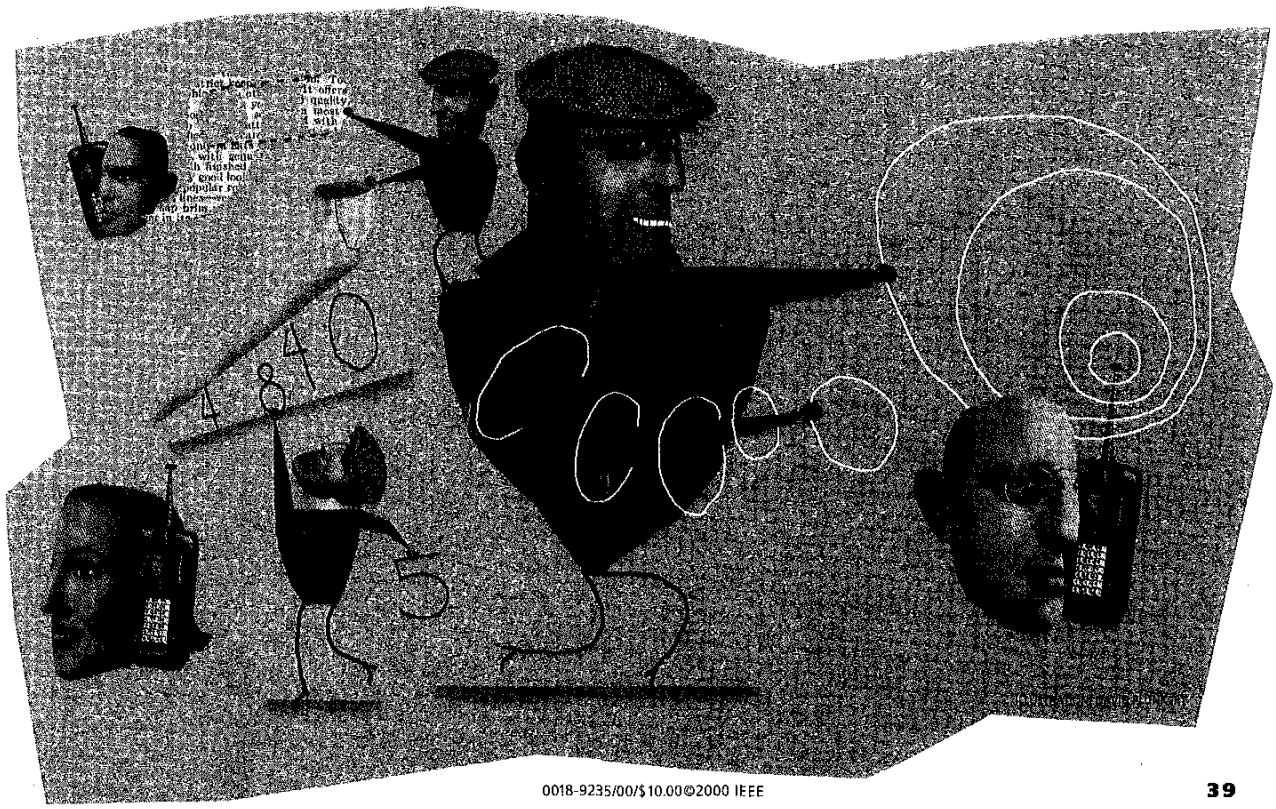
Cellular security: better, but foes still lurk

MICHAEL J. RIEZENMAN
Senior Engineering Editor

NOT BEING PRINCE CHARLES or Newt Gingrich, most of us give little thought to cell phone eavesdropping. After all, who cares if someone overhears you telling your husband you're stuck in traffic. Of course, if the conversation is of a sensitive nature, then one of your concerns is—or should be—the security of your phone.

Cellular service providers have a different security problem. Their great concern is service theft, through which criminals succeed in using a cell phone without paying for it.

In the early days of cellular telephony, service theft mostly meant cloning. People with radio scanners would simply "sniff" the cellular frequency bands, pick up cell phone identification numbers, and program them into other phones. That problem has been reduced by almost two orders of magnitude through the application of some thoughtful technology. But it has been replaced by other problems: subscription fraud (the same problem that bedevils issuers of credit cards) and the misapplication of service provider subsidies on handsets.



