Different operating systems have various names for privileged accounts—super-user, root, system manager—but these accounts must always be jealously guarded against outsiders.

What if an outside hacker became privileged on our system? For one thing, he could add new user accounts.

A hacker with super-user privileges would hold the computer hostage. With the master key to our system, he could shut it down whenever he wishes, and could make the system as unreliable as he wishes. He could read, write, or modify any information in the computer. No user's file would be protected from him when he operates from this privileged high ground. The system files, too, would be at his disposal—he could read electronic mail before it's delivered.

He could even modify the accounting files to erase his own tracks.

The lecturer on galactic structure droned on about gravitational waves. I was suddenly awake, aware of what was happening in our computer. I waited around for the question period, asked one token question, then grabbed my bike and started up the hill to Lawrence Berkeley Labs.

A super-user hacker. Someone breaks into our system, finds the master keys, grants himself privileges, and becomes a super-user hacker. Who? How? From where? And, mostly, why?

3

IT'S ONLY A QUARTER MILE FROM THE UNIVERSITY OF California to Lawrence Berkeley Labs, but Cyclotron Road is steep enough to make it a fifteen-minute bike ride. The old ten-speed didn't quite have a low enough gear, so my knees felt the last few hundred feet. Our computer center's nestled between three particle accelerators: the 184-inch cyclotron, where Ernest Lawrence first purified a milligram of fissionable uranium; the Bevatron, where the anti-proton was discovered; and the Hilac, the birthplace of a half-dozen new elements.

Today, these accelerators are obsolete—their mega-electron volt energies long surpassed by giga-electron volt particle colliders. They're no longer winning Nobel prizes, but physicists and graduate students still wait six months for time on an accelerator beamline. After all, our accelerators are fine for studying exotic nuclear particles and searching out new forms of matter, with esoteric names like quark-gluon plasmas or pion condensates. And when the physicists aren't using them, the beams are used for biomedical research, including cancer therapy.

Back in the heyday of World War II's Manhattan project, Lawrence's cyclotron was the only way to measure the cross sections of nuclear reactions and uranium atoms. Naturally, the lab was shrouded in secrecy; it served as the model for building atomic bomb plants.

During the 1950s, Lawrence Berkeley Laboratory's research

remained classified, until Edward Teller formed the Lawrence Livermore Laboratory an hour's drive away. All the classified work went to Livermore, while the unclassified science remained in Berkeley.

Perhaps to spread confusion, both laboratories are named after California's first Nobel Laureate, both are centers for atomic physics, and both are funded by the Atomic Energy Commission's offspring, the Department of Energy. That's about the end of the similarity.

I needed no security clearance to work in the Berkeley Lab—there's no classified research, not a military contract in sight. Livermore, on the other hand, is a center for designing nuclear bombs and Star Wars laser beams. Hardly the place for a long-haired ex-hippie. While my Berkeley Lab survived on meager scientific grants and unreliable university funding, Livermore constantly expanded. Ever since Teller designed the H-bomb, Livermore's classified research has never been short of funds.

Berkeley no longer has huge military contracts, yet openness has its rewards. As pure scientists, we're encouraged to research any curious phenomena, and can always publish our results. Our accelerators might be peashooters compared to the behemoths at CERN in Switzerland, or Fermilab in Illinois; still, they generate huge amounts of data, and we run some respectable computers to analyze it. In fact, it's a source of local pride to find physicists recording their data at other accelerators, then visiting LBL to analyze their results on our computers.

In raw number-crunching power, Livermore's computers dwarfed ours. They regularly bought the biggest, fastest, and most expensive Crays. They need 'em to figure out what happens in the first few nanoseconds of a thermonuclear explosion.

Because of their classified research, most of Livermore's computers are isolated. Of course, they have some unclassified systems too, doing ordinary science. But for their secret work—well, it's not for ordinary mortal eyes. These classified computers have no connections to the outside world.

It's just as impossible to import data into Livermore from the outside. Someone designing nuclear bomb triggers using Livermore's classified computers has to visit the lab in person, bringing his data in on magnetic tape. He can't use the dozens of networks crossing the country, and can't log in from home, to see how his program is running. Since their computers are often the first ones off the production line, Livermore usually has to write their own operating systems, forming a bizarre software ecology, unseen outside of their laboratory. Such are the costs of living in a classified world.

While we didn't have the number-crunching power of Livermore, our computers were no slouches. Our Vax computers were speedy, easy to use, and popular among physicists. We didn't have to invent our own operating systems, since we bought Digital's VMS operating system, and grabbed Unix from campus. As an open lab, our computers could be networked anywhere, and we supported scientists from around the world. When problems developed in the middle of the night, I just dialed the LBL computer from my home—no need to bicycle into work when a phone call might solve it.

But there I was, bicycling up to work, wondering if some hacker was in our system. This just might explain some of my accounting problems. If some outsider had picked the locks on our Unix operating system and acquired super-user privileges, he'd have the power to selectively erase the accounting records. And, worse, he could use our network connections to attack other computers.

I ducked my bike into a corner and jogged over to the cubicle maze. By now it was well past five, and the ordinary folks were at home. How could I tell if someone was hacking inside our system? Well, we could just send an electronic mail message to the suspicious account, saying something like, "Hey, are you the real Joe Sventek?" Or we could disable Joe's account, and see if our troubles ended.

My thoughts about the hacker were sidetracked when I found a note in my office: the Keck Observatory needed to know how the quality of the telescope's images degraded if they loosened the specifications for the mirrors. This meant an evening of model building, all inside the computer. I wasn't officially work-

ing for them anymore, but blood's thicker than water . . . by midnight, I'd plotted their graphs.

The next morning, I eagerly explained my suspicions about a hacker to Dave Cleveland. "I'll bet you cookies to doughnuts it's a hacker."

Dave sat back, closed his eyes, and whispered, "Yep, cookies for sure."

His mental acrobatics were almost palpable. Dave managed his Unix system with a laid-back style. Since he competed for scientists with the VMS systems, he had never screwed down the security bolts on his system, figuring that the physicists would object and take their business elsewhere. By trusting his users, he ran an open system and devoted his time to improving their software, instead of building locks.

Was someone betraying his trust?

Marv Atchley was my new boss. Quiet and sensitive, Marv ran a loose group that somehow managed to keep the computers running. Marv stood in contrast to our division head, Roy Kerth. At fifty-five, Roy looked like Rodney Dangerfield as a college professor. He did physics in the grand style of Lawrence Laboratory, bouncing protons and anti-protons together, looking at the jetsam from these collisions.

Roy treated his students and staff much as his subatomic particles: keep them in line, energize them, then shoot them into immovable objects. His research demanded heavy number crunching since his lab generated millions of events each time the accelerator was turned on. Years of delays and excuses had soured him on computer professionals, so when I knocked on his door, I made sure we talked about relativistic physics and ignored computing.

Now, Dave and I could guess Roy's reaction to our problem: "Why the hell did you leave our doors wide open?"

Our boss's reaction might be predictable, but how should we react? Dave's first thought was to disable the suspect account and forget about it. I felt we ought to send a nasty-gram to whoever was breaking in, telling him to stay away or we'd call his parents. After all, if someone was breaking in, it was bound to be some student from down on campus.

But we weren't certain that someone was breaking into our stem. It might explain some of our accounting problems—meone learns the system manager's password, connects to our achine, creates a new account, and tampers with the accounting stem. But why would someone use a new account if they eady had access to the system manager account?

Our boss never wanted to hear bad news, but we swallowed rd and called a lunchtime meeting. We had no clear proof of a cker, just circumstantial pointers, extrapolated from trivial counting errors. If there was a break-in, we didn't know how it extended, nor who was doing it. Roy Kerth blasted us. Why are you wasting my time? You don't know anything and u haven't proven a whit. Go back and find out. Show me oof."

So how do you find a hacker? I figured it was simple: just tch for anyone using Sventek's accounts, and try to trace their nnection.

I spent Thursday watching people log into the computer. I ote a program to beep my terminal whenever someone conted to the Unix computer. I couldn't see what each user was ing, but I could see their names. Every couple minutes my terinal beeped, and I'd see who had logged in. A few were friends, ronomers working on research papers or graduate students gging away on dissertations. Most accounts belonged to angers, and I wondered how I could tell which connection ght be a hacker.

At 12:33 on Thursday afternoon, Sventek logged in. I felt a h of adrenaline and then a complete letdown when he disapared within a minute. Where was he? The only pointer left for was the identifier of his terminal: he had used terminal port 3.

Sitting behind a computer terminal, fingers resting on his keyrd, someone was connecting into our lab. My Unix computer e him the address of port tt23.

Well, that's a start. My problem was to figure out which physiwires corresponded to the logical name tt23.

Terminals from our laboratory and modems from dial-in tele-

phones are all assigned "tt" labels, while network connections show up as "nt." I figured that the guy must be either from our laboratory or dialing in on a phone line over a modem.

For a few seconds, I'd sensed a hesitant feeler into our computer. Theoretically, it must be possible to trace the path from computer to human. Someone must be at the far end of that connection.

It would take six months to track that path, but my first step was to trace the connection out of the building. I suspected a dial-in modem, connected from some telephone line, but it conceivably might be someone at the laboratory. Over the years, well over five hundred terminals had been wired in, and only Paul Murray kept track. With luck, our homegrown hardware connections were documented better than the home-brew accounting software.

Paul's a reclusive hardware technician who hides in thickets of telephone wire. I found him behind a panel of electronics, connecting some particle detector to the lab-wide ethernet system. Ethernets are electronic pipelines connecting hundreds of small computers. A few miles of orange ethernet cable snaked through our lab, and Paul knew every inch of it.

Cursing me for surprising him in the middle of soldering a wire, he refused to give me any help until I proved that I had a legitimate need to know. Aw, hell. Hardware technicians don't understand software problems, and software jockeys know nothing about hardware.

Years of ham radio had taught me to solder, so Paul and I had at least one common denominator. I picked up his spare soldering iron and earned his grudging respect after a few minutes of burning my fingers and squinting. Finally, he disentangled himself from the ethernet cables and showed me around the LBL communications switchyard.

In this roomful of wires, the telephones, intercoms, radios, and computers were all interconnected by a tangle of cables, wires, optical fibers, and patch panels. The suspicious port tt23 entered this room and a secondary computer switched it to one of a thousand possible terminals. Anyone dialing into the lab would be

randomly assigned to a Unix port. The next time I saw a suspicious character, I'd have to run over to the switchyard and unwind the connection by probing the switching computer. If he disappeared before I disentangled the connection, well, tough. And even if I did succeed, I'd only be able to point to a pair of wires entering the laboratory. I'd still be a long way from the hacker.

By lucky accident, though, the noontime connection had left some footprints behind. Paul had been collecting statistics on how many people used the switchyard. By chance he had recorded the port numbers of each connection for the past month. Since I knew the time when Sventek was active on port tt23, we could figure out where he came from. The printout of the statistics showed a one-minute 1200-baud connection had taken place at 12:33.

1200 baud, huh? That says something. The baud rate measures the speed that data flows through a line. And 1200 baud means 120 characters per second—a few pages of text every minute.

Dial-up modems over telephone lines run at 1200 baud. Any lab employee here on the hill would run at high speed: 9600 or 19,200 baud. Only someone calling through a modem would let their data dribble out a 1200-baud soda straw. And the anonymity and convenience of these dial-in lines are most inviting to strangers. So pieces were beginning to fit together. I couldn't prove that we had a hacker in the system, but someone dialed into our lab and used Sventek's account.

Still, the 1200-baud connection was hardly proof that a hacker entered our system. An incomplete trace, especially one that went no farther than my building, would never convince my boss that something was up, something weird. I needed to find incontrovertible evidence of a hacker. But how?

Roy Kerth had shown me the high-energy particle detectors attached to the Bevatron: they find jillions of subatomic interactions, and 99.99 percent are explainable by the laws of physics. Spending your time exploring each particle trail will lead you to conclude that all the particles obey known physics, and there's nothing left to discover. Alternatively, you could throw away all

the explainable interactions, and only worry about those that don't quite satisfy the canonical rules.

Astronomers, distant cousins of high-energy physicists, work along similar lines. Most stars are boring. Advances come from studying the weirdies—the quasars, the pulsars, the gravitational lenses—that don't seem to fit into the models that you've grown up with. Knowing cratering statistics on the planet Mercury tells you how often the planet was bombarded in the early solar system. But study the few craters intersected by scarps and ridges and you'll learn how the planet shrank as it cooled during its first billion years. Collect raw data and throw away the expected. What remains challenges your theories.

Well, let's apply this way of thinking to watching someone visiting my computer. I've got a terminal on my desk, and can borrow a couple others. Suppose I just watched the traffic coming into the computer center. There's about five hundred lines entering the system. Most of these lines run at 9600 baud, or around one hundred fifty words per second. If half the lines are used at any time, I'd have to read well over ten thousand pages every minute. Right. No way could I monitor that kind of traffic on my terminal.

But the high-speed lines come from people at LBL. We'd already traced one suspicious connection to a 1200-baud line. There are fewer of them (we can't afford too many incoming phone lines), and they're slower. Fifty lines at 1200 baud might generate a hundred pages a minute, still far too fast to watch on the screen of my terminal. I might not be able to watch fifty people running at once, but maybe I could print out all their interactive sessions, and read the piles of paper at my leisure. A paper printout would provide hard proof of someone messing around; if we found nothing suspicious, we could drop the whole project.

I'd record everything that happened during each 1200-baud connection. This would be technically challenging—since I didn't know which line the hacker was calling, I'd have to monitor four dozen. More worrisome was the ethical problem of monitoring our communications. Did we have the right to watch the traffic running through our lines?

My sweetheart, Martha, was just finishing law school. Over a

deep-dish pizza, we talked about the implications of someone breaking into a computer. I wondered how much trouble I'd be in by listening to incoming traffic.

"Look," she mumbled, burning the roof of her mouth on the vulcanized mozzarella. "You're not the government, so you don't need a search warrant. The worst it would be is invasion of privacy. And people dialing up a computer probably have no right to insist that the system's owner not look over their shoulder. So I don't see why you can't."

So with a clear conscience, I started building a monitoring system. We had fifty 1200-baud lines, and a hacker might be using any of them. I had no equipment designed to record the traffic.

But there's an easy way to record a hacker's activity. Modify the Unix operating system so that whenever a suspicious person logged in, the system records all the keystrokes. This was tempting because I only had to add some lines of code to the Unix daemon software.

The daemons themselves are just programs that copy data from the outside world into the operating system—the eyes and ears of Unix. (The ancient Greek daemons were inferior divinities, midway between gods and men. In that sense, my daemons are midway between the god-like operating system and the world of terminals and disks.)

I could split the daemon's output like a T-joint in a pipe, so the hacker's keystrokes would simultaneously go to both the operating system and a printer. Software solutions are simple and elegant.

"Muck with the daemons at your own risk," Dave Cleveland said. "Just respect their timing needs."

Wayne also warned me, "Look, if you goof up, you'll break the system for sure. It will turn the system into molasses, and there's no way you'll follow everything that happens. Just wait till you see the system console print out 'Panic kernel mode interrupt'—don't come crying on my shoulder!"

Dave chipped in, "Hey, if your hacker has any Unix experience, he's bound to notice a change in the daemons."

That convinced me. A sharp systems person would notice that

we'd changed the operating system. The moment the hacker knew someone was watching him, he'd trash our databases and scram. Our wiretaps had to be completely undetectable, even to an omnipotent super-user. Silent, invisible monitors to trap the hacker's activity.

Maybe just tape recording the telephone lines would work, but tape recorders didn't feel right, too much of a kludge. We'd have to play them back, and couldn't watch the keystrokes until long after a hacker had disconnected. Finally, where would I find fifty tape recorders?

About the only other place to watch our traffic was in between the modems and the computers. The modems converted the tones of a telephone into electronic pulses, palatable to our computers and the daemons in their operating systems. These modem lines appeared as flat, twenty-five conductor wires, snaking underneath the switchyard's false floor. A printer or personal computer could be wired to each of these lines, recording every keystroke that came through.

A kludge? Yes. Workable? Maybe.

All we'd need are fifty teletypes, printers, and portable computers. The first few were easy to get—just ask at the lab's supplies desk. Dave, Wayne, and the rest of the systems group grudgingly lent their portable terminals. By late Friday afternoon, we'd hooked up a dozen monitors down in the switchyard. The other thirty or forty monitors would show up after the laboratory was deserted. I walked from office to office, liberating personal computers from secretaries' desks. There'd be hell to pay on Monday, but it's easier to give an apology than get permission.

Strewn with four dozen obsolete teletypes and portable terminals, the floor looked like a computer engineer's nightmare. I slept in the middle, nursing the printers and computers. Each was grabbing data from a different line, and whenever someone dialed our system, I'd wake up to the chatter of typing. Every half hour, one of the monitors would run out of paper or disk space, so I'd have to roll over and reload.

Saturday morning, Roy Kerth shook me awake. "Well, where's your hacker?"

Still in my sleeping bag, I must have smelled like a goat. I blinked stupidly and mumbled something about looking at the fifty piles of paper.

He snorted, "Well, before you start poking around those printouts, return those printers. You've been running around here like a maniac swiping equipment used by people who are getting work done. You've pissed off a dozen astronomers. Are *you* getting work done? No. Whaddya think this place is, your own personal sandbox?"

Bleary-eyed, I dragged each printer back to its rightful owner. The first forty-nine showed nothing interesting. From the fiftieth trailed eighty feet of printout. During the night, someone had sneaked in through a hole in the operating system.

8

AND JUST IN TIME. WEDNESDAY, SEPTEMBER 10, AT 7:51 A.M., the hacker appeared in our system for six minutes. Long enough to ring the alarm on my terminal, but not enough time to do anything about it. I had stayed at home that night: "Five days at the lab are enough," Martha said.

I wasn't at the lab to watch, but the printer saved three pages of the hacker's trail. He had logged into our Unix-4 computer as Sventek. Well, I understand that—he had Sventek's password, and had entered from Tymnet.

But he didn't hang around my Unix-4 computer. Instead he leapfrogged through it and landed in the Milnet. Now it was no news flash that the Milnet existed—it's a part of the Internet, a computer network that cross-links a hundred other networks. From our Unix computer, we can reach the Internet, and from there, the Milnet.

The Milnet belongs to the Department of Defense.

My hacker connected to Milnet address 26.0.0.113, logged in there as "Hunter," and checked that he had a copy of Gnu-Emacs, then disappeared.

When I biked in around noon, there was no trace to follow upstream. Bu the hacker left an indelible trail downstream. Where was that Milnet address? The Network Information Center decoded it for me: the U.S. Army Depot, in Anniston, Alabama. The home of the Army's Redstone missile complex, two thousand miles away from Berkeley.

