Federal computer security concerns

"The inherent ability of current computer systems to protect themselves and their data is appallingly low," says Robert L. Brotzman, director of the federal government's computer security center in Fort George G. Meade, Md. "Computer security requires a fundamental change in the way industry designs and builds computers," adds Col. Joseph S. Greene Jr., the center's deputy director.

These remarks, made last week at the National Computer Security Conference in Gaithersburg, Md., reflect one major concern among officials responsible for ensuring that all federal computer systems adequately protect data. With the rapid growth of computer networks, information systems are "more vulnerable today than they were four years ago," says Greene. "Without a major initiative... the existing and future inventory will remain largely vulnerable to attack, at least through the next decade."

A recent survey of 17,070 computers in the Department of Defense (DOD) shows that at least half need stricter controls on access. Yet there are only three properly certified, commercially available products that DOD can use to upgrade the systems, and these work on fewer than 400 of DOD's machines. The report also notes that, in general, the government lags behind the private sector in adding on security measures, even when they are available.

Furthermore, a subcommittee reporting to the National Security Council recently concluded that the federal government's present approach to computer security is "fragmented and somewhat inconsistent." It also found that the lack of a clear policy "does little to convince industry to respond to the government's computer security needs."

To help bring some order into a chaotic situation, last fall President Reagan signed a directive setting up a central organization — with Cabinet representation — responsible for government-wide computer security policy. The directive also broadens the government's data protection policy to include "sensitive" but unclassified government and nongovernment information.

"With classified information, the systems are secured as necessary to prevent compromise or exploitation," says Lt. Gen. William E. Odom, National Security Agency director. "With regard to other sensitive information, the protection shall be in proportion to the threat and potential damage to the national security," he says. "This policy means that our responsibility for information protection extends across the entire federal government and, in some instances, requires the cooperation of the private sector."

Although it isn't clear yet what this policy will mean in practice, some industry executives are worried about the policy's implications. The government has tried to reassure them. "The federal government in no way wants to assume the 'big brother' role with private industry," insists Odom. "Instead, it will actively seek information and advice from the private sector."

Government security experts are very interested in promoting awareness of potential computer security problems in business (SN: 4/5/83, p. 294). This would help build a market for "trusted" computer equipment that automatically includes a variety of security features and meets DOD security standards. "Nursing systems that were born weak is only a stop-gap, not a solution," says Brotzman. "We need... to create systems with solid security features designed in from the beginning."

The Computer Security Center, originally formed in 1981 to serve DOD (SN: 7/3/82, p. 12) and now operating on a national level, is responsible for developing standards, demonstrating which methods work best and doing research that tackles a variety of security problems. "The [research and development] challenge we face is an incredibly difficult one," says Odom.

For example, says Greene, "we don't know how to build software that does exactly what it is supposed to do and nothing else." This leaves open the possibility that a computer programmer can sneak in a "Trojan horse" — a hidden program feature that allows the programmer or a knowledgeable user to, say, copy a sensitive file when such an action is normally forbidden. At the computer security meeting, two researchers at the Honeywell Secure Computing Technology Center in Minneapolis described a partial solution to the "Trojan horse" problem in a new, complex computer being designed with DOD's security needs in mind.

Furthermore, military computer systems shared by many users should be able to handle data that may fall under different security classifications. This introduces sticky problems such as the level of security necessary and feasible for a word processor used to write the unclassified version of a classified report.

Researchers are also studying devices like "smart" cards, which incorporate integrated circuits that can store information, to replace or supplement passwords. Employees, for example, would use individualized cards for access to various computers. Each card would automatically record what information was accessed where and when, leaving an "audit trail" that can be checked periodically.

The main computer security problems are still "dumb human error" and "casual intrusion," says Dennis K. Branstad of the National Bureau of Standards in Gaithersburg, Md. "The problem has grown in magnitude, but the solutions are becoming available." —*I. Peterson*

New daminozide review

An Environmental Protection Agency (EPA) scientific advisory panel met late last month to review the agency's proposed ban of daminozide, a widely used plant-growth regulator (SN: 9/7/85, p. 149). Now, the panel reports, the studies on which EPA based its claim that daminozide was a likely human carcinogen do not support EPA's assessment of a health risk.

Such findings do not obligate EPA to withdraw its proposed ban. However, says EPA's Al Heier, the panel's report is going to make EPA's decision on whether to push for a ban "a very tough one," because the panel sidestepped altogether the issue of whether these studies might still be adequate to justify suspending use of the chemical until better data become available. EPA is awaiting additional required, and equally nonbinding, comments on its proposed ban from the Department of Agriculture. Those comments are expected around the end of the month. □

Animal-abuse case update

Federal funding for the University of Pennsylvania's head-injury research involving baboons will remain under suspension, Health and Human Services Secretary Margaret M. Heckler announced last week. That research was shut down in mid-July amidst allegations of possible laboratory-animal abuse (SN: 7/27/85, p. 53). In a Sept. 23 letter to Edward Stemmler, dean of the university's medical school, National Institutes of Health (NIH) Director James Wyngaarden listed what changes and written assurances would be necessary before its funding of the project could be resumed. However, Wyngaarden added, even if NIH resumed funding, this particular University of Pennsylvania project would be under a five-year probationary scrutiny that would include, among other things, unannounced site inspections.

Investigations and videotapes of the head-injury research project caused Wyngaarden to conclude "that the university failed materially to comply with the terms and conditions of [its NIH contract] with respect to the care and use of nonhuman primates...." In particular, NIH identified:

- unacceptable variation in the management of anesthesia, analgesia and sedation.
- animal surgery under conditions and techniques that might not be sterile.
- lack of proper training and immediate supervision for laboratory assistants working with animals.
- inadequate participation by the staff veterinarian in choice and use of drugs and anesthetics.
- staff who "failed to maintain high standards of cleanliness" and who ate, drank and smoked during animal work. □