CHAPTER

17

Telecom System Security

I rarely had to resort to a technical attack. Companies can spend millions of dollars toward technological protections and that's wasted if somebody can basically call someone on the telephone and either convince them to do something on the computer that lowers the computer's defenses or reveals the information they were seeking.

—KEVIN MITNICK

17.1 Introduction

The protection of telecommunications systems is an important case study for a number of reasons. First, many distributed systems rely on the underlying fixed or mobile phone network in ways that are often not obvious. Second, the history of security failures in telecoms is instructive. Early attacks were carried out on phone companies by enthusiasts ("phone phreaks") to get free calls; next the phone system's vulnerabilities began to be exploited by crooks to evade police wiretapping; then premium rate calls were introduced, which created the motive for large-scale fraud; then, when telecoms markets were liberalized, some phone companies started conducting attacks on each other's customers, and some phone companies have even attacked each other. At each stage, the defensive measures undertaken were not only very expensive but also tended to be inadequate for various reasons. It appears that the same pattern is repeating with the Internet—only that history will be much speeded up.

17.2 Phone Phreaking

The abuse of communication services goes back centuries. In the days before postage stamps were invented, postage was paid by the recipient. Unsolicited mail became a

huge problem (especially for famous people), so recipients were allowed to inspect a letter and reject it if they wished rather than paying for it. People soon worked out schemes to send short messages on the covers of letters which their correspondents rejected, and the regulations brought in to stop this were never really effective [594]. The early optical telegraphs, which worked using semaphores or heliographs, were abused by people to place foreknowledge bets on races; here, too, attempts to legislate the problem away were a failure [729].

The telephone was to be no different.

17.2.1 Attacks on Metering

Early metering systems were wide open to abuse.

- In the 1950's, the operator in some systems had to listen for the sound of coins dropping on a metal plate to tell that a callbox customer had paid, so some people acquired the knack of hitting the coinbox with a piece of metal that struck the right note.
- Initially, the operator had no way of knowing which phone a call had come from, so she had to ask the caller his number. The caller could give the number of someone else, who would be charged. This was risky to do from your own phone, but people did it from callboxes. When operators started calling back to verify the number for international calls, people worked out social engineering attacks ("This is IBM here; we'd like to book a call to San Francisco, and because of the time difference, we'd like our managing director take it at home tonight. His number is xxx-yyyy"). Therefore, callbox lines had a feature added to alert the operator. But in the U.K. implementation, there was a bug: a customer who had called the operator from a callbox could depress the rest for a quarter-second or so, whereupon he'd be disconnected and reconnected (often to a different operator), with no signal this time that the call was from a callbox. He could then place a call to anywhere and bill it to any local number.
- This system also signalled the entry of a coin by one or more pulses, each of which consisted of the insertion of a resistance in the line followed by a brief open circuit. At a number of colleges, enterprising students installed "magic buttons" that could simulate this in a callbox in the student union so people could phone for free. (The bill in this case went to the student union, for which the magic button was not quite so amusing.)

Attacks on metering mechanisms continue. Many countries have changed their payphones to use chip cards in order to cut the costs of coin collection and vandalism. Some of the implementations have been poor (as I remarked in the chapter on tamper resistance) and villains have manufactured large quantities of bogus phone cards. Other attacks involve what's called *clip-on:* physically attaching a phone to someone else's line to steal their service.

In the 1970s, when international phone calls were very expensive, foreign students would clip their own phone on to a residential line in order to call home; an unsuspecting home owner could get a huge bill. Despite the fact that, in most countries, the cable was the phone company's legal responsibility up to the service socket in the

house, phone companies were mostly adamant that householders should pay, and could threaten to blacklist them if they didn't. Now that long distance calls are cheap, the financial incentive for clip-on fraud has largely disappeared. But it's still enough of a problem that the Norwegian phone company designed a system whereby a challenge and response are exchanged between a wall-socket-mounted authentication device and the exchange software before a dial tone is given [426].

Clip-on fraud had a catastrophic effect on a family in Cramlington, a town in the Northeast of England. The first sign they had of trouble was hearing a conversation on their line. The next was a visit from the police, who said there'd been complaints of nuisance phone calls. The complainants were three ladies, all of whom had a number that was one digit different from a number to which this family had supposedly made a huge number of calls. When the family's bill was examined, there were also calls to clusters of numbers that turned out to be payphones; these had started quite suddenly at the same time as the nuisance calls. Later, when the family had complained to the phone company about a fault, their connection was rerouted and this had solved the problem.

The phone company denied the possibility of a tap, despite the report from its maintenance person, who noted that the family's line had been tampered with at the distribution box. (The phone company later claimed this report was in error.) It turned out that a drug dealer had lived close by, and it seemed a reasonable inference that he had tapped their line in order to call his couriers at the payphones using the victim's calling line ID. But both the police and the local phone company refused to go into the house where the dealer had lived, claiming it was too dangerous—even though the dealer had by now got six years in jail. The Norwegian phone company declined an invitation to testify about clip-on for the defense. The upshot was that the subscriber was convicted of making harrassing phone calls, in a case widely believed to have been a miscarriage of justice. Discussion continues about whether the closing of ranks between the phone company and the police was a policy of denying that clip-on was possible, a reflex to cover a surveillance operation—or something more sinister.

Stealing dial tone from cordless phones is another variant on the same theme. In the early 1990s, this became so widespread in Paris that France Telecom broke with phone company tradition and announced that it was happening, claiming that the victims were using illegally imported cordless phones that were easy to spoof [475]. Yet to this day I am unaware of any cordless phones—authorized or not—with decent air link authentication. The new digital cordless phones use the DECT standard, which allows for challenge-response mechanisms [769]; but the terminals fielded so far seem to simply send their names to the base station.

Social engineering is another widespread trick. A crook calls you pretending to be from AT&T security, and asks whether you made a large number of calls to Peru on your calling card. When you deny this, she says that the calls were obviously fake, but, in order to reverse the charges, can she confirm that your card number is 123–456–7890–6543? No, you say (if you're not really alert), it's 123–456–7890–5678. Because 123–456–7890 is your phone number, and 5678 your password, you've just given that caller the ability to bill calls to you.

The advent of premium rate phone services has also led to scamsters developing all sorts of tricks to get people to call them: pager messages, job ads, fake emergency messages about relatives, "low-cost" calling cards with 900-access numbers—you name it. The 809 area code for the Caribbean used to be a favorite cover for crooks

targeting U.S. subscribers; recently, the introduction of new area codes there, such as 345 for the Cayman Islands, makes it even harder to spot the numbers of premium rate operators. Phone companies' advice is "Do not return calls to unfamiliar telephone numbers" and "Beware of faxes, email, voice mail, and pages requesting a return call to an unfamiliar number" [13]. But just how practical is that?

