# Power Cracking of Cash Card Codes

Loaded with electronic cash that has been protected by an encryption scheme, a smart card represents a convenient, versatile medium for business transactions. Roughly the size of a standard credit card, it incorporates circuitry for processing information and keeping records.

That microcircuitry also makes it vulnerable to attack. Cryptographers have now identified techniques for breaking the security system built into a smart card. They cracked the codes by monitoring power consumption as the circuitry performed its cryptographic operations.

"We have implemented these attacks against a large number of smart cards and, at this point, do not believe that any cryptographic smart cards on the market are immune to these analysis techniques," says Paul Kocher of the consulting firm Cryptography Research in San Francisco.

Last week, Kocher and his coworkers Joshua Jaffe and Benjamin Jun posted their report revealing the security flaw. It can be found on the World Wide Web at *http://www.cryptography.com/dpa/*.

"[The flaw] is indeed a serious security threat to many existing systems," says Ross Anderson of the University of Cambridge Computer Laboratory in England. "It allows relatively low-budget attackers to get at key material that previously required a moderately well-equipped lab."

The integrated circuits on smart cards consist of vast arrays of transistors, which act as voltage-controlled switches. Different microprocessor instructions initiate characteristic switching patterns. The resulting motion of electric charge consumes power and generates electromagnetic radiation, which can be detected outside the card.

Researchers have already demonstrated that it is possible to accumulate enough data to deduce secret keys—strings of 1s and 0s—required to decrypt confidential information stored on smart cards. Using sophisticated tools, they've measured the duration of cryptographic operations (SN: 12/16/95, p. 406) or exploited processing errors (SN: 2/1/97, p. 78).

In the new threat, an attacker can use less expensive equipment to monitor a smart card's electronic responses. Fluctuations in power consumption correspond to different stages in a cryptographic process. By magnifying the signal, it is possible to detect individual microprocessor instructions and distinguish between various arithmetic operations.

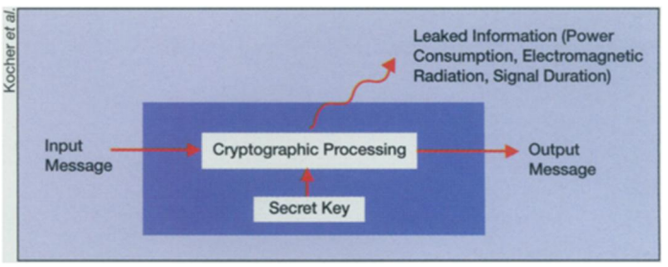
A more sophisticated analysis of these data relies on the application of statistical and error-correction techniques to extract information useful for deducing secret keys. Once the secret key is found, a criminal could make a copy of the smart card and obtain unauthorized access to someone else's account or, in some systems, automatically refill the card with cash.

Such threats, however, require that criminals have special equipment attached to or physically near the card. Smart cards are safe when stored in a wallet or purse, Kocher says.

Stolen or lost smart cards are another matter, because they can be connected to a power sensor and computer.

One approach to increased security is to recognize a smart card's vulnerability. An electronic cash system used by Visa International, for example, checks for unusual account activity. When that system was designed, Anderson says, "we did not know as much about breaking into smart cards as we do now, but we suspected that it would be done." Other companies have also started to adopt countermeasures.

Security expert Peter G. Neumann of SRI International in Menlo Park, Calif., notes that "unfortunately, attacks such as Paul Kocher's merely remind us of how difficult—if not impossible—it is to achieve security that can withstand very determined and well-funded attacks." *—I. Peterson*




*Information leaked by microcircuitry may allow security breaches.*

# Flies carry gene for alcohol sensitivity

Just as some human party-goers get tipsy after only a few drinks, some fruit flies carry a genetic mutation that makes them unusually wobbly when exposed to alcohol vapors.

The mutant strain of flies, fittingly dubbed *cheapdate*, fall out of a lab apparatus filled with ethanol fumes faster than normal flies. Identification of this alcohol-sensitivity gene, reported in the June 12 CELL, may aid efforts to find a genetic basis for alcoholism in humans (SN: 7/8/95, p. 20).

Scientists have not firmly connected a specific human gene to alcoholism or alcohol tolerance, although alcoholism shows a hereditary pattern. People with a high tolerance for alcohol are more likely to develop the disease, and scientists suspect that differences in people's tolerance for alcohol have genetic roots.

Now scientists will look for a counterpart to the mutant fly gene in mice and humans, predicts Robert Karp, a geneticist at the National Institute on Alcohol Abuse and Alcoholism in Bethesda, Md. Two previously identified human genes with similarities to the fly gene play roles in hormone production.

The flies, of the widely studied *Drosophila melanogaster* species, offer a largely untapped resource to identify other genes that might influence alcohol's effects in mammals, Karp and others say. The insects can be bred and tested faster and more cheaply than rodents.

"In flies, genetic technology is so powerful because you can [find] lots of mutants and analyze them quickly," Karp says. Despite the obvious differences between humans and flies, a lot is conserved at the genetic level, he adds.

Geneticist Ulrike Heberlein of the University of California, San Francisco and her colleagues isolated the alcohol-sensitive flies by using a device they call an inebriometer. They loaded flies into the top of a 4-foot glass tube lined with baffles, which resemble rungs on a ladder.

After 20 minutes of exposure to alcohol-laden air, normal flies typically lost their ability to cling to the baffles and fell from the bottom of the tube. Flies possessing the *cheapdate* mutation plummeted out after an average of just 15 minutes.

The gene altered by the *cheapdate* mutation is part of a cellular pathway that activates hormones via a molecule called cyclic AMP. Scientists had previously found that mutations in this gene cause memory and learning deficiencies in flies.

Flies with these mutations appear to manufacture below-normal amounts of cyclic AMP. When the scientists treated *cheapdate* flies with chemicals that increased their production of cyclic AMP, their alcohol tolerance rose to that of normal flies. The researchers do not yet understand why low cyclic AMP production increases alcohol sensitivity. *—J. Brainard*