Chinks in Digital Armor

Exploiting faults to break smart-card cryptosystems

By IVARS PETERSON

The days of a thick wallet bulging with coins, bills, and assorted plastic cards may be numbered. Instead, a single card—a computer in your wallet—could serve as electronic cash, driver's license, credit card, and personal identifier.

So-called smart cards, which incorporate circuitry for processing information and keeping records, are already widely used in Europe and elsewhere for automatically paying tolls, making telephone calls, authorizing access to pay-TV or restricted facilities, carrying medical data, and performing bank transactions.

In the future, many of these functions may be integrated into a single unit. Personal computers could come equipped with smart-card readers to handle transactions over the Internet.

For such a system of electronic commerce to work effectively, however, providers and users must have absolute assurance that any recorded information is safe from prying eyes, that the desired transactions are legitimate, and that both parties to a transaction are who they say they are.

To provide an appropriate degree of security and authentication, smart cards typically incorporate additional circuitry for encrypting digital information. Following a mathematical formula, the embedded cryptosystem scrambles the bits—1s and 0s—representing data, messages, or signatures into gibberish unintelligible to an eavesdropper.

Now, security experts have revealed that smart cards protected by current cryptographic schemes are potentially vulnerable to a novel type of attack. It's possible to force a card into making an error in the calculations used in the encryption process and from the result to obtain clues needed to break the cryptosystem and trick the card into leaking its secrets.

"Our attack is basically a creative use of a device's miscalculations, or faults," says computer scientist Dan Boneh of Bellcore in Morristown, N.J. Boneh is a member of the team that first identified the problem last fall in a specific type of smart-card cryptosystem.

Other researchers quickly confirmed the theoretical results described by Boneh and his colleagues and extended them to cover additional cryptographic schemes. Then, Ross J. Anderson of the University of Cambridge in England and Markus G. Kuhn of Purdue University in West Lafayette, Ind., demonstrated how such attacks could be mounted in practice against smart cards now in use.

"This is a new and exciting field of research and one that secure system designers would be prudent to follow closely," Anderson says.

A smart card resembles a standard credit card, but it includes, wedged within the plastic, a memory for storing sets of instructions and recording data and a microprocessor for performing calculations and other bit manipulations according to the embedded instructions. In addition, some types of smart cards have a microwave antenna for transmitting and receiving messages.

Cards that rely on cryptography for security usually have an additional processor and extra memory to provide a secret environment for handling the calculations necessary to encrypt and decrypt digital information and to provide digital signatures.

The most commonly used form of smart-card encryption requires a key—typically a string of random numbers, often binary—shared by both sender and recipient. Numbers selected from the key are used in a series of mathematical operations to scramble the digits representing information stored or transmitted by the card.

One widely used example of such a cryptosystem is the Data Encryption Standard (DES), which in its simplest form requires keys that are 56 bits long and involves 16 rounds of scrambling during encryption. Deciphering the information means going through the same operations in reverse order, using the same key.

Relatively easy to implement, a shared-key scheme has the disadvantage that both the card and the reading system must have access to the same key in order to understand each other.

An alternative method, known as public-key cryptography, requires the use of a pair of complementary keys instead of a single, shared key. One key, which is openly available, is used to encrypt information; the other key, known only to the intended recipient (or encoded in the smart card), is used to decipher the message.

In other words, what the public key does, the secret key can undo. Moreover, the secret key can't be easily deduced from the public key.

The most popular type of public-key encryption, invented by Ronald L. Rivest of the Massachusetts Institute of Technology, Adi Shamir of the Weizmann Institute of Science in Rehovot, Israel, and Leonard M. Adleman of the University of Southern California in Los Angeles, is known as the RSA cryptosystem.

In the RSA scheme, the secret key consists of two prime numbers that are multiplied together to create the lengthier public key. Its security rests on the observation that it's easy to multiply two large prime numbers to obtain a larger number as the answer. The reverse process of factoring a large number to determine its prime-number components presents a formidable computational challenge (SN: 5/7/94, p. 292).

Designers and manufacturers generally describe their smart cards as resistant to tampering. They maintain that it is virtually impossible to take a smart-card chip apart and read the individual bits and bytes of the instructions built into and stored on the chip.

Smart-card cryptosystems, however, are potentially vulnerable to attacks that exploit certain features of how the systems operate. For example, public-key cryptosystems often take slightly different amounts of time to decrypt different messages. In 1995, Paul C. Kocher, a cryptography consultant in Stanford, Calif., described how secret keys can be found by surreptitiously measuring the duration of many such operations (SN: 12/16/95, p. 406).

Last year, computer scientist Richard J. Lipton of Princeton University made the crucial observation that once a device performs a faulty computation, it may leak information that can be used in breaking a cryptosystem. Such a fault could arise from something as simple as the switch of a bit from 0 to 1 or 1 to 0 at a random position in a secret key.

