NSA Knew of Flaw in "Knapsack" Code

The National Security Agency (NSA) apparently discovered some time ago that a cryptography system that has potentially wide use in the private sector has a flaw. NSA has a policy, however, of not informing others when it finds that such systems are insecure, and the flaw was only recently brought to public attention by an Israeli mathematician, Adi Shamir.

The system, known as knapsack, is a so-called public key cryptosystem. These systems were widely hailed as a revolutionary new idea in cryptography when they were proposed in 1977 by Martin Hellman of Stanford University and his graduate students, Whitfield Diffie, now at BNR, and Ralph Merkle, now at Elxsi. The NSA, however, hit upon the idea "several years" before Hellman, according to former NSA director Admiral Bobby Inman.

Inman publicly announced that the NSA knew of these systems and knew of the flaw in knapsack at a meeting in New York of the 1983 National Computer Security Conference. As reported by David Kahn in *Newsday*, Inman remarked, "Classified government research many years ago had uncovered both the potential system and its potential flaw and had not proceeded to use the system for communications security, where you needed 40 years of protection."

There has been much talk of using public key systems in the private sector, in banking or for protecting corporate computer messages, for example. Since NSA has long known of these systems and their potential flaws, should the agency have informed potential users?

Inman, reached at his home in Virginia, told *Science* that the NSA independently invented public key systems several years before Hellman, Merkle, and Diffie. Cipher Deavours, a former NSA employee who is now at Kean College in New Jersey, says that the NSA examined these systems in the late 1960's and early 1970's.

According to Inman, the NSA still believes that one of the public key systems—the so-called RSA system—is "very secure" but that it "is too slow to be used in a high speed communications system." The knapsack system, although flawed, might still be usable, although not by the NSA. "The question you still have to ask is what kind of risk you want to take," he says.

It is not entirely clear whether the agency informs potential users that cryptographic systems are insecure. Inman says it does not. "The general view at the NSA is never to say when codes are insecure." On the other hand, informed sources say the agency did tell AT&T not to use the knapsack code. And Deavours says he knows of several instances when the NSA told companies not to use certain insecure systems.

Hellman believes this is an issue that, at the very least, warrants public discussion. "A few years ago, I said, 'We've come up with these systems. Would the NSA tell us if they figured out how to break them?' What obligation, if any, do they have to tell us?" It depends on whether national security is viewed in a broad sense, meaning that the security of communications in the private sector is a concern, or in a narrow sense, Hellman concludes. At the very least, he says, "It's something we ought to be thinking about."

—GINA KOLATA

Academy Group to Study U.S. Toxin Defenses

If others have not, the Army at least has taken to heart its own reports that the Soviets and their allies are using mycotoxin weapons in Afghanistan and Southeast Asia. The Army is so concerned, in fact, that it has commissioned a special review by the National Academy of Sciences (NAS) to get advice on defensive measures that might be taken. A 13-member Committee on Protection Against Mycotoxins held its first meeting in Washington on 8 December to hear a briefing by Army officials and draw up a plan of work.

According to the chairman, David Talmage, an immunologist and director of the Webb-Waring Lung Institute at the University of Colorado Medical Center, the group hopes to be finished in 1 year. "We are reviewing only unclassified material, and we've been told that most of the relevant data are unclassified in any case," he says. Although a good deal is known about grain contaminated with tricothecenes (the variety of mycotoxin allegedly used in Asia) and about poisoning by ingestion, very little is known about the effect of inhaling mycotoxins. This is something the group will look into.

The official charge to the committee, as summarized in an NAS document, is to "undertake a study of T2 and related mycotoxins so that means of protecting military personnel and civilian populations against their actions may be devised." Specifically, the committee is being asked to examine four possibilities:

- Developing a way to detect the presence of mycotoxins quickly and accurately at low concentrations.
- Developing means for destruction or disposal of toxins.
- Developing antidotes or protective gear that would allow people to carry on with their work or war-making unimpeded.
- Developing treatments for mycotoxin-induced abnormalities.

—ELIOT MARSHALL

Brittle Reactors: NRC Has a Plan

The nuclear plant hazard known as pressurized thermal shock is large and improbable, like a rhinoceros. Because it would be so unmanageable if it occurred—the scenario includes a reactor vessel cracking and spilling its coolant—the Nuclear Regulatory Commission (NRC) took new steps on 9 December to see that the thing is unlikely ever to rear its head.

According to the NRC, the new policy should reduce the probability of such an accident to less than once in 10,000 years of reactor operation. This problem involves old reactors exclusively, about 18 in all. The newer ones do not have the same design flaws.

Concern about vessel cracking in so-called "brittle reactors" arose when NRC engineers made a review of mishaps or "transients" at nuclear plants in the late 1970's. The review was inspired in part by the accident at Three Mile Island. The staff made two troubling discoveries.

