BY JACK HITT AND PAUL TOUGH

Terminal Delinquents

ONCE, THEY STOLE HUBCAPS AND SHOT OUT STREETLIGHTS. NOW THEY'RE STEALING YOUR SOCIAL SECURITY NUMBER AND SHOOTING OUT YOUR CREDIT RATING. A LAYMAN'S GUIDE TO COMPUTER HIGH JINKS

On a muggy Friday night, we putter about the entrance to the Chelsea Hotel in New York City, nervously chatting about nothing in particular, pacing, thumping a dead coffee cup, waiting. A massive sun—garishly orange, unnaturally close—tries to wash this skeezy neighborhood with its maudlin rays, but this is Manhattan, the Chelsea, where Nancy Spungen asked Sid Vicious to stab her to death; no way. It moves on, down the runway of Twenty-third Street to the Hudson River, like all the traffic on this block, unnoticed. We are here to meet Kool and Ikon ,* reputedly two of the most talented computer hackers this side of New-

Outlaws

*All hacker names have been changed.

ark. They had agreed to reveal the secrets of their craft, but only if we chose a place such as the Chelsea, where our work would be untraceable.

The film-noir tactics are necessary these days because hackers are on the lam. During the last few months a federal sweep of computer hackers, known as Operation Sun Devil, has targeted the country's hacker elite. Last spring, Secret Service agents raided the homes of scores of kids, seizing not only computers but every piece of electronic equipment in sight, down to answering machines, cassette recorders, even soldering irons. These searches had all the subtlety of SWAT raids: six armed agents—guns drawn—to take one teenager into custody. In one Manhattan bust, a fourteen-year-old boy stepped from the shower into the sights of an agent's shotgun. In all, the government has seized twenty-seven thousand computer disks from forty suspected hackers. Two of them are to meet us tonight.

Hacking, as most of us know it, means breaking into private computer systems. More broadly, hacking is about solving problems, getting around obstacles, clearing the way. It involves not only the technical methods of skirting computer security, but also convincing the people who run the machines to divulge their passwords. Here at the Chelsea, the obstacle we're circumventing is the U.S. Secret Service.

Until recently, hacking was done in the comfort of one's bedroom, plugged into Mom and Dad's home phone. But a government wiretap can do a lot to change old habits. Now many hackers carry mobile computer rigs that attach to any phone—whether it's a pay phone on the street or the room phone in a hotel.

According to the media kit issued by the Secret Service, the boys we are scheduled to meet pose a clear and present danger to the security of both the government and the American people: "The conceivable criminal violations of this operation have serious implications for the health and welfare of all individuals, corporations, and United States government agencies relying on computers and telephones to communicate." In other words, for "the health and welfare" of us all.

But when the boys finally arrive and the four of us stand in the lobby of the Chelsea, chatting, we find that they are courteous, even deferential. It is difficult to see them as the new Communists, the new menace, the enemy within. And if it is hard to see them as the government's clichés, it is equally difficult to see them as the media's, which has chosen adjectives from a different page of the thesaurus, depicting hackers either as a group of buck-toothed dweebs or the lazy sons of the white middle class whose loathing of their parents is so intense that they wreak their Freudian revenge upon the aptly named Ma Bell.

The most recent poster boy for computer subversion is Robert Morris Jr., a former Cornell graduate student convicted earlier this year of releasing a virus that disabled nearly six thousand computers nationwide. Morris's father was the head of the National Computer Security Center, the government's computer-security agency, and the media delighted in painting Morris Jr. as the spoiled son of privilege ruining his father's good name. The Ivy League student stared out from a thousand newspaper photos, pale and owl-like in his glasses. No longer would the government be forced to denounce phantoms; computer hacking now had a face and a name.

But these boys are teenagers—nearly ten years younger than Morris—olive skinned, descended from Mediterranean stock. Home is a working-class urban neighborhood in New Jersey. They could never consider graduate school at Cornell; they're thinking about Passaic County Community College.

SAYS A HACKER: "I THINK I COULD CALL AND SAY, 'HI, I'M EATING A BANANA SPLIT. GIVE ME YOUR PASSWORD.'"

Though handsome, they possess the awkwardness of youth—they are seventeen and eighteen years old—so with a little imagination, we could certainly write them up as geeks. Their clothes are standard issue for peer-pressured teens: baggy jeans, no belt, low-top sneaks, long-sleeved T-shirt. No pocket protector, but no hair sculpted into a Dairy Queen offering, either; just careless teenage hair. They are similar in appearance—medium height and lanky. Ikon is the shorter of the two and tends to be the more serious. His jokes are often put-downs, mocking the stupidity of those around him. Kool's humor is more playful, even lewd; he's constantly checking out the girls.

Their language is urban, toughened by *dems* and *dozes*; and youthful, brimming with *uhs*, *likes*, and *you knows*. But take out that oral punctuation, and the syntax is textbook correct. Their conversations are surprisingly sophisticated in their understanding not only of the complex workings of the computer but of the caprices of the human heart as well.