17.2.2 Attacks on Signalling

The term phone phreaking refers to attacks on signalling, as well as to pure toll fraud. Until the 1980s, phone companies used signalling systems that worked *in-band* by sending tone pulses in the same circuit that carried the speech. The first attack I've heard of dates back to 1952; and by the mid-to-late 1960s, many enthusiasts in both America and Britain had worked out ways of rerouting calls. They typically used homemade tone generators, of which the most common were called *blue boxes*. The trick was to call an 800 number, then send a tone that would *clear down* the line at the far end—that is, disconnect the called party while leaving the caller with a trunk line connected to the exchange. The caller could now enter the number he really wanted and be connected without paying. Notoriously, Steve Jobs and Steve Wozniak first built blue boxes before they diversified into computers [319].

Phone phreaking started out with a strong ideological element. In those days, most phone companies had monopolies. They were large, faceless, and unresponsive. People whose domestic phone lines had been tapped in a service theft found they were stuck with the charges. If the young man who had courted your daughter was (unknown to you) a phone phreak who hadn't paid for the calls he made to her, you would suddenly find the company trying to extort either his name or a payment. Phone companies were also aligned with the state. In many countries, it turned out that there were signalling codes or switch features that would enable the police to tap your phone from the comfort of the police station, without having to send out a lineman to install a wiretap. Back in the days of Vietnam and student protests, this was inflammatory stuff. Phone phreaks were counterculture heroes, while phone companies aligned themselves firmly with the Forces of Darkness.

As there was no way to stop blue-box type attacks as long as telephone signalling was carried in-band, the phone companies spent years and many billions of dollars upgrading exchanges so that the signalling was carried out-of-band, in separate channels to which the subscribers had no easy access. Gradually, region by region, the world was closed off to blue-box attacks, though there are still a few places left. For example, the first time that USAF operations were disrupted by an information warfare attack by noncombatants was in 1994, when two British hackers broke into the Rome Air Force Base via an analog link through an ancient phone system in Argentina. This cut-out was used effectively to hold up investigators [722]. But to defeat a modern telephone network, different techniques are needed.

17.2.3 Attacks on Switching and Configuration

The second wave of attacks targeted the computers that did the switching. Typically, these were Unix machines on a LAN in an exchange, which also had machines with administrative functions such as maintenance scheduling. By hacking one of these less well-guarded machines, a phreak could go across the LAN and break into the switching

equipment—or into secondary systems such as subscriber databases. For a survey of PacBell's experience of this, see [167]; for Bellcore's, see [462].

Using these techniques, unlisted phone numbers could be found, calls could be forwarded without a subscriber's knowledge, and all sorts of mischief became possible. A Californian phone phreak called Kevin Poulsen got root access to many of PacBel's switches and other systems in 1985–1988; this apparently involved burglary as much as hacking (he was eventually convicted of conspiring to possess 15 or more counterfeit, unauthorized, and stolen access devices.) He did petty things like obtaining unlisted phone numbers for celebrities, and winning a Porsche from Los Angeles radio station KIIS-FM. (Each week, KIIS would give a Porsche to the 102nd caller, so Kevin and his accomplices blocked out all calls to the radio station's 25 phone lines save their own, made the 102nd call, and collected the Porsche.) Poulsen was also accused of unlawful wiretapping and espionage; these charges were dismissed. In fact, the FBI came down on him so heavily that there were allegations of an improper relationship between the agency and the phone companies, along the lines of "you scratch our backs with wiretaps when needed, and we'll investigate your hacker problems" [294].

Although the unauthorized wiretapping charges against Poulsen were dismissed, the FBI's sensitivity does highlight the possibility that attacks on phone company computers can be used by foreign intelligence agencies to conduct remote wiretaps. Some of the attacks mentioned in [167] were from overseas, and the possibility that such tricks might be used to crash the whole phone system in the context of an information warfare attack has for some years been a concern of the NSA [321, 480]. Also, prudent nations assume that their telephone switchgear has vulnerabilities known to the government of the country in which it was made.

But although high-tech attacks do happen—and newspaper articles on phone phreaking tend to play up the "evil hacker" aspects—most real attacks are much simpler. Many involve insiders, who deliberately misconfigure systems to provide free calls from (or through) favored numbers. This didn't matter all that much when the phone company's marginal cost of servicing an extra phone call was near zero, but with the modern proliferation of value-added services, people with access to the systems can be tempted to place (or forge) large numbers of calls to accomplices' sex lines. Deregulation, and the advent of mobile phones, have also made fraud serious, as they give rise to cash payments between phone companies [200]. Insiders also get up to mischief with services that depend on the security of the phone network. In a hack reminiscent of Poulsen, two staff at British Telecom were dismissed after they each won 10 tickets for Concorde from a phone-in offer at which only one randomly selected call in a thousand was supposed to get through [754].

As for outsiders, consider the "arch-hacker," Kevin Mitnick. He got extensive press coverage when he was arrested and convicted following a series of break-ins, many of which involved phone systems, and which made him the target of an FBI manhunt. But he testified after his release from prison that almost all of his exploits had involved social engineering. His congressional testimony, quoted at the head of this chapter, sums up the problem neatly [555]. Phone company systems are vulnerable to careless insiders as well as to malicious insiders—just like hospital systems and many others I've discussed.

17.2.4 Insecure End Systems

After direct attacks on the systems kept on phone company premises, the next major vulnerabilities of modern phone systems are insecure terminal equipment and feature interaction.

There have been a number of cases where villains exploited people's answering machines by tricking them into dialing premium rate numbers. The problem arises from phone company switches that give you dial tone 12 seconds after the other party hangs up. So I can record 13 blank seconds on your answering machine, followed by the tones of the number to which I'd like a message delivered, with the message; I then call again, get the machine to play back its messages and hang up on it. Recently, a similar trick has been done with computers—that three-hour call to a sex line in Sierra Leone that appears on your phone bill may well have been dialed by a virus on your PC.

But the really big frauds using insecure end systems are directed against companies. Fraud against corporate *private branch exchange* systems (PBXes) had become big business by the mid-1990s, and costs business billions of dollars a year [202]. PBXes are usually supplied with facilities for *refiling* calls, also known as *direct inward system access* (DISA). The typical application is that the company's sales force can call in to an 800-number, enter a PIN or password, then call out again, taking advantage of the low rates a large company can get for long distance calls. As you'd expect, these PINs become known and get traded by villains [564]. The result is known as *dial-through* fraud.

In many cases, the PINs are set to a default by the manufacturer, and never changed by the customer. In other cases, PINs are captured by crooks who monitor telephone traffic in hotels to steal credit card numbers; phone card numbers and PBX PINs are a useful sideline. Many PBX designs have fixed engineering passwords that allow remote maintenance access, and prudent people reckon that any PBX will have at least one back door installed by the manufacturer to give easy access to law enforcement and intelligence agencies (it's said, as a condition of export licensing). Of course such features get discovered and abused. In one case, the PBX at Scotland Yard was compromised, and used by villains to refile calls, costing the Yard a million pounds, for which they sued their telephone installer. The crooks were never caught [745]. This case was particularly poignant, as one of the criminals' motivations in such cases is to get access to communications that will not be tapped.

