Computer hacking and security costs

About once in 10 tries, a person can break into a typical computer system connected to a telephone network. All that person needs is a telephone link to a computer communications system like the commercial TELENET system.

By selecting an area code, then sequentially trying code numbers and listening for a recognizable signal, a "hacker," as these invaders are called, can identify a computer brand's characteristic signal. Manuals for that machine list standard passwords installed when the system was shipped from the factory. Sometimes these passwords are still applicable. Once the hacker gets into the system, he or she can discover other passwords or codes that allow access to, for instance, privileged accounts or sensitive data.

Although such unauthorized invasions of computer systems have been going on for more than a decade, new attention is focusing on computer security. In particular, fears concerning computer vulnerability have been fanned by the wide publicity given to a young group of Milwaukee hackers, the 414s (named for the city's telephone area code), who dialed into bank, laboratory and hospital computers "for fun," and by the movie "WarGames," which portrayed a high school student's accidental entry into a military computer system. Last week, the topic was a major concern in New York at the annual conference of the Association for Computing Machinery (ACM) and the subject of Senate hearings in Washington, D.C.

At the ACM meeting, Kenneth L. Thompson, a computer programmer at AT&T Bell Laboratories in Murray Hill, N.J., acknowledged that the acts of groups like the 414s have caused "extreme consternation" within the computer industry. He blamed the media for overstating the danger and glorifying the hackers.

"What they [the media] have done is to cause legislation to start popping up in state legislatures and [Congress] to stamp out this 'horrible' problem," Thompson said. This legislation would impose heavy criminal penalities for unauthorized access to computers. In Thompson's view, this is an unnecessarily harsh response to acts more like "computer joy-riding." The answer is to teach the youngsters "that what they are doing is nothing short of vandalism," Thompson said, "and that the whole activity should be viewed simply as very similar to breaking into someone else's house — even if you don't steal anything, even if the door is unlocked."

David H. Brandin, ACM president, however, said, "People that operate unprotected computer systems are guilty, too — of contributory negligence.... We need to raise their consciousness also."

But for most institutions, businesses and government agencies, now heavily committed to computer use, new security problems keep cropping up (SN: 7/3/83, p. 12). Generally, the intrusions of hackers are a much less serious concern than the increasing number of people gaining access to computers where they work. Leslie D. Ball of Babson College in Babson Park, Mass., noted, for example, that an enormous number of workstations — which may be as simple as a portable keyboard with a liquid-crystal display — are now connected to large central computers or to other workstations.

"The 'trusted group' was once a small number of people within an organization who required access to the system or components of the system," Ball said. "Now that trusted group is so large, its membership can only be estimated." One panelist commented that the only way one company could find out how many personal computers, many with access to a network or the main computer, were in use was to count up the number of insurance claims after a fire caused damage to the offices.

Ball added, "This expanded, trusted group does not have the security awareness ... [that] long-time employees at the central site have." Thus, seemingly routine security problems like losing data-carrying computer diskettes, writing over data that are not permanently stored elsewhere and leaving workstations turned on although they are not in use are widespread.

Media coverage of computer crimes seems to have alerted senior management in many companies to the substantial risks involved in failing to take reasonable precautions to protect a computer system from abuse. Lawyer Susan H. Nycum of Palo Alto, Calif., reported, "Many companies that had previously considered that their security measures were adequate are now asking me to perform updates to the security reviews and resulting security plans that they or we performed in the past."

However, despite current concerns, sales of security technology like encryption devices have not increased substantially, if at all. In many cases, although a wide variety of security measures are available, they are expensive to implement and frequently interfere with the convenience that authorized computer users expect. For example, passwords should be changed often, but not so often that people will forget them easily and need to write them down (creating a new security problem) or so seldom that passwords become generally known within an office. The correct balance is difficult to hit.

One security analyst commented, "We have a real problem here. The only thing you can do is to make [unauthorized access] more difficult. You can never make it impossible." It becomes question of how much a company is willing to pay — in inconvenience and in dollars. —*I. Peterson*

Bypass surgery not always necessary

A man suffering from heart disease and scheduled for open heart surgery asked his physician last week whether his bypass operation was one of the "unnecessary ones." His surgeon replied, "Certainly not."

The patient asked the question, according to his surgeon, Henry Spotnitz of the Columbia Presbyterian Medical Complex in New York, because he had heard about the Coronary Artery Surgery Study (CASS), which the National Institutes of Health released last week. The study concludes that for patients with mild to moderate coronary artery disease, like those in the study, there are no significant survival differences between those who receive medical treatment and those who undergo surgery. For these mild to moderately diseased patients, surgery can be safely delayed until symptoms worsen, according to the study. Altogether, patients in this category accounted for 25,000 of last year's 170,000 bypass operations, which cost $10,000-$25,000 each.

In the 15-center, five-year study, 390 patients initially were treated medically and 390 had bypass surgery. The patients in the study either had mild to moderate chest pain, with or without a history of heart attack, or had no chest pain but a history of heart attack. The average age of the patients studied was 51; 90 percent were male, and 60 percent reported having had a prior heart attack. After five years, 95 percent of the surgically assigned patients and 92 percent of the medically assigned ones were alive.

The study also concludes that the "quality of life" was better in the surgically treated patients. The director of the CASS steering committee, Thomas Killip of Detroit's Henry Ford Hospital, said, "As expected, surgical patients in the study have enjoyed great relief from angina [chest pain] during follow-up. They were also able to exercise longer and took fewer drugs than the medical group. However, there is no difference between the two groups in recreational activity or return to work. There are more hospitalizations in the surgical patients."

The study was designed for learning more about the patients with mild symptoms where the need for bypass surgery is unclear and *not* for the patients with more severe symptoms. Eugene Passamani, associate director for cardiology at the National Institutes of Health in Bethesda, Md., said, "Coronary artery bypass surgery is clearly indicated in patients with 60 percent or greater narrowing of the left main coronary artery and in patients whose symptoms impose unacceptable limitations. In these two categories, surgery increases both the quantity and quality of life."

As for whether these results will have