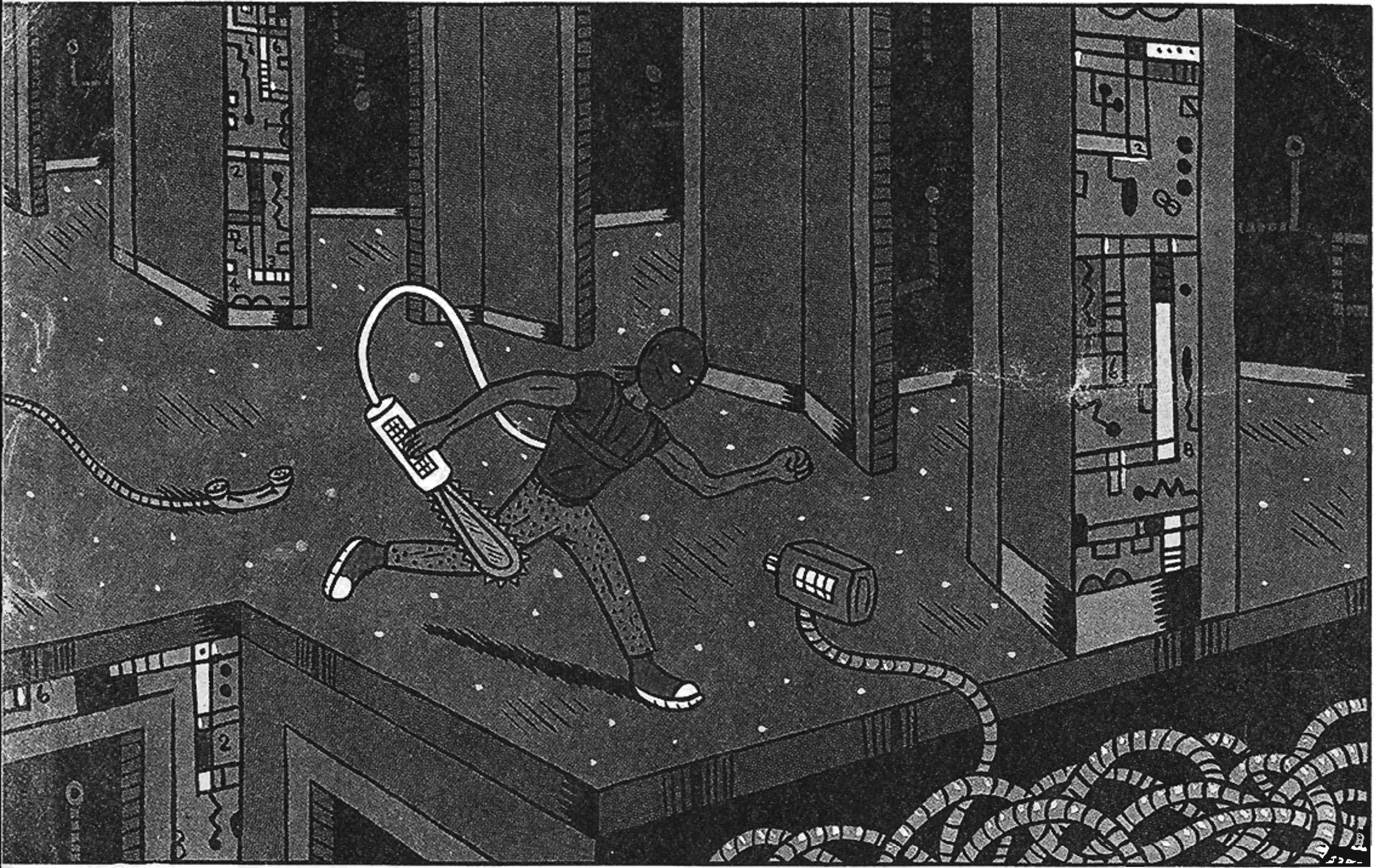
Under false names and paying in cash, we check into our cheap room, a space just big enough for the four of us, painted white every year for half a century and furnished with flimsy items stained the color of cocoa. We quickly redecorate, hauling the desk next to the bed and pulling up the chair so that we can all sit and see. We set their portable laptop computer on the desk and string a tangle of wires among the computer, various electronic gadgets, and the hotel telephone. Ikon's fingers fly across both the phone's keypad and the computer's keyboard with blinding speed.

Eeeep. We have connected. We are here to learn how to do this, but for now we just stare into the shimmering green screen. In a matter of minutes we are deep in the heart of the telephone company's computers. It appears that Ma Bell has been expecting us; the screen suddenly displays a boxed note, unambiguous in its meaning:

> WARNING
>
> Access to this computer and to the computer data and computer materials accessible by use of this computer is restricted to those whose access has been authorized by NYNEX or its subsidiary companies. This computer, computer data, and computer materials may only be used for approved business purposes of NYNEX or its subsidiary companies. Use by unauthorized individuals or use for unauthorized purposes is a violation of Federal and/or State Laws.

KOOL ASKS JACK FOR his home telephone number. More light-speed hand movements. The room is still with concentration, interrupted occasionally by an incomprehensible chatter of acronyms and a strange, bureaucratic-sounding shorthand. Suddenly, a series of numeric patterns

Jack Hitt *and* **Paul Tough** *are writers living in New York.*



blooms on the screen. It looks like this:

```
M 00 TR01 555 0000
0 0 0 0
LEN 10 121 306
001 000 000 000 000 000 4
000 000 000 000 000 000 000 000
0 0 0 0
0 0 0 0 0
```

VFJ-DN

‘DOESN’T MEAN MUCH to you, does it Jack?” asks Ikon. “This is what a phone number really looks like. The LEN is your line-equipment number. It’s the actual hardware, the only thing that matters. Your phone number is just scratch-pad nonsense. I could change it right now, if I wanted to. It could be anything at all.”

More clacking on the keyboard, and a new image appears:

IAESS

NN* XX-

```
M 01 TR75 1 DN 555 0000 00000002
PIC 222 TTC
```

IKON MAKES A FEW CHANGES, and the configuration looks like this:

```
M 12 TR75 1 DN 555 0000 00000003
PIC 288 TWC TTC
```

JACK HAS JUST BEEN granted three-way calling (TWC) and has switched his long-distance carrier from MCI (222) to AT&T (288). At such profound digital levels, these changes will escape the NYNEX business office. Consequently, Jack will never be billed.

This deep into the system, many other things are possible—from the simple, such as finding an unlisted phone number with an address or a name, to the sinister, such as monitoring the conversation of anyone we choose by quietly dropping in on the phone line like an operator, undetected. All of it is rather simple, they insist, once you understand the structure of the system. If you’re not *stupid* (the ultimate hacker put-down), if you apply common sense to the system, hacking is a piece of cake.

The image of the powerful and reckless hacker, capable of rooting around in our most-secret computer systems, unleashing crippling computer viruses, disrupting phone service, crashing hospital computers, and changing school records, is the one most often affirmed by law-enforcement officials and the daily media. This is so not only because it easily suits the respective purposes of these institutions—whip up public loathing so the little sons of bitches can be arrested; sell newspapers—but also because it is largely true. This representation fails, however, because it doesn’t answer the most obvious question: If hackers really have the knowledge to do such things, why haven’t they used it? Why aren’t we living in a constant nightmare of paralyzed phone systems and crashing computer banks? To answer this question, we have spent the last year getting to know more than a dozen of the best hackers in America. Over time, we won their trust and were admitted into their ranks. We apprenticed ourselves to them so that we could learn what damage they really *can* do and why they don’t do it.

HACKING, AT ITS MOST mechanical, requires that you arrange an electronic conversation between your humble laptop (Radio Shack, $800) and a huge computer—brimming with information—inside some corporate headquarters, government agency, or university. The conversation takes place in a very human way—using a telephone. The laptop uses a modem (Radio Shack, $150) to translate the digital pulses of a computer into the hisses and beeps that travel over regular phone lines.

In the comfort of your home, a modem can be plugged directly into the back of the telephone. When you’re using plugless phones, like hotel phones and pay phones, one more step is required. An acoustic coupler (Laptop Shop, $150), tightly strapped to the phone receiver, allows the computer

ILLUSTRATIONS BY KAZ

VF: DN SUV; FEATRS, DN, XXXXXXX, 1, PIC!

to fire audio tones directly through the handset, the way we do when we speak.

