sometimes feel that their faculty constituents are refactory to explanation," Kennedy and Coor said. The fact that both sides acknowledged the problem and agreed to try to have a useful "dialog" is, in itself, considered a mark of progress in an argument that must ultimately be settled by Congress, which has not gone along with recent attempts to reduce funds for indirect cost reimbursement. The issue is likely to come up again when the next NIH budget is prepared. It is also the subject of a report soon to be released by the General Accounting Office.—**BARBARA J. CULLITON**

Computer Break-Ins Fan Security Fears

But experts say computers containing classified material are invulnerable and that others can be made more secure

In early August, it was reported that a group of young people in Milwaukee broke into a computer at Los Alamos National Laboratory. The break-in attracted an extraordinary amount of publicity, in part stimulated by the popular movie *War Games*, in which a teenager is depicted breaking into a Defense Department computer and almost precipitating World War III.

Shortly after the Los Alamos break-in was reported, an alarming entry into a computer at Memorial Sloan-Kettering Cancer Center in New York hit the headlines. In this incident, a computer hack, who apparently is a member of the Milwaukee group, used a $1200 Apple computer to gain access to patient records.

These incidents have raised concerns that classified data and other sensitive information stored in computers might be readily available to anyone with a terminal, including foreign agents or people engaged in industrial espionage. Computer security experts maintain, however, that computers containing highly classified information are virtually invulnerable because they are not linked to any outside system. It is therefore impossible for anyone to dial into them. Moreover, experts say that even computers that are linked to outside networks can be made more secure so that break-ins can be quickly detected.

The Los Alamos computer was being used to develop an electronic mail system and it contained no sensitive information. Therefore it was not heavily protected against break-ins. Such a procedure makes excellent sense, says Robert Courtney, a computer crime consultant living in New York. "It would be dead wrong to secure that which is not worth securing. The idea is to try and make systems as usable as you can," Courtney explains. The key point about the Los Alamos and Sloan-Kettering break-ins are that the security controls on the computers there were not at all like those on computers containing classified information. Yet even with those relatively lax controls, the Milwaukee youths were traced and identified.

The controls on computers that contain classified information cannot be broken at all, experts say. "I do not know any way even remotely possible of getting into those computers without a breach of trust," says Robert Morris, a computer security expert at Bell Laboratories in Whippany, New Jersey, who is often asked to try to break into computers to test their vulnerability.

Computers containing classified data are isolated from the outside world, so that no one—not even people with clearances to work on the computers—can dial a phone number from their home or other insecure area and log into them. The Milwaukee group dialed into networks that connect insecure computers and then logged into computers in the network. The Los Alamos and Sloan-Kettering computers are connected to Telenet, a commercial network.

The Cray computer at Sandia National Laboratory is typical of those that contain classified information. No unauthorized persons are allowed into the heavily guarded facility where scientists primarily work on the engineering of nuclear weapons. The Cray is "Tempest-certified" by the National Security Agency (NSA), meaning that no electromagnetic radiation can be detected outside the computer room. The NSA worries that if radiation escapes, it could be "read" by special equipment to reveal what information the computer is processing. Every terminal for the Cray is also Tempest-certified.

The Cray computer is linked to a computer at Los Alamos that also contains classified information. But the data that flow between the two computers cannot be read by tapping the link between them. Those data are encrypted with codes supplied by the NSA. The keys for decrypting at either end are delivered by courier. "I don't expect to see one of those [codes] broken during my career," says Gus Simmons, the manager of Sandia's mathematics department.

Many computers containing classified information are not linked to other computers at all. But the Department of Defense and the intelligence agencies do have their own private networks to connect secure computers. The DOD network is called World Wide Military Command and Control System, or WWMCCS, and the network used by the NSA and the Central Intelligence Agency is called Community On-Line Intelligence Network System, or COINS. Like those at Sandia and Los Alamos, computers in these networks cannot be reached by dialing outside telephones. They can only be used in "secure areas" that are Tempest-certified and the data flowing between the computers are encrypted. "I'm a skeptic, not a believer, but everything I've seen of those systems makes me feel secure," Morris says.

But security comes at a price: the computers are fairly cumbersome to use. Mostly because of the inconvenience of working in the special rooms at Sandia containing the Cray terminals, members of Simmons' group tend not to use the Cray unless it is absolutely necessary. Currently, only 3 of the 24 group members are using the Cray, Simmons says.

Another difficulty with these computers is that only people with the highest security clearances can use them. For example, if a computer contains both top secret, secret, and confidential information, only people with top secret clearances would be allowed to use it because it is impossible, in most cases, to prevent people from getting at any files they want once they have access to a computer.

This stratification of computers is expensive and awkward and the DOD would very much like to see computers designed so that they can effectively separate different classes of users. One computer, the Multex, built by Honeywell, can apparently keep one group of

users away from another groups's data, and it is being used by the Air Force within the Pentagon to store secret and top secret information. Honeywell has submitted the Multex design to the NSA's Computer Security Center for certification that it is as secure as advertised. So far, the NSA has reached no decision on it. But the problem of keeping three classes of data on the same computer is still unsolved.

Although computers linked to outside networks are potentially much more vulnerable, security has improved considerably in recent years. Until fairly recently, for example, it was easy to break into computers that are linked together by systems like Telenet simply by dialing the computer on your telephone and then continually guessing at likely passwords until you hit on one that the computer accepts. (This was the tack that succeeded in *War Games*.) It was not too difficult to hit on a password because people tend to choose words that are easy for them to remember, such as their names. But after Morris and Ken Thompson of Bell Laboratories in Murray Hill, New Jersey, published a paper showing that they could guess 50 percent of the passwords at Bell Laboratories, people have become more cautious about the words they choose. In addition, many computers no longer let you keep guessing away at passwords. Now, says Courtney, "Most of the better business systems let you try two times, but on the third try they either shut you out completely or let you in to see some insensitive information while they trap you by tracing the call."