Dial-through fraud is mostly driven by premium rate services; the main culprits are crooks who are in cahoots with premium line owners. Secondary culprits are organized criminals who use the calling line ID of respectable companies to hide calls, such as from the United States to Colombia, or from England to Pakistan and China—often via a compromised PBX in a third country to mask the traffic. (This appears to be what happened in the Scotland Yard case, as the crooks made their calls out of America) Most companies don't understand the need to guard their dial tone, and wouldn't know how to even if they wanted to. PBXes are typically run by company telecoms managers who know little about security, while the security manager often knows little about phones.

Exploits of insecure end-systems sometimes affect domestic subscribers too, now that many people have computers attached to their phones. A notorious case was the Moldova scam. In 1997, customers of a porn site were told to download a "viewer" program, which dropped their phone line and connected them to a phone number in

Moldova (having turned off their modem speakers so they wouldn't notice). The new connection stayed up until they turned off their computers. The result was that thousands of subscribers incurred hundreds of thousands of dollars in international long distance charges at over $2 per minute. Their phone companies tried to collect this money, but there was an outcry; eventually, the subscribers got their money back and the Federal Trade Commission enjoined and prosecuted the perpetrators [284]. Since then, there have been a number of copycat scams; most recently, AT&T has been getting complaints about calls to Chad, routed there by a Web company that appears to be in Ireland [543]

Premium rate scams and anonymous calling are not the only motives. As phones start to be used for tasks such as voting, securing entry into apartment buildings, checking that offenders are observing their parole terms, and authenticating financial transactions, more motives are created for evermore creative kinds of mischief, especially for hacks that defeat caller line ID. One of the more extreme cases occurred in London. A crook turned up to buy gold bullion with a bank check; the bullion dealer phoned the bank to verify it; and having got assurances from the voice at the other end, he handed over the gold. The check turned out to be forged; an accomplice had tapped the bank's phone line at the distribution box in the street.

Sometimes, attacks are conducted by upstanding citizens for perfectly honorable motives. A neat example, due to Udi Manber, is as follows. Suppose you have bought something that breaks, and the manufacturer's helpline has only an answering machine. To get service, you have to take the answering machine out of service. This can often be done by recording its message, and playing it back so that it appears as the customer message. With luck, the machine's owner will think it's broken and it'll be sent off for maintenance.

17.2.5 Feature Interaction

More and more cases of telephone manipulation involve feature interaction.

- Inmates at the Clallam Bay Correctional Center in Washington state, who were only allowed to make collect calls, found an interesting exploit of a system that the phone company (Fone America) introduced to handle collect calls automatically. The system would call the dialed number, after which a synthesized voice would say: "If you will accept a collect call from (name of caller), please press the number 3 on your telephone twice." Prisoners were supposed to state their name for the machine to record and insert. The system had, as an additional feature, the capability to have the greeting delivered in Spanish. Inmates did so; and when asked to identify themselves, said, "If you want to hear this message in English, press 33." This worked often enough that they could get through to corporate PBXes and talk the operator into giving them an outside line. The University of Washington was hit several times by this scam [298].
- In November 1996, British Telecom launched a feature called Ringback. If you dialed an engaged number, you could then enter a short code; as soon as the called number was free, both your phone and theirs would ring. The resulting call would be billed to you. However, when it was used from a payphone, it was the phone's owner who ended up with the bill, rather than the caller. People with private payphones, such as pub landlords and shopkeepers,

lost a lot of money, which the phone company was eventually obliged to refund [412].

- Call forwarding is a source of many scams. There have been cases in which hackers have persuaded a phone company operator to forward calls for someone they didn't like to a sex line. The victim then gets billed for the premium rate charges.
- Conference calls also cause a lot of trouble. For example, football hooligans in some countries are placed under a curfew that requires them to be at home during a match, and to prove this by calling the probation service, which verifies their number using caller ID. The trick is to get one of your kids to set up a conference call with the probation service, and the mobile you've taken to the match. If the probation officer asks about the crowd noise, you tell him it's the TV and you can't turn it down or your mates will kill you. (And if he wants to call you back, you get your kids to forward the call.)

This brings us to the many problems caused by mobile phones.

17.3 Mobile Phones

Since the early 1980s, mobile phones have ceased to be an expensive luxury and have become one of the big technological success stories, with 30–50 percent annual sales growth worldwide. In some countries, notably Scandinavia, most people have at least one mobile, and many new electronic services are built on top of them. For example, there are machines that dispense a can of soda when you call a number displayed on the front; the drink gets added to your phone bill. Growth is particularly rapid in developing countries, where the wireline network is often dilapidated and people used to wait years for phone service to be installed.

Also, although most people use their mobiles sparingly because of the call charges (most phone calls by duration are made from and to wireline phones), criminals make heavy use of mobiles. In Britain, for example, over half of the police wiretaps are now on mobile numbers.

So mobile phones are very important to the security engineer, both as part of the underlying infrastructure and as a channel for service delivery. They can also teach us a lot about fraud techniques and countermeasures.

17.3.1 Mobile Phone Cloning

The first generation of mobile phones used analogue signals and no real authentication. The handset simply sent its serial numbers in clear over the air link. (In the U.S. system, there are two of them: one for the equipment, and one for the subscriber.) So villains built devices that would capture these numbers from calls in the neighborhood. (I've even seen a phone that was reprogrammed to do this by a simple software hack.) One of the main customers was the *call-sell operation*, which would steal phone service and resell it cheaply, often to immigrants or students who wanted to call home. The

call-sell operators would hang out at known pitches with cloned mobiles, and their customers would line up to phone home for a few dollars.

A black market developed in phone serial numbers, and enterprising engineers built *tumblers*—mobile phones that used a different identity for each call. Tumblers are designed to be hard for the police to track [406]. The demand for serial numbers got so large that satisfying it was increasingly difficult, even by snooping at places like airports where lots of mobiles were turned on. So as well as passive listening, active methods started to get used.

Modern mobile phones are cellular, in that the operator divides the service area up into cells, each covered by a base station. The mobile uses whichever base station has the strongest signal, and there are protocols for "handing off" calls from one cell to another as the customer roams. (For a survey of mobile phone technology, see [636].) The active attack consists of a fake base station, typically at a place with a lot of passing traffic such as a freeway bridge. As phones pass by, they hear a stronger base station signal and attempt to register by sending their serial numbers.

A number of mechanisms have been tried to cut the volume of fraud. Most operators have intrusion detection systems that watch out for suspicious patterns of activity, such as calls being made from New York and Los Angeles within an hour of each other, or a rapid increase in the volume of calls. A number of heuristics have been developed. For example, genuine mobiles that roam and that call home regularly, but then stop calling home, have usually been stolen.

