<-> Hackers in the MOB <->

****

According to Schmidt, the dollar amounts are only part of the story, GTE Telemail, an electronic mail system, was broken into by at least four gangs of hackers, he says. "They were raising hell. The system got shut down one time for a day. None of these people have been charged, nor have any of the 414s been charged yet.

"We have a major problem with hackers, phreaks and thieves," says Schmidt, who estimates that 75% of criminal hackers are teenagers and the other 25% are adults using teenagers to do their dirty work for them.

"Adults are masterminding some of this activity. There are industrial spies, people playing the stock market with the information- just about any theft or fraud you can do with a computer. There are no foreign agents or organized crime yet, but it's inevitable," he says. "I believe there are some people out there now with possible organized-crime connections.

"It's an epidemic. In practically every upper-middle class high school this is going on. I know of a high-school computer class in a school in the north Dallas suburbs where the kids are trying everything they can think of to get into the CIA computers."

"It's a strange culture," says SRI's Parker, "a rite of passage among technology-oriented youth. The inner circle of hackers say they do it primarily for educational purposes and for curiosity. They want to find out what all those computers are being used for. There's a meritocracy in the culture, each one trying to out do the other. The one who provides the most phone numbers and passwords to computer systems rises to the top of the hackers.

"For the most part it's malicious mischief," Parker says. "They rationalize that they're not really breaking any laws, just 'visiting' computers. But that's hard to believe when they also say they've got to do their hacking before they turn 18 so they don't come under adult jurisdiction. After 18, they have to do it vicariously through surrogates. They are some grand old men of hacking who egg on the younger ones... There have been some cases of a Fagin complex- a gang of kids led by one or more

adults- in Los Angeles."

Who are the hackers and what secret knowledge do they have?

A 17-year-old youth in Beverly Hills, California, announced himself to other hackers on a bulletin board in this way: "Interests include exotic weapons, chemicals, nerve gases, proprietary information from Pacific Telephone..."

Prized secret knowledge includes the two area codes in North America that have not yet installed electronic switching system central-office equipment. Using this information you can call those areas and use a blue box to blow the central office equipment, and then call anywhere in the world without charge. Other secret information lets you avoid being traced when you do this.

A knowledge of the phone systems lets hackers share one of the technological privileges usually available only to large corporate customers: long-distance conference calls connecting up to 59 hackers. Schmidt estimates there are three or four conference calls made every night. The hackers swap more inside information during the phone calls.

Thanks to packet-switching networks and the fact that they don't have to pay long-distance charfus, time and distance mean almost nothing to hackers. Desktop microcompters hook into phone lines via modems make it easy to obtain copyrighted software without human intervention.

"Software piracy exists only because they can do it over the phone long distance without paying for it," Schmidt says. "some stuff gets sent through the mail, but very little. There are bulletin boards that exist solely for the purpose of pirating software. A program called ASCII Express Professional (AE Pro) for the Apple was designed specifically for modem-to-modem transfers. You can make a copy of anything on that computer. It can be copyrighted stuff- WordStar, anything. There are probably about three dozen boards like that. Some boards exchange information on breaking onto mainframes.

"In 1982 the FBI really didn't know what to do with all this information," Schmidt says. "There isn't a national computer-crime statue. And unless there's $20,000 involved, federal prosecutors won't touch it."

Since then, the public and federal prosecutors' interest has picked up. The film War Games and the arrest of 414 group in

Milwaukee "created a lot of interest on Congress and with other people," FBI instructor Lewis says. "But, for ourselves it didn't really have any impact."

"We'd been providing the training already," says Jim Barko, FBI unit chief of the EFCTU (economic and financial crimes training unit). He says public interest may make it easier to fight computer crime. "There are more people interested in this particular area now as a problem. War Games identified the problem. But I think it was just circumstantial that the movie came out when it did."

Despite the help of knowledgeable informants like Schmidt, tracking down hackers can be frustrating business for the FBI. SRI's Parker explains some of the pitfalls of going after hackers: "Some FBI agents are very discouraged about doing something about the hacking thing. The cost of investigation relative to the seriousness of each case is just too high," he says. "Also, federal regulations from the Department of Justice make it almost impossible for the FBI to deal with a juvenile."

An FBI agent cannot question a juvenile without his parents or a guardian being present. The FBI approach has been mostly to support lhe local police because local police are the only ones who can deal with juveniles. Another difficulty the agency faces is the regulations about its jurisdiction.

"There has to be an attack on a government agency, a government contractor or a government-insured institution for the FBI to have clear-cut jurisdiction," Parker says.

The FBI gets called into a case only after a crime has been detected by the complaining party. The FBI has done a generally competent job of investigating those crimes it was called in to investigate, in Parker's view. But the federal agency's job is not to help government or financial institutions attempt to prevent crimes, nor is its function to detect the crimes in the first place.

"We're not out detecting any type of crime," says Lewis. "We like to think we can prevent them. We can make recommendations. But do we detect bank robberies or are they reported to us? Or kidnapping- do we detect those? Or skyjacking? There must be some evidence of crime, a crime over which the FBI has jurisdiction. Then we open a case." And despite the spate of arrests and crackdowns last summer, it looks like the FBI will have its hands full in the future: The hackers have not gone away. Like mice running through the utility

passages of a large office building, they create damage and inconvenience, but are tolerated as long as their nuisance remains bearable.

That status could change at any time, however.

Meanwhile, little electronic "sting" operations similar to Abscam keep the element of danger on the hacker's game. An Air Force telephone network called AUTOVON (a private telephone system connecting computers on every Air Force installation in the world), was reportedly cracked by a hacker last last year. The hacker published lists of AUTOVON dialups on a bulletin board.

The breach came to the attention `oo the Department of Defense on late 1983, but apparently nothing was done to stop the hackers. Then, in January, the AUTOVON number was answered in a sultry female voice. We wish to thank one and all for allowing us to make a record of all calls for the past few months. You will be hearing from us real soon. Have a happy New Year."

That's a New Year's message calculated to give any hacker a chill.

-End of file-

.