The passwords at Sloan-Kettering were not peoples' names and therefore, say officials there, they should have been difficult to guess. Radhe Mohan, who is director of the medical physics computing service at the hospital, says no one has any idea how the Milwaukee youth got into the computer through Telenet. Radhe explains that the computer was linked to Telenet so that 80 other hospitals could have access to medical data stored there.

Password-type security cannot be made foolproof, however. Morris says people often get passwords from exemployees, family members of employees, or even by walking into a computer room where, frequently, passwords and access codes are taped to a terminal.

The type of security used in the Los Alamos and Sloan-Kettering computers, says Simmons, is like a lock on a car door. "You might lock your car and leave your groceries in it, but you wouldn't leave your jewels inside."

A number of corporations and banks are now taking steps to increase their computer security. At AT&T, says Morris, computer hacks "don't have a prayer of getting into computers containing corporate information. Those computers have no outside connections." Even computers that contain relatively insensitive data are getting increasingly hard to penetrate, and if a break-in does occur, it is possible to get an extensive audit trail to trace the source of the break-in.

Morris no longer finds that he can get any data he wants out of Bell Labs computers with impunity. "If I'm messing around, I have to go extreme lengths to avoid detection. The days are long gone when I could pick up the phone and log into a computer without getting caught. Now if I do something bad, chances are they will catch me for that single instance." Morris emphasizes that he is specifically authorized by Bell Laboratories to try and break into computers and that his background as a computer designer gives him some advantages.

This is not to say that there is no longer a computer security problem. Although corporations like AT&T are in the forefront of protecting computer data, other corporations and much of the federal government lag far behind. But more and more people are becoming aware of the problem of computer security and are beginning to take steps to foil computer crime or to catch the criminals in the act.—GINA KOLATA

IOM Elects New Members

The Institute of Medicine has elected 36 new members, raising the total active membership to 456 when their terms begin next 1 January. Five persons were elected to senior membership, bringing that total to 194.

The new members are: **Ronald M. Andersen**, Center for Health Administrative Studies and Graduate Program In Hospital Administration, University of Chicago; **Howard L. Bailit**, department of health administration, School of Public Health, Columbia University; **James W. Bawden**, department of pedodontics, Dental Research Center, University of North Carolina, Chapel Hill; **Steven C. Beering**, Purdue University; **Allan Beigel**, Southern Arizona Mental Health Center, Tucson; **George B. Benedek**, department of physics, Massachusetts Institute of Technology; **J. Robert Buchanan,** Massachusetts General Hospital; **William B. Carey**, private practice, pediatrics, Media, Pennsylvania; **Purnell W. Choppin**, virology, Rockefeller University; **Peter B. Dews**, psychiatry and psychobiology, Harvard Medical School.

Rhetaugh G. Dumas, School of Nursing, University of Michigan, Ann Arbor; **Mitzi L. Duxbury**, School of Nursing and Center for Health Services Research, University of Minnesota, Minneapolis; **David M. Eddy**, Center for Health Policy Research and Education, Duke University; **Charles C. Edwards**, Scripps Clinic and Research Foundation; **Edward V. Evarts,** Laboratory of Neurophysiology, National Institute of Mental Health; **Charles J. Fahey**, aging studies, Third Age Center, Fordham University; **Howard E. Freeman**, sociology, University of California, Los Angeles; **Jerome H. Grossman**, New England Medical Center; **Melvin M. Grumbach**, department of pediatrics, University of California, San Francisco; **Curtis G. Hames**, private practice, medicine, Claxton, Georgia; **Edward W. Hook**, department of internal medicine, University of Virginia, Charlottesville; **Lyle V. Jones**, department of psychology, University of North Carolina, Chapel Hill; **Robert Katzman**, department of neurology, Albert Einstein College of Medicine.

Stuart A. Kornfeld, medicine and biochemistry, School of Medicine, Washington University; **Paul E. Lacy**, department of pathology, School of Medicine, Washington University; **Claude Lenfant**, National Heart, Lung, and Blood Institute; **Lawrence S. Lewin**, Lewin and Associates, Inc., (health policy consultants), Washington, D.C.; **C. S. Lewis, Jr.**, private practice, internal medicine and cardiology, Tulsa, Oklahoma; **Hugh O. McDevitt**, medical microbiology and medicine, Stanford University School of Medicine; **James A. Pittman Jr.,** School of Medicine, University of Alabama, Birmingham; **Charles E. Rosenberg,** department of history, University of Pennsylvania, Philadelphia; **Louise B. Russell**, economic studies program, The Brookings Institution, Washington, D.C.; **Bruce J. Sams, Jr.**, The Permanente Medical Group, Inc., Oakland, California; **Robert T. Schimke,** department of biological sciences, Stanford University; **Margretta M. Styles**, School of Nursing, University of California, San Francisco; **Sheldon M. Wolff,** department of medicine, Tufts University School of Medicine.

The new senior members are: **Tibor J. Greenwalt**, Hoxworth Blood Center, University of Cincinnati Medical Center; **Robert Hofstadter**, physics, Stanford University; **Moshe Prywes**, University Center for Health Sciences, Ben Gurion University of the Negev, Beer Sheva, Israel; **Malcom Randall**, Veterans Administration Medical Center, Gainesville, Florida; **John R. Seal** (retired), disease prevention, Office of the Director, National Institutes of Health.