In the chapter on electronic warfare, I mentioned RF fingerprinting, a formerly classified military technology in which signal characteristics that vary from one handset to another are used to identify individual devices and tie them to the claimed serial numbers [341]. Although this technique works—it was used by Vodafone in Britain to nearly eliminate cloning fraud from analogue mobiles—it is expensive, as it involves modifying the base stations. (Vodafone also used an intrusion detection system, which tracked customer call patterns and mobility, described in [769]; its competitor, Cellnet, simply blocked international calls from analogue mobiles—which helped move its high-value customers to its more modern digital network.) Another proposed solution was to adopt a cryptographic authentication protocol, but there are limits on how much can be done without changing the whole network. For example, one can use a challenge-response protocol to modify the serial number [305]. But many of the mechanisms people have proposed to fortify the security of analogue cellular phones have turned out to be weak [780].

Eventually, the industry decided that it made sense to redesign the entire system, not just to make it more secure but to support a host of new features such as the ability to roam from one country to another without requiring a new handset (important in Europe where lots of small countries are jammed close together), and the ability to send and receive short text messages.

17.3.2 GSM System Architecture

The second generation of mobile phones uses digital technology. By the year 2000, most handsets worldwide used the *Global System for Mobile Communications*, or GSM, which was designed from the start to facilitate international roaming, and launched in 1992. The United States, Japan, and Israel have different digital standards (although there is a competing GSM service in parts of America).

GSM's designers set out to secure the system against cloning and other attacks; the goal was that it should be at least as secure as the wireline system it was to replace. What they did, how they succeeded, and where they failed, make an interesting case history.

17.3.3 Communications Security Mechanisms

The authentication protocols used in GSM are described in a number of places, such as [141] (which also describes the mechanisms in an incompatible U.S. system). But the industry tried to keep secret the cryptographic and other protection mechanisms that form the core of the GSM security system. This didn't work; some eventually leaked, and the rest were discovered by reverse-engineering. I'll describe them briefly here; more can be found on sites such as [713].

Each network has two databases, a *home location register* (HLR), which contains the location of its own mobiles, and a *visitor location register* (VLR), for the location of mobiles that have roamed in from other networks. These databases enable incoming calls to be forwarded to the correct cell; see Figure 17.1 for an overview.

The handsets are commodity items. They are personalized using a *subscriber identity module* (SIM), a smartcard you get when you sign up for a network service, and which you load into your handset. The SIM can be thought of as containing three numbers:

1. There's a *personal identification number*, which you use to unlock the card. In theory, this stops stolen mobiles being used. In practice, many networks set an initial PIN of 0000, and most users never change it.
2. There's an *international mobile subscriber identification* (IMSI), a unique number that maps on to your mobile phone number.
3. Finally there is a *subscriber authentication key* K_i, a 128-bit number that serves to authenticate that IMSI and is known to your home network.

Unlike the banks, which used master keys to generate PINs, the phone companies decided that master keys were too dangerous. Instead of diversifying a master key, KM, to manufacture the authentication keys as $K_i = \{\text{IMSI}\}_{KM,}$ the keys are generated randomly and kept in an authentication database attached to the HLR.

The protocol used to authenticate the handset to the network runs as follows. On power-up, the SIM requests the customer's PIN; once this is entered correctly, it emits the IMSI, which the handset sends to the nearest base station. This is sent to the subscriber's HLR, which generates five *triplets*. Each triplet consists of:

- RAND, a random challenge
- SRES, a response
- K_c, a ciphering key

The relationship between these values is that RAND, encrypted under the SIM's authentication key K_i, gives an output that is SRES concatenated with K_c:

$$\{RAND\}_{Ki} = (SRES \mid K_c)$$

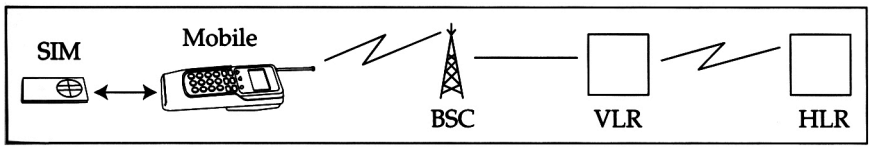

Figure 17.1 GSM authentication system components.

The standard way to do this encryption is using a one-way function called Comp128, or A3/A8 (A3 refers to the SRES output, and A8 to the K_c output). (This is a hash function with 40 rounds, described in detail in [138].) The basic idea is much like in Figure 5.10; each round consists of table look-ups followed by mixing. There are five tables, with 512,256,128,64, and 32 byte entries each, and the hash function uses them successively in each block of five rounds; there are eight of these blocks.

On the face of it, this looks like such a complex hash function that it should be impossible to find preimages of output hash values. Yet once its design finally leaked, a vulnerability was noticed. Four of the bytes—i, $i + 8$, $i + 16$, and $i + 24$, at the output of the second round depend only on the value of the same bytes of the input. Two of these input bytes (i and $i + 8$) are bytes of the key, and thus are fixed for any given SIM card, while the other two bytes of the input come from the challenge input.

This four-byte-to-four-byte channel is called a *narrow pipe*, and it's possible to probe it by varying the two input bytes that come from the challenge. Since the rounds are nonbijective, you can hope for a collision to occur after two rounds; and the birthday paradox guarantees that collisions will occur pretty rapidly (since the pipe is only four bytes wide). Once all the details have been worked out, it turns out that you need about 60,000 suitably chosen challenges to extract the key [781, 783]. The effect is that, given access to a SIM issued by a network that uses Comp128, the authentication key can be extracted in several hours using software that is now available on the Net. Almost all networks do use Comp128. So someone who rents a car with a mobile phone could clone its SIM overnight using his laptop and a suitable adaptor; and someone who sells you a GSM mobile phone might have made a "spare copy" of the authentication key, which he can use later to bill calls to your account.

This attack is yet another example of the dangers of using a secret cryptographic primitive that has been evaluated by only a small group of people. The cryptanalytic techniques necessary to find the flaw were well known [773], and it's likely that if Comp128 had been open to public scrutiny, the flaw would have been found.

Anyway, the triplets are sent to the base station, which now presents the first RAND to the mobile. It passes this to the SIM, which computes SRES. The mobile returns this to the base station; if it's correct, the mobile and the base station can now communicate using the ciphering key K_c. The whole authentication protocol looks like that shown in Figure 17.2.

There's a vulnerability in this protocol. In most countries, the communications between base stations and the VLR pass unencrypted on microwave links. (They tend to be preferred to the local wireline network because the local phone company is often a competitor, and, even if not, microwave makes installation simpler and quicker.) So an attacker could send out an IMSI of his choice, then intercept the triplet on the microwave link back to the local base station. A German mobile operator, which offered a reward of 100,000 Deutschmarks to anyone who could bill a call to a mobile number

whose SIM card was held in its lawyer's office, backed down when we asked for the IMSI [30].

