Timing attack beats cryptographic keys

To foil eavesdroppers, banks and other businesses handling electronic transactions have turned to various forms of cryptography to scramble and hide sensitive information.

Now, a researcher has identified a potentially serious vulnerability in certain widely used cryptosystems. This flaw may threaten the security of encrypted data transfers across computer networks.

Cryptography expert Paul C. Kocher, an independent digital security consultant in Stanford, Calif., posted his findings this week on the Internet. "The general idea of the attack is that secret keys can be found by measuring the amount of time used to process messages," he says.

Kocher's approach applies to public-key cryptosystems. In such schemes, each person gets a pair of keys, or sets of numbers used in a computer program for encrypting and decrypting messages. One key is published openly, so anyone can use it to encrypt a message. But only the recipient knows the corresponding private key needed to unscramble it.

Kocher discovered that these cryptosystems often take slightly different amounts of time to decrypt different messages. By surreptitiously measuring the duration of many such operations, an attacker can accumulate enough data to deduce the private key and read the confidential information.

"The attacks are particularly alarming because they often require only known ciphertext, work even if timing measurements are somewhat inaccurate, are computationally easy, and are difficult to detect," Kocher says.

"This is a real problem, especially for keys that stay around for a long time," says Peter G. Neumann of SRI International in Menlo Park, Calif.

Attacks that involve keeping track of how long operations take have been considered in the past, but they were of real interest only to such groups as the National Security Agency. The increasing use of public-key cryptography in commercial dealings on computer networks has now focused new attention on these concerns.

"You have to take it seriously," says Joan Feigenbaum of AT&T Bell Laboratories in Murray Hill, N.J. "But that doesn't mean this weakness is fatal."

Researchers are already considering cryptographic schemes that take the same amount of time for all possible keys or use additional randomizing to disguise the time that operations require.

Kocher's report is posted on the World Wide Web at the address *http://www.cryptography.com/*. — *I. Peterson*

Schizophrenia: Data point to early roots

Three new studies lend support to the theory that many cases of schizophrenia stem from derailments of brain development that begin early in life, perhaps in the womb.

The findings, published in the December AMERICAN JOURNAL OF PSYCHIATRY, add to recent efforts to illuminate schizophrenia's developmental origins (SN: 5/29/93, p.346). Still, researchers remain puzzled as to the precise alterations that bring about the disorder's debilitating symptoms, such as apathy, social withdrawal, incoherent trains of thought, and hallucinations.

Schizophrenia typically appears during young adulthood.

"Unique findings coming now and in the future on never-medicated and first-episode patients [with schizophrenia] are likely to provide a fresh and clarified picture of . . . this complex disease," writes Patricia S. Goldman-Rakic, a neuroscientist at Yale University School of Medicine, in a comment accompanying the reports.

Exposure to viral infections during certain months of fetal development may promote some cases of schizophrenia. Previous studies have uncovered an increased rate of schizophrenia in the offspring of women whose second trimester of pregnancy coincided with an influenza epidemic.

Robin M. Murray of the Institute of Psychiatry in London and his colleagues now report that the mothers of 121 persons hospitalized for schizophrenia recall having had more viral infections in the second trimester of those pregnancies than in the first and third trimesters combined.

Influenza accounted for 14 of the 20 second-trimester infections. Six women cited infections at other times during the pregnancy; two of these infections were influenza.

On average, patients who had been exposed to prenatal infections weighed less at birth and experienced more medical complications at delivery than those who had not had such infections.

A second project documents brain changes typical of chronic schizophrenia in 12 men and 12 women between the ages of 19 and 28 who experienced schizophrenia for the first time. The findings indicate that disturbances of brain development occurring in adolescence or earlier may underlie the disease, propose Peg Nopoulos of the University of Iowa Hospitals and Clinics in Iowa City and her coworkers.

The researchers compared brain scans of young adults with schizophrenia who had not taken antipsychotic drugs with those of healthy people of the same age. Patients had markedly less frontal lobe tissue and more cerebrospinal fluid in their brains.

The third study, directed by Anjan Chatterjee of Hillside Hospital in Glen Oaks, N.Y., notes muscular rigidity and related movement disturbances in 15 of 89 first-episode schizophrenics, all young adults who had not received antipsychotic drugs. Patients who had difficulty moving displayed the most severe symptoms of schizophrenia.

For some schizophrenic patients, decreased transmission of dopamine—a chemical messenger in a region of the brain linked to muscle control—may occur early in life, speculates Goldman-Rakic. — *B. Bower*

Vaccine triggers cocaine mop-up in rats

For all the millions of dollars spent to find a way to halt cocaine abuse, physicians still lack a useful medicine to break the drug's addictive power. The exact site and chemistry of addiction remain a puzzle. Moreover, many of the brain pathways influenced by cocaine coincide with paths essential to normal function, so targeting one can knock out the other.

Now, researchers report that they can mop up cocaine in the bloodstream of rats before it reaches the brain.

Scientists at the Scripps Research Institute in La Jolla, Calif., have developed a vaccine that calls up antibodies against the drug, resulting in antibody-cocaine complexes too unwieldy to enter the rats' brains. Cocaine itself rarely sparks an immune reaction. But by linking the part of cocaine that antibodies recognize to a molecule that triggers antibody production, the researchers made a vaccine that halves the concentration of free cocaine in the rats' blood.

Cocaine in the brain drops accordingly.

In the study, published in the Dec. 14 NATURE, scientists injected rats with the experimental vaccine or with a form missing the cocaine component. Next, they gave the animals a dose of cocaine. Animals in the first group had 77 percent less cocaine in the cerebellum—a site of the drug's action—than the controls did.

"Blocking cocaine by keeping it outside the brain should have fewer side effects than manipulating the way it behaves at specific nerve sites inside," says Scripps researcher George F. Koob. Drugs that work in the brain can stop people from taking cocaine, he explains, but they also make people unable to move.

The researchers observed the rats' behavior to determine whether cocaine had reached the brain. Rats on cocaine typically can't keep still; they engage in