In a couple minutes, he'd connected through our lab and into some Army base. The printout left little doubt that this was the hacker. Nobody but the hacker would use Sventek's account. And who else would check for the Gnu-Emacs security hole on some computer in Alabama?

Nobody was around to tell me to ignore it, so I called Anniston information. Sure enough, the Anniston Army Depot had a computer center, and eventually I found Chuck McNatt, the Anniston Unix wizard.

"Hi, Chuck. You don't know me but I think we found someone screwing around with your computer."

"Who are you? How do I know *you're* not trying to break in?"

After a few minutes of disbelief, he asked for my phone number, hung up, and called me back. Here's someone that doesn't trust strangers. Or did he call me back on a secure phone line?

"Bad news," I said. "I think I saw someone breaking into your system."

"Aw, hell—that son of a bitch, Hunter?"

"Yeah. How'd you know?"

"I've seen his ass before."

Chuck McNatt explained through a thick Alabama drawl that the Army's Redstone Missile Arsenal kept track of its supplies on a couple of Unix computers. To get orders processed quickly, they'd hooked up to Chuck's computer at the Anniston Depot. Most of their traffic was news updates—not many people logged in remotely.

One Saturday morning, to escape the August heat, Chuck had gone into work and checked the users on his system. Someone named Hunter was using up an enormous amount of computing time. Surprised to see anyone on a Saturday, Chuck had flashed a message on Hunter's screen, saying, "Hey! Identify yourself!"

The mysterious Hunter typed back, "Who do you think I am?"

Chuck wasn't that gullible. He sent another message, "Identify yourself now or I'll knock you off the system!"

Back came Hunter's reply, "I cannot answer."

"So I bumped him off the machine," Chuck said. "We called the FBI, but they didn't give a damn. So we talked CID into tracing every damn connection coming in on our phone lines."

"What's the CID—Chestnut Inspection Department?"

"Be serious," Chuck said. "The CID's the Army's cops. The criminal investigation division. But they're not doin' much."

"No classified material lost, huh?"

The FBI in Montgomery, Alabama, told Chuck about the same story as Oakland had told me. They'd investigate when a million dollars disappeared. Until then, don't bother 'em. Computer crimes weren't sexy.

"Who'd you find?"

"The weirdest thing," Chuck continued. "I caught Hunter sneaking into my computer two or three more times, but my telephone recorders didn't show a thing."

"Betcha I know why. He's been coming in through your back door. Your Milnet connection. Some hacker's been breaking into our system, and he got into your computer this morning."

Chuck cursed—he'd missed the three-minute connection. He had set traps on all his telephone lines, but hadn't thought to watch his network links.

"We're trying to find out who's hacking our system," I said. "We figure he's a student here in Berkeley, and we're gearing up to track him down. Our first trace points to Oakland or Berkeley."

"Well, I know how you feel. We all suspect it's a student here in Alabama," Chcuk said. "We thought about closing up, but we're out to git him. I'd rather see him behind bars than behind a terminal."

For the first time, I worried for this hacker's welfare. If the Army caught the guy, he'd have a rough time.

"Hey, Chuck, have I got a kicker for you. Betcha this guy's super-user on your system."

"Naw. He might have stolen an account, but no way he'd get to be super-user. We're an Army base, not some goofball college."

I let the swipe at Berkeley pass. "He went looking for your Gnu-Emacs move-mail file."

"Yeah. So what?"

"What do you know about the nesting habits of cuckoos?" I explained the workings of the Gnu-Emacs security hole.

Chuck was taken aback. "You mean we've had this hole since

White Sands sent us this Gnu file?" Chuck whistled. "I wonder how long he's been poking around." He understood the hole and the implications.

The hacker listed files at the Anniston system. Judging from the dates of these files, he'd been in Anniston's computers since early June. For four months, an illegitimate system manager used an Alabama Army computer. Yet he'd been discovered by accident, not through some logic bomb or lost information.

No obvious damage.

Looking closely at the morning's printout, I saw that the hacker had executed the change password command. On the Anniston computer, he had changed Hunter's password to be "Hedges." A clue at last: of zillions of possible passwords, he'd chosen Hedges. Hedges Hunter? Hunter Hedges? A hedge hunter? Time to flip through the H's in the Berkeley telephone book.

Three phone calls to H. Hunter turned up Harold, Heidi, and Hilda Hunter. "Hi, are you interested in a free subscription to *Computer Reviews?*" No dice. None of them said they cared about computers.

What does a physics lab in Berkeley have in common with an Army depot in Anniston, Alabama? You couldn't find more politically opposite locations: a good-old-boy Army base and a radical hippie town. Yet technically, we shared quite a bit. Both our computers ran Unix and connected through the Milnet network.

But wait—Anniston's system ran AT&T Unix, not the Berkeley dialect. If I believed Dave Cleveland, then the hacker was at home on Anniston's system. Might it be a Southern hacker?

9

I COULDN'T STAND THE STERILE, FLUORESCENT LIGHTED halls of the lab anymore, so I went outside to look at the panoramic view of the Bay Area below me. The Berkeley campus lay directly beneath my laboratory. Once the home of the free speech movement and antiwar protests, the campus is still known for its wild politics and ethnic diversity. If I were a little closer, I could probably hear the Young Republicans baiting the Socialist Workers, while the Chinese Club looked on in amazement.

Smoky coffeehouses crowded next to the campus, where haggard grad students scribbled their theses, fueled by espresso. At nearby ice cream shops, giggling sorority girls mingled with punks in black leather and spiked hair. Best of all—Berkeley's bookstores.

From the front of the lab, I could look farther south, to the pleasant streets of north Oakland, where we lived. There I shared an old bungalow with an assortment of zany roommates. Across the bay, shrouded in fog, was San Francisco—Oz.

Three years ago, Martha had moved here to study law and I'd tagged along. She'd been worth crossing the country for. She was a damned good hiking partner and caver. I first met her when I fell thirty feet inside a cave; she came to the rescue, rappelling down to where I lay incapacitated by a bad sprain and utter infatuation. My injuries healed, thanks to her chicken soup; my affection for the smart-aleck kid who climbed rocks so fearlessly ripened into love.

Now we lived together. She actually enjoyed studying law. She didn't want to be a lawyer, but a legal philosopher. She was obsessed with aikido, a Japanese martial art, and often came home bruised but grinning. She cooked, gardened, pieced quilts, did carpentry, and made stained-glass windows. For all our zaniness, we wallowed in disgustingly wholesome domestic bliss.

I bicycled home and told Martha about the Alabama break-in, speculating about who might be behind it.

"So there's technocratic vandals," she said. "What else is new?"

"That's news in itself. Technicians now have incredible power to control information and communication," I said.

"So what? Somebody's always had control over information, and others have always tried to steal it. Read Machiavelli. As technology changes, sneakiness finds new expressions."

Martha was still giving me a history lesson when Claudia bustled in, complaining about her fifth graders. Life in Berkeley usually includes a roommate or two. Claudia was ours, and a perfect one at that. She was generous and cheerful, eager to share her life, her music, and her kitchen gadgets with us. She was a professional violinist eking out a living by playing in two symphony orchestras and a chamber music trio, and giving lessons to kids.

Claudia was seldom still or quiet. In her few moments between jobs, she simultaneously cooked meals, talked on the phone, and played with her dog.

At first I listened, but soon her voice became like the background chirp of a parakeet while I worried about how malicious this hacker might be. While I'm at home, how do I know what he's up to?

Claudia knew how to take my mind off the hacker: she brought home a video, *Plan 9 from Outer Space*—aliens in tinfoil flying saucers drag vampires from graves.

Wednesday, September 17, was a drizzly Berkeley day. As the only California couple without a car, Martha and I had to bicycle through the rain. On my way into the lab, I visited the switch-

yard, to check for any visits by the hacker. Water dripped off my sopping hair onto the printout, smudging the ink on the paper.

Sometime during the night, someone had connected to our computer, and methodically tried to log into the Unix-4 computer. First they tried to log into the Guest account, using the password "Guest." Then they tried the Visitor account, with password "Visitor"; then accounts Root, System, Manager, Service, and Sysop. After a couple of minutes, the attacker left.

Could this be a different hacker? This guy didn't even try valid accounts like Sventek or Stoll. He simply tried obvious account names and simple passwords. I wondered how often such an attack might succeed.

Not often—with six-letter passwords a hacker had a better chance of winning the lottery than randomly guessing a particular password. Since the computer hangs up after a few log-in failures, the attacker would need all night to try even a few hundred possible passwords. No, a hacker couldn't magically enter my system. He'd need to know at least one password.

By 12:29, most of my clothes had dried off, though my sneakers still squished. I was part way into a soggy bagel, and most of the way through an astronomy article about physics of the icy satellites of Jupiter. My terminal beeped. Trouble in the switchyard. A quick (though squeaky) trot down the hallway let me watch the hacker connect into our system as Sventek.

Again the adrenaline rush: I called Tymnet and quickly found Ron Vivier. Ron started the trace, and I huddled over the Decwriter, which now tapped out the hacker's commands.

The hacker wasted no time. He issued commands to show all the active users and any background jobs running. He then fired up Kermit.

Named after the Muppet hero, Kermit is the universal language for connecting computers together. In 1980, Frank da Cruz of Columbia University needed to send data to a number of different computers. Instead of writing five different, incompatible programs, he created a single standard to exchange files between any systems. Kermit's become the Esperanto of computers.

Absentmindedly chewing on a bagel, I watched as the hacker

used Kermit to transfer a short program into our Unix computer. Line by line, faithful Kermit reassembled it, and soon I could read the following program:

```
echo -n "WELCOME TO THE LBL UNIX-4 COMPUTER"
echo -n "PLEASE LOG IN NOW"
echo -n "LOGIN:"
read account_name
echo -n "ENTER YOUR PASSWORD:"
(stty -echo; \
read password; \
stty echo; \
echo " "; \
echo $account_name $password >> /tmp/.pub)
echo "SORRY, TRY AGAIN."
```

Yikes! Now here was a strange program! This program, when installed in our computer, would prompt a user to enter his name and password. An ordinary user who ran this program would see on his screen:

```
WELCOME TO THE LBL UNIX-4 COMPUTER
PLEASE LOGIN NOW
Login:
```

His terminal would then wait until he entered his account name. After he typed his name, the system responds:

```
ENTER YOUR PASSWORD:
```

And he'd naturally type in his password. The program then stashes the unlucky user's name and password into a file, tells the user,

```
SORRY, TRY AGAIN
```

and then disappears.

Thinking they've mistyped their passwords, most people will just try to log in again. By then, their password will already have been stolen.

Four thousand years ago, the city of Troy fell when Greek soldiers snuck in, hidden inside the Trojan horse.

Deliver a gift that looks attractive, yet steals the very key to your security. Sharpened over the millennia, this technique still works against everyone except the truly paranoid.

The hacker's Trojan horse program collected passwords. Our visitor wanted our passwords badly enough to risk getting caught installing a program that was bound to be detected.

Was this program a Trojan horse? Maybe I should call it a mockingbird: a false program that sounded like the real thing. I didn't have time to figure out the difference—within a minute, he was bound to install his program in the systems area, and start it running. What should I do? To disable it would show him that I was watching him. Yet doing nothing would give him a new password every time someone logged in.

But legitimate super-users have power too. Before the hacker could run his program, I changed one line in it, making it look like he'd made a trivial error. Then I diddled a couple system parameters to slow down the system. Slow enough that the hacker would need ten minutes to rebuild his program. Enough time to let us respond to this new attack.

I shouted down the hall for Guru Dave.

"What do you feed a Trojan horse?"

Dave came running. We shifted the computer into high speed, and prepared a fodder of bogus accounts and false passwords.

But our panic wasn't necessary. The hacker rebuilt his Trojan horse, but didn't install it properly. Dave instantly realized that it had been placed in the wrong directory. His Trojan horse would be happy in standard AT&T Unix, but couldn't cavort in the fields of Berkeley Unix.

Dave grinned. "I won't say, 'I told you so,' but we're watching someone who's never been to California. Every Unix jockey on the West Coast would use Berkeley style commands, yet your hacker's still using AT&T Unix."

Dave descended from his tower to explain what he meant. "The spelling of his commands is different from Berkeley Unix. But so is the very feel of the program. Kinda like how you can tell

that a writer is British rather than American. Sure, you'll see words like 'colour' and 'defence,' but you can feel the style difference as well."

"So what's the difference?" I asked.

Dave sneered, "The hacker used the command 'read' to get keyboard data. Any civilized programmer would use the 'set' command." For Dave, civilized computers spoke Berkeley Unix. All others were uncouth.

The hacker didn't realize this. Confident that he'd put his Trojan horse in the right pasture, he ran it as a background process, and logged off. Before he disconnected, Ron Vivier had traced the hacker through Tymnet's network, and into an Oakland, California, telephone line. The dust hadn't yet settled on our court order, so we couldn't start the phone trace.

The hacker had left, but his Trojan horse stayed behind, running as a background task. As Dave predicted, it collected no passwords, for it had been installed in a place that wasn't referenced during log-in. Sure enough, twenty minutes later, the hacker reappeared, searched for a collection of passwords, and must have been disappointed to find his program had failed.

"Look, Dave, the poor guy needs your help," I said.

"Right. Should we send him some electronic mail telling him how to write a Trojan horse program that works?" Dave replied.

"He's got the basics right—imitating our log-in sequence, asking for the username and password, then storing the stolen information. All he needs is a few lessons in Berkeley Unix."

Wayne stopped by to watch the hacker flounder. "Aw, what do you expect? There's just too many varieties of Unix. Next time make it easier on those inept hackers, and give them Digital's VMS operating system. It might not be easier to hack, but at least it's standardized. IOTTMCO." Intuitively obvious to the most casual observer.

Wayne had a good point. The hacker's Trojan horse attack had failed because the operating system wasn't exactly what he was accustomed to. If everyone used the same version of the same operating system, a single security hole would let hackers into all the computers. Instead, there's a multitude of operating systems:

Berkeley Unix, AT&T Unix, DEC's VMS, IBM's TSO, VM, DOS, even Macintoshes and Ataris. This variety of software meant that no single attack could succeed against all systems. Just like genetic diversity, which prevents an epidemic from wiping out a whole species at once, diversity in software is a good thing.

Dave and Wayne continued bickering as they left the switchyard. I hung around a few more minutes, reloading paper. At 1:30 P.M., the hacker reappeared; I was still adjusting the printer when he started typing.

This second session was predictable. Our visitor looked at his special file for passwords and found none. He listed his Trojan horse program and tested it a couple times. It didn't work. Apparently, he didn't have a Dave Cleveland for help. Obviously frustrated, he erased the file and logged off in a couple minutes.

But even though he'd been on for only a few minutes, Tymnet managed to trace him, again into Oakland. Ron Vivier, who'd traced Tymnet's connections, apparently welcomed any emergency that might extricate him from a meeting, so he jumped when I called. If we could only get the phone company to continue the trace, we could wrap up everything in a couple days.

Dave felt he could exclude anyone coming from the West Coast. Chuck in Anniston suspected a hacker from Alabama. Tymnet's traces pointed to Oakland.

Me? I didn't know.

10

OUR TYMNET TRACES REACHED INTO OAKLAND, AT VARIous times the home of Jack London, Ed Meese, and Gertrude Stein. A twenty-minute bike ride from the Berkeley campus led to the Oakland Paramount Theater, with its sublime art-deco architecture and eye-popping murals. A few blocks away, in the basement of an ugly modern building, Tymnet rents space for fifty dialup modems. Ron Vivier had traced the hacker from our lab into this bank of modems. Now it was my local telephone company's turn.

A two-inch-thick cable runs under Broadway, connecting Tymnet's modems to an unmarked, windowless building. There, Pacific Bell's Franklin office houses an electronic switch to handle ten thousand telephone lines in area code 415 with the prefix 430. Tymnet leases fifty of these lines.

From somewhere, the hacker had dialed 415/430-2900. The path to our mysterious visitor led to Pac Bell's ESS-5 switch.

Across San Francisco Bay, Lee Cheng's office overlooks a grungy alley off Market Street. Lee is Pac Bell's bloodhound; from his office or up on a telephone pole, he traces phone lines.

Lee's degree is in criminology, and his graduate work is in accident reconstruction and causation. But eight years of telephone tracing gives him an engineer's view of the phone company and a cop's view of society. To him, communities are split by area codes, exchanges, and trunk lines, as well as precincts and neighborhoods.

tired of this after reading a few scientific papers, several boring research proposals, and a detailed description of how to measure the nuclear cross section of some beryllium isotope. Yawn. Breaking into computers sure wasn't the key to power, fame, and the wisdom of the ages.

Getting into our two Unix systems hadn't satisfied my voracious foe. He'd tried hurdling the moat around our secured Unix-8 computer, but failed—Dave had sealed off that machine. Frustrated at this, he printed a list of remote computers available from our site.

Nothing secret there, just the names, phone numbers, and electronic addresses for thirty Berkeley computers.

12

WITH THE FULL MOON, I EXPECTED MORE HACKING AND planned on sleeping under the desk. The hacker didn't show up that evening, but Martha did. Around seven, she biked up, bringing a thermos of minestrone and some quilting to keep me occupied. There's no shortcut to hand stitching a quilt. Each triangle, square, and parallelogram must be cut to size, ironed, assembled, and sewn to its neighbors. Up close, it's hard to tell the pieces from the scraps. The design becomes visible only after the scraps are discarded, and you stitch the pieces together. Hmmm. A lot like understanding this hacker.

Around 11:30, I gave up my watch. If the hacker wanted to show up at midnight, the printers would catch him anyway.

The next day, the hacker turned up once. I missed him, preferring to share lunch with Martha just off campus. It was worth it: on a street corner, a jazz band played 1930s tunes.

The singer belted out some '30s ditty, "Everybody loves my baby, but my baby loves nobody but me."

"That's absurd," Martha said between tunes. "Logically analyzed, the singer must be his own baby."

"Huh?" It sounded fine to me.

"Look. 'Everybody' includes my baby. Since 'Everybody loves my baby,' then my baby loves herself. Right?"

"Uh, yeah." I tried to follow.

"But then he says, 'My baby loves nobody but me.' So my

baby, who must love herself, cannot love anyone else. Therefore, my baby must be me."

She explained it twice before I understood. The singer had never learned elementary logic. Neither had I.

By the time I returned from lunch, the hacker was long gone, leaving his trail on a paper printout.

For once, he didn't become super-user. Yes, in his paranoid way, he checked for systems people and monitoring processes, but he didn't sneak through the hole in the operating system.

Instead, he went fishing over the Milnet.

A single isolated computer, out of communication with the world, is immune to attack. But a hermit computer has limited value; it can't keep up with what's happening around it. Computers are of the greatest use when they interact with people, mechanisms, and other computers. Networks let people share data, programs, and electronic mail.

