Back to Article Click to Print

TIME
IN PARTNERSHIP WITH CNN

Monday, Aug. 29, 1983

Computers: The 414 Gang Strikes Again

By Jamie Murphy;Philip Elmer-DeWitt;Magda Krance

Pranksters disrupt a hospital, and nobody is laughing

The red brick Memorial Sloan-Kettering Cancer Center on Manhattan's Upper East Side is an example of advanced medical technology. Every year more than 10,000 patients, ranging from infants with leukemia to statesmen with brain tumors, are admitted to this world-renowned research hospital, where they are analyzed, probed and treated by the most sophisticated high-tech equipment available. There are giant X-ray scanners, imaging devices and accelerators for beaming particles on diseased tissues, many operating under computer control.

One Friday morning last June, Chen Chui, systems manager of the hospital's medical physics computer service, discovered to his great astonishment that a Digital VAX 11/780 computer, which monitors the radiation treatment for 250 patients, had inexplicably failed during the night. Looking into the machine's log, he found that a file of billing records worth about $1,500 was missing and that passwords had been issued to five unauthorized accounts. Chui deleted the new names and took the extra precaution of replacing all the passwords for those authorized to change patient records.

Chui hoped that that would be the last of it. It was not. After the weekend he discovered that someone had made contact with the computer through a telephone hookup and introduced a new program: whenever a legitimate user typed in his password, the code name was immediately sent to the intruder. "It was panic," says Dr. Radhe Mohan, director of the computer service. "Someone was up to big mischief that could have conceivably caused harm."

Sloan-Kettering officials called the New York City police, the FBI and New York Telephone security, which tapped the phone lines connected to the machine. Then Chui tried to reach the intruders by leaving messages in their computer terminals. "You have done some harm to the system," read one plea. "Please call us and help us repair the damage." About an hour after the message went out, someone called back. "He said he was sorry," recalls Chui. "But when we asked how he got into the system he refused to answer."

The intruder appeared chastened, yet over the next two months there were about 20 other calls to the computer; the most recent took place on Aug. 11. In July the hospital received a tip identifying two young men in the Milwaukee area as the source of the trouble. The two were innocent, but the Milwaukee connection turned out to be the break that police needed. For months, FBI agents had been tracking the activities of a loosely organized gang of computer enthusiasts in and around Milwaukee who call themselves "the 414s" after that city's telephone area code. Using home computers connected to ordinary telephone lines, they had been breaking into computers across the U.S. and Canada, including one at a bank in Los Angeles, another at a cement company in Montreal and, ominously, an unclassified computer at a nuclear weapons laboratory in Los Alamos, N. Mex.

Earlier this month federal authorities were investigating seven members of the group, ages 15 to 22, for illegally penetrating dozens of computer systems, including the one at Los Alamos. Last week papers filed in Federal District Court in Milwaukee identified Gerald Wondra of West Allis, Wis., a 21-year-old member of the 414s, as one of the people who broke into the medical center's computer.

The Sloan-Kettering caper and this summer's hit movie WarGames—the story of a young computer buff who nearly sets off a nuclear war when he accidentally gets into one of the Defense Department's most sensitive machines—have focused attention on a serious question: How

to safeguard information stored inside computers? The potential for fraud is awesome. The American banking system alone moves more than $400 billion between computers every day. Corporate data banks hold consumer records and business plans worth untold billions. Military computers contain secrets that, if stolen, could threaten U.S. security. Many of these machines are hooked into the telephone system, which enables them to communicate with other computers and with users in remote locations. But as the 414s have demonstrated, anyone with one of the popular new microcomputers has the potential, however remote, to unlock the secrets contained in machines operated by banks, hospitals, corporations and even military installations.

In the wake of the Milwaukee investigation, hundreds of companies and individual computer owners were scrambling to see whether their information was safe from computer tampering. "Our phone has literally been ringing off the hook," said Robert Campbell, president of Advanced Information Management in Woodbridge, Va., a consulting firm that advises banks and credit-card services on how to protect their computer information. Campbell and others in the computer security field, whose fees range up to $1,000 a day, say that since January there have been at least a dozen major cases of tampering or theft of computer data in the U.S. "There is a whole epidemic of malicious system hacking going on," says Donn Parker, computer crime specialist at SRI #tml97ut5.24in Menlo Park, Calif. Concurs Ron Zeitz, a spokesman for GTE Telenet, the computer network used to get into the Sloan-Kettering system: "It's like the skyjacking phenomenon. People are going to try what other people are getting away with."

The consultants advise clients that the surest way to protect their information is to put their computers under lock and key. But as networks of computers connected by phone lines grow, that kind of isolation becomes irrelevant. More elaborate precautions like passwords, dedicated telephone lines and voice analyzers offer some degree of security. Encryption, which scrambles messages, is perhaps the best way to protect data sent over the wires. It is expensive (up to $5,000 per terminal) and difficult to use. Nonetheless, for those willing to pay the price, the technology for protection exists.

— By Philip Elmer-DeWitt

Reported by Magda Krance/Chicago and Jamie Murphy/New York