0018-9235/00/$10.00©2000 IEEE

Subscription fraud has several forms: pretending to be another, real person; pretending to be a nonexistent person; and even just being yourself and pretending you intend to pay your bill. Subsidy fraud involves taking a phone whose cost has been heavily subsidized by a cellular carrier and activating it on a different carrier's network.

Solutions to these problems exist. However, the newest and best of them cannot be implemented on old handsets, so the technical situation is not without interest. Some of the solutions, particularly those used to fight subscription fraud, tend by their very nature to inhibit sales—after all, the idea is to eliminate deadbeats—which presents the executives of cellular companies with a dilemma. On the one hand, many of them need the revenue stream from a large number of subscribers to help them pay off the huge investments they made when they bid wildly for spectrum space back in 1995. On the other, they have no desire to be cheated.

As the practice of conducting serious business over the Internet continues to grow, other security issues will arise. In particular, someone conducting business on a cell phone needs to be confident of the identity of the other instrument's user. The technical solutions to be discussed here, like RF fingerprinting and authentication, do a good job of guaranteeing that the handset is what it claims to be, but they guarantee nothing about the person using it.

Several approaches are being pursued to user identification. The problem, in fact, is not finding solutions, but getting everyone to agree on which to use. To do banking over a cell phone, "your bank, your cellular service provider, and your phone must agree upon the same end-to-end solution. And we, as an industry, must standardize that solution to drive mass-market end-user accessibility," pointed out Tom Deitrich, vice president for business operations at Ericsson Inc., Research Triangle Park, N.C., among others.

Biometrics may play a role here. In fact, one company, AuthenTec Inc., Melbourne, Fla., is developing a fingerprint sensor that can be integrated into a cell phone without adding noticeably to the phone's weight, price, or energy consumption [see "How a phone can check fingerprints," facing page].

Annotated acronyms

CDMA: code division multiple access, a multiplexing scheme in which all conversations share the same spectrum, but each is modulated by its own code.

ESN: electronic serial number, an identification number programmed into a cell phone at manufacture.

MIN: mobile identity number, a cell phone's phone number—the number a caller dials to reach it.

PIN: personal identity number, a number keyed in by a user to identify himself.

TDMA: time division multiple access, a multiplexing system in which each conversation is assigned its own individual time slot in a digital data stream.

ANALOG YES, DIGITAL NO

When it comes to eavesdropping, the situation is pretty simple. Analog phones are easy to bug; digital are hard. Although it is illegal to sell scanners in the United States today that are capable of receiving the frequency bands used for cellular telephony (824–849 MHz, 869–894 MHz, 1.85–1.91 GHz, and 1.93–1.99 GHz), older units that can receive them are readily available. Moreover, it is hardly rocket science to modify a new, compliant receiver to add the extra bands. (The scanners are inherently capable of receiving at least the lower bands; they have just been rigged to block them.)

Lest anyone think that analog cellular telephony is an old, dead technology, as of June 1999, over 70 percent of the subscribers in the United States still used analog handsets, according to Boston's Yankee Group. And many who have dual-mode phones (capable of analog and digital operation) turn to the analog mode when roaming, especially in rural areas.

The latest figures from the Cellular Telecommunications Industry Association (CTIA), Washington, D.C., say merely that digital penetration today exceeds 50 percent. But the CTIA counts dual-mode handsets as digital, so its number may not be so different from the Yankee Group's. Whatever the precise numbers, the message is clear: eavesdropping is not of only historical interest.

Digital phones, be they of the time- or code-division multiple-access (TDMA or CDMA) variety, are, unlike analog units, quite proof against eavesdropping by ordinary mortals. Would-be listeners-in, for one thing, have to know what system they are trying to tap into, since TDMA and CDMA are utterly different. For TDMA, what can be snatched out of the ether is a digital data stream representing one side of each of three multiplexed conversations. Eavesdroppers need to lock onto the correct time slot to get the conversation they want.

In the case of CDMA, what they wind up with is an even thornier problem—a mishmash of half a dozen conversations, each modulated by a different pseudorandom code, all occupying the same band. So the signal has to be decoded with the same code, which has been obtained in some mysterious fashion.

Plus, in digital systems, voice is vocoded. The sound is not only digitized, but compressed as well. As before, someone interested in decompressing it needs to know the compression algorithm used.