What's on a computer network? What do computers have to say to each other? Most personal computers satisfy the needs of their owners, and don't need to talk to other systems. For word processing, accounting spreadsheets, and games, you really don't need any other computers. But hook up a modem to your computer, and your telephone will report the latest from the stock market, news wires, and rumor mills. Connecting to another computer gives you a powerful way to tune in the latest news.

Our networks form neighborhoods, each with a sense of community. The high-energy physics networks transfer lots of data about subatomic particles, research proposals, as well as gossip about who's pushing for a Nobel prize. Unclassified military networks probably pass along orders for shoes, requests for funding, and rumors of who's jockeying for base commander. Somewhere, I'll bet there are classified networks, to exchange secret military orders and top secret gossip like who's sleeping with the base commander.

These electronic communities are bounded by the limits of their communications protocols. Simple networks, like public bulletin boards, use the simplest ways to communicate. Anyone with a personal computer and a telephone can link into them.

Advanced networks require leased telephone lines and dedicated computers, interconnecting hundreds or thousands of computers. These physical differences set boundaries between networks. The networks themselves are linked together by gateway computers, which pass reformatted messages between different networks.

Like Einstein's universe, most networks are finite but unbounded. There's only a certain number of computers attached, yet you never quite reach the edge of the network. There's always another computer down the line. Eventually, you'll make a complete circuit and wind up back where you started. Most networks are so complicated and interwoven that no one knows where all their connections lead, so most people have to explore to find their way around.

Our lab's computers connect to a dozen computer networks. Some of them are local, like the ethernet that ties computers in one building to a lab next door. Other nets reach to an extended community: the Bay Area Research Net links a dozen northern California universities. Finally, the national and international networks let our scientists connect to computers around the world. But the premier network is the Internet.

In the mid 1950s, the Federal government started building the interstate highway system, a twentieth-century marvel of pork-barrel public-works politics. With memories of wartime transportation shortages, military leaders made certain that the interstate system could handle tanks, military convoys, and troop carriers. Today, few think of interstate highways as a military system, though they're just as capable of sending tanks across the country as trucks.

With the same reasoning, the Department of Defense began developing a network to link military computers together. In 1969, the Defense Advanced Research Projects Agency's (DARPA) experiments evolved into the Arpanet and then into the Internet: an electronic highway interconnecting a hundred-thousand computers around the world.

In the world of computing, the Internet is at least as successful as the interstate system. Both have been overwhelmed by their

success, and every day carry traffic far beyond what their designers dreamed. Each regularly inspires complaints of traffic jams, inadequate routes, shortsighted planning, and inadequate maintenance. Yet even these complaints reflect the phenomenal popularity of what was an uncertain experiment only a few years ago.

At first, DARPA's network was simply a testbed to prove that computers could be linked together. Since it was seen as an unreliable experiment, universities and laboratories used it, and mainstream military people ignored it. After eight years, only a few hundred computers connected into the Arpanet, but gradually, others were attracted by the network's reliability and simplicity. By 1985 the network directory listed tens of thousands of computers; today, there must be over one hundred thousand. Taking a census of networked computers would be like counting the cities and towns reachable from the interstate system—it's hard to name many places which can't be reached via some convoluted route.

The network's growing pains have been reflected in name changes. The first Arpanet was a backbone connecting random university, military, and defense contractor computers. As military people grew to depend on the network for carrying messages and mail, they decided to split the network into a military portion, the Milnet, and a research section, the Arpanet.

But there's not much difference between the military and academic nets, and gateways let traffic flow between them. Indeed, any Arpanet user can connect to any Milnet computer without so much as an invitation. Together, the Arpanet, Milnet, and a hundred other networks make up the Internet.

There are thousands of university, commercial, and military computers connected through the Internet. Like buildings in a city, each has a unique address; most of these addresses are registered at the Network Information Center (NIC) in Menlo Park, California. Any one computer may have dozens or hundreds of people using it, so individuals as well as computers are registered in the NIC.

The NIC's computers provide a directory: just connect to the NIC and ask for someone, and it'll tell you where they're located. They don't have much luck keeping their database up to date

(computer people change jobs often), but the NIC still serves as a good phone directory of computer people.

During my lunch break, the hacker ducked into the NIC. Our printer quietly saved the session as he searched the NIC for the abbreviation, "WSMR":

```
9
LBL> telnet NIC.ARPA The hacker asks for the Network Information Center
Trying . . .
Connected to 10.0.0.51.
Escape character is '^]'.
+---------------------DDN Network Information Center---------------------
|
| For user and host information, type: WHOIS <carriage return>
| For NIC information, type: NIC <carriage return>
|
+-------------------------------------------------------------------------
@ whois wsmr He searches for WSMR
White Sands Missile Range      WSMR-NET-GW.ARMY.MIL      26.7.0.74
White Sands Missile Range      WSMR-TRAPS.ARMY.MIL       192.35.99.2
White Sands Missile Range      WSMR-AIMS.ARMY.MIL        128.44.8.1
White Sands Missile Range      WSMR-ARMTE-GW.ARMY.MIL    128.44.4.1
White Sands Missile Range      WSMR-NELARMY.MIL          128.44.11.3
```

WSMR? White Sands Missile Range. With two commands and twenty seconds, he found five computers at White Sands.

Astronomers know Sunspot, New Mexico, as one of the finest solar observatories. Clear skies and great telescopes make up for the utter isolation of Sacramento Peak, a few hundred miles south of Albuquerque. The only road to the observatory runs through White Sands, where the Army tests their guided missiles. Once, when I was studying the solar corona, an observing run took me to Sunspot, past the desolation of White Sands. The locked gates and guardhouses discourage onlookers; if the sun doesn't fry you, the electric fences will.

I'd heard rumors that the Army was designing rockets to shoot down satellites. Seemed like an SDI/Star Wars project, but civilian astronomers can only guess. Maybe this hacker knew more about White Sands than I did.

No doubt, though, that the hacker wanted to know more about White Sands. He spent ten minutes trying to log into each of their computers, connecting to them over the Internet.

The printer recorded his steps:

```
LBL> telnet WSMR-NET-GW.ARMY.MIL      Connect to a White Sands
Trying . . .                                  computer
Connected to WSMR-NET-GW.ARMY.MIL

4.2 BSD UNIX
Welcome to White Sands Missile Range
login: guest                          Try the guest account
Password: guest                       Guesses a password
Invalid password, try again           But no luck
login: visitor                        Try another likely account name
Password: visitor
Invalid password, try again           No luck
login: root                           He tries yet another account
Password: root
Invalid password, try again           Still no luck
login: system                         And a fourth try
Password: manager
Invalid password, disconnecting after 4 tries
```

For each computer, he tried to log in as guest, visitor, root, and system. We saw him failing, time after time, as he tried to guess passwords. Perhaps those accounts were valid; the hacker couldn't enter them because he didn't know the right passwords.

I smiled at the printout. No doubt, the hacker wanted to get into White Sands. But they didn't fool around with security. Between their electric fences and passwords, neither tourist nor hacker could enter. Someone at White Sands had locked their doors.

With a snicker, I showed his attempts to the boss, Roy Kerth.

"Well, what do we do about it?" I asked. "Since he didn't get into White Sands, should we tell them?"

"Hell, yes, we'll tell them," Roy responded. "If someone tries to break into my neighbor's house, I'll tell 'em. I'll call the cops, too."

I asked what cops were in charge of the Internet.

"Damned if I know," Roy said. "But here's our policy, from here out: anyone that's attacked, we tell them. I don't care if the hacker didn't get in, you call them on the phone and tell them. Remember, keep this out of electronic mail. And find out who the cops are."

"Yessir."

It took only one phone call to find out that the FBI wasn't policing the Internet. "Look, kid, did you lose more than a half million dollars?"

"Uh, no."

"Any classified information?"

"Uh, no."

"Then go away, kid." Another attempt at rousing the feds had failed.

Maybe the Network Information Center would know who policed their net. I called Menlo Park and eventually found Nancy Fischer. To her, the Internet wasn't just a collection of cables and software. It was a living creature, a brain with neurons extending round the world, into which ten thousand computer users breathed life every hour. Nancy was fatalistic: "It's a miniature of the society around us. Sooner or later, some vandal's going to try to kill it."

It seemed that there were no network police. Since the Milnet—now called the Defense Data Network—isn't allowed to carry classified data, nobody paid much attention to its security.

"You ought to be talking to the Air Force Office of Special Investigations," she said. "They're the narcs of the Air Force. Drug busts and murders. Not exactly white-collar crime, but it can't hurt to talk to them. I'm sorry I can't help you, but it's really not my bailiwick."

Three phone calls later, I'm in a conference call with Special Agent Jim Christy of the AFOSI and Major Steve Rudd of the Defense Communications Agency.

Jim Christy made me nervous—he sounded like a narc. "Let me get this straight. Some hacker broke into your computer, then got into an Army computer in Alabama, and is now going for White Sands Missile Range?"

"Yes, that's about what we've seen." I didn't want to explain the Unix Gnu-Emacs security hole. "Our traces aren't complete yet; he might be from California, Alabama, Virginia, or maybe New Jersey."

"Oh . . . you're not shutting him out so that you can catch the bastard." He was ahead of me.

"And if we close him out, he'll just enter the Internet through some other hole."

Steve Rudd, on the other hand, wanted the hacker nailed. "We can't let this continue. Even without classified information, the Milnet's integrity demands that spies be kept out."

Spies? My ears pricked up.

The narc spoke next. "I don't suppose the FBI has lifted a finger."

I summarized our five calls to the FBI in one word.

Almost apologetically, Jim Christy told me, "The FBI isn't required to investigate every crime. Probably they look at one in five. Computer crimes aren't easy—not like kidnapping or bank robbery, where there's witnesses and obvious losses. Don't blame them for shying away from a tough case with no clear solution."

Steve pressed Jim. "OK, so the FBI won't do anything. How about AFOSI?"

Jim answered slowly, "We're the Air Force computer crime investigators. We usually hear about computer crimes only after a loss. This is the first one that we've come across in progress."

Steve cut in, "Jim, you're a special agent. The only difference between you and an FBI agent is your jurisdiction. Doesn't this fall in your court?"

"It does. It's a strange case that falls in several courts." Over the phone, I could almost hear Jim think. "We're interested, all right. I can't tell if this is a serious problem or a red herring, but it's well worth investigating."

Jim continued, "Look, Cliff. Each agency has thresholds. Our resources are finite so we're forced to choose what we investigate. That's why the FBI asked you about the dollar loss—they're looking to get the most bang for their effort. Now if classified stuff gets stolen, it's a different story. National security doesn't equate to dollars."

Steve interrupted, "But unclassified information can also equate to national security. The problem is convincing law enforcement people."

"So what'll you do?" I asked.

"Right now, there's really not much we can do. If this hacker's using the military networks, though, he's walking on our territory. Keep us informed and we'll sharpen our stingers."

In hopes of encouraging AFOSI, I sent Jim a copy of my logbook, and samples of the hacker's printouts.

After this conversation, Jim Christy explained about the Milnet. What I called the Milnet, Jim knew as the unclassified Defense Data Network, run by the Defense Communications Agency. "The Department of Defense runs the Milnet for all the services—Army, Navy, Air Force, and Marines. That way, each service has equal access to the network, and you'll find computers from every branch on the net."

"So why is Steve Rudd in the Air Force?"

"He's really a purple-suiter—he works for all three branches. Naturally, when he smelled a problem, he called the Air Force investigators."

"And you work full time on computer crime?"

"You betcha. We're watching ten thousand Air Force computers."

"Then why can't you wrap up this case in a snap?"

Jim spoke slowly. "We've got to clearly define our territory. Unless we do, we step on each other's toes. You, Cliff, have no worries that you'll be busted by the OSI—our bailiwick is the Air Force base."

Bailiwicks always belong to someone else.

You know, much as I complained about bailiwicks, I realized that they protected my own rights: our constitution prevents the military from grubbing around civilian affairs. Jim had put this into a new light—sometimes these rights actually do interfere with law enforcement. For the first time, I realized that my civil rights actually limit what police can do.

Whoops. I'd forgotten the boss's instructions to call White Sands. Another few minutes on the phone, and I reached Chris McDonald, a civilian working for the missile range.

I outlined the case—Unix, Tymnet, Oakland, Milnet, Anniston, AFOSI, FBI.

Chris interrupted, "Did you say Anniston?"

"Yes, the hacker was super-user at Anniston Army Depot. It's a little place in Alabama, I think."

"I know Anniston, all right. They're our sister Army base. After we test our missiles, we ship 'em off to Anniston," Chris said. "And their computers come from White Sands as well."

I wondered if this was just coincidence. Perhaps the hacker had read data in the Anniston computers, and realized that the good stuff came from White Sands. Maybe the hacker was sampling every site where the Army stored missiles.

Or maybe the hacker had a list of computers with security holes. "Say, Chris, do you have Gnu-Emacs on your computers?"

Chris didn't know, but he'd ask around. But to exploit that hole, the hacker had to log in first. And the hacker had failed, after trying four times on each of five computers.

White Sands kept their doors locked by forcing everyone on their computers to use long passwords, and to change them every four months. A technician wasn't allowed to choose her own password—the computer assigned unguessable passwords, like "agnitfom" or "nietoayx." Every account had a password, and none could be guessed.

I didn't like the White Sands system. I couldn't remember computer-generated passwords, so I'd write them in my wallet or next to my terminal. Much better to allow people to choose their own passwords. Sure, some people would pick guessable passwords, like their names. But at least they wouldn't complain about having to memorize some nonsense word like "tremvonk," and they wouldn't write them down.

But the hacker got into my system and was rebuffed at White Sands. Maybe random passwords, obnoxious and dissonant, are more secure. I don't know.

I'd followed the boss's orders. The FBI didn't care about us, but the Air Force sleuths were on the case. And I'd notified White Sands that someone was trying to break in. Satisfied, I met

Martha at a vegetarian pizza stand. Over slices of thick-crust spinach and pesto, I described the day's events.

"Vell, Natasha, we have accomplished mission one."

"Vonderful, Boris, vhat a victory. Boris . . . vhat is mission one?"

"We have made rendezvous vith ze secret air force police, Natasha."

"Yes, Boris?"

"Ve have alerted ze missile base to ze counter-counter-intelligence efforts."

"Yes, Boris?"

"And we have ordered ze secret spy pizza."

"But Boris, ven do we catch ze spy?"

"Patience, Natasha. Zat is mission two."

It wasn't until we started walking home that we got to the serious side of our game.

"This thing is getting weirder and weirder," Martha said. "It started out as a hobby, chasing some local prankster, and now you're talking to these military people who wear suits and have no sense of humor. Cliff, they're not your type."

I defended myself stuffily. "This is a harmless and possibly beneficial project to keep them busy. After all, this is what they're supposed to be doing—keeping the bad guys out."

Martha wouldn't let that sit. "Yeah, but what about you, Cliff. What are you doing hanging out with these people? I understand that you have to at least talk to them, but how deeply are you getting involved?"

"Every step makes perfect sense from my point of view," I said. "I'm a system manager trying to protect my computer. If someone hacks into it, I have to chase him. To ignore the bastard will let him wreck other systems. Yes, I'm cooperating with the Air Force police, but that doesn't mean I approve of everything the military stands for."

"Yes, but you have to decide how you want to live your life," Martha said. "Do you want to spend your time being a cop?"

"A cop? No, I'm an astronomer. But here's someone threatening to destroy our work."

18

BY THE END OF SEPTEMBER, THE HACKER WAS APPEARing every other day. Often, he'd pop up his periscope, look around, and disappear in a few minutes. Not enough time to trace, and hardly worth getting excited about.

I was tense and a little guilty. I often passed up dinner at home to sneak in some extra hacker watching.

The only way I could keep following the hacker was by disguising my efforts as real work. I'd muck around with computer graphics to satisfy the astronomers and physicists, then fool with the network connections to satisfy my own curiosity. Some of our network software actually needed my attention, but usually I was just tinkering to learn how it worked. I called other computer centers ostensibly to clear up network problems. But when I'd talk to them, I'd cautiously bring up the subject of hackers—who else had hacker problems?

Dan Kolkowitz at Stanford University was quite aware of hackers in his computer. He was an hour's drive away from Berkeley, but that was an all-day bicycle ride. So we compared notes on the phone, and wondered if we were watching the same rodent gnawing at our systems.

Since I'd started watching my monitors, I'd seen an occasional interloper trying to get onto my computer. Every few days, someone would dial into the system and try to log on as *system* or

guest. These inevitably failed, so I didn't bother following them. Dan had it much worse.

"Seems like every kid in Silicon Valley tries to break into Stanford," Dan moaned. "They find out passwords to legitimate student accounts, then waste computing and connect time. An annoyance, but something we'll have to tolerate so long as Stanford's going to run a reasonably open system."

"Have you thought about clamping down?"

"To really tighten up security would make everyone unhappy," Dan said. "People want to share information, so they make most of the files readable to everyone on their computer. They complain if we force them to change their passwords. Yet they demand that their data be private."

People paid more attention to locking their cars than securing their data.

One hacker in particular annoyed Dan. "Bad enough that he found a hole in Stanford's Unix system. But he had the nerve to call me on the phone. He talked for two hours, at the same time pawing through my systems files."

"Did you trace him?"

"I tried. While he was talking on the phone, I called the Stanford police and the phone company. He was on for two hours, and they couldn't trace it."

I thought of Lee Cheng at Pacific Bell. He needed just ten minutes to trace clear across the country. And Tymnet unwound their network in less than a minute.

We compared the two hackers. "My guy's not wrecking anything," I said. "Just scanning files and using my network connections."

"Precisely what I see. I changed my operating system so that I can watch what he's doing."

My monitors were IBM PC's, not modified software, but the principle was the same. "Do you see him stealing password files and system utilities?"

"Yes. He uses the pseudonym of 'Pfloyd' . . . I bet he's a Pink Floyd fan. He's only active late at night."

This was a difference. I often watched my hacker at noon. As I

thought about it, Stanford was following different people. If anything, the Berkeley hacker seemed to prefer the name, "Hunter," though I knew him by the several different account names he stole.

Three days later, the headlines of the October 3 *San Francisco Examiner* blared, "Computer Sleuths Hunt A Brilliant Hacker." Reporter John Markoff had sniffed out the Stanford story. On the side, the newspaper mentioned that this hacker had also gotten into the LBL computers. Could this be true?

The story described Dan's snares and his inability to catch Stanford's Pfloyd hacker. But the reporter got the pseudonym wrong—the newspaper reported "a crafty hacker using the name 'Pink Floyd.' "

Cursing whoever leaked the story, I prepared to close things up. Bruce Bauer of our lab's police department called and asked if I'd seen the day's paper.

"Yeah. What a disaster. The hacker won't show up again."

"Don't be so sure," Bruce said. "This may be just the break we're looking for."

"But he'll never show up, now that he knows that we know there's a hacker in our system."

