The complexity of computer security

"To a good approximation, every computer in the world is connected to every other computer — with few exceptions," says Robert Morris, chief scientist at the National Security Agency. That level of sharing brings with it both great benefits and serious problems. Computer users can share information, resources and processing power. However, using the same links, they can destroy or alter a rival's data, eavesdrop on private communications or pass on insidious computer programs capable of proliferating like viruses, overwhelming networks and taking over computer operations.

Morris was on a panel of computer security experts appearing this week before the Computer Science and Technology Board at the National Academy of Sciences in Washington, D.C. The board is interested in initiating a study addressing computer security issues, especially those affecting the creation of a national computer network for research (SN: 6/18/88, p.394).

Most commercial computer systems — from linked personal computers in an office to nationwide data networks — have weak controls on access and poor protection against accidental errors and intentional misuse, says Peter G. Neumann, a computer security specialist at SRI International in Menlo Park, Calif. Often, such system limitations and vulnerabilities are poorly understood.

"And the stakes are increasing dramatically," Neumann says. For instance, in December 1987, a seemingly innocuous Christmas message originating in West Germany spread into a network of IBM machines in the United States. The message sent copies of itself to everyone on any "infected" computer's mail distribution list, rapidly clogging and shutting down the network.

There's more to computer security than keeping out intruders, stopping computer viruses or averting misuse by insiders, several panel members insisted. It also means ensuring that computer systems work reliably, predictably and accurately.

The real problem is complexity, Morris says. Computer scientists have a hard time understanding and analyzing computer programs more than a few thousand lines long. When complicated software is combined with intricate electronic machines, elaborate communications systems and the quirks of users, a typical computer system represents an exceedingly high level of complexity. Such systems can fail in many different and unexpected ways.

"Simply put, modern-day, complex mechanisms do not work properly," Morris says. "We have to learn to cope with complexity."

Computer scientists now have techniques for proving mathematically that certain computer programs and microprocessor designs are correct. But that method is effective only for short programs and fails to address more general security concerns. Still missing are techniques for understanding what happens when tested and verified components are put together into a system. Without this kind of fundamental understanding, no one can guarantee that a given computer system will handle data correctly and safely.

"Any weak link allows someone to abuse the system," Neumann says. "It's dangerous to try to look for simple answers." — *I. Peterson*

Discovery: TDRS and other plans

The major mission activity in the upcoming flight of Discovery, representing the shuttle program's return to life 32 months after the Challenger disaster, continues a satellite project that never did get off on the right foot.

It was in the early 1970s that NASA first began planning the use of a network of satellites to replace the ground stations with which it tracks spacecraft and relays their data. The hope was to greatly increase the amount of time for which satellites — including the then-untried shuttle itself — could communicate with the ground. The first Tracking and Data-Relay Satellite (TDRS-1) was launched on April 4, 1983 (Challenger's maiden flight). But trouble with its booster rocket left it in too low an orbit, which required nearly three months of gradual nudges to correct. The second TDRS was destroyed in 1986 with Challenger itself.

The latest TDRS is the heaviest item in Discovery's payload, weighing more than 2 tons, plus 16 tons for its booster. TDRS-1 is now relaying data for the Solar Maximum Mission satellite, the Solar Mesosphere Explorer, the Earth Radiation Budget Satellite and Landsats 4 and 5. NASA plans to phase out many of its ground stations, but the TDRS system must first consist of two operational satellites plus a third in orbit as a spare. The third is tentatively scheduled for launch early next year, to be followed later by one to replace the now-aging TDRS-1.

Besides deploying the new TDRS, Discovery's astronauts are to conduct microgravity experiments in materials processing and life sciences, as well as observing lightning and other phenomena below. They also plan to test a system of secure on-board communications using infrared devices like television remote-control units, which produce no radio transmissions that can be picked up outside the shuttle. — *J. Eberhart*

Opening delayed for nuclear waste site

Regulatory problems and safety questions forced the Energy Department to postpone its planned October opening of the $700 million facility for storing nuclear waste underneath the New Mexico desert, federal officials told a House subcommittee last week. Even evaluators within the Energy Department have joined the criticism of the agency's safety analyses, according to internal memos made public at the hearing.

Called the Waste Isolation Pilot Plant (WIPP), the facility contains 56 rooms carved out of salt deposits located 2,100 feet below ground near Carlsbad, N.M. It is designed to store wastes from the Defense Department's nuclear weapons program that are contaminated with radioactive transuranic elements.

The Energy Department has yet to demonstrate that the facility will meet Environmental Protection Agency standards for storing nuclear waste. It had planned to start placing waste in the facility next month as part of a five-year-long series of tests designed to demonstrate compliance with the standards. Last month, however, the department announced it would not meet its schedule, and it has offered no revised date for opening WIPP, according to Richard Marquez, Energy Department spokesman in Albuquerque, N.M.

Earlier this year, the department scaled down the amount of waste it planned to use for the test project (SN: 3/19/88, p.188). Prior to that decision, water leaking into the facility led a New Mexico state scientific advisory committee to criticize the department's plans for the testing period (SN: 1/23/88, p.54).

Several major impediments stand in the way of opening WIPP:

- The Energy Department must finish testing the canisters that hold the waste as it is transported to the WIPP facility. The Nuclear Regulatory Commission must then certify the canisters.
- The Energy Department has pledged to publish a complete plan outlining the tests it will perform during the next five years to demonstrate compliance with EPA standards. An earlier, unpublished draft of the plan was not acceptable, says Lokesh Chaturvedi of the Environmental Evaluation Group, the New Mexico committee overseeing WIPP.
- The Energy Department must publish a Final Safety Analysis Report to be reviewed by its own safety board and by the Environmental Evaluation Group. At the hearing, Rep. Mike Synar (D-Okla.) released internal Energy Department memos that criticized a preliminary version of the report, saying it failed to convince evaluators the plant was safe to operate. — *R. Monastersky*