SIM → HLR	IMSI
HLR → BSC	(RAND, SRES, K_c), ...
BSC → SIM	RAND
SIM → BSC	SRES
BSC → mobile	$\{\text{traffic}\}_{K_c}$

Figure 17.2 GSM authentication protocol.

Triples can also be replayed. An unscrupulous foreign network can get five triples while you are roaming on it, then keep on reusing them to allow you to phone as much as you want. This means that the network doesn't have to refer back to your network for further authorization (and even if they do, it doesn't protect you, as the visited network might not send in its bills for a week or more). So your home network can be prevented from shutting you off while you roam, and (depending on the terms of the contract between the phone companies) it may still be liable to pay the roamed network the money. This means that even if you thought you'd limited your liability by using a prepaid SIM, you might still end up with your network trying to collect money from you. This is why, to enable roaming with a prepaid SIM, you're normally asked for a credit card number. You can end up being billed for more than you expected.

I have no reliable report of any frauds being carried out by outsiders (that is, attackers other than phone company staff) using these techniques. When GSM was introduced, the villains simply switched their modus operandi to buying phones using stolen credit cards, using stolen identities, or bribing insiders [807]. Robbery is also getting big; in the London borough of Lewisham, theft of mobile phones accounts for 30–35% of street robberies, with 35% of victims being male and under 18 [501].

From about 1997, prepaid mobile phones were introduced, and many criminals promptly started using them. In most European countries, prepaids can be bought for well under $100, including enough airtime for three months' worth of moderate use. Prepaids have turned out to be very good not just for evading police wiretapping but for stalking, extortion, and other kinds of harrassment. Prepaid phones are also liable to all sorts of simple frauds. For example, if your identity isn't checked when you buy it, there's little risk to you if you recharge it, or enable roaming, with a stolen credit card number [214].

In addition to authentication, the GSM system is supposed to provide two additional kinds of protection: location security and call content confidentiality.

The location security mechanism is that once a mobile is registered to a network, it is issued with a *temporary mobile subscriber identification* (TMSI), which acts as its address as it roams through the network. The attack on this mechanism uses a device called an *IMSI-catcher*, which is sold to police forces [308]. The IMSI-catcher, which can be operated in a police car tailing a suspect, acts as a GSM base station. Because it is closer than the genuine article, its signal is stronger, so the mobile tries to register with it. The IMSI-catcher claims not to understand the TMSI, and so the handset helpfully sends it the cleartext IMSI. (This feature is needed if mobiles are to be able to roam from one network to another without the call being dropped, and to recover from failures at the VLR [769].) The police can now get a warrant to intercept the traffic to

that mobile or—if they're in a hurry—just do a middleperson attack, in which they pretend to be the network to the mobile and the mobile to the network.

The GSM system is supposed to provide call content confidentiality by encrypting the traffic between the handset and the base station once the authentication and registration are completed. The speech is digitized, compressed, and chopped into packets; each packet is encrypted by xor-ing it with a pseudorandom sequence generated from the ciphering key K_c and the packet number. The algorithm commonly used in Europe is A5.

A5, like Comp128, was originally secret; like Comp l28, it was leaked and attacks were found on it. The algorithm is shown in Figure 17.3. It has three linear feedback shift registers of lengths 19,22, and 23; their outputs are combined using exclusive-or to form the output keystream. The nonlinearity in this generator comes from a majority-clocking arrangement, whereby the middle bits c_i of the three shift registers are compared and the two or three shift registers whose middle bits agree are clocked.

The obvious attack on this arrangement is to guess the two shorter registers, then work out the value of the third. As there are 41 bits to guess, one might think that about 2^{40} computations would be needed on average. But it's slightly more complex than this, as the generator loses state; many states have more than one possible precursor, so more guesses are needed. That said, Alex Biryukov and Adi Shamir found that by putting together a number of suitable optimizations, A5 could be broken without an unreasonable amount of effort. Their basic idea was to compute a large file of special points to which the state of the algorithm converges, then look for a match with the observed traffic. Given this precomputed file, the attack could use several seconds of traffic and several minutes' work on a PC, or several minutes of traffic and several seconds' work [104].

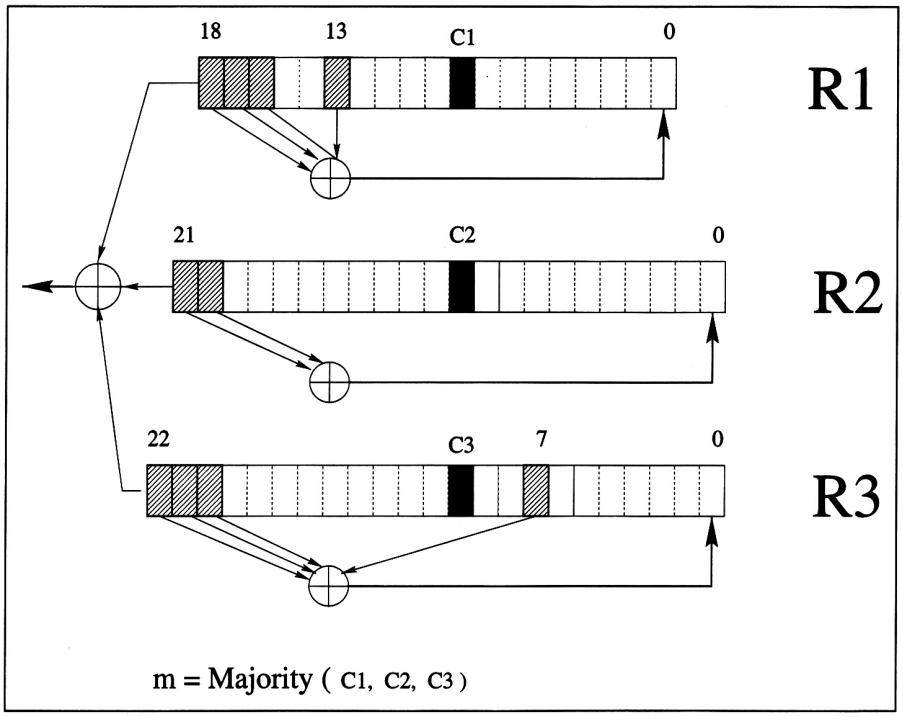

Figure 17.3 A5 (courtesy of Alex Biryukov and Adi Shamir).

Reverse-engineering actual systems also showed that the keying of A5 was deliberately weakened. Although, in theory, A5 has a 64-bit key (the initial loads for the shift registers) the actual implementations set the ten least significant key bits to zero. What's more, phones sold to phone companies in many countries have a further weakened version of A5, called A5/2. (There was a political row in Australia when it was realized that A5/2 was being used there.)