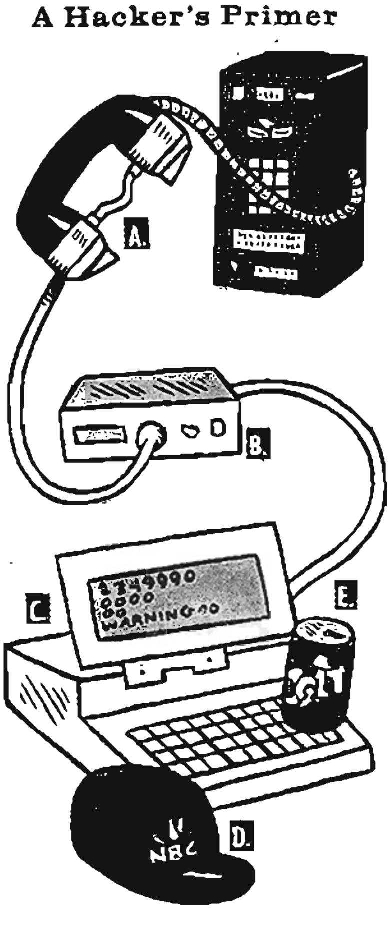
Just like people, computers have phone numbers, known as "dialups." When you call a computer, its own modem hears the tones coming through the phone line and translates your hisses and beeps back into the electronic pulses the computer can understand. You're connected. The hacking can begin.

There are thousands of systems to hack, and dozens of hackers for each one. For Kool and Ikon, though, there's only one game in town—the phone company.

Hacking Ma Bell dates back to the late Sixties, when phone hackers, then dubbed "phone phreaks," discovered that the entire AT&T phone system could be controlled by whistling tones at various frequencies directly into a phone. One notorious hacking pioneer, John Draper, made the farcical discovery that the toy whistle in a box of Cap'n Crunch perfectly mimicked the 2,600-hertz tone that engaged a long-distance line, enabling him to make free calls anywhere in the world. Draper assumed the cereal's name as his *nom de haque,* and he and his generation spent years deciphering the meanings of different tones. The perfection of the "blue box"—a portable device that duplicated the tones needed to master the phone system—became the ultimate mission.

A Hacker's Primer

Here's What You'll Need



A. ACOUSTIC COUPLER: Sleek suction cups fit over the earpiece and mouthpiece of your phone. Portable and sturdy, these are perfect for home or the road. $150.

B. MODEM: Although many top-of-the-line laptops come with a modem built in, the budget hacker will need an external modem to connect the computer to the acoustic coupler. $150.

C. LAPTOP: When the situation demands prudence, the cautious hacker uses a portable laptop for work outside of the home. $750–$2,000.

D. NBC CAP: No hacker can do without this handsome and versatile social-engineering prop. Perfect for those late nights at the Empire State Building. $10.

E. JOLT COLA: *The* soft drink of elite hackers has "all the sugar and twice the caffeine." One can will keep you hacking until dawn. $.60.

With the advent of long-distance calling cards, which are easily filchable, hackers today take free long-distance calls for granted. What interests Captain Crunch's descendants are the computers that control and link our phones. Soon after the Captain Crunch era, AT&T was broken up into a network of "baby Bells" (regional phone systems). These are now the main event. Kool and Ikon hack NYNEX, which handles phone service for all of New York and New England.

The first stop for your phone line, after it snakes out of your house, is a local switching center. This "switch" directly controls all the phones in your neighborhood. A switch performs the same service as Lily Tomlin's cranky operator, Ernestine, who would plug your phone jack into the line that you were calling. Today, your switch makes that connection electronically, and does it for as many as 150,000 phones.

Each neighborhood switch is controlled by its own huge computer; these computers are the essential targets of the phone-company hacker. If you can access the computer for a switch, you can control every phone it does. You can turn those phones on and off, reroute calls, and change numbers.

When this knowledge grows boring, the explorer can investigate the dozens of NYNEX's more complicated computer systems, each containing hundreds of new passageways and strange domains. For the advanced hacker, one of the more attractive is the infelicitously named NYNEX Packet Switched Network, or NPSN. Its beauty is its strength: The system allows you to enter each of the more than one thousand switches in New York and New England. Even more appealing, it allows you to ricochet off onto regional maintenance systems such as COSMOS and MIZAR. Among its many talents, COSMOS sends out instructions to create an kill phone numbers. The local MIZAR actually does the work. Since COSMO keeps the records and MIZAR doesn't most hacking done on a MIZAR is undetectable. MIZARs are a hacker favorite.

In order to get into any computer, yo need a dialup number, an account name (o "login"), and a password. Most people encounter the basics of this process every tim they approach an automatic-teller machine. Knowing where to find an ATM i your dialup; placing your card with it black magnetic stri in the slot is like entering your accoun punching in you personal identification number is lik typing your password. The secret o obtaining these thre keys for breakin into a phone-company computer—o any computer—i simple, our tuto explain, and can b learned as easil over a banana spl in an air-conditioned diner as ove a computer screen We abandon ou sweltering room a the Chelsea an head to the loca joint. On the plate glass window of th restaurant we notic a decal that boasts INSIDE: A PUBLIC PHONE YOU CAN DEPEND ON.

Over burgers and ice cream, we learn that there are several mechanical ways o learning accounts and passwords, but tha there's an easier way, known as social engineering. Basically, social engineering is bullshitting—calling someone who has access to a system and convincing them that you are a legitimate user who needs a dialup number, an account, and a password.

For the adventurer, social engineering may seem like cheating. Getting a password *can* be done by purely technical hacking means: programming a computer to try thousands of passwords. But to these guys (and even to their apprentices after a few weeks), this method is as irritating as playing the first levels of a video game after you've mastered them. You want to whiz right past such tedium to the more interesting levels. Getting a password is not hacking. It is a pain in the ass.

Social-engineering a used-car dealer (see sidebar, this page) is easy, even if you don't know what you're doing (because he doesn't, either—although his natural suspicion as a civilian often means you don't get past the hellos). Social-engineering a computer specialist with high-level access is easy only if you *do* know what you're doing. The professional needs to hear a few bits of jargon, just enough artfully expressed codes to make him feel that he is talking to a member of the guild. Both forms are surprisingly successful.

"Sometimes," says Kool, "it's so *simple*. I used to have contests with my friends to see how few words we could use to get a password. Once I called up and said, 'Hi, I'm from the social-engineering center and I need your password,' and they gave it to me! I swear, sometimes I think I could call up and say, 'Hi, I'm in a diner, eating a banana split. Give me your password.' "

LIKE ITS mechanical counterpart, social engineering is half business and half pleasure. It is a social game that allows the accomplished hacker to show off his knowledge of systems, his mastery of jargon, and especially his ability to manipulate people. It not only allows the hacker to get information; it also has the comic attractions of the old-fashioned prank phone call—fooling an adult, improvisation, cruelty.

In the months we spent with the hackers, the best performance in a social-engineering role was by a hacker named Oddjob. With him and three other guys we pulled a hacking all-nighter in the financial district, visiting pay phones in the hallway of the World Trade Center, outside the bathrooms of the Vista Hotel, and in the lobby of the international headquarters of American Express.