In short, eavesdroppers need to build what amounts to the receiving part of a cellular phone base station in order to have a chance of "overhearing" a call. Small wonder that none of the system operators or phone manufacturers interviewed for this report regards eavesdropping on digital cell phones as a problem.

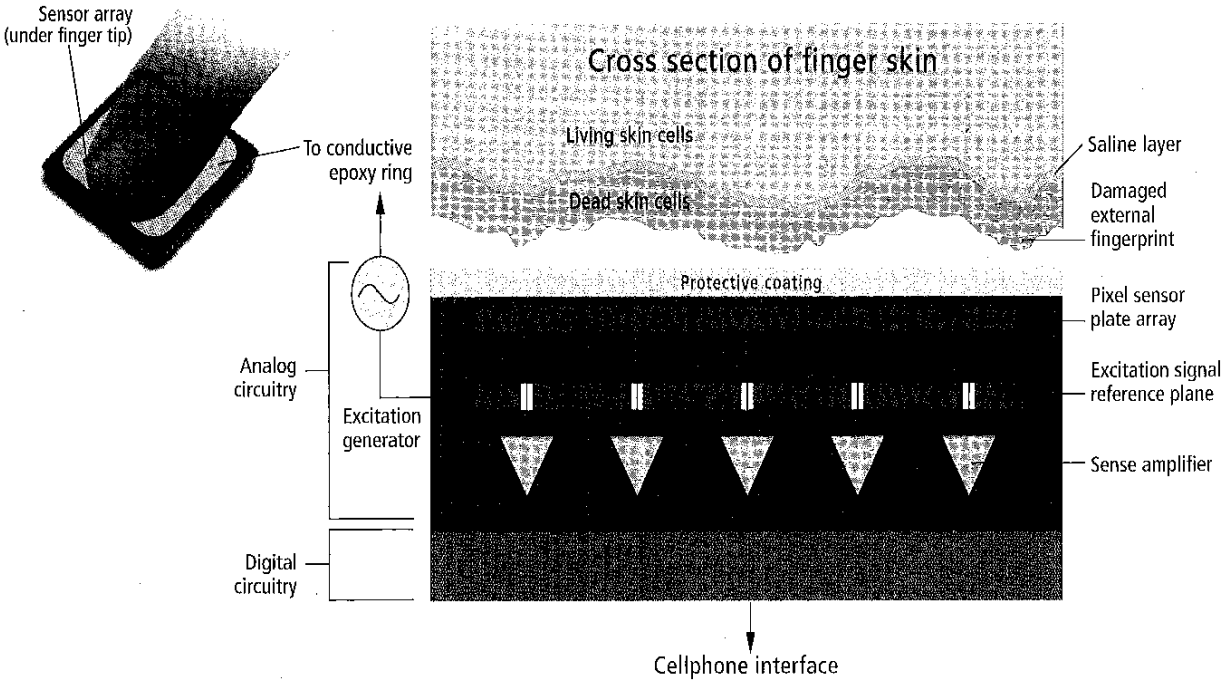
ETHEREAL SIGNATURES

The fight against cloning analog handsets has gone a lot better than efforts to combat eavesdropping. Conceived in innocence, early analog phones were almost comically vulnerable to security attacks. For one thing, the signaling between handset and base station takes place in the clear, so anyone with a suitable RF scanner can simply listen in and learn the phone numbers (called mobile identity numbers, or MINs) of handsets in the vicinity and the electronic serial numbers (ESNs) that go with them. To program those numbers into another handset is the work of a minute, and behold! another cloned phone is ready for use.

Once the problem manifested itself, service providers began taking steps to protect themselves. Working with the U.S. Secret Service, they persuaded Congress in 1998 to amend the law pertaining to "Fraud and related activity in connection with access devices" (Title 18, Section 1029, of the U.S. Code), so as to make it a Federal crime to own a scanning receiver or a cell phone programmer with intent to defraud. That same law also makes it a crime knowingly, and with intent to defraud, to use a counterfeit phone, to traffic in such phones, or to possess 15 or more of them. The law is serious, specifying maximum prison terms of 10 or 15 years (for first-time offenders), depending on the exact nature of the crime.

The service providers also instituted the use of personal identification numbers (PINs) that a user had to key in before a call could be completed. PINs certainly made it tougher for thieves to use stolen phones. But since the PINs were transmitted in the clear, they were not very effective against cloning.