"Maybe. But he'll want to see if you shut him out of the computer. And he's probably confident that if he can outwit the Stanford people, he can sneak past us as well."

"Yes, but we're nowhere near tracing him."

"That's actually what I called about. It'll be a couple weeks before we get the search warrant, but I'd like you to stay open until then."

After he hung up, I wondered about his sudden interest. Could it be the newspaper story? Or had the FBI finally taken an interest?

The next day, doubtless thanks to Bruce Bauer, Roy Kerth told me to keep working on following the hacker, though he pointedly said that my regular duties should take precedence.

That was my problem. Every time the hacker showed up, I'd spend an hour figuring out what he did and how it related to his other sessions. Then a few more hours calling people, spreading

the bad news. Then I'd record what happened in my logbook. By the time I'd finished, the day was pretty much wasted. Following our visitor was turning into a full-time job.

In my case, Bruce Bauer's intuition was right. The hacker returned a week after the article appeared. On Sunday, October 12, at 1:41, I was beating my head against some astronomy problem—something about orthogonal polynomials—when my hacker alarm went off.

I ran down the hallway and found him logged into Sventek's old account. For twelve minutes, he used my computer to connect to the Milnet. From there, he went to the Anniston Army base, where he had no trouble logging in as Hunt. He just checked his files and then disconnected.

On Monday, Chuck McNatt from Anniston called.

"I dumped this weekend's accounting logs and found the hacker again."

"Yes, he was on your system for a few minutes. Just long enough to see if anyone was watching." My printouts told the whole story.

"I think I'd better close my doors to him," Chuck said. "There's too much at risk here, and we don't seem to be making headway in tracking him."

"Can't you stay open a bit longer?"

"It's already been a month, and I'm afraid of him erasing my files." Chuck knew the dangers.

"Well, OK. Just be sure that you really eliminate him."

"I know. I'll change all the passwords and check for any holes in the operating system."

Oh well. Others didn't quite have the patience to remain open to this hacker. Or was it foolishness?

Ten days later, the hacker reappeared. I got to the switchyard just as he was trying Anniston.

```
LBL> Telnet ANAD.ARPA
Connecting to 26.1.2.22
Welcome to Anniston Army Depot
login: Hunt
password: jaeger
```

```
Bad login. Try again.
login: Bin
password: jabber
Welcome to Anniston Army Depot.
Tiger Teams Beware!
Watch out for any unknown users
Challenge all strangers using this computer
```

Chuck had disabled the Hunt account, but hadn't changed the password on the system account, *Bin*.

The greeting message warned the hacker that someone had noticed him. He quickly checked his Gnu-Emacs files, and found they had been erased. He looked around the Anniston system and found one file that had been created July 3. A file that gave him super-user privileges. It was hidden in the public directory /usr/lib. An area that anyone could write into. He'd named the file, ".d". The same name he used to hide his files on our LBL system.

But he didn't execute that program. Instead he logged off the Anniston system and disconnected from LBL.

Chuck hadn't noticed this special file. On the phone, he said he'd changed every user's password—all two hundred. But he hadn't changed any of the system passwords like *Bin*, since he assumed he was the only one who knew them. He'd thought that he'd thoroughly eradicated any dangerous files, but he'd missed a few.

That *.d* file at Anniston was a useful benchmark. The hacker had laid this egg on July 3, yet remembered exactly where he'd hidden it three months later.

He didn't guess or hunt around for the *.d* file. No, he went straight for it.

After three months, I can't remember where I stash a file. At least not without a notebook.

This hacker must be keeping track of what he's done.

I glanced at my own logbook. Somewhere, someone was keeping a mirror-image notebook.

A kid on a weekend lark doesn't keep detailed notes. A college joker won't patiently wait three months before checking his prank. No, we were watching a deliberate, methodical attack, from someone who knew exactly what he was doing.

19

EVEN THOUGH YOU HAVE TO COAST SLOWLY BY THE guardhouse, you can reach thirty miles an hour by pedaling down the LBL hill. Tuesday evening I was in no hurry, but pedaled anyway: it's a kicker to feel the wind. A mile downhill, then a rendezvous at the Berkeley Bowl.

The old bowling alley was now a huge fruit and vegetable market, the cheapest place for kiwis and guavas. Year 'round, it smelled of mangoes—even in the fish section. Next to a pyramid of watermelons, I saw Martha knocking some pumpkins, hunting for the filling to our Halloween pie.

"Vell, Boris, ze secret microfilm is hidden in ze pumpkin patch." Ever since I met the CIA, I was a spy in Martha's eyes.

We decided on a dozen little pumpkins for a carving party, and one fresh big one for the pie. After stuffing them in our backpacks, we biked home.

Three blocks from the fruit market, at the corner of Fulton and Ward, there's a four-way stop. With a can of spray paint, someone's changed one stop sign to read, "Stop the CIA." Another, "Stop the NSA."

Martha grinned. I felt uneasy, and pretended to adjust my backpack. I didn't need another reminder of Berkeley politics.

At home, she tossed pumpkins to me, and I stashed them in a box. "What you're missing is a flag," she said, throwing the last one low and inside, "some sort of pennant for chasing hackers."

She ducked into a closet. "I had a bit left over from my costume, so I stitched this together." She unrolled a shirt-sized banner, with a snake coiled around a computer. Underneath, it said, "Don't Tread on Me."

In the weeks before Halloween, both of us sewed furiously to make costumes. I'd made a pope's outfit, complete with miter, scepter and chalice. Martha, of course, kept her costume hidden—you can't be too careful when your roommate uses the same sewing machine.

Next day, I hoisted my hacker-hunter flag just above the four monitors that watched the incoming Tymnet lines. I'd bought a cheap Radio Shack telephone dialer, and connected it to an expensive but obsolete logic analyzer. Together, these waited patiently for the hacker to type in his password, and then silently called my telephone.

Naturally, the flag fell down and got caught in the printer, just as the hacker showed up. I quickly unsnarled the shreds of paper and cloth, just in time to see the hacker change his passwords.

The hacker apparently didn't like his old passwords—*hedges, jaeger, hunter and benson*. He replaced them, one by one, with a single new password, *lblhack*.

Well, at least he and I agreed on what he was doing.

He picked the same password for four different accounts. If there were four different people involved, they'd each have a separate account and password. But here in one session, all four accounts were changed.

I had to be following a single person. Someone persistent enough to return over and over to my computer. Patient enough to hide a poisonous file in the Anniston Army base and return to it three months later. And peculiar in aiming at military targets.

He chose his own passwords. "Lblhack" was obvious. I'd searched the Berkeley phone book for Jaegers and Bensons; maybe I ought to try Stanford. I stopped by the library. Maggie Morley, our forty-five-year-old document-meister, plays rough and tumble Scrabble. Posted on her door is a list of all legal three-letter Scrabble words. To get in, you have to ask her one. "Keeps 'em fresh in my mind," she says.

"Bog," I said.

"You may enter."

"I need a Stanford telephone book," I said. "I'm looking for everyone in Silicon Valley named Jaeger or Benson."

Maggie didn't have to search the card catalog. "You need directories for Palo Alto and San Jose. Sorry, but we don't have either. It'll take a week or so to order 'em."

A week wouldn't slow things down, at the rate I was going.

"Jaeger. A word that's been kind to me," Maggie smiled. "Worth sixteen points, but I once won a game with it, when the 'J' landed on a triple-letter score. Turned into seventy-five points."

"Yeah, but I need it because it's the hacker's password. Hey, I didn't know names were legal in Scrabble."

"Jaeger's not a name. Well, maybe it's a name—Ellsworth Jaeger, the famous ornithologist, for instance—but it's a type of bird. Gets its name from the German word meaning hunter."

"Huh? Did you say, 'Hunter'?"

"Yes. Jaegers are hunting birds that badger other birds with full beaks. They harass weaker birds until they drop their prey."

"Hot ziggity! You answered my question. I don't need the phone book."

"Well, what else can I do for you?"

"How about explaining the relationship between the words *hedges, jaeger, hunter and benson?*"

"Well, Jaeger and Hunter is obvious to anyone who knows German. And smokers know Benson and Hedges."

Omigod—my hacker smokes Benson and Hedges. Maggie had won on a triple-word score.

20

I WAS ALL SET ON HALLOWEEN MORNING. I'D FINISHED my pope's costume, even the miter. Tonight's party would be a gas: pasta with a dozen lunatics, followed by Martha's fantastic pumpkin pie, and an excursion into San Francisco's Castro district.

But first I had to dodge my bosses at the lab. The physicists were ganging up on the computer center, refusing to pay our salaries. Supporting central computing was expensive. The scientists figured that they could buy their own small machines, and avoid the overhead of paying our programming staff.

One of our managers, Sandy Merola, tried to convince them otherwise. "You can hitch a thousand chickens to your plow or one horse. Central computing is expensive because we deliver results, not hardware."

To placate them, Sandy sent me to write a few graphics programs. "You're a scientist. If you can't make 'em happy, at least listen to their problems."

So I spent the morning sitting in the back row of a physics seminar. A professor droned on about the quark function of the proton—something about how each proton has three quarks. I wasn't tired enough to sleep, so I pretended to take notes while thinking about the hacker.

Returning from the seminar, Sandy asked if I'd learned anything.

"Sure." I glanced at my notes. "The distribution function of quarks isn't quantized over the proton. Happy?"

"Be serious, Cliff. What did the physicists say about computing?"

"Not much. They know they need us, but don't want to pay."

"Same as the Air Force," Sandy smiled. "I just got off the phone with one Jim Christy of their Office of Special Investigations."

"Hey, isn't he the narc with the military spooks?"

"Be serious. He's a detective working for the Air Force, please."

"OK, he's an all-American good guy. So what did he say?"

"He says the same thing as our physicists. They can't support us, but they don't want us to go away."

"Did he make any progress with the Virginia phone company?"

"Naw. He called around, and they won't budge without a Virginia search warrant. He checked out the Virginia state law, and the hacker's committing no crime there."

"Breaking into our computer isn't a crime?" I couldn't believe it.

"Breaking into a California computer isn't a crime in Virginia."

"I don't suppose the Air Force can lean on the FBI to get a warrant?"

"Nope. But they want us to keep monitoring, at least until the Air Force decides it's a dead end."

"Did they cough up any dimes?" My time was funded through the grants of astronomers and physicists. They weren't pleased to watch me spend their money chasing some ghost.

"No bucks, nothing but an unofficial request. When I asked for support, Jim gave me the bailiwick story."

Sandy wasn't going to give in. "It's been two months since we started, and nobody's listened to us. Let's stay open for another week, then call it quits."

By five o'clock, I was ready for the Halloween party. On my way out, I checked the floppy disks on the monitors. The printer suddenly started up. There was the hacker. I glanced at the time—17:43:11 PST.

No. Not now. I've got a party to go to. A costume party no less. Can't he choose any other time?

The hacker logged into the old Sventek account, and checked who was on our system. Dave Cleveland was there, running under the alias of Sam Rubarb, but the hacker couldn't know.

He moved over to our accounting files, and collected the past months' files in one place. He scanned that long file, searching for the word "Pink Floyd."

Hmmmm. Interesting. He didn't search for the word "Pfloyd," which was the Stanford hacker's pseudonym. Rather, he searched for the pseudonym that was reported in the newspaper.

My hacker wasn't the same guy as Stanford's. If he were, he wouldn't have to search for "Pink Floyd"—he'd know when he had been active.

In fact, my hacker wasn't even in contact with Stanford's. If the two had met, or even written to each other, my hacker would know to search for "Pfloyd," not "Pink Floyd."

The hacker must have read the news. But it had been almost a month since the article was published. Dave Cleveland must be right: the hacker wasn't from the West Coast.

At 6 P.M., the hacker gave up searching our accounting logs. Instead, he went through our computer onto the Milnet. From there, he went straight for the Anniston army base in Alabama. "Which hole will he sneak into this time?" I wondered.

```
LBL> Telnet Anad.arpa
Welcome to Anniston Computer Center
Login: Hunter
Password: Jaeger
Incorrect login, try again.
Login: Bin
Password: Jabber
Incorrect login, try again.
Login: Bin
Password: Anadhack
Incorrect login, 3 tries and you're out.
```

Chuck McNatt had finally locked him out. By changing all his passwords, Chuck had nailed his door shut. He still might have holes in his system, but this hacker couldn't exploit them.

The hacker didn't give up. He reached over into the building design group.

Some scientists at Lawrence Berkeley Lab worry about how to design energy efficient homes. Most other physicists look down on them—"Yech, applied physics." Protons and quarks are sexy. Saving ten dollars on your monthly heating bill isn't.

The building design group searches for new glasses that let light in, but block the infra-red. They build new insulators to prevent heat leaks through walls. They'd just started analyzing basements and chimneys for thermal efficiency.

The hacker learned this because he dumped all their files. Page after page of thermal emissivity data. Memos about paint absorption in the ultraviolet. And a note saying, "You can move to the Elxsi computer next week."

He didn't need to see that note twice. He interrupted his listing, and commanded my Unix computer to connect him to the Elxsi system.

I'd never heard of this computer. But my computer had. Within ten seconds, he'd made the connection and the Elxsi prompted him for an account name and password. I watched him try to get in:

```
LBL> Telnet Elxsi
Elxsi at LBL
login: root
password: root
incorrect password, try again.
login: guest
password: guest
incorrect password, try again.
login: uucp
password: uucp
WELCOME TO THE ELXSI COMPUTER AT LBL.
```

He got into the UUCP account. No password protection. Wide open.

UUCP is the account for Unix to Unix copying. When one Unix computer wants to copy a file from another, it logs into the UUCP

account and gets the file. People should never be able to connect to this special account. The system manager should disable it from human log-ins.

Worse, this Elxsi had its UUCP account set up with system privileges. It took the hacker only a minute to realize that he'd stumbled into a privileged account.

He didn't lose any time. He edited the password file, and added a new account, one with system manager privileges. Named it *Mark*. "Keep it bland," I thought.

But he didn't know much about this computer. He spent an hour dumping its files, and learned about designing energy efficient buildings. Nothing about the computer itself.

So he wrote a program to time the Elxsi computer. A short C program that measured its speed and reported its word length.

He needed three tries to get his program to work, but finally it flew. He found the Elxsi to have thirty-two bit words, and he measured it at about ten million instructions per second.

Eight-bit and sixteen-bit computers are diddlysquat machines; the thirty-two-bit systems are the biggies. Thirty-two bits meant a big machine, ten MIPS meant fast. He'd entered a supermicrocomputer. One of the fastest in Berkeley. One of the most mismanaged.

As I watched him walk through the Elxsi, I talked to Tymnet. While the hacker tried to understand the new computer, Ron Vivier searched out the needle that pointed where the hacker came from.

"No news. He's coming in from Oakland again." Ron knew that meant a phone trace.

"No use calling the phone company. They'll just tell me to get a Virginia search warrant."

I hung up, disappointed. A long connection like this was perfect for tracing him. I couldn't shut him out of our system when he was into computers I'd never even heard of. When he finally signed off at 7:30, he'd pretty much mapped out our lab's major computers. He might not be able to get into each of them, but he knew where they were.

7:30. Damn, I'd forgotten the party. I ran down to my bike and

pedaled home. This hacker wasn't wrecking my computer, he was destroying my life. Being late for a Halloween party—that's a capital crime in Martha's book.

Not only was I late, but I'd shown up without a costume. I slinked guiltily through the kitchen door. What a scene! Princess Diana, tastefully attired in a tailored dress, pillbox hat and white gloves, shuddered as she removed a dripping handful of seeds from a pumpkin. Alice and the Mad Hatter were serving the last of the lasagna. Charlie Chaplin was dipping apples in caramel. In the midst of this swirl of activity stood a small but fierce samurai warrior in full battle gear, shouting orders. "You're late," the samurai scowled. "Where's your costume?"

Buried in the back of the closet, I found my white velvet robe. Worn over Martha's nightgown, with a sheet pinned around my shoulders and a tall, jeweled miter of construction paper and sequins, I suddenly became . . . Pope Cliff the First. I went around blessing the guests. Martha's friend Laurie, who usually wore a crew cut, jeans, and hiking boots, sidled up in a short black cocktail dress and long pearl necklace. "Come on, your holiness, let's go forth and bless the Castro."

We piled into the Mad Hatter's car (Laurie rode her motorcycle) and crossed the bridge to Babylon. Halloween is San Francisco's favorite holiday. Five blocks along Castro Street are cordoned off, and thousands of elaborately costumed revelers jostle up and down, looking at one another and at the drag queens in sequined gowns who lip-sync to Ethel Merman on the fire escapes overlooking the street.

This year's costumes were incredible: a person dressed as a bag of groceries, complete with giant paper replicas of vegetables and cans; various creatures from outer space; and several rival samurai, whom Martha fought off with her plastic sword. White-faced draculas mingled with witches, kangaroos, and butterflies. Over near the trolley stop, an assortment of ghouls harmonized with a three-legged pickle.

I offered benedictions left and right—to demons and angels, gorillas and leopards. Medieval knights knelt to me, and nuns (some with mustaches) rushed up to greet me. A trio of sturdy,

cheerful fellows in pink tutus and size-thirteen ballet shoes bowed gracefully to receive my blessings.

Despite layoffs at the factories, rent payments due, drugs, and AIDS, somehow San Francisco celebrated life.

Next Monday I showed up late, expecting to find a message from the manager of the Elxsi computer. No such luck. I called around the building design group, and talked with the physicist in charge of the Elxsi computer.

"Noticed anything strange on your Elxsi?"

"No, we've only had it a month. Anything wrong?"

"Who set up your accounts?"

"I did. I just signed on as system manager, then added users."

"Do you run accounting?"

"No. I didn't know you could."

"Someone broke into your computer through the UUCP account. He became system manager and added a new account."

"I'll be damned. What's the UUCP account?"

Here's the problem. This guy's a physicist, bored by computers. He didn't know about managing his machine. Probably didn't care.

This guy wasn't the problem. Elxsi was. They sold their computers with the security features disabled. After you buy their machine, it's up to you to secure it. Just plow through a dozen manuals to find a paragraph saying how to modify the permissions granted to the UUCP account. If you know that account exists.

Right.

The same thing must be happening all over. The hacker didn't succeed through sophistication. Rather he poked at obvious places, trying to enter through unlocked doors. Persistence, not wizardry, let him through.

Well, he wasn't going to get into our Elxsi anymore. Knowing my adversary, I could easily lock him out in a way that would mystify him. I built a trapdoor into our Elxsi: whenever the hacker touched the purloined accounts on that machine, it notified me and pretended to be too busy to accept another user. The Elxsi didn't say, "Go away"; rather, it slowed down to a crawl

whenever the hacker showed up. The hacker wouldn't realize that we were on to him, yet the Elxsi was protected against him.

Still, we were treading water. Without search warrants, our phone traces went nowhere. Sure, we read every word he typed into our computer, but how much did we miss? He might be using a dozen other computers to get onto the Milnet.