The conspiracy theorists had a field day with all this—security mechanisms being deliberately weakened at the behest of intelligence agencies to make mobile phones easy to tap. The truth is, as always, more subtle.

Intelligence agencies gain access to cleartext from their own countries' networks and from countries where an outstation (such as in an embassy) can intercept a suitable microwave link. Even in the home country, interception can occur with or without the cooperation of the phone company; equipment to grab traffic from the microwave links is fairly widely available. But in most countries, police are getting laws passed that give them direct access to phone company systems, as this gives them even more—such as location register data which enables them to track the past movements of suspects. There was a storm in Switzerland in 1997 when the press found that the phone company was giving location data to the police [618]. In the United States, the FCC ordered mobile phone companies to be able to locate people "so that 911 calls could be dispatched to the right place." This was imposed on every user of mobile phone service, rather than letting users decide whether to buy mobile location services or not. U.S. privacy activists are currently in litigation with the FCC over this.

Undoubtedly, there has been agency interference in the design of GSM, but the benefits from having weak authentication and confidentiality mechanisms appear limited to tactical sigint situations. Consider the case mentioned in the chapter on electronic warfare, where the New Zealand navy sent a frigate to monitor a coup in Fiji. Even if the Fijian phone company had been allowed to use A5 rather than A5/2, this would not have frustrated the mission, because signals intelligence officers could snatch the triplets off the microwave links, hack the location register, or whatever. If all else failed, a key could be found by brute force. But being able to break the traffic quickly is convenient— especially when you are dispatched on a peacekeeping mission in a country to which your intelligence people have never paid enough attention to emplace a hack (or a human asset) in the local phone company.

The net effect is that the initial GSM security mechanisms provided slightly better protection than the wireline network in countries allowed to use A5, and slightly worse protection elsewhere. The vulnerabilities in the communications security mechanisms neither expose subscribers in developed countries to much additional wiretapping, nor prevent the frauds that cause them the most grief.

17.3.4 The Next Generation: 3gpp

The third generation of digital mobile phones was initially known as the *Universal Mobile Telecommunications System* (UMTS) but now as the *Third-Generation Partnership Project* (3gpp). The security is much the same as GSM, but upgraded to deal with a number of GSM's known vulnerabilities. The system is supposed to enter service in 2003–2004; some of the design details are still being worked on, so this section is necessarily somewhat tentative. However, the overall security strategy is described in [786], and the current draft of the security architecture is at [775].

The crypto algorithms A5 and Comp l28 are replaced by a block cipher called Kasumi [442]. This is public and is based on a design by Mitsuru Matsui, called Misty, which has withstood public scrutiny for some years [527]. All keys are now 128 bits. Cryptography will be used to protect the integrity and confidentiality of both message content and signalling data, rather than just content confidentiality—although in the first phase of 3gpp the protection will not be end-to-end. The practice of transferring triples in the clear between base stations will cease, as will the vulnerability to rogue base stations; so IMSI-catchers will not work against third-generation mobiles. Instead, there will be a properly engineered interface for lawful interception [776]. Originally, this was supposed to supply plaintext only; now, the provision of key material will also be available as a national option.

In the basic 3gpp protocol, the authentication is pushed back from the base station controller to the visitor location register. The home location register is now known as the *home environment* (HE), and the SIM as the *UMTS SIM* (USIM). The home environment chooses a random challenge *RAND* as before, and enciphers it with the USIM authentication key *K* to generate a response *RES*, a confidentiality key *CK*, an integrity key *IK*, and an anonymity key *AK*.

$$\{RAND\}_K = (RES \mid CK \mid IK \mid AK)$$

There is also a sequence number *SEQ* known to the HE and the USIM. A MAC is computed on *RAND* and *SEQ*, then the sequence number is masked by exclusive-or'ing it with the anonymity key. The challenge, the expected response, the confidentiality key, the integrity key, and the masked sequence number are made up into an *authentication vector AV*, which is sent from the HE to the VLR. The VLR then sends the USIM the challenge, the masked sequence number, and the MAC; the USIM computes the response and the keys, unmasks the sequence number, verifies the MAC, and, if it's correct, returns the response to the VLR (see Figure 17.4).

3gpp has many other features, including details of sequence number generation, identity and location privacy mechanisms, backward compatability with GSM, mechanisms for public key encryption of authentication vectors in transit from HEs to VLRs, and negotiation of various optional cryptographic mechanisms. Many of these still were not defined at the time of writing.

USIM → HE	IMSI (this can optionally be encrypted)
HE → VLR	RAND, XRES, CK, IK, $SEQ \oplus AK$, MAC
VLR → USIM	RAND, $SEQ \oplus AK$, MAC
USIM → VLR	RES

Figure 17.4 The 3gpp authentication protocol.

In first phase of 3gpp, confidentiality will be, in effect, a higher-quality implementation of what's already available in GSM: eavesdropping on the air link will be prevented as before, and the currently possible attacks on the backbone network, or by bogus base stations, will be excluded. Police wiretaps will still be possible at the VLR.

In the second phase, 3gpp is proposed to have end-to-end encryption, so that the call content and some of the associated signalling will be protected from one handset to another. This has led to government demands for the use of a *key escrow protocol*—a protocol that would make keys available to police and intelligence services on demand. The catch is that, if a mobile phone call takes place from a British phone company's subscriber using a U.S. handset, roaming in France, to a German company's subscriber roaming in Switzerland using a Finnish handset, and the call goes via a long-distance service based in Canada and using Swedish exchange equipment, then which of these countries' intelligence agencies will have access to the keys? (Traditionally, most of them would have had access to the call content one way or another.)The solution favored by the agencies in Britain and France (at least) is the so-called Royal Holloway protocol [418], designed largely by Vodafone. It gives access to the countries where the subscribers are based (in this case, Britain and Germany). This is achieved by using a variant of Diffie-Hellman key exchange, in which the users' private keys are obtained by encrypting their names under a super-secret master key known to the local phone company and/or intelligence agency. Although this protocol has been adopted in the British civil service and the French health service, it is at odds with the phone company security philosophy that master keys are a bad thing. Quite apart from this, and from the unease which many people feel with built-in eavesdropping facilities, the protocol is clunky and inefficient [50]. There is also tension with local law enforcement requirements: in the above example, the police forces of the two countries in which the targets are roaming (France and Switzerland) will also want access to the traffic [776]. The debate continues; one possible resolution is *tromboning*, an established wiretap technique in which traffic is routed from the switch to the monitoring service and back, before going on its way. However, internetwork tromboning can introduce noticeable delays that could alert the target of investigation.

Consequently, 3gpp won't provide a revolution in confidentiality. As with GSM, its design goal is that security should be comparable with that of the wired network [390]. This looks like being doable.

