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