This much is for sure: I was now dedicated to catching this hacker. The only way to snag this guy was to watch every minute of the day. I had to be ready all the time—noon or midnight.

That was the problem. Sure, I could sleep under my desk and rely on my terminal to wake me up. But at the cost of the domestic tranquility: Martha wasn't pleased at my office campouts.

If only my computer would call me whenever the hacker appeared, then the rest of the time would be my own. Like a doctor on call.

Of course. A pocket pager. I had a bank of personal computers watching for the hacker to appear. I'd just program them to dial my pocket pager. I'd have to rent a pager, but it'd be worth the $20 a month.

It took an evening to write the programs—no big deal. From now on, wherever I went, I'd know within seconds of the hacker's arrival. I'd become an extension of my computer.

It was him against me now. For real.

There wasn't much I could do. Hacker or not, I wasn't about to call Steve White on New Year's morning. Anyway, I doubted that the German Bundespost could do much about it on a holiday. Most of all, I was ten miles from my laboratory.

I felt caged in while the hacker had free run. If he wanted to tweak my nose, he'd found the way. Just show up when I couldn't do anything.

Well, I couldn't do much beyond worry, so I tried to sleep. With Martha's arm around me, rest came easily. "C'mon, sweetie," she purred. "Give the hacker a holiday." I sank into the pillows. Hacker or not, we would celebrate the New Year. We slept the rest of the morning. Around noon, we found our way back home. Claudia greeted us with a violin sonata . . . she'd spent New Year's Eve playing at some millionaire's party.

Martha asked about her job. "You should have seen the canapés!" Claudia answered. "We had to sit and stare at them for *hours* before they finally saw us looking pathetic and brought us some. They had a whole smoked salmon and caviar and strawberries dipped in chocolate and—"

Martha cut in, "I meant what music you played."

"Oh, we played that Mozart sonata everyone likes that goes diddle dum diddle da da da. Then they started making requests for really icky things like 'My Wild Irish Rose.' I thought I'd get sick but after all it was $125 for two hours and it was on the way to my mom's so I could drop the dog off there, and do some shopping up at Santa Rosa—"

Martha snuck in a word about brunch. We were all in the kitchen mixing waffle batter and making fruit salad when my beeper sounded.

Damn. The hacker again. Martha cursed, but I hardly heard her: I zipped over to my Macintosh and dialed the lab.

There was the hacker, all right, logged in as Sventek. It looked like he was using the Milnet, but I couldn't be sure until I went to the lab. Meanwhile, I'd better call Steve White at Tymnet.

No time—the hacker disappeared within a minute. He was playing New Year's games.

There wasn't much to do but pick up the pieces. I scarfed down the waffles and biked over to the lab. There, the hacker's New Year's celebration was saved on my printers. I scribbled notes on the printouts, next to each of his commands.


```
4.2 BSD UNIX (lbl-ux4)
login: sventek                    The hacker logs in as Sventek
Password: lblhack                 and gives his current password
Last login: Mon Dec 29 13:31:43 on ttyi7
4.2 BSD UNIX #20: Fri Aug 22 20:08:16 PDT 1986
z
% telnet                          He's going out over the Milnet
telnet> open optimis              And into the Optimis Army Database

******OPTIMIS******

For user assistance, call 695-5772, (AV)225

Username: ANONYMOUS               He logs in there as
                                  anonymous
Password: GUEST                   And uses an obvious password

Welcome to the Army OPTIMIS database
If you use these databases and they achieve a savings in
time spent on a project or money saved to the government or both,
please send a mail message outlining the details to
Maj Gene LeClair, Chief, OPTIMIS

                WELCOME TO
                OPTIMIS
        THE DATA BASE WAS LAST UPDATED
             ON 861024 AT 102724
        AND CONTAINS 3316 DOCUMENTS

This data base is an extract of AR 25-400-2, Modem Army Record-
keeping System (MARKS) to help you identify information for filing.

Please enter a word or            Looking for SDI dope
'EXIT'.
/ sdi
The word "sdi" was not found.     But there's none there.
Please enter a word or
'EXIT'.
```

```
/ stealth                          Any word on the Stealth bomber?
The word "stealth" was not found.  No such luck
Please enter a word or 'EXIT'.
/ sac                              Strategic Air Command?
The word "sac" was not found.      Nope
```

Whee! The hacker had entered an Army database and searched for secret Air Force projects. Even an astronomer would know better. He caught on quickly, though:

```
Please enter a word or 'EXIT'.
/ nuclear
Thank you.
I have found 29 document(s) containing the phrase 'nuclear'.
ITEM #   MARKS #   TITLE
= = =    = = = =   = = = = =
1        20-lf     IG Inspections (Headquarters, Department
                     of the Army)
2        50a       Nuclear, chemical, and biological national
                     security affairs
3        50b       Nuclear, chemical and biological warfare
                     arms controls
4        50d       Nuclear and chemical strategy formulations
5        50e       Nuclear and chemical politico-military affairs
6        50f       Nuclear and chemical requirements
7        50g       Nuclear and chemical capabilities
8        50h       Theater nuclear force structure developments
9        50i       Nuclear and chemical warfare budget
                     formulations
10       50j       Nuclear and chemical progress and statistical
                     reports
11       50k       Army nuclear, chemical, and biological
                     defense program
12       50m       Nuclear and chemical cost analyses
13       50n       Nuclear, chemical warfare, and biological
                     defense scientific and technical information
14       50p       Nuclear command and control
                     communications
15       50q       Chemical and nuclear demilitarizations
16       50r       Chemical and nuclear plans
```



```
17       50-5a     Nuclear accident/incident controls
18       50-5b     Nuclear manpower allocations
19       50-5c     Nuclear surety files
20       50-5d     Nuclear site restorations
21       50-5-1a   Nuclear site upgrading files
22       50-115a   Nuclear safety files
23       55-355FRTd Domestic shipment controls
24       200-1c    Hazardous material management files
25       385-11k   Radiation incident cases
26       385-11m   Radioactive material licensing
27       385-40c   Radiation incident cases
28       700-65a   International nuclear logistics files
29       1125-2-300a Plant data
```

Well, I'd never come across such things. I'd always thought that a theater was somewhere to watch movies, not a place to develop nuclear forces. This hacker wasn't playing games.

And he wasn't satisfied with the titles to these documents—he dumped all twenty-nine over the line printer. Page after page was filled with army double-talk like:

```
TITLE: Nuclear, chemical, and biological national security affairs
DESCRIPTION: Documents relating to domestic, foreign, and military
police for the
application of atomic energy, utilization of nuclear and chemical
weapons, and
biological defense relating to national security and national level
crises management. Included are studies, actions, and directives
of and related to the
President, National Security Council, Assistant to the President
for National Security Affairs, and interdepartmental groups and
committees addressing national security affairs regarding nuclear
and chemical warfare and
biological
defense.
```

There, my printer jammed. The old Decwriter had paid its dues for ten years, and now needed an adjustment with a sledge hammer. Damn. Right where the hacker listed the Army's plans for nuclear bombs in the Central European theater, there was only an ink blot.

I didn't know much about movie theaters in Central Europe, so I gave Greg Fennel a call at the CIA. Amazingly, he answered his phone on New Year's Day.

"Hi, Greg—what brings you in on New Year's?"

"You know, the world never sleeps."

"Hey, what do you know about movie houses in Central Europe?" I asked, playing the fool.

"Oh, a bit. What's up?"

"Not much. The hacker just broke into some Army computer at the Pentagon."

"What's that got to do with movies?"

"I dunno," I said, "but he seemed especially interested in nuclear force structure developments in Central European theaters."

"You dunce! That's Army tactical warfare plans. Jeez. How did he get it?"

"His usual techniques. Guessed the password to the Army Optimis database in the Pentagon. It looks like a bibliography of Army documents."

"What else did he get?"

"I can't tell. My printer jammed. But he searched for keywords like 'SDI,' 'Stealth,' and 'SAC.' "

"Comic book stuff." I wasn't sure if Greg was joking or serious. He probably thought the same of me.

Come to think of it, how did the spooks know if I was putting them on? For all they knew, I might be inventing everything. Greg had no reason to trust me—I had no clearance, no badge, not even a trench coat. Unless they were spying behind my back, my credibility remained untested.

I had only one defense against this quicksand of distrust—the facts.

But even if they believed me, they weren't likely to do anything. Greg explained, "We can't just send Teejay overseas and bust down someone's door, you know."

"But can't you, well, sorta snoop around there and find out who's responsible for this?" I imagined spies in trench coats again.

Greg laughed. "That's not how things work. Trust me—we're working on it. And this latest news will add fuel to the fire." So much for the CIA. I just couldn't tell if they were interested or not.

On January 2, I called the Alexandria FBI office and tried to leave a message for Mike Gibbons. The duty agent who answered the phone said in a dry voice, "Agent Gibbons is no longer working this case. We suggest you contact the Oakland office."

Super. The only FBI agent that knows the difference between a network and a nitwit has been pulled off the case. No explanation given.

And just when we need the FBI. Wolfgang was still waiting for a warrant from the U.S. Legal Attaché in Bonn. A week of waiting, and it still hadn't come through. Time to knock on another door.

No doubt the National Security Agency would want to know about leaks from a Pentagon computer. Zeke Hanson at Fort Meade answered.

"Did the Army information go directly to Europe?" Zeke asked.

"Yeah, though I don't know exactly where," I said. "Looks like Germany."

"Do you know which International Record Carrier they used?"

"Sorry, I don't. But I can fish it out of my records if it's that important." Why would NSA want to know who had carried this traffic?

Of course. NSA is rumored to tape-record every transatlantic telephone conversation. Maybe they'd recorded this session.

But that's impossible. How much information crosses the Atlantic every day? Oh, say there's ten satellites and a half-dozen transatlantic cables. Each handles ten thousand telephone calls. So the NSA would need several hundred thousand tape recorders running full time. And that's just to listen to the phone traffic—there are computer messages and television as well. Why, fishing out my particular session would be nearly impossible, even with supercomputers to help. But there was an easy way to find out. See if NSA could obtain the missing data.

"The New Year's Day sessions were interrupted by a paper jam," I told Zeke, "so I'm missing an hour of the hacker's work. Think you could recover it?"

Zeke was cagey. "What's its importance?"

"Well, I can't quite say, since I haven't seen it. The session started at 8:47 on New Year's Day. Why don't you see if someone in Ft. Meade can find the rest of the traffic from this session?"

"Unlikely at best."

The NSA was always willing to listen but clammed up tight whenever I asked questions. Still, if they were doing their homework, they'd have to call me and see if our results were the same. I waited for someone to ask to see our printout. Nobody did.

Come to think of it, two weeks ago, I'd asked Zeke Hanson at the NSA to find out an electronic address. When I first traced a line into Europe, I passed the address to Zeke. I wondered what he'd done with it.

"Did you ever find out where that DNIC address comes from?" I asked.

"Sorry, Cliff, that information is unavailable." Zeke sounded like one of those Magic-8 balls, the kind that say, "Reply hazy, ask again later."

Fortunately, Tymnet had already figured out the address . . . it only took Steve White a couple hours.

Perhaps NSA has lots of electronics wizards and computer geniuses, listening to the world's communications. I wonder. Here, I'd presented them with two fairly easy problems—find an address and replay some traffic. Maybe they did, but they never told me a whit. I suspect they do nothing, hiding behind a veil of secrecy.

Well, there was one more group to inform. The Air Force OSI. The Air Force narcs couldn't do much about the hacker, but at least they could figure out whose computer was wide open.

Jim Christy's gravelly voice crackled over the phone lines: "So it's the Army Optimis system, huh? I'll make a few calls and bang a few heads." I hoped he was joking.

So 1987 started on a sour note. The hacker still had the free run of our computers. The only competent FBI agent had been pulled from the case. The spooks wouldn't say a thing, and NSA seemed uninspired. If we didn't make some headway soon, I'd give up too.

37

AROUND NOON ON SUNDAY, JANUARY 4, MARTHA AND I were stitching a quilt when my beeper sounded. I jumped for the computer, checked that the hacker was around, then called Steve White. Within a minute, he'd started the trace.

I didn't wait while Steve tracked the call. The hacker was on my computer, so I biked up to the lab and watched from there. Another twenty-minute race up the hill, but the hacker took his time: he was still typing when I reached the switchyard.

Underneath the printer, an inch-thick printout had accumulated. The hacker hadn't been lazy today. The top line showed him masquerading behind Sventek's name. After checking that none of our system managers were around, he went back to the Pentagon's Optimis database. Not today: "You are not authorized to log in today," was the Army computer's reply.

Well, hot ziggity! Jim Christy must have bashed the right heads.

Scanning the printout, I could see the hacker going fishing on the Milnet. One by one, he tried fifteen Air Force computers, at places like Eglin, Kirtland, and Bolling Air Force Bases. No luck. He'd connect to each computer, twist the doorknob once or twice, then go on to the next system.

Until he tried the Air Force Systems Command, Space Division.

He first twisted on their doorknob by trying their System account, with the password of "Manager." No luck.

Then Guest, password of "Guest." No effect.
Then Field, password "Service":

```
Username: FIELD
Password: SERVICE

WELCOME TO THE AIR FORCE SYSTEM COMMAND-SPACE DIVISION
VAX/VMS 4.4
IMPORTANT NOTICE
   Computer System problems should be directed to the Information
   Systems Customer Service Section located in building 130, room 2359.
   Phone 643-2177/AV 833-2177.

      Last interactive login on Thursday, 11-DEC-1986 19:11
      Last non-interactive login on Tuesday, 2-DEC-1986 17:30
WARNING - Your password has expired; update immediately with SET
PASSWORD!

$ show process/privilege
4-JAN-1987 13:16:37.56      NTY1:          User: FIELD
Process privileges:
      BYPASS       may bypass all system protections
      CMKRNL       may change mode to kernel
      ACNT         may suppress accounting messages
      WORLD        may affect other processes
      OPER         operator privilege
      VOLPRO       may override volume protection
      GRPPRV       group access via system protection
      READALL      may read anything as the owner
      WRITEALL     may write anything as the owner
      SECURITY     may perform security functions
```

Shazam: the door had swung wide open. He'd logged in as Field Service. Not just an ordinary user. A completely privileged account.

The hacker couldn't believe his luck. After dozens of attempts, he'd made the big time. System operator.

His first command was to show what privileges he'd garnered. The Air Force computer responded automatically: System Privilege, and a slew of other rights, including the ability to read, write, or erase any file on the system.

He was even authorized to run security audits on the Air Force computer.

I could imagine him sitting behind his terminal in Germany, staring in disbelief at the screen. He didn't just have free run of the Space Command's computer; he controlled it.

Somewhere in Southern California, in El Segundo, a big Vax computer was being invaded by a hacker halfway around the world.

His next moves weren't surprising: after showing his privileges, he disabled the auditing for his jobs. This way, he left no footprints behind; at least he thought not. How could he know that I was watching from Berkeley?

Confident that he was undetected, he probed the nearby computers. In a moment, he'd discovered four on the Air Force network, and a pathway to connect to others. From his high ground, none of these were hidden from him; if their passwords weren't guessable, he could steal them by setting up Trojan horses.

This wasn't a little desktop computer he'd broken into. He found thousands of files on the system, and hundreds of users. Hundreds of users? Yep. The hacker listed them all.

But his greediness got in his way. He commanded the Air Force computer to list the names of all its files; it went merrily along typing out names like "Laser-design-plans" and "Shuttle-launch-manifest." But he didn't know how to shut off the spigot. For two hours, it poured a Niagara of information onto his terminal.

Finally, at 2:30, he hung up, figuring that he'd just log back into the Air Force computer. But he couldn't get back on. The Air Force computer informed him:

```
Your password has expired. Please contact the system manager.
```

Looking back over the printout, I realized his goof. The Air Force computer had expired the "field service" password; he'd received a warning when he first broke in. Probably, the system automatically expired passwords after a few months.

To stay on the machine, he should have immediately reset his

password. Instead, he ignored the request. Now the system wouldn't let him back.

From thousands of miles away, I could sense his frustration. He desperately wanted to get back into that computer, but he'd been foiled by his own stupid mistake.

He'd stumbled on the keys to a Buick, and locked them in the car.

The hacker's mistake solved one problem: what should I tell the Air Force Space Division? Since it was a Sunday, there was nobody to call today. And because the hacker had locked himself out, he was no longer a danger to the Air Force computer. I'd just report the problem to the Air Force narcs, and let them handle it.

While the hacker stepped through the Air Force computer, Steve White traced Tymnet's lines.

"He's coming through RCA," Steve said. "TAT-6."

"Huh? What's that mean in English?"

"Oh, nothing really. RCA is one of the international record carriers, and today the hacker is coming across the number six transatlantic cable." Steve dealt in worldwide communications like a taxi driver in midtown traffic.

"Why isn't he on a satellite link?"

"Probably because it's a Sunday—the cable channels are less crowded."

"You mean that people prefer cable to satellite links?"

"Sure. Every time you connect through a satellite, there's a quarter-second delay. The undersea cables don't slow down your messages so much."

"Who would care?"

"People on the telephone, mostly," Steve said. "Those delays make for jittery conversations. You know, where each person tries to speak at the same time, then they both back off."

"So if the phone companies try to route over the cables, who wants the satellites?"

"Television networks, mostly. TV signals can't be squeezed into submarine cables, so they grab the satellites. But fiber optics will change everything."

I'd heard of fiber optics. Running communications signals over strands of glass, instead of copper wires. But who was running fiber-optic cables under the ocean?

"Everyone wants to," Steve explained. "There's a limited number of satellite channels available—you can crowd only so many satellites over Equador. And the satellite channels aren't private—anyone can listen in. Satellites may be fine for television, but cable's the way to go for data."

My conversations with Steve White began with tracing the hacker, but inevitably slipped into other topics. A short talk with Steve usually became a tutorial on communications theory.

Realizing that the hacker was still connected, I asked Steve for the details of the trace.

"Oh yeah. I checked with Wolfgang Hoffman at the Bundespost. Your visitor is coming from Karlsruhe today. The University of Karlsruhe."

"Where's that?"

"I don't know, but I'd guess the Ruhr valley. Isn't that along the Rhine?"

The hacker was still chipping away at the Air Force computer, but after he left, I jogged over to the library. Yes, there's Karlsruhe. Three hundred miles south of Hannover.

Draped across the floor of the Atlantic Ocean, the TAT-6 cable ties together Europe and America. The western end of the connection came through Tymnet, then Lawrence Berkeley Laboratory, across the Milnet, and ended at the Air Force Systems Command Space Division.

Somewhere in Germany, the hacker tickled the eastern end of the connection, unaware that we were zeroing in on him.

Three different places in Germany. My hacker was moving around. Or maybe he was staying in one place, playing a shell game with the telephone system. Perhaps he really was a student, visiting different campuses and showing off to his friends. Was I certain that there was only one hacker—or was I watching several people?