Here's How You Do It: Social Engineering

Social engineering in practice can be staggeringly easy. One good session, for instance, is all a hacker needs to break into TRW, the company that houses the credit files on 170 million Americans. Like to check your neighbor's credit rating? Here's how:

Call information in a faraway town and ask for a used-car dealership. Say you get Louie's Used Cars. Call and ask for the finance department. Whoever answers will be the one who uses the TRW account at Louie's to check on the credit worthiness of customers. Now lay on the bullshit, as Kool says, "in your best Joe Isuzu voice." Here's one riff that works only too frequently: "Hi, my name is Gary Jenkins with Compuline. We're doing a few repairs on the TRW lines in your area. Have you been having any trouble with your terminal?"

Now, who among us has *not* had trouble with a computer? Your friend at Louie's will likely greet you enthusiastically, thanking God you called. So proceed: "Okay, we need to check the line. Could you start up your system and talk me through this? First of all, what dialup are you using?" He'll then give you his local dialup for TRW. Write it down.

"Yeah, that's what I thought. Okay, when you first get in, what do you type?" The ten-character sequence he gives you is his account. There's no password; this is all you need. Write it down. Tell him you'll check out the problem and call back. Thank him for his help. Always be courteous; you may need to call again.

Now that you have a dialup and an account, you can call TRW from anywhere. All you need is a person's name and address to uncover his or her social security number, credit-card numbers, and credit history.

Oddjob's magnum opus takes place along the south wall of the phone bank leading to the Vista's bathrooms. We bolshevize six chairs from the women's powder room and attach our computer to a pay phone. Throughout the night, the hackers compliment one another on the sheer genius of the place: chairs, a dozen phones, a computer with coupler, a snack bar down the hall, and—on a nasty, humid city night—air conditioning.

At the rarefied level these four have reached, an evening's work often revolves around the links between networks in the NYNEX system. On this night, one of our links is down; a password has been changed. Oddjob begs for a chance to social-engineer something, anything. His method, he explains, is to sound like a regular person, to assume the accents of those who do the day-to-day keypunching and processing—the heavy lifting of the information age. He has a considerable repertoire—Brooklyn guy, polite blue-collar type, southern redneck. "You should hear my black woman," he boasts. Tonight's composition will be performed in the key of Flatbush.

Oddjob paces furiously on his lilliputian stage, tethered to the pay phone by the irritatingly short steel line, firing suggestions to the crowd on whom to call, taking in ideas. Part of the thrill of social engineering is clearly the improvisation of it all. But it's improvisation with a competitive edge. You show your machismo by waiting until the last possible second to prepare yourself. The moment after dialing, before the phone is answered, a true hacker will suddenly request vital information: "Where should I say I'm calling from?" "Who do I ask for?" or even "Where am I calling?" Oddjob is feigning such recklessness when the phone is answered. He opens by establishing his credentials in thick Brooklynese:

"Yeah, hoi deh. Dis is Tucker calling from Pearl Street operations. Yeah, hi. You guys havin' trouble gettin' into NPSN deh? You guys are goin' through a packet switch, right? Yeah, when you go into COSMOS. Okay, 'cause dat's where the problems are—ya day guy reported it. Okay, what do you use for the packet switch when you first connect—do you have your own code?"

She does have her own code; unfortunately, she is not about to give it to him. She tells him to solve his problem by checking the manual. So Oddjob loudly flips through the pages of a nearby phone book, pretending to read from its pages, and finally, frustrated, heaves the phone book toward the wall, with a crash. But it's done in a way that says: *Geez, aren't these manuals frustrating? We, the folks who do all the work, are supposed to make sense of these?* She's beginning to cotton to him and reveals that the first part of the code is the user's initials. Oddjob cranks up the charm and moves in for the kill.

"Okay, so what do you put in? GWT? Are those your initials? What's your name? Gail? That's a nice name. Mine? Tucker. Yeah, that's my last name. I don't like my first name because it sounds really dumb. No, I'm not telling. *Noooooooo*. I'm not 'gonna tell you. *Ooooooohh.* You really want to know? Okay, it's... Edmonton. Oh, come on, Edmonton is *not* distinguished, it's silly. They used to kid me in school. Yeah. Heh, heh. Anyway, just so I can get to the right system, would you walk me through it?" She does, and he gets most of the information he wants.

BY 4:00 A.M. we had been thrown out of the Vista and were spread out across the waxy, marble lobby of American Express headquarters, listening to Oddjob con another sucker on the phone. Kool was trying out a few breakdancing moves. The evening had been devoted almost exclusively to social engineering; we hardly used the laptop at all.

As the edge of the horizon began to lighten and the two of us had said goodnight to the hackers and were walking home, we realized that the entire evening had provoked an eerie déjà vu. As teenagers, we had both survived many of these Friday nights; trying halfheartedly to get into trouble, sitting around with the guys, waiting for something to happen. It's no accident that there are no hackers older than about twenty-one; serious hacking requires the kind of tireless devotion that only teenagers possess.

As with all teenage pursuits, hacking doesn't last forever. For most hackers, manipulating technology in imaginative ways is nothing more than rebellion. They learn high-tech pranks, such as changing the outgoing message on their algebra teacher's home answering machine, or they figure out how to chat with other hackers around the country for free. But these amateurs lack the patience and resolve to ascend to the levels our companions have attained. They fool around for six months or a year, get bored, and quit.

Like any group of teenagers with a common pursuit, serious hackers have nothing but contempt for amateurs. And when a fellow pro moves on, they treat it almost as betrayal, scorning the traitor as having "faded away into society." They can't imagine it happening to them.

Hackers are a group that has always existed in teenage society. They are not the genius nerds seen on TV. Nerds, by definition, are prosaic. They lack the creativity, the badass guts needed to hack. Nerds, in fact, are the ones who grow up and *get* hacked. Real hackers are the rebellious brains: the video-game addicts, the crystal-radio connoisseurs, the Dungeons & Dragons freaks. They are the guys who understand, even love, the way systems work: They don't just take things apart and put them back together—they make them do something else, something *better*. Where we see only a machine's function, they see its potential. This is, of course, the noble and essential trait of the inventor. But hackers warp it with teenage anarchic creativity: Edison with attitude.

Consider the fax machine. We look at it; we see a document-delivery device. One hacker we met, Kaos, looked at the same machine and immediately saw the Black Loop of Death. Here's how it works: Photocopy your middle finger displaying the international sign of obscene derision. Make two more copies. Tape these three pages together. Choose a target fax machine. Wait until nighttime, when you know it will be unattended, and dial it up. Begin to feed your long document into your fax machine. When the first page begins to emerge below, tape it to the end of the last page. Ecce. This three-page loop will continuously feed your image all night long. In the morning, your victim will find an empty fax machine, surrounded by two thousand copies of your finger, flipping the bird.

IKON AND KOOL HAVE BEEN hacking the NYNEX phone system for about six years. Although much of their work has been done alone, they have each been in dozens of informal partnerships and groups, which tend to form quickly and dissolve just as fast. In the early Eighties, some of the best hackers in the country formed the Legion of Doom, which, despite its wicked name, basically served as a conduit for information. The quest to understand NYNEX is a far-flung, collective enterprise, like the space program, only run by teenagers—experiments aren't done in scrubbed laboratories but in hotel lobbies; information isn't exchanged at symposia in Geneva but at hastily called meetings in peculiar locations. One such meeting has been institutionalized: first Friday of every month, Manhattan Citicorp building at Fifty-third and Lexington at—where else?—the pay phones.