What did help was a technology pioneered by the military for keeping track of enemy troop movements, namely, RF fingerprinting. Corsair Communications Inc., Palo Alto, Calif., is currently the only company active in the field. As explained by John Martin, its senior director of product management, the technology involves measuring several (unspecified) parameters associated with RF signals and characterizing them (again, in a proprietary manner) to produce a signature unique to the transmitter being studied. Even nominally iden-



How a phone can check fingerprints

As everyone knows, the time-tested way to verify a person's identity is through his or her fingerprints. For the present application, the question is can it be done quickly, without expert assistance, when the person is out in the field somewhere using a cell phone?

The answer, according to the people at AuthenTec Inc., Melbourne, Fla., is yes. All it takes is the company's FingerLoc fingerprint sensor, its accompanying software, and a microprocessor on which the software can run.

Finding a microprocessor is no problem, according to Peter Sherlock, vice president for product development, who has overall responsibility for AuthenTec's engineering operations. Modern digital handsets, he points out, contain quite powerful processors that have nothing to do when a cell call is not in progress.

The FingerLoc sensor [see drawing] is a monolithic silicon chip comprising a sensing array and its associated circuitry, all covered by a fairly thick (75 μm) proprietary coating. It can be easily embedded in the surface of a cell phone, where the robust coating will protect it from the rigors of normal usage.

FingerLoc's key advantage over other (optical) fingerprint sensors, Sherlock said, is that it ignores the external fingerprint, which is often dirty or damaged or has even disappeared. Instead, it senses the fingerprint in a buried layer of living cells, where fingerprints are created, and where they are found in pristine condition.

What it does is apply a low-voltage ac signal to the fingertip and then measure how the resulting electric field varies in amplitude over the fingertip surface. The signal is applied by means of a conductive epoxy ring surrounding the sensor area [see photo]; it is defined and measured with respect to a reference plane within the chip [see drawing, again].

The electric field is set up between the reference plane and a thin layer of highly conductive saline liquid that resides at the interface of the living skin tissue and the dead skin. The saline layer has the same shape as the living tissue—the shape of the fingerprint. Being highly conductive, it imposes its shape as a boundary condition on the field, thereby spatially modulating the field into an analog of the fingerprint.

An array of tiny antennas arranged in a square matrix of 96 rows and columns does the actual sensing. Located above the reference plane, the array measures about 6.5 mm on a side, giving the sensor a linear resolution of about 15 pixels per millimeter.

The sensed analog electric field values are scanned from the sensor matrix a row at a time, digitized, and sent from the FingerLoc chip to the cell phone's microprocessor for further processing.

In the cell phone, a module from AuthenTec's software suite analyzes the fingerprint pattern and extracts information from it, which it converts into a unique representation of the fingerprint's owner. To "enroll" a user, that representation, called a template, is stored in nonvolatile memory for future use. To authenticate a user, it is compared with all of the stored templates to determine his or her identity.

What happens next depends on how the cell phone manufacturer and service provider have set things up. If the handset does not recognize the applicant, service will probably be denied. It gets more interesting when the system does recognize the fingerprint, because each user can have a stored profile, which personalizes the phone for him or her.

For example, a child may have the phone set so that it can do nothing but call home, no matter which button it presses. Older users may have their personal phone books automatically loaded, and certain calling privileges activated or blocked. And, of course, with the right standards in place, the sensor can be part of a verification and authentication system for electronic commerce. —*M.J.R.*

tical transmitters, manufactured on the same assembly line to the same specifications, have slight differences, which are sufficient for PhonePrint (as Corsair named its product) to tell them apart.

PhonePrint is a combination of hardware and software that cellular operators install in base stations in high-fraud areas. Once installed, it characterizes all the handsets that ask it for service (by monitoring the reverse control channel) and creates a database of their RF signatures, or fingerprints. The database soon acquires entries for almost all of the active users in the area. On subsequent service requests, PhonePrint compares the stored signature with the live one. If they fail to match, the call is torn down—that is, broken before it can be completed.

PhonePrint had its origins at TRW Inc., from which Corsair spun off in 1994. The Cleveland, Ohio, company developed similar systems for military use. Such systems can tell that an enemy unit supposedly stationed at position X has in fact moved to position Y by recognizing the RF signatures associated with the unit's radios. Obviously, as this feat implies, RF fingerprinting will work with any phone, and indeed, with any transmitter. It is therefore particularly suitable for legacy analog cell phones, which have no built-in fraud-fighting provisions.