The solution depended on completing a trace. Not just to a country or a city, but all the way to an individual. But how do I get a phone trace from six thousand miles away?

account. He searched for an old, unused account and modified it. Some Air Force officer, Colonel Abrens, had an account, but hadn't been around this computer in a year.

The hacker slightly modified Colonel Abrens' account, giving it system privileges and a new password: AFHACK.

AFHACK—what arrogance. He's thumbing his nose at the United States Air Force.

From now on, he didn't need the Field Service account. Disguised as an officer in the Air Force, he had unlimited access to the Space Division's computer.

Heavy duty. This guy wasn't tinkering around. Air Force OSI had left for the day. What should I do? Leaving the hacker connected would leak sensitive information from the Air Force. But disconnecting him would only cause him to use a different route, bypassing my lab's monitors.

We'd have to chop him off at the Space Command.

But first, I wanted him traced. A call to Steve White started things rolling. Within five minutes, he'd traced the connection to Hannover, and called the Bundespost.

A few minutes of silence. "Cliff, does the connection look like it will be a long one?"

"I can't tell, but I think so."

"OK." Steve was on another telephone; I could only hear an occasional shout.

In a minute, Steve returned to my line. "Wolfgang is tracing the call in Hannover. It's a local call. They're going to try to trace it all the way."

Here's news! A local call in Hannover meant that the hacker's somewhere in Hannover.

Unless there's a computer in Hannover doing his dirty work.

Steve shouted instructions from Wolfgang: "Whatever you do, don't disconnect the hacker. Keep him on the line if you can!"

But he's rifling files at the Air Force base. It was like letting a burglar rob your home while you watched. Should I boot him out or let the trace go ahead? I couldn't decide.

Well, I ought to call some authority. How about Mike Gibbons of the FBI? He's not around.

Hey—the National Computer Security Center might be a good place to call. Zeke Hanson will know what to do.

No luck. Zeke wasn't in and the voice at the far end of the line explained, "I'd like to help you, but we design secure computers. We don't get involved in the operational aspects." I'd heard that before, thank you.

Well, there wasn't anyone else to tell but the Air Force. I hooked into the Milnet Network Information Center and looked up their phone number. Naturally, they'd changed their phone number. They even listed the wrong area code. By the time I reached the right person, the hacker had thoroughly penetrated their computer.

"Hi, I'm looking for the system manager of the Space Command's Vax computer."

"This is Sergeant Thomas. I'm the manager."

"Uh, I don't know how to explain this to you, but there's a hacker in your computer." (Meanwhile, I'm thinking, "He won't believe me and will want to know who I am.")

"Huh? Who are you?" Even over the phone, I could feel him giving me the hairy eyeball.

"I'm an astronomer at Lawrence Berkeley Laboratory." (First mistake, I think, nobody's gonna believe that.)

"How do you know there's a hacker?"

"I'm watching him break into your computer over the Milnet."

"You expect me to believe you?"

"Just look at your system. List out your users."

"OK." I hear typing in the background.

"There's nothing strange here. We've got fifty-seven people logged in, and the system's behaving normally."

"Notice anyone new?" I asked.

"Let's see . . . No, everything's normal." Should I tell him or just beat around the bush?

"Do you know someone named Abrens?"

"Yeah. Colonel Abrens. He's logged in right now. Hey, what are you getting at?"

"Are you sure that Abrens is legit?"

"Hell, yes. He's a colonel. You don't mess with the brass."

I was getting nowhere by asking leading questions. Might as well tell him. "Well, a hacker's stolen Abrens' account. He's logged on right now, and he's dumping your files."

"How do you know?"

"I watched him. I've got a printout," I said. "He came in on the Field Service account, then reset Abrens' password. Right now, he's got system privileges."

"That's impossible. Just yesterday, I reset the password to the Field Service account. It had expired."

"Yes, I know. You set the password to 'service.' The same as it's been for the past year. Hackers know this."

"Well, I'll be damned. Hold on." Over the phone, I hear Sergeant Thomas call someone over. A couple minutes later, he's back on the line.

"What do you want us to do?" he asked. "I can shut off my computer right now."

"No, hold off for a bit," I said. "We're tracing the line right now, and we're closing in on the hacker." This was no fib: Steve White had just relayed Wolfgang Hoffman's request to keep the hacker on the line as long as possible. I didn't want Sergeant Thomas to cut the line before the trace was complete.

"OK, but we'll call our commanding officer. He'll make the final decision." I could hardly blame them. A total stranger calls from Berkeley and tells them that someone's breaking into their system.

Between these phone calls, I watched the printer punch out the hacker's every command. Today, he didn't list the names of every file. Quite the contrary: he listed individual files. He already knew the names of the files he was looking for; he didn't need to scramble around searching for their names.

Aah. This was an important clue. Three days ago, the hacker listed the names of a thousand files. Today, he went straight to those files that interested him. He must have printed out his entire session. Otherwise, he would have forgotten the names of the files.

So the hacker's printing out everything he gets. I already knew that he kept a detailed notebook—otherwise, he'd have forgotten

some of the seeds that he'd planted months ago. I remembered my meeting with the CIA: Teejay had wondered if the hacker kept recordings of his sessions. Now I knew.

At the far end of the connection, somewhere in Germany, sat a determined and methodical spy. Every printout that came across my monitor was duplicated in his lair.

Which files did he list? He skipped over all the programs and ignored system management guidelines. Instead, he went for operational plans. Documents describing Air Force payloads for the space shuttle. Test results from satellite detection systems. SDI research proposals. A description of an astronaut-operated camera system.

None of this information had the comment "classified" on it. It wasn't secret, top secret, or even confidential. At least, none of the files carried those labels.

Now, no military computer on the Milnet is allowed to carry classified information. There's another computer network, completely separate, that handles classified data. So in one sense, the Systems Command's Space Division had nothing to lose: its computer is unclassified.

But there's a deeper problem. Individually, public documents don't contain classified information. But once you gather many documents together, they may reveal secrets. An order from an aircraft manufacturer for a load of titanium sure isn't secret. Nor is the fact that they're building a new bomber. But taken together, there's a strong indicator that Boeing's new bomber is made of titanium, and therefore must fly at supersonic speeds (since ordinary aluminum can't resist high temperatures).

In the past, to pull together information from diverse sources you'd spend weeks in a library. Now, with computers and networks, you can match up data sets in minutes—look at how I manipulated Mitre's long-distance phone bills to find where the hacker had visited. By analyzing public data with the help of computers, people can uncover secrets without ever seeing a classified database.

Back in 1985 Vice Admiral John Poindexter worried about just this problem. He tried to create a new classification of informa-

tion, "Sensitive but unclassified." Such information fit below the usual levels of Top Secret, Secret, and Confidential; but access to it was to be denied to certain foreigners.

Poindexter clumsily tried to apply this to academic research—naturally, the universities refused, and the idea died. Now, standing in front of my monitor, watching the hacker prowl through the Space Command's system, I realized his meaning. Air Force SDI projects might not be top secret, but they sure were sensitive.

What? Me agreeing with Vice Admiral Poindexter? The guy that shipped arms to Iran? How could I have any common ground with Ollie North's boss? Yet dancing across my screen was just what he'd described: sensitive but unclassified data.

Tymnet came back on the line. "I'm sorry, Cliff, but the trace in Germany is stymied."

"Can't they trace the call?" I asked, unsure of who I meant by "they."

"Well, the hacker's line comes from Hannover, all right," Steve replied. "But Hannover's phone lines connect through mechanical switches—noisy, complicated widgets—and these can only be traced by people. You can't trace the call with a computer."

I started to understand. "You mean that someone has to be in the telephone exchange to trace the call?"

"That's it. And since it's after 10 P.M. in Hannover, there's nobody around."

"How long will it take to get someone into the exchange?"

"About three hours."

To trace the line, a Bundespost telephone technician would have to visit the telephone exchange and follow the switches and wires. For all I knew, he might even have to climb telephone poles. Bad news.

Meanwhile, the hacker was slithering through the Air Force computer. Sergeant Thomas was still on hold—he'd probably called all sorts of Air Force brass by now.

I popped my phone to the Air Force line. "Well, we can't trace things any further today."

"Gotcha. We'll cut off the hacker right now."

"Wait for a second," I said. "Don't make it look like you're just booting him off your system. Instead, find a way that he won't suspect that you're on to him."

"Yeah. We figured out a plan," Sergeant Thomas replied. "We'll broadcast an announcement to everyone on the system that our computer's malfunctioning, and will have to be serviced."

Perfect. The hacker will think the system's going down for repairs.

I waited for a minute and in the middle of a page of SDI proposals, this message interrupted the hacker's screen:

System going down for maintenance, back up in 2 hours.

He saw it right away. The hacker immediately logged off and disappeared into the void.

40

"WAKE UP, YOU SLOTH," SAID MARTHA AT THE OBSCENELY early hour of nine on a Saturday morning. "Today we prepare the ground for our tomato plants."

"It's just January," I protested. "Everything is dormant. Bears are hibernating. I am hibernating." I pulled the covers over my head, only to have them snatched away. "Come on outside," said Martha, taking a viselike grip on my wrist.

At first glance, it seemed that I was right. The garden was dead and brown. "Look," Martha said, kneeling beside a rose bush. She touched the swelling pink buds. She pointed at the plum tree, and looking more closely, I saw a mist of tiny green leaves emerging from the bare branches. Those poor California plants—without a winter to sleep through.

Martha gave me a shovel, and we began the yearly cycle; turning over the soil, adding fertilizer, planting tiny tomato seedlings in their furrows. Every year we carefully planted several varieties that took different amounts of time to ripen, and staggered the planting by several weeks, so we would have a steady supply of tomatoes all summer. And every year, every single tomato ripened on the fifteenth of August.

It was slow, heavy work because the soil was dense with clay and wet from the winter rains. But we finally got the plot spaded, and, dirty and sweaty, stopped to take a shower and have brunch.

In the shower, I felt revived. Martha sudsed my back while I basked in hot water. Maybe the wholesome rustic life wasn't so bad after all.

Martha was in the midst of shampooing my hair when the nasty whine of my beeper, buried in a pile of clothing, destroyed our peace. Martha groaned and started to protest: "Don't you dare. . . ."

Too late. I jumped out of the shower and ran to the living room, switched on my Macintosh, and called the lab computer. Sventek.

A second later, I'm talking to Steve White at his home. "He's here, Steve."

"OK. I'll trace him and call Frankfurt."

A moment later, Steve's back on the line. "He's gone. The hacker was here a moment ago, but he's disconnected already. No use calling Germany now."

Damn. I stood there in utter frustration; stark naked, wet and shivering, standing in a puddle in our dining room, dripping blobs of shampoo onto my computer's keyboard.

Claudia had been practicing Beethoven, but startled by the sight of her roommate charging, naked, into the living room, she'd put down her violin and stared. Then she laughed and played a few bars of a burlesque tune. I tried to respond with a bump and grind, but was too obsessed with the hacker to pull it off.

I wandered sheepishly back into the bathroom. Martha glowered at me, then relented and pulled me into the shower again, under the hot water.

"I'm sorry, sweetheart," I apologized. "It's our only chance to nail him, and he wasn't around long enough to catch."

"Great," Martha said. "Long enough to drag you out of the shower, but not enough time to find out where he is. Maybe he knows you're watching him, and he's purposely trying to frustrate you. Somehow, he telepathically knows when you're in the shower. Or in bed."

"I'm sorry, sweetheart." I was, too.

"Honey, we've got to do something about this. We can't let this

guy keep yanking us around. And all those spooks in suits you keep talking to—what have they ever done to help? Nothing. We have to take this into our own hands."

She was right: I'd spent hours on the phone to the FBI, CIA, NSA, OSI, and the DOE. Still others, like the BKA, knew about our problem, yet nobody took the initiative.

"But what can we do without the government's help?" I asked. "We need search warrants and all that. We need official permission to do phone traces."

"Yeah, but we don't need anyone's permission to put stuff in our own computer."

So what?

Under the steaming water, Martha turned to me with a sly look.

"Boris? Darlink, I hev a plan . . ." Martha shaped a goatee and mustache out of soap suds on my face.

"Yes, Natasha?"

"Ees time for ze secret plan 35B."

"Brilliant, Natasha! Zat will vork perfectly! Ah, darlink . . . vhat is secret plan 35B?"

"Ze Operation Showerhead."

"Yes?"

"Vell, you see, zee spy from Hannover seeks ze secret information, yes?" Martha said. "We give him just vhat he vants—secret military spy secrets. Lots of zem. Oodles of secrets."

"Tell me, Natasha dahlink, zees secrets, vhere shall ve get them from? Ve don't know any military secrets."

"Ve make zem up, Boris!"

Yow! Martha had come up with the obvious solution to our problem. Give the guy what he's looking for. Create some files of phony information, laced with bogus secret documents. Leave 'em lying around my computer. The hacker stumbles on them, and then spends a couple hours lapping it up, copying it all.

Elegant.

How much stuff? As I rinsed Martha's hair, I calculated: we want him on for two hours. He's connected over a 1200-baud line, which means he can read about one hundred twenty characters a second. In two hours, he could scan about one hundred fifty thousand words.

"Oh, Natasha, my charming counter-counter-spy, there's just vun problem. Where do ve find five hundred pages of fake secrets?"

"Simple, dollink. Ze secrets, ve invent. Ze regular data, ve use vhat's already lying around."

As the hot water ran out, we clambered out of the shower. Martha grinned as she explained further. "We can't invent that much information overnight. But we can create it as we go along, staying just ahead of him. And we can take ordinary bureaucratic documents, modify them a bit, and give them secret-sounding titles. Real secret documents are probably thick with boring, bureaucratic jargon . . ."

". . . So we'll just take a bunch of those unintelligible Department of Energy directives that are always littering my desk, and change them to look like state secrets."

Martha continued. "We'll have to be careful to keep it bland and bureaucratic. If we head a document with 'CHECK OUT THIS TOP SECRET ULTRA-CLASSIFIED NEAT STUFF,' then the hacker's going to get suspicious. Keep it all low-key. Forbidden enough to keep him interested, but not an obvious trap."

I rolled her ideas around my mind and realized how to implement them. "Sure. We invent this secretary, see, who works for people doing this secret project. And we let the hacker stumble onto her word processing files. Lots of rough drafts, repetitive stuff, and interoffice memos."

Claudia greeted us in the living room, where she had mopped up the pond I'd left behind. She listened to our plan and suggested a new wrinkle: "You know, you could create a form letter in your computer that invites the hacker to write in for more information. If the hacker fell for it, he might include his return address."

"Right," said Martha, "a letter promising more information, of course!"

The three of us sat around the kitchen table with devious grins, eating omelets and elaborating on our plan. Claudia

described how the form letter should work: "I think it ought to be like a prize in a crackerjack box. Write to us, and we'll send you, uh . . . a secret decoder ring."

"But come on," I said, "there's no way he'll be stupid enough to send us his address." Seeing that I had thrown cold water on my coconspirators, I added that it was worth a try, but the main thing is to give him something that'll take a couple of hours to chew on.

Then I thought of another problem. "We don't know enough about military stuff to make sensible documents."

"They don't have to make sense," Martha grinned diabolically. "Real military documents don't make sense either. They're full of jargon and double-talk. You know, like 'the procedure for implementing the highly prioritized implementation procedure is hereinafter described in section two, subparagraph three of the procedural implementation plan.' Eh, Boris?"

Well, Martha and I biked up to the laboratory and logged onto the LBL computer. There we shoveled through a mound of real government documents and directives, which were overflowing with far more turgid bureaucratese than we could ever invent, changing them slightly so that they'd look "classified."

Our documents would describe a new Star Wars project. An outsider reading them would believe that Lawrence Berkeley Laboratory had just landed a fat government contract to manage a new computer network. The SDI Network.

This bogus network apparently linked together scores of classified computers and extended to military bases around the world. By reading our files, you'd find lieutenants and colonels, scientists and engineers. Here and there, we dropped hints of meetings and classified reports.

And we invented Barbara Sherwin, the sweet, bumbling secretary trying to figure out her new word processor and to keep track of the endless stream of documents produced by our newly invented "Strategic Defense Initiative Network Office." We named our fictitious secretary after an astronomer, Barbara Schaefer, and used the astronomer's real mailing address. I mentioned to the real Barbara to watch for any strange mail addressed to Barb Sherwin.

Our fake memoranda included budget requests ($50 million for communications costs), purchase orders, and technical descriptions of this network. We cribbed most of them from files lying around the computer, changing the addresses and a few words here and there.

For a mailing list, I grabbed a copy of the lab newsletter's list of names and addresses. I just flipped every "Mr." to "Lieutenant," every "Mrs." to "Captain," every "Dr." to "Colonel," and every "Professor" to "General." The addresses? Just stir in an occasional "Air Force Base" and "Pentagon." In half an hour, my ersatz mailing list looked like a veritable military Who's Who.

Some of the documents, however, we fabricated completely: correspondence between managers and petty bureaucrats. An information packet describing the technical capabilities of this network. And a form letter saying that the recipient could get more information on the SDI Network by writing to the project office.

"Let's label the account, the 'Strategic Information Network Group,' " I said. "It's got a great acronym: STING."

"Naw. He might catch on. Keep it bureaucratic," Martha said. "Use SDINET. It'll catch his eye, all right."

We put all the files under one account, SDINET, and made certain that I was the only one who knew the password. Then I made these files entirely inaccessible to everyone except the owner—me.

Large computers let you make a file world-readable, that is, open to anyone who logs into the system. It's a bit like leaving an office cabinet unlocked—anyone can read the contents when they wish. You might set world-read on a file containing the scores of the office's volleyball tournament.

With a single command, you can make a file readable by only certain people—for example, your co-workers. The latest sales report, or some manufacturing designs, need to be shared among a few people, but you don't want everyone to scan them.

Or a computer file can be entirely private. Nobody but you can read it. Like locking your desk drawer, this keeps everyone out. Well, almost everyone. The system manager can bypass the file protections, and read any file.

By setting our SDI files to be readable only by their owner, I made sure that nobody else would find them. Since I was the owner and the system manager, nobody else could see them.

Except, perhaps, a hacker masquerading as system manager.

For the hacker could still break in and become system manager. It would take him a couple of minutes to hatch his cuckoo's egg, but he'd then be able to read all the files on my system. Including those bogus SDI files.

If he touched those files, I'd know about it. My monitors saved his every move. Just to make certain, though, I attached an alarm to those SDI network files. If anyone looked at them—or just caused the computer to try to look at them—I'd find out about it. Right away.

My snare was baited. If the hacker bit, he'd take two hours to swallow the bait. Long enough for the Germans to track him down.

The next move was the hacker's.