Although the channels hackers use to communicate are highly sophisticated, the way information travels is similar to the way knowledge is passed on in an oral tradition. Teleconferences are held on "bridges"—illicit phone links; technical information is exchanged on private computer bulletin-board systems run out of hackers' bedrooms; samizdat magazines are distributed with names like *Phrack* and *2600*. The latter name is an homage to Captain Crunch's 2,600-hertz tone, a tacit recognition that this oral tradition stretches back decades.

"Even though hippies were blue-boxing for all it was worth in the Sixties," explains Ikon, born the year Captain Crunch went to jail, "they didn't really understand what they were doing. In the Nineties, we're on a

(continued on page 211)

Hackers *(continued from page 183)*

search for technical knowledge; what *we're* doing is figuring out how the phone system really *works*."

Once you understand the architecture of the system, all sorts of opportunities present themselves. Consider those telephone hybrids found beside most automatic-teller machines—the ones that connect you immediately with a bank employee. We see a way of getting help; a hacker sees unlimited free long-distance phone calls. Here's how:

When you pick up that phone, you hear a moment of silence before the automatic dialer beeps out the seven tones that call the bank's service center. That silence represents an open phone line, waiting to be told what to do. So instead of waiting for the automatic dialer, click the phone's hook ten times in rapid succession. This action perfectly imitates the ten sputtering pulses of the last hole on the rotary dial—the operator. When the seven tones sound, they are ignored; you've already seized control of the phone line. Wait a moment and the operator will answer. Explain that you're having trouble reaching a certain number in the Gobi Desert; could she dial it for you? Piece of cake.

Here's What Happens If You Get Caught

In the past, hacking was done with little concern for legal ramifications. But these days, as the federal government mops up a three-year investigation of computer hackers known as Operation Sun Devil, the conversation at hacker get-togethers is as likely to concern jail time as the intricacies of newly discovered systems.

Sun Devil has cast a wide net, snaring not only hackers but fanning out to nab even those suspected of *associating* with hackers. Craig Neidorf, publisher of the hacker magazine *Phrack*, was indicted in February for printing a document that had been hacked out of a BellSouth computer. The government based its case on BellSouth's claim that the purloined text was worth $79,449. When a BellSouth employee reluctantly admitted on the witness stand that the document was available from a catalogue for just $13, the case against Neidorf collapsed. Neidorf was left to figure out how to pay his $100,000 legal bill, and his magazine is defunct.

As more cases come to trial, angry prosecutors are seeking severe penalties for the perpetrators of what they describe as an "astronomical" crime wave. But when the judges hand down the sentences to those accused of unlawful curiosity, they might reflect on the parable of the two Steves. Among the earliest hackers, Steve Jobs and Steve Wozniak built their own "blue boxes"—the small, illegal devices designed to let you make free long-distance phone calls. Not only did they use them to call the pope, they also peddled them door-to-door in the Berkeley dorms. In 1976 Wozniak and Jobs applied the lessons of the blue box to more complicated circuitry and, from a garage in California, started Apple Computer.

YET IF technology giveth, it also taketh away. One hot Friday night in July, we get the call to pick up the boys at Penn Station. They are bringing along some friends and a full agenda. Tonight, we're informed, will hold many lessons for us. When we meet, Ikon gravely explains the situation: "We seem to have lost our resources." It appears that NYNEX is starting to change passwords on them, and the one dialup into NPSN that was still working is now disabled. It just rings and rings. We will be starting practically from scratch.

We walk east on Thirty-fourth Street toward the Empire State Building. We've already hacked from two New York landmarks; why not a third? At 7:00, the building is pretty empty. Tourists are either taking the escalator down to the Guinness World of Records Exhibition or the elevator up to the Observation Deck. We're roaming the halls, scoping out pay-phone banks, and feeling rather conspicuous—six young men with a big black suitcase. A security guard, trying to be helpful, spooks us, and all six of us bolt simultaneously for six pay phones, pretending to be in midconversation. A ludicrous paranoia is setting in.

Eventually we find a velvet rope draped across a corridor, guarded only by a man polishing the floor. A few furtive glances down the hall, and we're over and in, ensconced in a secluded phone bank. We unpack our laptop, our modem, and our acoustic coupler; happily, the entire contraption fits on the phone's shelf.

Ikon starts pounding digits on the pay phone, trying to get that one dialup to work. But there is only continuous ringing. Suddenly he gets an idea. It's a long shot—a solution hopelessly simple. He calls the actual office whose computer he's trying to break into and politely asks the woman to (please) turn on the computer's modem.

Ecstasy.

"We're back on!"

"Yo! We're worth something!"

"It's MIZAR! It's everything!"

"We have a reason to live!"

With access to NPSN, we now set out to "liberate" one of these pay phones, that is, to free it from its addiction to quarters. We get into the switching computer for this neighborhood and disconnect the pay phone. "The beast," Ikon declares, "is dead. We have killed it." Picking up the beast's receiver proves that he's right; no dial tone. "Now we bring the beast back to life," Ikon announces, and resurrects it as a regular phone, able to make local and long-distance calls for free.

Kool takes out his black marker and writes on the pay phone in the wild style of graffiti artists: "The PLO Lives," and then adds, "Payphone Liberation Organization." We reconnect the computer to the liberated phone.

A second security guard happens along. He has a distinct interest in being told just what the—just what in *hell* is going on around here, anyway? Kool takes him aside for a bit of impromptu social engineering. "We're, uh, sending a story over the phones. We're with NBC." The guard notices the peacock logo on Ikon's white NBC baseball cap (NBC Studios gift shop, $10) and somehow makes sense of this—a bunch of teenagers, the middle of the night, Cheez Doodles, Jolt Cola; of *course* they're TV reporters. Now he wants to chat *us* up.

"What's the story on?" he asks eagerly.

"It's on the pay phones at the Empire State Building," replies Kool. "You know, uh, what kind of problems they have...." Kool's improvisation is getting almost comically desperate, but the guard still buys it. After a moment, he moves on to complete his rounds.