How effective is it against cloning fraud? According to Martin, Corsair to date has torn down over 300 million calls.

AUTHENTICATION SECRETS

With the advent of digital and more advanced analog phones, an even more effective fraud-fighting technology came into use—authentication. A sort of handshaking process, authentication makes use of secret numbers that are stored in the phone and known to the network, but never passed over the air. Every time a call is made, the network sends the handset a random number, which the handset then combines with its secret number using an algorithm designed for the task. The result is another random number that the handset sends back to the network, which has meanwhile performed the same calculations. If the numbers match, the call is completed; if not, it is not.

The algorithm is designed to avalanche very quickly. If the input numbers are off by even a single bit, the resulting number will not even be close to the right answer. Since cell phones not for economic reasons, but rather in the pursuit of anonymity. Mary Riley, a special agent with the Secret Service, told *IEEE Spectrum* that 80 percent of narcotics dealers arrested in 1998 were found to be in possession of cloned phones, according to testimony from the Drug Enforcement Administration, Arlington, Va.

Call counting is another technique that can be used instead of—more often, in addition to—authentication. Like authentication, it requires a phone capable of performing its part of the process. With call counting, both the handset and the network track the number of calls made by the handset. Those numbers are compared whenever a call is made. If they do not match or if they disagree by more than a specified amount (generally one call), then the call is not allowed. Obviously, if someone has cloned a phone, then both he and the legitimate users will be making calls, so the network will have their combined number, while each handset will have only its own.

RF fingerprinting and authentication between them have proven extremely effective. According to Rick Kemper, CTIA director for wireless technology and security, cloning fraud has dropped about 95 percent over the past four to five years. It has been replaced, however, by another kind of fraud called identity theft, also known as subscription fraud.

WHO ARE YOU?

Criminals, like electrons, tend to take the path of least resistance. Make it really hard to steal what they want one way, and they find a different way to get it. In the case of cell phones—or, more accurately, cell phone service—the defenses in place against cloning have motivated criminals to adopt the various techniques used by credit card thieves, which are all lumped together under the rubric of subscriber fraud.

As with cloning, the industry's first defensive move was to persuade Congress to strengthen the relevant statute (in this case Title 18, Section 1028 of the U.S. Code, "Fraud and related activity in connection with identification documents and information"). As the law now stands, it is a Federal crime merely to steal someone's identity information with intent to defraud. Previously, the Government had to wait till fraud was committed before it could act.

The industry became particularly sus- fraud losses at a tolerable level. They are going to have to verify addresses against credit card data bases, for example. But, as Steven Lum, director of fraud detection at AT&T Wireless Services Inc., Paramus, N.J., pointed out, there are legitimate reasons for discrepancies, since people may have just moved or they may maintain multiple residences. So methods must be developed for screening out bad risks without turning off legitimate customers.

Technology as such is of limited value in this area. One thing computers are being used to do is keep track of subscriber calling patterns—the numbers they tend to call or receive calls from. If a subscriber is terminated for nonpayment of bills, and if a "new" subscriber shows up with pretty much the same calling pattern, then an alarm can be raised calling attention to the possibility that this may be the same person, and the company can look more closely at him.

SUBSIDY LOSS

According to Ericsson's Tom Deitrich, a major problem, especially in Latin America, is what he calls phones moving sideways through the distribution channels. Cellular handsets are often heavily subsidized by service providers, who supply them to subscribers on condition that the subscribers remain with the company for a specific period, typically a year. But what sometimes happens is that the phones wind up being activated on some other carrier's network.

A distributor, for example, who has purchased a batch of subsidized handsets at a low price from one carrier may find that he can sell them at a handsome profit to a dealer who is not affiliated with that carrier. In Latin America, that dealer may not even be in the same country as the distributor. The result, the carrier loses the money it invested in subsidizing the phone.

As with subscriber fraud, the remedy is mostly a matter of running a tighter ship. But, Deitrich expects some sort of technological fix will also be developed, which he described as an authentication kind of approach for the activation process. He foresees it showing up in some second-generation phones, and believes it will be part of any third-generation deployment. ◆

TO PROBE FURTHER

For some statistical highlights on cellular phone fraud, see the Web page maintained