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

various repetitive movements—episodes of sniffing, for example. These behaviors lessened greatly in the vaccinated rats. New experiments, Koob says, will highlight the vaccine's effect on more crucial addictive behavior, in which the rats repeatedly press a bar to get the drug.

The vaccine also appears to be highly specific. It does not prevent the effects of amphetamines, another type of stimulant.

A similar vaccine to treat addiction in people remains distant. For one thing, the particular antibody-stimulating part of the vaccine, which comes from marine limpets, may do too good a job. "We'd need to rule out potential autoimmune problems," says Koob.

"I see a possible place for a vaccine with people who want to get off the drug, who are highly motivated but tempted," says Koob. Heroin addicts determined to kick the habit need constant monitoring to stay on drugs that block heroin's pleasurable effects, says George Uhl of the National Institute on Drug Abuse's Baltimore laboratories. A vaccine might reduce the need for monitoring.

"I don't think you'd ever grab people using crack cocaine off the street, immunize them, and expect this is going to work," says Koob. Psychiatrist David W. Self of Yale University School of Medicine agrees. Vaccination, he says, does not target the basic process of addiction in those already addicted.

Koob suggests that a vaccine may someday serve as an adjunct to behavior-shaping therapy and drugs. "It would put up a significant barrier for cocaine."

— M. Centofanti

Heart drug busts brain clots from stroke

A clot-busting drug commonly used to treat heart attacks also curtails brain damage caused by the most prevalent type of stroke.

A collaborative study of people who suffered strokes caused by blood clots in the brain indicates that patients treated with tissue plasminogen activator (t-PA) were 30 percent more likely to make excellent recoveries than patients given a placebo.

"This is a real breakthrough," says John R. Marler of the National Institute of Neurological Disorders and Stroke in Bethesda, Md., which funded and coordinated the work. "It is the first time a drug has shown a clear benefit in treating acute stroke."

Marler notes that the researchers also confirmed suspicions that t-PA increases a person's risk of having a serious brain hemorrhage. Even so, approximately the same number of patients died in each group. Moreover, fewer patients treated with t-PA sustained permanent disability.

Approximately 500,000 people in the United States suffer strokes annually. Ischemic strokes, which result when a blood clot reduces blood flow to the brain, constitute 80 percent of these cases. The rest—known as hemorrhagic strokes—are caused by bleeding in the brain.

The trial, conducted by researchers across the United States, included 624 patients who received either intravenous t-PA or a placebo within 3 hours of initial stroke symptoms. Before giving either treatment, researchers used very fast computerized tomography to confirm that the patient was having an ischemic stroke.

As reported in the Dec. 14 NEW ENGLAND JOURNAL OF MEDICINE, patients treated with t-PA faced less disability after 3 months than those given the placebo. Hemorrhaging in the brain occurred in 6.9 percent of the patients on t-PA but in only 0.6 percent of those taking the placebo.

Stroke researchers are excited, despite the treatment's risk of hemorrhage. "This is the first stroke treatment which has withstood the crucible of scientific investigation," says Charles H. Tegeler of Wake Forest University's Bowman Gray School of Medicine in Winston-Salem, N.C. J.P. Mohr of Columbia University's College of Physicians and Surgeons notes that "this finding is the first of hopefully many that will change the public attitude from 'nothing to be done' to 'everything to be done.'"

While the findings impress Cathy A. Sila of the Cleveland Clinic Foundation, she emphasizes that "it is amazing that the researchers mobilized the community to recognize the symptoms of stroke and get [the patient] to the hospital." Strokes are often painless, but warning signs include sudden weakness or numbness, loss of vision, severe headache or dizziness, and difficulty in moving—symptoms the victims themselves often don't recognize.

Marler notes the need for further research and training before this treatment becomes the standard of care.

— L. Seachrist

Hubble finds an off-center black hole

Over the past few years, astronomers have gathered compelling evidence that black holes lurk at the heart of several galaxies. However, the latest finding has caught researchers by surprise: The newest unseen monster lies slightly askew.

Instead of residing at the exact center of the elliptical galaxy NGC 4261, the suspected black hole lies slightly to one side, astronomers reported at a Hubble Space Telescope workshop in Paris last week. But how did a black hole more massive than a billion suns move 9 light-years from the center, its presumed birth site?

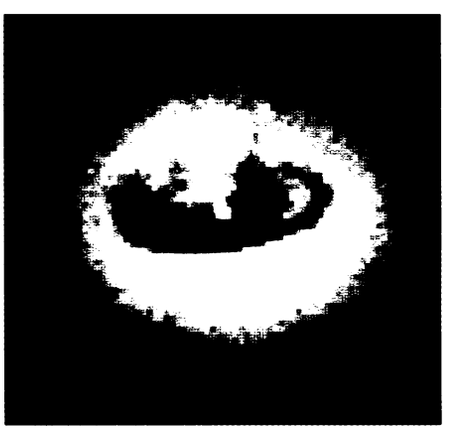
Still considered hypothetical by many scientists, black holes represent a collapsed state of matter so extreme that not even light can escape their gravitational tug. Evidence over the past decade suggests that these invisible objects power the fireworks at the core of many active galaxies.

Astronomers have suspected for more than 15 years—ever since radio telescopes detected twin, oppositely directed jets of radiowaves streaming out of the galaxy's center—that NGC 4261 harbors a black hole. Last August, Hubble's faint-object spectrograph measured the rotational speed of a disk of gas and dust at the galaxy's core. The high velocity betrays the presence of a massive black hole, report Laura Ferrarese and Holland Ford of Johns Hopkins University in Baltimore and Walter Jaffe of Leiden University in the Netherlands.

Both the disk and the calculated location of the black hole lie slightly apart from the exact center of the galaxy. According to one theory, the location of the disk suggests that an intruder galaxy collided with NGC 4261 long ago. Material from the off-center disk falling onto the black hole may have propelled the hole away from the galaxy's center.

Douglas O. Richstone of the University of Michigan in Ann Arbor believes that the orientation of the disk rather than its location implies a past galactic collision. Because the disk lies perpendicular to the plane of the galaxy, stars in NGC 4261 could not have provided the gas to make the disk, he asserts. Instead, Richstone says, the gas must have come from a colliding galaxy.

— R. Cowen



Ferrarese/NASA

Disk of gas and dust in the galaxy NGC 4261.