From our current perch in NPSN, we want to hop onto the Brooklyn COSMOS maintenance system. The password we've been using no longer works; they've changed the locks. This is a serious problem. Social engineering at this level is extremely difficult, because the operators have been burned too many times to just hand over a password. What's more, there is no direct phone number to COSMOS, no dialup; COSMOS can only be reached from NPSN. But there is, as always, another way. This time it's called "pad-to-pad," probably the most advanced hacking procedure, because it calls for an artful use of both mechanical and social-engineering talents. Here's how it works:

Call an office in Brooklyn where you know they use COSMOS. Tell the person who answers that you're troubleshooting her COSMOS account, and you need her help. Ask her to type *stat* on her keyboard and read off the number that appears. With it, you can connect directly to her computer terminal; now *your* screen is *her* screen. Everything she types you can read, and vice versa. Begin the social engineering: Ask her to sign on to COSMOS and enter her password. She thinks everything is fine because she isn't telling you anything over the telephone, and she isn't, exactly; she's just typing on her terminal. And you type on yours, faking the computer's commands. When she types in her account number, you respond—as the computer would—by typing "Password?" Of course, her password won't get her onto COSMOS, since she's connected only to your computer; instead, it appears in glowing letters on your screen. You type "login incorrect." Before she tries again, detach your terminal from hers and keep talking, offering friendly advice.

At the Empire State Building, standing at a pay phone, our first shot at pad-to-pad works perfectly. Our victim puzzles over why the system won't grant her access and tries again. In a flash she hears the familiar clicks and squeaks that assure her she is safely on, and she and Ikon exchange cheerful banter as the COSMOS warning flashes on her screen:

ATTENTION ALL USERS

Under no circumstances should you disclose your logon password to anyone on the phone or in person.

IKON STRINGS HER ALONG for another few minutes, listening to her complaints, completing the lie: "Well, it seemed to be okay from this end. The first time it said 'login incorrect,' huh? You think you might have typed it in wrong?"

But he's barely listening now, performing the coda by rote, because he's already connected to the Brooklyn COSMOS with her account, and he's exploring, looking for a backdoor program he installed here the last time he was on, before they moved the mainframe from Brooklyn to Massachusetts.

"It's here!" Ikon shouts.

"They're so stupid, man," says Kool.

"When they copied all the commands they copied our backdoor command over too," Ikon explains.

We execute this old command, disappear through the "back door," and surface on a higher, more powerful level of the machine. For the next few hours, we explore this strange new land, trying to figure out the look of the place. We are a dozen hands groping in darkness, feeling our way along the wall of a system somewhere in Massachusetts. While one hacker works the keyboard, the others throw out suggestions. Over time, ideas are winnowed, attempts are assayed. Failures are common, but they are relieved by moments of hope. A small obstacle is surmounted or a new passageway is discovered. The fun of gaining entry is over; now most of the hacking is trial and error, banging away at an obstacle until a path over, around, or through is revealed. At this remove—we are relayed off three computers and extended across four states—even the easiest hacking problems can suddenly become complex again.

We, the reporters, try to buoy our own interest by peppering the hackers with questions. But after a while, the answers are numbingly similar: "We're trying to get in." "We're just looking around." "We're trying to figure out what this does." After three hours, we are slumped against a wall, contemplating the significance of our boredom. At times, accompanying hackers is about as exciting as watching a graduate student flip through a card catalogue. During the fourth hour, several of the hackers grow restless. One leaves; another calls some friends. Kool slides down the wall to join us, and wistfully recalls the old days, when he could hack for twelve hours without a break.

Ikon outlasts everyone, which is not unusual. He's deep within the machine now, wired, intense, alert. He waves off the occasional call for food, ignoring his own hunger and fatigue. He's been standing before this unit for five hours without rest; he barely bothers to shift his weight from one leg to another. All we hear are the occasional staccato clicks as he attempts yet another entry. From time to time a security guard approaches and peers in. Our paranoia has yielded to exhaustion. We wave.

IKON'S REVERIE DOESN'T END until the battery pack on the laptop dies. Everyone else is relieved; we've been ready to go for hours.

As we pack up our equipment and head out into the night, Kool's attention is suddenly distracted by a low-slung, high-tech car. "Yo, check out that Porsche with the cellular phone. I'd give up hacking for that car."

"Who needs a Porsche?" asks Ikon. "We have MIZAR."

Kool looks at him with amazement, but Ikon goes on. "I'd rather have all of NYNEX than a Porsche. I mean, can you get passwords with a Porsche?"

Kool, still dumbfounded, states the obvious: "You can get *girls* with a Porsche! Can you get girls with a password?"

HACKERS WARP THE NOBLE TRAITS OF THE INVENTOR WITH TEENAGE ANARCHIC CREATIVITY: EDISON WITH ATTITUDE.

They're laughing, but we all know it's true: For Ikon, there is no higher purpose than hacking NYNEX. Kool, on the other hand, is willing to make a few exceptions. As they discuss the next day's hacking agenda, Kool admits that he's getting a little bored with the endless exploration, and suggests that they try some *cool* stuff. "Maybe we could forward calls to a radio station and be the only ones who can get through," he suggests. "We could win tickets to, like, a Depeche Mode concert."

Ikon is dismissive. "No. The Project."

"C'mon, let's think of something to *do*."

"No, wait. The Project, the Project." He is insistent: We will continue to chart the landscape of the telephone company. Nothing else matters.

We're with Kool, frankly: When do we get to start changing the orbit of satellites and listening in on Madonna's phone calls? For that matter, when do we conquer the entire NYNEX system? When does it end?

"The thing that keeps us so interested," Ikon tells us later, "is that with NYNEX, or any other system with good security, we'll *never* have permanent access. We'll always lose what we need, and we'll be forced to find another way to get back into it. It's almost like a game. It's like a never-ending role-playing adventure game, but it's real. The thing that makes it interesting is that you can never win."

"So why play?" we ask. "Why spend years at a keyboard, risking jail, to play a game you'll never win?"

"It's like having the edge. That's the whole thing," says Ikon. "The name of the game is having the edge."

"Over whom?" we ask.

"Over anyone else," he replies. "Some people spend their whole lifetime trying to find the one thing that they're really good at. We've found it already. We're hackers. You know, there are always these computer know-it-alls who say, 'Oh yeah, I used to be a hacker.' That's crap. If you're an ex-hacker, you were never a hacker to begin with. It's not something that dies. It's a way of life. It's a way of thinking."

What's the purpose of all this exploration? After a dozen nights, it hits us: Hacking *has* no practical purpose. Every hacker starts as a utilitarian, viewing phone systems as means to an end, such as free calls or high-tech pranking. But over time the means *become* the end. Advanced hackers are nothing more than aestheticians; they marvel not at the system's use but at the system itself. Suddenly a nagging contradiction makes sense. Throughout our apprenticeship, the hackers consistently scorned our "juvenile" requests to hack into TRW. Now we understand why. The best hackers are *bored* by TRW (and other record-keeping systems, like those at hospitals and schools) despite the juicy information they contain. These computers are simple data-retrieval units, not much more complicated than the word processor used to write this article. The TRW computer isn't worth hacking, because, as Kool so sweetly puts it, "it's a piece of shit." The phone networks *are* worth hacking, not because of what a hacker can use them for, but because of their vast size. "It goes back to what Crunch said," Ikon explains. "The phone system is the largest network in the entire world." It's the hardest thing to hack, and therefore, it's the only thing *worth* hacking. It is from these hackers that the law and the corporations have the least to fear. Ironically, these are the ones getting busted.