The security of the billing mechanisms is a thornier issue. The GSM billing mechanism is inadequate for 3gpp, for a number of reasons:

- *A call detail record* (CDR) is generated only after the calling phone goes on-hook. This is an established feature of wireline networks, but when the environment changed to mobile, it became a serious problem. The attack is that someone running a call-sell operation sets up a long conference call using a mobile that was stolen, or a prepaid for which roaming was enabled using a stolen credit card (as discussed in Section 17.3.3). His clients join and leave this call one after the other, and the advice-of-charge facility lets him know how much to bill them. The phone stays off-hook continuously for several days. As soon as it goes on-hook, a CDR for several thousand dollars is generated, and the alarm goes off. So he throws the phone in the river and starts using the next one. By 1996, this had become so serious that Vodafone introduced a six-hour limit on all mobile calls.

- However, it won't be acceptable to just drop all 3gpp calls after six hours. Many users are expected to have always-on internet connections (such as from their laptops) with relatively light packet traffic most of the time.
- The phone companies also want to be able to charge for relatively high-value product and service delivery, ranging from the current premium services through services based on location ("give me a map showing me how to drive to the nearest McDonald's") to multimedia services.[1] Customers will be charged not just by the phone company but by other service providers; in addition to call duration and data volume, they will be billed according to the quality of service they receive, such as the effective bandwidth.
- Finally, the European Commission intends to require that all 3gpp operators retain location information on mobile phones for at least a year, for law enforcement purposes. Having a location history in the subscriber billing records may be the cheapest way to do this.

It is clear that the existing GSM mechanisms are inadequate—even adding such features as real-time international settlement would be extremely expensive. A redesign is needed. The proposed solution is to redesign the CDR to contain the required data quantity, location and quality-of-service information, and to build an online cost-control mechanism to limit the charges incurred for each user [558]. The cost-control mechanisms are not being standardized, but can involve forwarding charging data from either the local network or the gateway to the home environment, which will be able to have the call terminated if the available credit is exhausted (as with a prepaid SIM card) or if the use appears to be fraudulent.

One proposed way of implementing this is to incorporate a micropayment mechanism [56]. The idea is that the phone will send regular *tick payments* to each of the networks or service providers that are due to be paid for the call. The tick payments can be thought of as electronic coins and are cryptographically protected against forgery.

At the start of the call, the handset will compute a number of phone ticks by repeated hashing: $t_1 = h(t_0)$, $t_2 = h(t_1)$, and so on, with t_k (for some credit limit k, typically 2^{10} units) being signed by the phone company. The phone will then release ticks regularly in order to pay for the services as the call progresses. It will start by releasing t_k, then t_{k-1}, then t_{k-2}, and so on. If a charge is subsequently disputed—whether by a subscriber or a network operator—the party claiming an amount of, say, j ticks must exhibit the ticks t_{k-j} and t_k, the latter with a certificate. As the hash function h is one-way, this should be hard to do unless the handset actually released that many ticks. The tick t_{k-j} can now be checked by applying the hash function to it j times and verifying that the result is t_k. (This protocol is an example of multiple simultaneous discovery, having

[1] Presumably, given that many new communications services are used first for porn, this will mean live strip shows to order on the screen of your mobile, beamed to you from a country with relaxed indecency laws. So more prudish governments will demand ways to get round the 3gpp privacy mechanisms so they can censor content—just as the music industry will want ways to prevent user-to-user copying. We'll discuss this more in Chapter 20.

been invented by our group at Cambridge, by Pedersen, and by Rivest and Shamir, independently in 1995 [26, 605, 648].)

One advantage of using a tick payment mechanism is that, as well as protecting the phone companies from conference call frauds, it could protect the subscriber from many more. Phone users will at least in principle be able to spot the kind of 900 numbers that charge $24 per call or that masquerade as ordinary numbers or both.

17.3.5 GSM Security: A Success or Failure?

Whether GSM security was a success or a failure depends on whom you ask.

From the point of view of cryptography, it was a failure. Both the Comp 128 hash function and the A5 encryption algorithm were broken once they became public. In fact, GSM is often cited as an object lesson in Kerckhoff's Principle—that cryptographic security should reside in the choice of the key, rather than in the obscurity of the mechanism. The mechanism will leak sooner or later, and it's better to subject it to public review before, rather than after, a hundred million units have been manufactured. (GSM security wasn't a disaster for most cryptographers, of course, as it provided plenty of opportunities to write research papers.)

From the phone companies' point of view, GSM was a success. The shareholders of GSM operators, such as Vodafone, have made vast amounts of money, and a (small) part of this is due to the challenge-response mechanism in GSM stopping cloning. The crypto weaknesses were irrelevant, as they were never exploited (at least not in ways that did significant harm to call revenue). One or two frauds persist, such as the long conference call trick; but, on balance, the GSM design has been good to the phone companies.

From the criminals' point of view, GSM was also fine. It did not stop them stealing phone service; their modus operandi merely changed, with the cost falling on credit card companies or on individual victims of identity theft or street robbery. It did not stop calls from anonymous phones; the rise of the prepaid phone industry made them even easier. (The phone companies were happy with both of these changes.) And, of course, GSM did nothing about dial-through fraud.

From the point of view of the large-country intelligence agencies, GSM was fine. They have access to local and international traffic in the clear anyway, and the weakened version of A5 facilitates tactical signint against developing countries. And the second wave of GSM equipment is bringing some juicy features, such as remote control of handsets by the operator [636]. If you can subvert (or masquerade as) the operator, then there seems to be nothing to stop you quietly turning on a target's mobile phone without his knowledge and listening to the conversation in the room.

From the point of view of the police and low-resource intelligence agencies, things are not quite so bright. The problem isn't the added technical complexity of GSM networks: court-ordered wiretaps can be left to the phone company (although finding the number to tap can be a hassle if the suspect is mobile). The problem is the introduction of prepaid mobile phones. This not only decreases the signal to noise ratio of traffic analysis algorithms and makes it harder to target wiretaps, but also encourages crimes such as extortion and stalking.

From the customer's point of view, GSM was originally sold as being completely secure. Was this accurate? The encryption of the air link certainly did stop casual eavesdropping, which was an occasional nuisance with analogue phones. (There had been some high-profile cases of celebrities being embarrassed, including one case in

Britain where Prince Charles was overheard talking to his mistress before his divorce, and one in the United States involving Newt Gingrich.) But almost all the phone tapping in the world is done by large intelligence agencies, to whom the encryption doesn't make much difference.

Things are even less positive for the subscriber when we look at billing. Cryptographic authentication of handsets can't stop the many frauds perpetrated by premium rate operators and phone companies. If anything it makes it harder to wriggle out of bogus charges, as the phone company can say in court that your smartcard and your PIN must have been used in the handset that made the call. The same will apply to 3gpp if micropayments aren't used. The one minor compensation is that GSM facilitated the spread of prepaid phones, which can limit the exposure.

So the security features designed into GSM don't help the subscriber much. They were designed to provide "security" from the phone company's point of view: they dump much of the toll fraud risk, while not interrupting the flow of premium rate business—whether genuine or fraudulent.