First, welds on some aging reactor

0036-8075/82/1224-1290$01.00/0

vessels were found to be turning brittle faster than expected, chiefly because they contained impurities not meant to be there. In all reactors the steel walls of the vessel are bombarded by neutrons from the fuel. The effect is to raise the metal's nil ductility temperature. This is the point below which the steel loses its distinctive toughness and flexibility. Impurities in the welds have accelerated the aging process, so that some reactor walls are becoming unacceptably brittle. The higher the nil ductility temperature, the more likely it is the vessel will crack under stress.

Second, in reviewing actual records of transients, the NRC found that the scenario for cold water shocking a hot, pressurized vessel was not only plausible; it had happened. (Fortunately, the reactors were not damaged.)

When the NRC voted on 9 December, it decided to do three things:

- Within 6 months the NRC hopes to have a new screening program that will require reactor owners to calculate the nil ductility temperature of their vessels and to project its rate of increase during the life of the plant. An upper limit or "screening criterion" will be set at 270°F for axial welds. If a vessel seems likely to exceed the limit during its lifetime, the NRC wants detailed remedial plans in hand at least 3 years before the temperature limit is reached.
- Some sort of regulatory inducement will be devised to get the Babcock & Wilcox company to provide the NRC with data on the vessels it has sold. Thus far B & W has been uncooperative, perhaps because it is enmeshed in litigation over the reactor at Three Mile Island. As a result, the NRC is uncertain about the exact condition of the B & W vessels.
- The NRC staff will meet with owners of the most endangered reactors to encourage them to take preventive steps immediately. In most cases, this will mean rearranging the fuel to reduce neutron output. Some owners have already made changes. Those who fail to see the merits of this approach may be sent formal notices asking for information, "to enable the Commission to determine whether or not the license should be modified, suspended, or revoked."

Ten plants will be able to reflect on this problem for a few years, but the NRC staff found that there are eight that will have to act quickly. Four of them will reach the screening temperature in just 10 years. These plants will have to spend something like $20 million each to make the initial changes and will probably incur a permanent loss in operating efficiency.

There is one high-risk plant, the H. B. Robinson unit 2 reactor in Hartsville, South Carolina, owned by the Carolina Power and Light Company. The NRC staff paper says that this vessel "is so close to reaching the screening criterion" that it may not be enough simply to rearrange the fuel. In December, the plant's owner wrote to the NRC outlining several possibilities for dealing with the problem. However, it still is not clear how this plant can meet the NRC criterion without resorting to drastic remedies, such as cutting back power or shutting down for major renovations.

—ELIOT MARSHALL

Environmental Destruction Hurts India's Development

Any doubts that pollution and environmental degradation are at least as severe in the developing countries as in the industrial world should be dispelled by a recent report on the state of India's environment. "India is rapidly becoming a wasteland. Indians cannot now close their eyes to this continuing degradation of their natural environment," the study concludes.*

Put together by the Center for Science and Environment, an organization based in New Delhi that works on issues related to science, technology, and development, the report is the first major attempt to provide a comprehensive assessment of India's environmental problems. It draws upon information supplied by groups throughout India, and the picture it paints is generally bleak.

In vast regions of the country, land is being degraded by soil erosion, salinity and waterlogging, and desertification, the study documents. More than half of India's agricultural land is threatened by severe erosion, and topsoil washing into rivers and lakes is causing widespread siltation. This, in turn, contributes to flooding: the land area prone to floods has doubled in the past decade, the report states. Moreover, up to half the lands brought under irrigation may eventually have to be taken out of cultivation because of salinity and waterlogging, unless remedial measures are taken.

One of every three persons in the world lacking clean water is an Indian.

One factor contributing to soil losses in hilly regions is deforestation. The report estimates that more than 1 million hectares are deforested each year and that only about 10 percent of the country is now covered by trees. Each year, the forested area shrinks, the report claims, because reforestation programs are insufficient to keep pace with logging.

Water resources, too, are in a generally dismal state. The report says that 70 percent of the country's rivers and lakes are heavily polluted, mostly with raw sewage, but increasingly with toxic wastes.

The report is not simply a catalog of disaster, however. It examines a range of national and local efforts that have had both beneficial and adverse impacts, and describes the effect of environmental destruction on the lives of people. According to Anil Agarwal, the report's principal author, the report is an attempt to explore the causes and consequences of India's environmental problems and their relation to development policies. The conclusion states: "virtually every ecological niche is occupied by some occupational or cultural human group for its sustenance. Each time an ecological niche is degraded or its resources appropriated by the more powerful in society, the deprived, weaker sections become further impoverished."

—COLIN NORMAN

**The State of India's Environment 1982*, available from International Institute for Environment and Development, Washington, D.C., $25.