It is true that everything Kool and Ikon do when hacking is illegal. All their calls are paid for fraudulently; all the systems they enter are proprietary. This fact occasionally provides a frisson of excitement (probably more so for us, the amateurs, than for serious hackers); more frequently, it is just ignored. What these hackers are doing makes absolute sense to them: They are gaining knowledge. If there are laws against that, they reason, they're not worth taking seriously. They've probably never heard Bob Dylan's code for the outlaw—"to live outside the law, you must be honest"—but they instinctively follow it.

If pressed, they will describe the havoc they could unleash on the phone system; they could easily write a simple virus that would disable switch after switch, shutting down phone service for all of New York and New England in a few hours. The damage, they estimate, could take NYNEX engineers months to repair. "We could handle it," says Ikon flatly. But asking them what sort of harm they could do to the phone system is like asking a surgeon what sort of harm he could do to a patient he's operating on. They could destroy it... but what kind of question is that?

KOOL IS AMAZED AT HIS PARTNER. "YOU CAN GET *GIRLS* WITH A PORSCHE! CAN YOU GET GIRLS WITH A PASSWORD?"

A COUPLE OF WEEKS after the night at the Empire State Building, we're sitting with four hackers in the appropriately named Cosmos Diner, watching four rail-thin adolescents attack four huge plates of meat. We ask them what had become an obvious question: What if the phone company actually offered them jobs?

"If NYNEX offered me a good job in an intelligent position, I'd take it in a second. I wouldn't even think about it," replies Ikon.

"Have you ever applied?"

"I called," Kool says. "They said all they had was repair, installation, and outside plant."

"Doofus stuff," explains Ikon. "All they have is dickhead jobs."

We ask how many people in the phone company know as much about the systems as they do.

"To tell you the truth," says Ikon, "I don't think there are *any*. I'll tell you why. Each person in NYNEX specializes in a single network, or just a part of a network. We, on the other hand, could easily assume the position of any person in any department for any reason."

"What would happen if they did hire you, and they said, 'Okay, you're in charge of stopping hackers'?"

"There's a problem with that," Ikon explains. "There's this Legion of Doom member from Michigan who was busted last year for something minor. They gave him a job in some bogus department within Michigan Bell security. They'd get him to try to engineer departments, or try to guess passwords and get into systems. And then they canceled the project."

"Would you do a project like that if they asked you?"

"Yeah!" replies Kool. "That would be my perfect position."

"And could you make NYNEX secure?"

"Sure," says Ikon. "I could do it in a minute. We know every single aspect of how to get into these systems. I could tell them in a minute how to—" He stops himself. "But the thing is, it wouldn't be worth it. They would hire us, they'd get a few secrets and tips from us, and then they'd fire us. That's what they did to the guy in Michigan. They found out exactly what he could do, and then they fired him.

"If we were offered a real opportunity to help," Ikon continues, "then we would help. But they'll never do that. They would never admit that they could possibly be helped by people half their age. They just have too much pride."

"When I called up NYNEX to ask for a job," says Kool, "I talked to this guy in Corporate Security. This guy didn't know shit about his network. I told him all these secrets, ways to break in; all they did was block all those entry points. I have yet to hear from anybody offering me a job."

"And later the same day, at home, we got back into the network through another entrance," says Ikon. "There's always another way."

"So fuck them," concludes Kool.

OVER THE LAST TEN YEARS, this country's relationship with technology has changed profoundly, in ways that we are only beginning to understand. Ten years ago, when we wanted to send a letter across town, we'd need a stamp and a few days to spare. Now we fax it in seconds. When we wanted money, we'd have to go cash a check with a real live bank teller. Now we don't even know when our banks are open. Personal computers, long-distance calling cards—we who have them can't imagine life without them.

During the same period, the many systems that we depend on—phone networks, banking transfers, even our national-security apparatus—have become increasingly dependent on computers. We trust these machines, sometimes unwittingly, with enormous amounts of personal information. This rarely concerns us; we have developed an almost religious faith in computers and in the people who run them. When we think of these systems at all, we trust that they are safe.

We are wrong.

Every one of these technological advances has made us less secure. Now our phones can be disabled; our credit histories can be changed; our medical profiles can be stolen; our social security information can be accessed. And it can all be done by an untraceable teenager at a pay phone, thousands of miles away.

There are no alarms being sounded by the people who run these systems. NYNEX, in fact, refused to allow any of its security personnel to be interviewed for this article. If computer-security professionals were to admit that the systems they manage are vulnerable, they would be asked how they could be made invulnerable. And at that point, they would have to admit that the systems cannot be, can never be.

Much of the public debate over computer hackers involves a search for the right metaphor. Are hackers simple trespassers, gliding through our houses without harming the contents? Are they armed robbers, breaking and entering? Are our computer systems like our homes, locked and protected? Or are they just a huge open field with a tiny sign saying KEEP OFF THE GRASS?

From a distance, a computer network looks like a fortress—impregnable, heavily guarded. As you get closer, though, the walls of the fortress look a little flimsy. You notice that the fortress has a thousand doors; that some are unguarded, the rest watched by unwary civilians.

All the hacker has to do to get in is find an unguarded door, or borrow a key, or punch a hole in the wall. The question of whether he's allowed in is made moot by the fact that it's unbelievably simple to enter.

Breaking into computer systems will always remain easy because the systems have to accommodate dolts like you and me. If computers were used only by brilliant programmers, no doubt they could maintain a nearly impenetrable security system. But computers aren't built that way; they are "dumbed down" to allow those who must use them to do their jobs. So hackers will always be able to find a trusting soul to reveal a dialup, an account, and a password. And they will always get in.

It is gradually dawning on us, thanks mostly to the exploits of hackers, that we have much less control over the computers that run our information society than we did over, say, file cabinets. Our general reaction has been to blame the messengers. In fact, to try to imprison them. Although they have never harmed the systems they hack, Kool and Ikon will probably be indicted early next year for a variety of acts made illegal by the Computer Fraud and Abuse Act of 1986; the charges they will face carry maximum sentences of many decades in prison. But even if hackers are jailed, hacking won't be eliminated; it's just too human an instinct, and just too easy a practice.

TOWARD THE END of the summer, we decide to attempt the kind of hack the government says is the main threat: We will try to hack the White House—specifically, the PROF system installed in 1982 by Admiral John Poindexter, then President Reagan's national security adviser. Poindexter chose PROF in an attempt to *eliminate* security breaches. If any system is unhackable, we reason, this is the one.

By the time we finally get together, however, a week after we first discuss PROF with the hackers, we learn that one of them has already called the White House computer center. He laid on the usual line about doing work on the system, and he got a dialup. The more difficult task, still ahead, is obtaining an account and a password.

We are sitting, as always, around a phone, safe in what one hacker describes as "a covert, undisclosed location somewhere in the tri-state area." He thumbs through a Federal Yellow Book, the publicly available directory for the executive branch of the U.S. government. "Why don't I call one of these people?" he suggests, pointing to the page headed, EXECUTIVE OFFICE OF THE PRESIDENT. He scans down the page—the staffs of Fitzwater, Sununu, Scowcroft—and decides randomly on a target a few doors down from the President.

