Subject: Penetrating the Phone System

PERSONAL COMPUTER USERS PENETRATING NATION`S TELEPHONE SYSTEM
By JOHN MARKOFF with ANDREW POLLACK (c.1988 N.Y. Times News Service)

adept at penetrating the nation's telephone system, raising questions about the security and privacy of the phone system, industry experts and law enforcement offiials say. The vulnerability of the phone system to such tampering has grown significantly in the past decade or so as telephone companies have largely replaced electro-mechanical call-routing equipment with computer-controlled switches.

As a result, people with the expertise can illegally connect their personal computers to the phone network. With the proper commands, these intruders can do such things as eavesdrop, add calls to someone's bill, alter or destroy data, have all calls to a particular number automatically forwarded to another number or keep someone's line permanently busy, it was disclosed in an internal memorandum written by a manager of electronic security operations at the San Francisco-based Pacific Bell Telephone Co. and in interviews with company officials.

Peter Neumann, a computer security consultant at SRI International Inc. in Menlo Park, Calif., said telephone companies are only beginning to awaken to the security problems created by the increasing computerization of the telephone network. ``As far as our vulnerability, we all have our heads in the sand,'' he said. ``We have to redefine our notions of what we entrust to computers and to communication networks.''

Some personal computer enthusiasts, often called ``hackers,'' view the task of breaking into the telephone system as a test of their skills and only infrequently inflict damage, industry officials and consultants say. But others act with criminal intent.

In his memo, the Pacific Bell security manager also warned that an electronic intruder could essentially disable an entire central switching office for routing calls, disrupting telephone service to entire neighborhoods. Furthermore, he said, organized-crime groups or terrorists might use such technology to their own advantage.

The integrity of customer bills could also be compromised, he said. Customers might rightfully or wrongfully dispute expensive calls, claiming the calls were placed on their bills by computer hackers.

Earlier this month, a teen-age computer enthusiast who requested anonymity provided The New York Times with the Pacific Bell memo, which was written a year ago. He said it had been obtained by a fellow hacker who illicitly eavesdropped on a facsimile transmission between Pacific Bell offices in San Francisco. The memo, which Pacific Bell verified as authentic, concluded that ``the number of individuals capable of entering Pacific Bell operating systems is growing'' and that ``computer hackers are becoming more sophisticated in their attacks.''

In one of two cases cited in the memo, a group of teen-age computer hobbyists were able to do such things as ``monitor each other's lines for fun'' and ``seize another person's dial tone and make calls appear on their bill,'' the memo said. One of the hackers used his knowledge to disconnect and tie up the telephone services of people he did not like. In addition, ``he would add several custom-calling features to their lines to create larger bills,'' the memo said.

In the second case, police searched the Southern California home of a man thought to be breaking into the computers of a Santa Cruz, Calif., software company. They discovered the man could also gain access to all of Pacific Bell's Southern California switching computers. wFiles were found containing codes and employee passwords for connecting with -- or ``logging on to'' -- the Pacific Bell switching systems and related computers. The man also had commands for controlling the equipment.

In another case involving tampering with telephone company switching equipment, local police and the FBI in the San Francisco area are investigating Kevin Poulsen, a former programmer at Sun Microsystems, said Joseph Burton, an assistant U.S. attorney in San Jose, and John Glang, a deputy district attorney for San Mateo County.

Authorities searched Poulsen's apartment in Menlo Park in February as well as the residence of a suspected accomplice in San Francisco, the officials said. Poulsen was said to be in Southern California and was unavailable for comment.

Burton said he could not discuss a current investigation. Glang would say only that the case had been taken over by the federal government because ``there are some potential national security overtones.''  But a security expert familiar with the case, who requested anonymity, said that Poulsen ``pretty clearly demonstrated you can get in and romp around inside a Bell operating system.'' ``What it pointed out,'' he said, ``was the serious vulnerability.''

Security consultants said other phone companies are equally vulnerable to such breaches. They noted that most phone service in the nation is provided by companies that were part of the Bell System until it was broken up in 1984 and still use similar equipment and procedures.

Michigan Bell officials said they had caught an intruder who tampered with the company's switching equipment last year. A spokesman declined to give details of the incident but said no arrest was made. ``We have been able to tighten our security arrangements,'' said Phil Jones, a company spokesman. ``There were lessons to be learned here.''

Jack Hancock, vice president for information systems at Pacific Bell, said his company had also taken steps to make it tougher to penetrate its systems. He said, however, that the company had to strike a balance between security and cost considerations so the phone system would still be widely affordable and easy to maintain.

``We could secure the telephone system totally, but the cost would be enormous,'' he said. ``A public service will probably always have certain insecurities in it.''

Though Pacific Bell refused to disclose the security measures it had taken, the company said it had restricted the ability to dial into its computers from

remote points.

As computerized communications become more sophisticated, companies will be able to improve security at a reasonable cost, said Barry K. Schwartz, a systems planning manager at Bell Communications Research, which does research for the seven Bell operating companies. It will be increasingly possible to program a computer so it will only answer a call from an authorized phone, he said. Another new technology on the horizon, he said, is electronic voice verification. A security system using this technology would be able to recognize those authorized to gain access to a computer by their voice patterns.

Telephone companies have long had to worry about electronic abuse of their networks. For several decades individuals have used electronic equipment to make long-distance phone calls for free. Some have used devices that generate a series of tones that provides access to long-distance lines. Telephone companies have installed equipment on their lines to detect and thwart such abuse. In other instances, people have used personal computers to find long-distance access codes belonging to other users. They do this by programming computers to keep trying various numbers until they hit upon one that works. But while costly, these kinds of abuse are not much of a threat to the integrity of the system because they do not affect the system itself.

The new problems involving network tampering are arising, experts say, because the switches that route calls are now mostly electronic, meaning they are essentially big computers. If a customer wants an option like call forwarding or call waiting added to his or her telephone service, that is done by typing commands into a computer, not by moving wires and switches.

Pacific Bell said 79 percent of its customers are now served by computerized switching systems. Experts say these electronic networks are especially vulnerable to tampering because it is possible to dial up the computers controlling the switches from the outside. Phone companies designed their systems this way to make it easier for them to change the system and diagnose problems. For example, a technician in the field trying to diagnose problems on a line needs to be able to dial certain test circuits in the central office. But such a dial-up capability can also be used by outsiders with personal computers and modems who know the proper numbers to call and the proper procedures to get on the system.

The ability to eavesdrop on telephone calls is included in the system to allow an operator to check to see whether a line that is busy for a long time is being used or whether the phone is off the hook or the line is broken.

One security consultant who requested anonymity said this capability had also made it much easier for law enforcement officials to wiretap a line. When the police receive court permission to conduct a wiretap, they can have the phone company dial up the switch serving the line so conversations can be monitored from a remote location. Obtaining the information needed to break into the phone system can be difficult, but intruders often do it by impersonating phone company employees -- a practice that hackers call ``social engineering.''

A teen-ager interviewed by Pacific Bell officials after his arrest told investigators that he had entered a number of Pacific Bell facilities in the San Francisco area disguised as a Federal Express delivery man in order to

search for manuals and other documents, according to the company memo. The youth also said he had impersonated telephone security officials to obtain passwords and other information.