41

I'D SCREWED UP AGAIN. OPERATION SHOWERHEAD WAS ready, all right. It might even work. But I'd forgotten an important detail.

I hadn't asked anyone's permission.

Normally, this wouldn't be a problem, since nobody cared what I did anyway. But bicycling up to the lab, I realized that every organization I'd been in contact with would want to know about our phony SDI files. Each place would have a different opinion, of course, but to go ahead without telling anyone would piss them all off.

But what if I asked their permission? I didn't want to think about it. Mostly, I worried about my boss. If Roy stood behind me, then the three-letter agencies couldn't touch me.

On January 7, I went straight to his office. We talked about relativistic electrodynamics for a while—which mostly meant my watching the old professor at the chalkboard. Say what you will about crusty college professors, there's no better way to learn than to listen to someone who's paid his dues.

"Say, boss, I'm trying to get out from under this hacker."

"CIA leaning on you again?"

Roy was joking, I hoped.

"No, but the Germans will only trace the line for one more week. After next weekend, we might as well call it quits."

"Good. It's been too long anyway."

"Well, I was thinking about planting some misleading data in our computer, to use as bait in catching the hacker."

"Sounds good to me. It won't work, of course."

"Why not?"

"Because the hacker's too paranoid. Still, go ahead. It'll be a useful exercise." Hot damn!

My boss's approval insulated me from the rest of the world. Still, I ought to tell the three-letter folks about our plans. I wrote a short proposal, framed as a scientific paper:

Proposal to Determine the Address of the Hacker

Problem:

A persistent hacker has invaded LBL's computers. Because he is coming from Europe, it takes an hour to trace the phone lines. We would like to learn his exact location.

Observations:

1. He is persistent.
2. He confidently works within our computers, unaware that we are watching him.
3. He searches for phrases like "sdi," "stealth," and "nuclear."
4. He is a competent programmer and is experienced at breaking into networks.

Suggested solution:

Provide fictitious information to keep him connected for more than an hour. Complete the phone tracing during this time.

My paper went on and on about History, Methodology, Implementation Details, and had footnotes about the chances of actually catching him. As boring as I could make it.

I sent this paper to the usual list of three-letter agencies: the FBI, CIA, NSA, and DOE. I included a note saying that unless someone objected, we'd carry out this plan next week.

A few days later, I called each agency. Mike Gibbons of the FBI understood what I was getting at, but wouldn't commit his agency one way or another. "What does the CIA have to say about it?"

Teejay at the CIA had also read my proposal, but was equally noncommittal:

"What did the guys at the 'F' entity say?"

"Mike said to call you."

"Well, ain't that dandy. Have you called the northern entity?" Northern entity? What's north of the CIA?

"Uh, Teejay, who's the northern entity?"

"You know, the big Fort M."

Oh—Fort Meade in Maryland. The NSA.

Yes, I had called Fort Meade, and Zeke Hanson at the NSA's National Computer Security Center had read my proposal. He seemed to like it, but he didn't want to have anything to do with it.

"Well, I sure can't tell you to go ahead," Zeke said. "Personally, I'd love to see what happens. But if you get into trouble, we don't have anything to do with it."

"I'm not looking for someone to take responsibility, I'm wondering if it's a bad idea." Sounds strange, but that's just what I was trying to do. Before you start an experiment, get the opinions of people who've been there before.

"Sounds good to me. But you really ought to check with the FBI." That closed the circle—everyone pointed their finger at someone else.

Well, I called the Department of Energy, the Air Force OSI, and a guy at the Defense Intelligence Agency. Nobody would take responsibility, of course, yet nobody blocked the idea. That's all I needed.

By Wednesday, it was too late for anyone to object. I was sold on Martha's idea, and was willing to back it up.

Sure enough, Wednesday afternoon, the hacker showed up. I'd been invited to lunch at the Cafe Pastorale in Berkeley with Dianne Johnson, the field representative of the Department of Energy. Along with Dave Stevens, the computer center's math whiz, we enjoyed some fine fettuccini, while talking about our progress and plans.

At 12:53 PST, in the middle of a cup of cappuccino, my beeper went off. The Morse code said the hacker was into our Unix-4

computer as Sventek. I didn't say a word—just ran to the phone booth and called Steve White at Tymnet ($2.25 in quarters), and he started the trace running. The hacker was on for only three minutes—just long enough to see who was logged onto my computer. I was back at the table before the coffee cooled off.

That spoiled the rest of lunch for me. Why had he stayed around only three minutes? Did he sense a trap? I couldn't tell until I saw the printout up at the lab.

The monitors showed him logging on as Sventek, listing the names of everyone currently logged on, and then disappearing. Damn him. He didn't look around long enough to discover our bogus files.

Oh—maybe our bait was too well hidden. The German phone technician would be around for only a couple more days, so I'd better make it more obvious.

From now on, I'd stay logged on to my computer. I would play sweet Barbara Sherwin, connected to the computer on the SDINET account. The next time the hacker raised his periscope, he'd see SDINET clunking away, trying to edit some file or another. If that didn't catch his attention, then nothing would.

Naturally, he didn't show up the next day, Thursday. We were running out of time. Nothing the next morning. I was about to call it quits, when my beeper sounded at 5:14 P.M., Friday, January 16. There's the hacker.

And I'm here, working in the SDINET account, playing with a word processing program. His first command, "who," listed ten people. I was the seventh on his list:

```
who
Astro
Carter
Fermi
Meyers
Microprobe
Oppy5
Sdinet
Sventek
Turnchek
Tompkins
```


There's the bait. Come on, go for it!

```
lbl> grep.sdinet/etc/passwd          He's searching for user "SDINET"
                                     in our password file
sdinet:sx4sd34x2:user sdinet, files in/u4/sdinet, owner sdi net-
work project
```

Ha! He swallowed the hook! He's hunting for information about the user SDINET! I knew what he'd do next—he'd search over in the SDINET directory.

```
lbl> cd/u4/sdinet          He's moving over to the SDINET directory
lbl> ls                    and trying to list the file names
file protection violation—you are not the owner.   But he can't see
                                                   them!
```

Of course he can't read the SDINET data—I've locked everyone out of those files. But he knows how to evade my lock. Just plant a little egg, using the Gnu-Emacs software. Become superuser.

None of my files are hidden from the system manager. And my visitor knows exactly how to grab those privileges. It just takes a few minutes. Would he reach into the monkey bottle?

There he goes. He's checking that the Gnu-Emacs move-mail program hasn't been changed. Now he's creating his own false atrun program. Just like the old days. In a couple more minutes, he'll be system manager.

Only this time, I'm on the phone to Steve White.

"Steve, call Germany. The hacker's on, and it'll be a long session."

"Spot-on, Cliff. Call you back in ten minutes."

Now it's the Germans' turn. Can they pull the plum from the pie? Let's see, it's 5:15 P.M. in Berkeley, so in Germany, it's uh, 2:15 in the morning. Or is it 1:15? Either way, it's sure not ordinary business hours. Sure hope that the Hannover technicians stayed late tonight.

Meanwhile, the hacker's not wasting time. Within five min-

utes, he'd built a special program to make himself super-user. He twisted the tail of the Gnu-Emacs program, moving his special program into the systems area. Any minute now, Unix will discover that program and . . . yep, there it goes. He's super-user.

The hacker went straight for the forbidden SDINET files. (I'm glued to my monitor, thinking, "Come on, guy, wait till you see what's sitting there for you.") Sure enough, he first lists the file names:

```
|bl> ls
Connections
Form-Letter
Funding
Mailing-Labels
Pentagon-Request
Purchase-Orders
Memo-to-Gordon
Rhodes-Letter
SDI-computers
SDI-networks
SDI-Network-Proposal
User-List
World-Wide-Net
Visitor-information
```

Many of these files aren't just single memos. Some are file directories—whole file cabinets full of other files.

Which one will he look at first? That's easy. All of them.

For the next forty-five minutes, he dumps out file after file, reading all the garbage that Martha and I created. Boring, tedious ore, with an occasional nugget of technical information. For example:

Dear Major Rhodes:

Thank you for your comments concerning access to SDINET. As you know, a Network User Identifier (NUI) is required for access to both the Classified and Unclassified SDINET. Although these NUI's are distributed from different locations, it is important that users who use both sections of the network retain the same NUI.

For this reason, your command center should contact the network

controllers directly. At our laboratory in Berkeley, we can easily modify your NUI, but we would prefer that you issue the appropriate request to the network controllers.

Sincerely yours,
Barbara Sherwin

Aah . . . there's a pointer in that letter saying that you can reach the SDINET from Lawrence Berkeley Laboratory. I'll bet that he'll spend an hour or two searching for the portal to reach that mythical SDINET.

Did he believe what I'd fed him? There's an easy way to find out. Just watch what he does—a disbeliever won't go hunting for the Holy Grail.

The files made a believer out of him. He interrupted his listing to search for a connection into our SDI network. On my monitor, I watched him patiently scan all our links to the outside world. Without knowing our system thoroughly, he couldn't search exhaustively, but he spent ten minutes checking the system for any ports labelled "SDI."

Hook, line, and sinker.

He returned to reading our fake SDINET files, and dumped the file named form-letter:

SDI Network Project
Lawrence Berkeley Lab
Mail Stop 50-351
1 Cyclotron Road
Berkeley, CA 94720

name name
address address
city city, state state, zip zip

Dear Sir:

Thank you for your inquiry about SDINET. We are happy to comply with your request for more information about this network. The following documents are available from this office. Please state which documents you wish mailed to you:

#37.6 SDINET Overview Description Document
19 pages, revised Sept, 1985

#41.7 Strategic Defense Initiative and Computer Networks:
Plans and implementations (Conference Notes)
227 pages, revised Sept, 1985

#45.2 Strategic Defense Initiative and Computer Networks:
Plans and implementations (Conference Notes)
300 pages, June, 1986

#47.3 SDINET Connectivity Requirements
65 pages, revised April, 1986

#48.8 How to link into the SDINET
25 pages, July 1986

#49.1 X.25 and X.75 connections to SDINET
(includes Japanese, European, and Hawaii nodes)
8 pages, December, 1986

#55.2 SDINET management plan for 1986 to 1988
47 pages, November 1985

#62.7 Unclassified SDINET membership list
(includes major Milnet connections)
24 pages, November, 1986

#65.3 Classified SDINET membership list
9 pages, November, 1986

#69.1 Developments in SDINET and Sdi Disnet
28 pages, October, 1986

NUI Request Form
This form is available here, but
should be returned to the Network Control Center

Other documents are available as well. If you wish to be added to our mailing list, please request so.

Because of the length of these documents, we must use the postal service.

Please send your request to the above address, attention Mrs. Barbara Sherwin.

The next high level review for SDINET is scheduled for 20 February, 1987. Because of this, all requests for documents must be received by us no later than close of business on 11 February, 1987. Requests received later than this date may be delayed.

Sincerely yours,
Mrs. Barbara Sherwin
Documents Secretary
SDINET Project

I wondered how he'd react to this letter. Would he send us his address?

It didn't make much difference. Steve White called back from Tymnet. "I've traced your connection over to the University of Bremen."

"Same as usual, huh?"

"Yeah. I guess they've reopened for classes," Steve said. "At any rate, the Bundespost has traced the Datex line from Bremen into Hannover."

"OK. Sounds like the hacker's in Hannover."

"That's what the Bundespost says. They've traced the Datex line into a dial-in port located near downtown Hannover."

"Keep going, I follow you."

"Now comes the tough part. Someone has dialed into the Datex system in Hannover. They're coming from Hannover, all right—it's not a long-distance line."

"Does the Bundespost know that phone number?"

"Almost. In the past half hour, the technician traced the line and has narrowed it down to one of fifty telephone numbers."

"Why can't they get the actual number?"

"Wolfgang's unclear about that. It sounds like they've determined the number to be from a group of local phones, but the next time they make a trace, they'll zero in on the actual telephone. From the sound of Wolfgang's message, they're excited about solving this case."

One in fifty, huh? The Bundespost is almost there. Next time, they'll have him.

Friday, January 16, 1987. The cuckoo laid its eggs in the wrong nest.

42

THE TRACE ALMOST REACHED THE HACKER. IF HE CAME by once more, we'd have him.

But the deadline was tomorrow night. Saturday, when the German telephone technicians would give up the chase. Would he show up?

"Martha, you don't want to hear this, but I'm sleeping at the lab again. This may be the end of the road, though."

"That's the dozenth time you've said that."

Probably was. The chase had been a constant stream of "I've almost got him" followed by "He's somewhere else." But this time it felt different. The messages from Germany were confident. They were on the right scent.

The hacker hadn't read all our bogus files. In the forty-five minutes that he'd linked into our system, he listed about a third of the data. He knew there was more, so why didn't he stay around and browse?

All the more likely that he'd come back soon. So once again, I crawled under my desk and fell asleep to the sound of a computer disk drive whining in the distance.

I woke up, for once, without a beeper squawking in my ear. Just a peaceful Saturday morning, alone in a sterile office, staring at the bottom of my desk. Oh well, I'd tried. Too bad the hacker didn't show up.

Since nobody else was around, I started to play with an astronomical program, trying to understand how mistakes in mirror-grinding affect images from a telescope. The program was just about working when my beeper called at 8:08 A.M.

A quick jog down the hall, and a glance at the monitor's screen. There's the hacker, just logging into the Unix-5 computer, on one of his old account names, Mark. No time to figure what he's doing here, just spread the word fast. Call Tymnet, and let them call the Bundespost.

"Hi Steve!"

"The hacker's back on, eh?" Steve must have heard it in the tone of my voice.

"Yep. Can you start the trace?"

"Here goes." He was gone for thirty seconds—it couldn't have been a full minute—when he announced, "He's coming from Bremen this time."

"Same as yesterday," I observed.

"I'll tell Wolfgang at the Bundespost." Steve hung up while I watched the hacker on my screen. Every minute the hacker visited, we were that much closer to unmasking him.

Yes, there he was, methodically reading our false data files. With every bureaucratic memo he read, I felt more satisfied, knowing he was being misled in two ways: his information was patently false, and his arrogant strides through our computer were leading him straight into our arms.

At 8:40, he left our computer. Steve White called back within a minute.

"The Germans traced him through the University of Bremen again," he said. "From there, into Hannover."

"Did they make any progress in getting his phone number?"

"Wolfgang says they've got all the digits of his phone number except the last two."

All but the last two digits? That didn't make sense—it meant that they'd traced the call to a group of one hundred phones. "But that's worse than yesterday, when they said they'd isolated him to one of fifty phones."

"All I can tell you is what I hear."

Disturbing, but at least they were tracing the lines.

At 10:17, he came back. By now, Martha had bicycled up to the lab, and the two of us were busy inventing new SDI files to feed him. We both ran to the monitors and watched him, expecting him to discover our latest work.

This time, he wasn't interested in SDI files. Instead, he went out over the Milnet, trying to break into military computers. One by one, trying to guess his way past their password protection.

He concentrated on Air Force and Army computers, occasionally knocking on the Navy's door. Places I'd never heard of, like the Air Force Weapons Lab, Descom Headquarters, Air Force CC OIS, the CCA-amc. Fifty places, without success.

Then he slid across the Milnet into a computer named Buckner. He got right in . . . didn't even need a password on the account named "guest."

Martha and I looked at each other, then at the screen. He'd broken into the Army Communications Center in Building 23, Room 121, of Fort Buckner. That much was obvious: the computer greeted the hacker with its address. But where's Fort Buckner?

About all I could tell was that its calendar was wrong. It said today was Sunday, and I knew it was Saturday. Martha took charge of the monitors, and I ran to the library, returning with their now familiar atlas.

Paging through the back pages, I found Ft. Buckner listed.

"Hey, Martha, you're not going to believe this, but the hacker's broken into a computer in Japan. Here's your Fort Buckner," I said, pointing to an island in the Pacific Ocean. "It's on Okinawa."

What a connection! From Hannover, Germany, the hacker linked to the University of Bremen, across a transatlantic cable into Tymnet, then into my Berkeley computer, and into the Milnet, finally reaching Okinawa. Jeez.

If someone in Okinawa had detected him, they'd have to unravel a truly daunting maze.

Not that this worldwide link satisfied him—he wanted Fort Buckner's database. For half an hour, he probed their system, finding it amazingly barren. A few letters here and there, and a list of about seventy-five users. Fort Buckner must be a very trusting place: nobody set passwords on their accounts.

He didn't find much on that system, outside of some electronic mail messages talking about when supplies would arrive from Hawaii. A collector of military acronyms would love the Fort Buckner computer, but any sane person would be bored.

"If he's so interested in military gobbledegook," Martha asked, "why not enlist?"

Well, this hacker wasn't bored. He listed as many text files as he could, skipping only the programs and Unix utilities. A bit after eleven in the morning, he finally grew tired, and logged off.

While he'd circled the globe with his spiderweb of connections, the German Bundespost had homed in on him.

The phone rang—had to be Steve White.

"Hi, Cliff," Steve said. "The trace is complete."

"The Germans got the guy?"

"They know his phone number."

"Well, who is he?" I asked.

"They can't say right now, but you're supposed to tell the FBI."

"Just tell me this much," I told Steve, "is it a computer or a person?"

"A person with a computer at his home. Or should I say, at his business."

Martha overheard the conversation and was now whistling a tune from *The Wizard of Oz:* "Ding-dong, the witch is dead. . . ."

At last, the trace was over. The police would bust him, he'd be arraigned, we'd press charges, and he'd be pacing a jail cell. So I thought.

But more important, my research was finished. Five months ago, I asked myself, "How come my accounts are imbalanced by 75 cents?" That question had led me across the country, under the ocean, through defense contractors and universities, to Hannover, Germany.

Martha and I biked home, stopping only to pick up a pint of heavy cream. We picked the last of our garden's strawberries and celebrated with homemade milkshakes. No doubt—there's no substitute for mixing 'em yourself. Toss in some ice cream, a couple bananas, a cup of milk, two eggs, a couple spoonfuls of

vanilla, and a handful of homegrown strawberries. Thicken it with just enough malt. Now that's a milkshake.

Claudia, Martha, and I danced around the yard for a while—our plans had worked out perfectly.

"In a couple days, the police will bust him, and we'll find out what he was after," I told them. "Now that someone knows who's behind this, it can't be long."

"Yow, you'll get your name in the newspaper," Claudia marveled. "Will you still talk to us?"

"Yeah, I'll even keep washing the dishes."

The rest of the day, Martha and I spent in San Francisco's Golden Gate Park, riding the merry-go-round and roller-skating.

After all these months, the problem was solved. We'd thrown a net around the cuckoo.

43

HE STARED BLEAKLY AT THE BROKEN GREASY VENETIAN blinds, a cigarette butt dangling from his clammy lips. The sickly green glow of the screen reflected on his sallow tired features. Silently, deliberately, he invaded the computer.