"I'll just talk to him really basic," he explains, dialing the target's direct number.

"I need a name to use." As the phone rings in the White House, he glances around the room and his eyes settle on a T-shirt, signed just above the pocket by the French designer François Girbaud.

The White House answers. The hacker's voice drops an octave.

Hacker: Yeah, how're you doin'? This is François Girbaud with the computer operations division.

White House: Mmm-hmm.

H: Yeah, I was just wondering if you had any access to the PROF system.

WH: Yeah, I do. I don't use it very often, though.

H: Yeah, I know. Cause we're, like, troubleshooting your account.

WH: Oh.

H: It seems that something's wrong with it. And, you know, we're wondering if maybe it's, like, one of the dialups that you're using to get in or something.

WH: Well, let me see. Hold on, I'm just getting out of what I was doing.

H: You know, if you're too busy I could call back later.

WH: No, that's okay, this is fine. Hold on one minute, I'm just saving what I was working on. Okay. [He logs into PROF too fast for the hacker to get his account.]

H: Wait, wait. Why don't you go back a little? We have to verify the account as you're typing it in.

WH: Oh, I'm sorry.

H: Yeah, we want to make sure that it's your account and not somebody else's.

WH: How do I get out of this?

H: Ah, don't worry about it. Just repeat your account. Just tell me the account you're using currently.

WH: Oh, I'm sorry. [And he reads off seven characters.]

H: [trying to decide his next move] Umm, okay...[but his next move is made for him].

WH: And do you need my password too?

H: Uh, yeah, sure. That would be good.

WITH AN ACCOUNT and a password secured, the hacker politely concludes the conversation, hangs up the telephone, and bursts into laughter: "Yo, man, *François Girbaud*! I just read the name off his shirt! It's like saying 'Levi's'—'Hi, this is Joe Levi's!' I shoulda said 'Calvin Klein.'" Another hacker joins in: "Or Dick Hertz!" And another: "Or Mike Hunt!" For the rest of the evening, François Girbaud is the punch line to every joke. No other hack could top this one, so we head out to McDonald's for burgers and Cokes—just a bunch of teenagers, hanging on a Friday night. Maybe tomorrow we will read George Bush's mail. ◼

Liberia *(continued from page 46)*

and legs at will, could make themselves invisible. The rapine and slaughter of this conflict were no more awful than those of other civil wars, but a certain sickly inference seemed to draw itself out of them: Insofar as they were attached by threads of superstition to the exercise of certain dark powers, these atrocities became inscrutable.

AND NOW, ON SEPTEMBER 28, the rice and the canned goods, the reinforcements and the ammunition, also a few tons of cooking oil and a handful of European journalists have arrived on the *River Oli*. The new folks can scarcely take in what they're seeing of Monrovia. Nothing works, nothing is for sale, everything's falling down, it's over for this place. The main street, U.N. Drive, lies ankle-deep in water and trash. Throngs mill up and down it destroying walls and fences and searching through buildings voraciously, but there's nothing left to loot. The ECOWAS soldiers fire continually in the air above the crowds, driving them back from the waterfront. DOE—MOTHER PUSSY, the graffiti reads, ESCAPE/WE WANT RICE and GOD SAVE LIBERIA and PEACE NO WAR. No surface is without its share of bullet holes. The drive is lined with burned structures and littered with twisted wrecks. A jackknifed semitruck blocks two of the four lanes crosswise, a streetlamp from the median crushed under it like a frond. The car dealerships' huge windows open jaggedly onto empty showrooms where families camp now, keeping out of the rain. Surprisingly, the dogs look healthy. Nobody eats the dogs, the journalists learn, because they feed on human corpses. The people are starving, but the dogs have put on weight.

The safest area to sleep in is Mamba Point, the district with the embassies. Johnson's men prowl the streets there, and the sound of gunfire is more or less constant, but a jujuesque sort of diplomatic immunity seems to pervade for a couple of square blocks, and people like to believe they're protected here. Nevertheless, the rattling of weaponry sounds too close too often—and yet it's impossible to say from *where* this gunfire is coming. Noncombatants ply between the buildings cautiously: Am I walking in a fatal direction? What's the weather like ahead? The beach down the hill still stinks of death, though most of the corpses have been covered with sand and marked with driftwood. There's a little bit of commerce, perhaps, with the British and American embassies, which get supplies by helicopter. Everybody's hungry in Mamba Point, but nobody's dead yet from starvation. The wet season is passing; still it rains enough to keep the barrels half full.

Field Marshal Prince Johnson—Brigadier General, Acting President of Liberia, and Commander in Chief of the Independent National Patriotic Front of Liberia (INPFL)—wages, as part of his revolutionary struggle, a haphazard, sometimes enigmatic public relations campaign. In late August he entertained ten Nigerian newsmen brought in by ECOWAS, taking them around his sector of Monrovia on a forty-five-minute tour during which he shot into a car containing a European couple, killing the man and wounding the wife, who was dragged off by Johnson's soldiers and has not been heard from since; he also executed a looter by firing his side arm point-blank into the person's face. Today, September 29, Prince Johnson takes the step of actually bringing reporters to his headquarters, inviting a couple of American journalists and a French TV crew, recent passengers on the *River Oli*.

The Field Marshal's base lies on the capital's outskirts in the residential compound of the Bong Iron Ore Mining Company: down U.N. Drive past Freeport, Monrovia's waterfront; past the BMW dealership, now housing an ECOWAS platoon; past the Liberian Nail Factory and the Faith Healing Temple of Jesus Christ and Liberian Marble and Terrazo Tile, Incorporated—all smashed, burned, looted, with some of Johnson's rebels on a second-story balcony tossing bottles of Star Beer down on the pavement below; past alternating ECOWAS and INPFL checkpoints, where Ghanaian troops inspect the vehicles, or Johnson's boys, brunette or blond or redheaded, peer out from behind their artificial bangs and stick the barrels of their rifles inside the cars; down a dirt lane and through the Caldwell Coffee Farm and past the one-room New Life Mission Church and School. Then the dozen or so buildings of the Bong Mining compound begin. The hub of Johnson's operation is a concrete hospitality building surrounded by gunnery teams, aimless troops, tents, and cars. The structure, no larger than the average American home, seems to float on a sea of vehicles, mostly Mercedes sedans with their hoods raised. From out over the fields comes the crack of gunfire—it's said that the INPFL executes several Liberians every day—and, from the building, the muffled whomp of amplified music.

Inside, Field Marshal Johnson is holding one of his morning concerts. The large main room is full of troops, and in the center of the throng stands Prince Johnson, holding an acoustic guitar and singing "Rivers of Babylon," a Creole-reggae version of the 137th Psalm. He's backed by other guerrillas on conga, two electric gui-