Working with Bellcore's Boneh and Richard DeMillo, Lipton showed in principle how random bit flips could be exploited to deduce the secret key in the RSA cryptographic scheme when used in a smart card.

The idea is to cause a random bit flip by zapping the card with a pulse of radiation or by suddenly changing the voltage or rate at which the card's chip normally operates. Mathematically inclined criminals could then compare the faulty values generated by the device against the correct values and thus derive the secret RSA key.

Because the method doesn't rely on actually factoring a large number to break the code, it can be equally effective against RSA keys of any length. Making the numbers longer is not enough to protect against such an attack.

"What is significant about the Bellcore attack is that an error introduced at nearly any stage of computation can produce a favorable result for the opponent," says Burton S. Kaliski Jr. of RSA Data Security in Redwood City, Calif.

"The security of RSA and other algorithms has not been questioned, only the security of particular implementations against one form of physical attack," he adds. "The attack can . . . be prevented by simple modifications to the cryptographic processing."

At the same time, it's dangerous to assume that the secret information stored in "tamperproof" smart cards can't be discovered by an adversary. Such devices must not only conceal the unit's inner circuitry but also effectively detect faults in processing, Boneh says.

Moreover, because all computers make errors from time to time, "our methods work even against machines that we cannot actively tamper with," Lipton says.

Within weeks of Bellcore's announcement that the new smart-card security is vulnerable, Shamir and Eli Biham of the Israel Institute of Technology (Technion) in Haifa found a way to modify the new approach to attack shared-key cryptosystems such as DES, which is used extensively in the financial world to protect electronic transactions.

The result, says Shamir, represents a major assault on nearly all cryptosystems proposed so far.

Theoretical studies indicate that an intruder could unravel DES' 56-bit secret key by analyzing fewer than 200 faulty encrypted messages and comparing them to a single flawless message. As in the case of the RSA system, making the keys longer doesn't help to ward off the attack.

More recently, Shamir and Biham have demonstrated that a fault-based attack can also be used to break a completely unknown cryptosystem, making it possible to extract the secret key stored in a tamperproof cryptographic device even when nothing is known about the structure or operation of the cryptosystem.

The results obtained by Shamir and Biham were all based on theory, and it isn't clear how applicable they would be to smart cards in actual use. Anderson and others point out that changing a single bit in a secret key, for example, would normally be detected by conventional error-checking methods built into the system.

"Although their attack is very elegant, it is not practical against many fielded systems," Anderson says. An electric pulse or jolt of radiation is more likely to cause the chip to crash than to lead to a faulty encrypted message.

Nonetheless, it is possible to mount a practical attack by causing a fault not in the secret key, but in the instructions of the program that orchestrates the calculations, Anderson says. Using this approach, it's possible to break DES with access to fewer than 10 encrypted messages.

To date, no one has reported a successful fault-based attack on an actual cryptographic device or smart card. However, such attacks are certainly feasible, Anderson contends.

Anderson's own studies have revealed that smart cards are not always as tamper-resistant as their manufacturers claim, and criminals have already taken advantage of such weaknesses. In the last few years, for example, organized gangs in Europe have acquired the capability of cloning the smart cards used for access to pay-TV.

"This raises the obvious risk that banking systems could be next," Anderson says. Indeed, the technology required to implement an attack based on causing a smart card to decode instructions incorrectly isn't much more complicated than that used to pirate TV signals.

Anderson and Kuhn delayed publishing their findings on breaking tamper-resistant processors until last November in order to give developers of banking systems time to adopt some countermeasures. The report appears in the proceedings of the second workshop on electronic commerce, held in Oakland, Calif.

Manufacturers of smart cards have been aware for some time of the importance of protecting against physical intrusions involving abrupt temperature changes, voltage spikes, and radiation bursts. Many devices already have circuitry to detect such abnormalities.

Moreover, simple procedures such as repeating calculations and checking to make sure the same answer comes out each time can provide additional safeguards, though they often slow smart-card operation unacceptably. Bellcore and other organizations have developed alternative strategies to circumvent the problem.

System developers could also learn from efforts in weapons and space research to develop chip-based circuitry that can survive electromagnetic pulses and other environmental hazards, says Jean-Jacques Quisquater of the Catholic University of Louvain in Belgium.

In spite of these security concerns, the popularity of smart cards for a variety of applications continues to grow. Just as people don't hesitate to write checks even though checks are easy to forge or continue to give credit card numbers over the telephone without worrying about being overheard, they readily use smart cards because of the convenience they offer.

Meanwhile, the cat-and-mouse game between cryptographers and security experts on the one side and technologically literate spies and criminals on the other goes on. □