In the medium term, the one ray of comfort for the poor subscriber is that one real vulnerability in GSM—the long conference call—may drive the introduction of micropayment schemes, which may, as a side effect, make premium rate scams harder. I say "may" rather than "will," as it will be interesting to see whether the phone companies implement them properly. There is a business incentive to provide a user interface that enables subscribers to monitor their expenditure (so they can be blamed for frauds they don't spot), while discouraging most of them from actually monitoring it (so the phone companies continue to make hundreds of millions from their share of the premium rate scam revenue). We shall have to wait and see.

17.4 Corporate Fraud

The question of corporate fraud is particularly relevant, as one of the fastest growing scams in the United States is the unscrupulous phone company that bills lots of small sums to unwitting users. It collects phone numbers in various ways. (For example, if you call an 800 number, then your own number will be passed to the far end regardless of whether you tried to block caller line ID.) It then bills you a few dollars. Your own phone company passes on this charge, and you find there's no effective way to dispute it. Sometimes, the scam uses a legal loophole: if you call an 800 number in the United States, the company may say, "Can we call you right back?" If you agree, you're deemed to have accepted the charges, which are likely to be at a high premium rate. The same can happen if you respond to voice prompts as the call progresses. These practices are known as *cramming*.

Another problem is *slamming*—the unauthorized change of a subscriber's long distance telephone service provider without their consent. The slammers tell your local phone company that you have opted for their services; your phone company routes your long distance calls through their service; they hope you don't notice the change and dispute the bill; and the telephone charges can then be jacked up. Some local

phone companies, such as Bell Atlantic, allow their customers to freeze their chosen long distance carrier [13].

It would be a mistake to assume that cramming and slamming are done only by small fly-by-night operators. AT&T is one of the worst offenders, having been fined $300,000 not only for slamming, but for actually using forged signatures of subscribers to make it look as if they had agreed to switch to their service. They got caught when they forged a signature of the deceased spouse of a subscriber in Texas [252].

Another problem *is* the fly-by-night phone company. Anyone in the United States is legally entitled to set up a phone company; it is fairly straightforward to set one up, collect some cash from subscribers, then vanish once the invoices for interconnect fees come in from the established players. In Britain, there is a company that advertises sex lines with normal phone numbers to trap the unwary; it then sends them huge bills at their residential addresses and tries to intimidate them into paying. In a case currently before the courts, they justify this in terms of non-discrimination rules: if British Telecom can make huge charges for phone sex, why can't they?

It's not just the small operators that indulge in dubious business practices. An example that affects even some large phone companies is the short termination of international calls.

Although premium rate numbers are used for a number of more or less legitimate purposes, such as software support, many of them exploit minors or people with compulsive behavior disorders. So regulators have forced phone companies in many countries to offer premium rate number blocking to subscribers. Phone companies get around this by disguising premium rate numbers as international ones. I mentioned the scams with Caribbean numbers in Section 17.2.1. Now, many other phone companies from small countries with lax regulators have got into the act, offering sex line operators a range of numbers on which they share the revenue.

Often, a call made to a small-country phone company doesn't go anywhere near its ostensible destination. One of the hacks used to do this is called *short termination*, and works as follows. Normally, calls for the small Pacific country of Tuvalu go via Telstra in Perth, Australia, where they are forwarded by satellite. However, the sex line numbers are marked as invalid in Telstra's system, so they are automatically sent via the second-choice operator—a company in New Zealand. (The girls—or to be more precise, the elderly retired hookers who pretend to be young girls—are actually in Manchester, England.) Technically, this is an interesting case of a fallback mechanism being used as an attack vehicle. Legally, it is hard to challenge, as there is an international agreement (the Nairobi Convention) that prevents phone companies selectively blocking international destinations. Thus, if you want to stop your kids phoning the sex line in Tuvalu, you have to block all international calls, which makes it harder for you to phone that important client in Germany.

Problems like these are ultimately regulatory failures, and they are increasingly common. (For example, in the Moldova scam mentioned above, the calls didn't go to Moldova but to Canada [151].) These problems may well get worse as technology makes many new, complex services possible and the regulators fail to keep up.

Even the phone companies themselves sometimes fall foul of the growing complexity. There are two cases before the courts as I write this, in which phone companies are chasing people who noticed that calling an international premium number at their best discount rate actually cost less than the amount they could get paid by operating the premium service. The profits they're alleged to have made have two commas rather

than the usual one. The phone companies claim this was fraud; the defendants that it was honest arbitrage. We shall have to wait and see what the juries think.

17.5 Summary

Phone fraud is a fascinating case study. People have been cheating phone companies for decades, and recently the phone companies have been vigorously returning the compliment. To start off with, systems were not really protected at all, and it was easy to evade charges and redirect calls. The mechanism adopted to prevent this—out-of-band signalling—has proved inadequate as the rapidly growing complexity of the system opened up many more vulnerabilities. These range from social engineering attacks on users through poor design and management of terminal equipment such as PBXes to the exploitation of various hard-to-predict feature interactions.

Overall, the security problems in telecoms have been the result of environmental changes. These have included deregulation, which brought in many new phone companies. However, the main change has been the introduction of premium rate numbers. While previously phone companies sold a service with a negligible marginal cost of provision, suddenly real money was involved; and while previously about the only serious benefit to be had from manipulating the system was calls that were hard for the police to tap, suddenly serious money could be earned. The existing protection mechanisms were unable to cope with this evolution.

The growing complexity nullified even the fairly serious effort made to secure the GSM digital mobile system. Their engineers concentrated on communications security threats rather than computer security threats; they also concentrated on the phone companies' interests at the expense of the customers'. The next-generation mobile service, 3gpp, looks capable of doing slightly better; but we shall have to wait and see how it gets implemented in practice.

Research Problems

Relatively little research has been done outside phone company and intelligence agency labs on issues related specifically to phone fraud and wiretapping. However, there is growing interest in protocols and other mechanisms for use with novel telecommunications services. The recently published 3gpp protocol suite is sufficiently large and complex that it may take some time for the formal methods and security protocol people to analyze fully. Next-generation value-added services are bound to introduce new vulnerabilities. The interaction between all these communications and security protocols, and the mechanisms used for distributed systems security, is fertile ground for both interesting research and horrendously expensive engineering errors: there are already regular workshops on how to use system engineering techniques to manage feature interactions in telecommunications.

Further Reading

There are a lot of scattered articles about phone fraud, but nothing I know of which brings everything together. A useful site for the fraud techniques currently being used in the United States is the Alliance to Outfox Phone Fraud, an industry consortium [13]. The underlying technologies are described in a number of reference books, such as [636] on GSM, and more can be found on Web sites such as [713]. An overview of UMTS can be found in [400], and the 'full Monty' in [56]. To keep up with phone fraud, a useful resource is the *Discount Long Distance Digest* [252].