Six thousand miles away, her longing white arms craved for him. He could feel her hot breath on his cheek, as her delicate fingers curled through his long brown hair. Her negligee parted invitingly, he sensed every curve through the thin silken gauze. She whispered, "Darling, don't leave me. . . ."

Suddenly the night was shattered—that sound again—he froze and stared at the night stand. A red light beckoned across the pitch-black room. His beeper sang its siren song.

Sunday morning, at 6:30, Martha and I were dreaming when the hacker stepped on my electronic tripwire. Damn. Such a great dream, too.

I slid out from under the quilts and called Steve White. He passed the message along to the Bundespost, and five minutes later, the trace was complete. Hannover again. Same guy.

From home, I couldn't observe him—he might notice me watching him. But only yesterday he'd finished reading all our phony SDI files. So why come back now?

It wasn't until I biked into work that I saw the hacker's targets. Milnet again. The printout showed him logging into my Berkeley

computer, then reaching out over the Milnet, then trying to log onto a system at the Eglin Air Force Base.

He tried account names like guest, system, manager, and field service . . . all his old tricks. Eglin's computer didn't put up with such nonsense: it kicked him out after his fourth try. So, he went on the European Milnet Control computer, and tried again. Still no luck.

Sixty computers later, he still hadn't gotten into a military computer. But he kept trying.

At 1:39 P.M., he succeeded in logging into the Navy Coastal Systems Center in Panama City, Florida. He got into their system by trying the account "Ingres" with the password "Ingres."

Ingres database software lets you quickly search thousands of accounting records for the one entry you need. You make queries like, "Tell me all the quasars that emit X-rays," or "How many Tomahawk missiles are deployed in the Atlantic fleet?" Database software is powerful stuff, and the Ingres system is among the finest.

But it's sold with a backdoor password. When you install Ingres, it comes with a ready-made account that has an easily guessed password. My hacker knew this. The Navy coastal Systems Center didn't.

Once logged on, he meticulously checked that nobody was watching him. He listed the file structures and searched for links to nearby networks. He then listed the entire encrypted password file.

There he goes again. That's the third or fourth time I'd seen him copy the whole password file into his home machine. Something's strange here—the passwords are protected by encryption, so he can't possibly figure out the original password. Still, why else would he copy the password file?

After an hour inside the navy computer, he grew tired and went back to knocking on doors along the Milnet. That, too, lost its excitement after a while; after fifty or a hundred times, even he tired of seeing the message, "Invalid Login—bad password." So he printed out some SDINET files again, pretty much the same stuff he'd seen in the past couple of days. Around 2:30 in the

afternoon he called it quits. He'd spent eight hours hacking on the military networks.

Plenty of time to trace his call. And time enough to learn that the German Bundespost has been in close contact with the Public Prosecutor in Bremen, Germany. They're contacting the authorities in Hannover, and they're also talking to the German BKA. Sounds like someone is about ready to close in on the hacker and make the arrest.

Who should I call about this break-in into the Navy computer?

A week ago, the Air Force OSI warned me not to call the system managers directly. Jim Christy said, "It just runs against military policy."

"I understand," I said. "But is there a clearinghouse to report these problems to?'

"No, not really," Jim explained. "You can tell the National Computer Security Center, but they're pretty much a one-way trap. They listen, all right, but they don't publicize problems. So if it's a military computer, call us," Jim said. "We'll go through channels and get the word to the right folks."

Monday morning brought the hacker again. Time to twist some more doorknobs. One by one, he scanned Milnet computers, ranging from the Rome Air Development Center in New York to someplace called the Naval Electronic Warfare Center. He tried fifteen places before he struck pay dirt—the Ramstein Air Force Base computer. This time, he discovered that the account, "bbncc," wasn't protected. No password needed.

Ramstein's computer seemed to be an electronic mail system for officers. He started listing everyone's mail. Quickly, it opened my eyes—this was stuff that he shouldn't be seeing.

OK, what should I do? I couldn't let him grab this information, yet I didn't want to tip my hand. Disconnecting him won't do much good—he'll just find another pathway. I can't call the place—I've no idea where Ramstein Air Force Base is. I can call Air Force OSI, but I've got to take action now—not in five minutes—before he reads the rest of their data.

I reached for the phone to call Jim Christy of the Air Force OSI. Naturally I can't remember his phone number. There in my

pocket is a key chain. Of course, the old key chain trick. Just add some noise to his connection.

I jangled my keys against the connector, shorting out the hacker's communications line. Just enough to appear as noise to the hacker. "Static on the line," he'd think. Every time he asked for electronic mail from Ramstein, I garbled his commands, and Ramstein's computer misunderstood him.

After a few more attempts, he gave up on Ramstein Air Force Base, and went back to scanning the Milnet, trying to get into other places.

I finally reached Jim Christy at Air Force OSI. "The hacker's gotten into someplace called Ramstein Air Force Base. Wherever it is, you'd better tell them to change all their passwords."

"Ramstein's in Germany."

"Huh?" I asked. I'd thought the occupation of Europe had ended in the '50s. "What's the U.S. Air Force doing in Germany?"

"Protecting you. But let's not go into that. I'll warn them right away. Go back to watching the hacker."

I'd missed ten minutes of the hacker. He was trying to break into more military systems, slowly and methodically trying dozens of sites.

The Milnet addresses seemed to be in alphabetical order; right now he was working near the end of the alphabet. Mostly R's and S's. Aha! Yes, that was it. He was working from an alphabetized list. Somehow, he'd obtained the Milnet directory, and was checking off each site after he tried it.

He'd made it halfway through the S's when he tried a computer called Seckenheim. Logged right in as "Guest." No password. This was getting embarrassing.

But though he got into that computer, he didn't stay long. A few minutes to make a couple scans of their system files, then he logged off. I wondered why.

Still, I'd better do something. Time to call the Air Force.

"Hey, the hacker just got into someplace called Seckenheim. It's on the Milnet, so it must be a military computer. But I've never heard of it."

"Snake in the grass," Jim growled.

"Huh?"

"Damn. Seckenheim is the Army Material Command in Europe. Near Heidelberg. Germany again."

"Oops. Sorry about that."

"I'll take care of it." The hacker's success meant problems for the narcs. I wondered how many overseas military bases the United States has. The technology I could handle. It was geography and bureaucracies that tripped me up.

After having cracked three computers today, the hacker was still not satisfied. He continued to bang away on the Milnet, so I kept watch in the switchyard. One by one, I watched as he tried passwords. At 11:37, he got into a Vax computer named Stewart. Logged right in there as "Field," password, "Service." I'd seen it before. Another Vax computer running VMS that hadn't changed their default passwords.

The hacker dived right in. The field service account was privileged, and he wasted no time taking advantage of this. He first disabled accounting, so that he'd leave no tracks behind. Then he went directly to the *authorize* utility—the system software in charge of passwords—and selected one user, Rita, who hadn't used the system for the past few months. He modified Rita's account to give it full system privileges. Then he set a new password. "Ulfmerbold."

Where had I heard that word? Ulfmerbold. It sounded German. Something to figure out later. Meanwhile, I've got to watch my hacker.

Finally, a bit after noon, the hacker left Berkeley. A productive day for him.

The Stewart computer turned out to belong to Fort Stewart, an Army base in Georgia. I called Mike Gibbons of the FBI, and he took care of calling them.

"Mike, have you ever heard of the word 'Ulfmerbold'?"

"Nope. Sounds German, though."

"Just checking. Say, the Germans have completed the trace. The Bundespost now knows who's making the calls."

"Did they tell you?"

"Naw. Nobody ever tells me anything. You know that."

Mike laughed. "That's the way we operate, all right. But I'll get the Legat on the case right away."

"Legat?"

"Oh. Legal Attaché. You know, the guy in Bonn that handles our affairs."

"How soon until they arrest the guy?" I just wanted to know who and why—the last pieces of the puzzle.

"I don't know. But when it happens, I'll tell you. Shouldn't be long now."

By chance, around 3 P.M. Teejay called from the CIA. "What's new?"

"We completed the trace over the weekend."

"Where is he?"

"In Hannover."

"Mmmm. Know the guy's name?"

"No, not yet."

"Does the 'F' entity know?"

"I don't think so. But call them and find out. They never tell me a thing." I doubted that the FBI would tell the CIA, and I didn't want to be squeezed between the two. It was weird enough to talk to either.

"Any clues to his identity?"

"Hard to say. Ever hear of the word Ulfmerbold?"

"Mmmm. What's that from?"

"The hacker chose that as a password when he broke into a computer this morning. At Fort Stewart, Georgia."

"He's not letting the grass grow, huh?" Teejay still tried to sound uninterested, but his voice had a tremor that gave it away.

"Yeah. He got into a couple other places too."

"Where?"

"Oh," I said, "no place special. Just a couple military bases in Germany. And a place called Fort Buckner."

"Son of a bitch."

"You know them?"

"Yeah. I used to work at Fort Buckner. Back in my Army days. Lived on base with my wife." A CIA agent with a wife? I'd never thought of it. Spy novels never mention spouses or kids.

The hacker had chosen a strange password for his use. Ulfmerbold. Nothing in my dictionary. Not in Cassell's German-English dictionary. The trusty atlas showed nothing. Yet I'd heard this word before.

Martha hadn't heard of it. Nor had any of her friends. Not even my sister, the one who'd risked her life prowling around a high school in McLean, Virginia.

It took three days, but my boss, Roy Kerth, figured it out. Ulf Merbold is the West German astronaut who'd made astronomical observations from the space shuttle.

Another clue to Germany, unnecessary, now that the evidence was overwhelming. But why pick an astronaut's name? Hero worship? Or some more sinister motive?

Could this explain why he kept breaking into computers? Could I have been following someone obsessed with the U.S. space program—a guy who dreamed about becoming an astronaut and collected information about the space program?

Nope. This hacker sought out military computers—not NASA systems. He wanted SDI data, not astronomy. You don't search for the space shuttle on Okinawa. You don't find an astronaut's biography by looking up the Army's nuclear warfare plans for Central Europe.

44

TUESDAY MORNING GREETED ME WITH A PILE OF MESsages from Tymnet. Steve White read some electronic mail from the Deutsche Bundespost. "Since the University of Bremen won't pay for any more international calls, you'll have to carry that cost."

He knew that we couldn't afford it. "Steve, my boss balks at paying my salary, let alone this hacker's connections."

"How much time are you putting in on this chase?"

"Oh, about ten hours a day." I wasn't kidding. Even a five-minute connection by the hacker ballooned into a morning of phone calls. Everyone wanted to hear what had happened. Nobody offered support.

"Well then, I've some good news for you," Steve said. "Wolfgang Hoffman says there's a meeting in Hannover tomorrow. Something about coordinating legal, technical, and law-enforcement activities."

"Why's that good news?"

"Because they expect to make an arrest this weekend."

Finally.

"But there's a couple problems. The Germans haven't heard from the FBI yet. So they're putting things on hold. Wolfgang asks that you pass this message to the FBI."

"Will do."

My next call to the FBI showed the flip side of the coin. Special Agent Mike Gibbons explained the situation.

He'd sent telegrams to Bonn telling the FBI's Legat to contact the German police. At the same time, he shipped by air a folder of information to the Attaché. But somewhere, the messages weren't getting through—Wolfgang still hadn't heard about any warrants from the FBI.

"You see, we can't talk to anyone except through our Legat," Mike said. "Still, I'll rattle the cage again, and see that they're awake in Bonn."

Well, that FBI agent sure wasn't dragging his heels. I never did find out much about the Legal Attaché—do they work for the FBI or the State Department? Is it one part-time person or a whole staff? What do they really do? Who do they talk to in the German government? What do you have to do to wake them up?

The CIA wouldn't leave me alone. Teejay wanted every detail about the past weekend. But the juicy stuff—the guy's name, his motives, and his backers—remained a mystery. All I knew was that he'd been fingered.

"Say, Teejay, if I find out some of this for you, is there any chance you might, uh, trade some gossip?"

"I don't copy," the spook said.

"I mean, suppose you figure out who was behind all this. What'll you tell me about it?" I really wanted to know if he could send some spy over there and find out what this clown was up to.

"Sorry, Cliff. We're listeners, not talkers."

So much for learning anything from the CIA.

Within a day, however, more news came by way of Tymnet. Having traced the hacker's phone number, they compared his name to that on the German Datex accounts.

Hmmm. They're doing their homework!

Seems that the hacker used three different identifiers when he manipulated the Datex network. The first identifier belonged to the hacker. Same name, same address. The second one belonged to another person. And the third . . . well, it belonged to a company. A small company in Hannover that specialized in computers.

Were these identifiers stolen? It's as easy to steal a network user identifier as it is to steal a telephone credit card number—

just watch over someone's shoulder as she makes a call. Perhaps the hacker has ripped off several people's Datex network account numbers. If they worked for big multinational firms, they might never notice.

Or was this guy in collusion with someone else?

I'd pretty much convinced myself that he was acting alone. If a couple people were working together, they'd have to constantly exchange passwords. Moreover, the hacker had a single personality—patient, methodical, an almost mechanical diligence. Someone else wouldn't have quite the same style when prowling around the Milnet.

A few of his targets weren't sleeping. The day after he tried to pry their doors open, two of them called me. Grant Kerr, of the Hill Air Force Base in Utah, phoned. He was annoyed that one of my users, Sventek, had tried to break into his computer over the past weekend. And Chris McDonald of White Sands Missile Range reported the same.

Super! Some of our military bases keep their eyes open. Thirty-nine in forty are asleep. But there are a few system managers who vigilantly analyze their audit trails.

For the next few days, the hacker kept me hopping. He kept scanning my SDINET files, so every few hours, I'd add a couple more. I wanted the files to reflect an active office—a backlog of work and a busy, chatty secretary who didn't quite know how her computer worked. Pretty soon, I was wasting an hour a day generating this flimflam, just feeding the hacker.

Zeke Hanson of the National Computer Security Center helped with these bogus files. I knew nothing about military ranks, so he gave me a few hints.

"The military's just like any other hierarchy. Up at the top, there's the flag officers. Generals. Below them are colonels, except in the Navy, where there's captains. Then there's lieutenant colonels, then majors and captains . . ."

Things are easier in grad school. Just call everyone with a tie "Professor," and anyone with a beard "Dean." When in doubt, just say "Doctor."

Well, every couple days the hacker would log into my system

and read the SDINET files. If he had any doubts about the validity of this information, he never showed it. In fact, he soon began trying to log into military computers using the account SDINET.

Why not? Some of these ersatz files described network links into Milnet computers. I made sure they were crammed with lots of jargon and technobabble.

Still, feeding the hacker bait wasn't leading us to an arrest. Every time he appeared, we traced him all right, but I kept waiting for a phone call saying, "He's at the police station now."

Now that the Germans had a suspect in mind, Mike Gibbons met with the U.S. attorney in Virginia. The FBI's news was mixed: if a German citizen is involved, extradition is unlikely, unless there's underlying espionage.

By the end of the week, the hacker had returned for five more sessions, each an hour or more. He checked into the Navy and Army computers, making sure that they still let him in. I wondered why they hadn't closed their holes yet. Then he played around our laboratory computer, again checking over the SDINET files.

Perhaps he worried that we knew he'd stolen Sventek's account, for he found yet another unused account at our lab, changed its password, and began using it for his hacking.

With all the high-powered computer folks in my department, I worried that one of them would post a notice to an electronic bulletin board, or casually leak the story in a conversation. The hacker still searched our system for words like "security" and "hacker," so he'd stumble onto this news and our bird would fly the coop.

The Germans had promised a bust this weekend. The hacker had what I hoped was his last fling on Thursday, January 22, when he broke into a computer at Bolt, Beranak, and Newman, in Cambridge, Massachusetts. This computer, called the Butterfly-vax, was as unprotected as the rest: you just logged in as "guest," with no password.

I'd heard of BBN—they had built the Milnet. In fact, most of the Milnet would soon be controlled by their Butterfly computers. The hacker had found a particularly sensitive computer—if

he planted the right kind of Trojan horse in this computer, he might steal all the passwords that ever crossed the Milnet. For this was where BBN developed their network software.

Stealing passwords at Lawrence Berkeley Labs only gives you access to nearby computers. The place to booby-trap software is where it's distributed. Slip a logic bomb into the development software; it'll be copied along with the valid programs and shipped to the rest of the country. A year later, your treacherous code will infest hundreds of computers.

The hacker understood this, but probably didn't realize that he'd stumbled into such a development system. He searched the system and found one glaring security hole: the root account needed no password. Anyone could log in as system manager without so much as a challenge. Whoa!

Someone was sure to discover such an obvious hole, so he wasted no time in exploiting it. He became system manager and created a new, privileged account. Even if the original flaw was discovered, he'd added a new backdoor into BBN's computer.

He created an account under the name Langman, with a password of "Bbnhack." I understood the password, all right, but why Langman? Could that be his real name? The German Bundespost won't tell me, but maybe the hacker himself did. What's the meaning of the name Langman?

No time to worry about it now. The hacker found a letter on the BBN computer, saying, "Hi, Dick! You can use my account at the University of Rochester. Log in as Thomas, with the password 'trytedj' . . ."

It didn't take him fifteen seconds to reach into the Rochester computer. He then spent an hour reading information about integrated circuit designs. Apparently, a graduate student at Rochester designed sub-micron circuits, using an advanced computer-controlled technique. The hacker started to grab everything, including the programs.

I wouldn't let him: this would be industrial espionage. Every time he started to copy some interesting files, I jingled my keys on the wires. He could look, but he'd better not touch. Finally, at 5:30, he gave up.

Meanwhile, I wondered about the word Langman. Was it someone's name?

Aah—there's a way to find out. Look it up in the phone book. Maggie Morley, our librarian, couldn't find a Hannover telephone directory, so she ordered one. A week later, with suitable aplomb, Maggie delivered the Deutschen Bundespost Telefonbuch, issue number seventeen, covering Ortsnetz and Hannover, with a rubber stamp on the side, "Funk-Taxi, 3811."

My atlas presented a dry, geographic Hannover. And the tourist guides spoke of a historic, scenic city, nestled along the river Leine. But the phone book, well, here's the city: the opticians, the fabric stores, a few dozen autohauses, even a perfumerie. And people . . . I spent an hour just paging through the white pages, imagining a whole different world. There were listings for Lang, Langhardt, Langheim, and Langheinecke, but not one Langman. Bum steer.

Steve White relayed a message from Germany. The Germans had been doing their homework. Apparently, when the hacker called a phone, the German police had printed out that phone number. Eventually, they figured out who was involved, just by piecing together the web of phone calls centered on the hacker.

Were the German authorities planning a simultaneous bust? Tymnet passed along a chilling message: "This is not a benign hacker. It is quite serious. The scope of the investigation is being extended. Thirty people are now working on this case. Instead of simply breaking into the apartments of one or two people, locksmiths are making keys to the houses of the hackers, and the arrests will be made when the hackers cannot destroy the evidence."