Wednesday, June 10, 1998

Cryptographers Discuss Finding of Security Flaw in 'Smart Cards'

by Peter Wayner, pwayner@nytimes.com

A team of San Francisco-based computer scientists has spoken for the first time openly about their discovery of a major new technique that allows them to break the security system in tamper-resistant "smart cards".

The technique, which monitors the cards' power consumption to break the codes, is a possible threat for some of the new digital transaction systems being tested in Europe and New York and makes life more complicated for computer security experts who often rely on these tamper-resistant cards to keep out intruders.

The results have shaken up the smart card industry. John Beric, the head of security for Mondex International, a company that uses the cards for financial transactions, said in an interview this week that the company had completely rewritten its software to deal with the threat. "We've changed our mindset", he said. "We [write software] in a different way now."

Marc Briceno, the director of the Smartcard Developer's Association, said of the development, "It's very real."

And Peter Neumann, a scientist at the SRI International, a think tank based in Menlo Park, Calif., said the discovery had "enormous potential as another technique for breaking weakly designed and badly implemented devices".

Adam Shostack, director of technology at the Boston-based computer security company Netect, said: "This is another example of why it is a bad idea to put your security in my pocket. These devices are exciting, but it doesn't mean they're ready for carrying money around."

The weakness was described by Paul Kocher, the president of Cryptography Research, a private consulting company in San Francisco, who along with two employees, Joshua Jaffe and Ben Jun, discovered how information about a smart card's secrets leaks out. The three have been experimenting with ways to track how chips use power as they scramble data.

Kocher said in a telephone interview on Sunday: "We have not yet encountered a card that couldn't be broken."

His company consults for many of the major computer and financial security vendors and is currently marketing rights to patents that may defend against these attacks. The company has been sharing its research with the "smart card" industry over the last year in order to give them time to develop defenses. He decided to make public the information after the Australian Financial Review published an article on the issue this weekend.

The technique used on the tamper-resistant card relies on the fact that semiconductor chips must use electrons to do calculations, and the flow of electrons can be measured by with a simple attachment to a personal computer that costs about $500. More accurate solutions can cost thousands of dollars. This insight makes it possible to recover a card's secret key by watching the power consumption because the calculations used to scramble the data depend on the values of the secret key.

For instance, in one of the simpler versions of the technique, the key from a popular RSA system can be extracted by watching an oscilloscope graphing the power consumption of a card. The key used in these systems is a pattern of about 2,000 binary bits that are either zeros or ones. The chip consumes slightly more power to process a one than a zero and the key can be extracted, in these simple cases, by simply reading the peaks and valleys in the graph of power consumption.

This secret key is normally guarded by the tamper-resistant design of the smart cards. Banks, for instance, rely on the smart card to hold the secret key internally and use it to create digital signatures guaranteeing transactions. Ordinarily, only the owner of the smart card would be able to operate it and create the digital signatures. Someone, however, could use this technique to extract the secret key, clone the smart card and forge transactions that could empty a person's account. In some systems, the cloning process could allow the criminal to create "evergreen" cards that automatically refill themselves with money.

Kocher's company also has developed more sophisticated statistical attacks that can be used to extract the key even when it is not readily understandable from the power consumption data. This technique, which the company describes with a trademarked phrase "differential power analysis", allows an attacker to extract each bit of the key by making guesses and testing them several times. The key can usually be recovered in about 1,000 or so trials, Kocher said.

The technique could be a serious threat to any installation that uses smart cards. Mondex International, for instance, is a company that developed smart card-based digital cash systems. MasterCard owns 51 percent of the company, while other major banks like Wells Fargo, First Chicago, and Chase own smaller shares. In the United States, seven banks have the franchise rights to use the system, and Chase currently is running a trial on the upper west side of Manhattan.

Visa International is a competitor of Mondex and Mastercard that has its own version of a payment system in pilot programs in 18 countries. In the United States, First Union bank in Atlanta is working with the system.

Both of these systems are vulnerable to this code-breaking technique because they both use the tamper-resistance of the smart card to replace a large centralized system. In ideal situations, transactions can be completed by connecting two cards without using a central computer system to authorize the deal. A person could go into a newsstand on a corner and transfer 60 cents without a phone line to use a central computer to supervise the transaction. Credit card companies currently link together large networks of gas pumps and store registers in real time to control fraudulent use.

Michael Keegan, the chief of Mondex, said in a telephone interview on Monday that the company has used the last year of consultation to restructure its software and make plans for redesigning the hardware.

"The new cards that we're distributing right now are upgraded and they're resistant to this class of attack", he said and added that the current solution being distributed depends upon software. Better fixes will depend upon new hardware that will be rolled out in the future.

When asked whether Mondex had detected any fraudulent use of the technique, Keegan noted: "We've got full detection analysis for all Mondex systems around the world. You can monitor redemption models. We've seen nothing."

Keegan also defended the decentralized architecture embraced by Mondex. "We think the model is still fit for purpose", he said. "We don't think that it's feasible to centrally clear every cup of coffee or newspaper."

Richard Phillimore, the senior vice president at MasterCard responsible for chip card problems, added in the telephone interview, "One of the attractions to us for Mondex was the architecture of the product. We were entirely comfortable with the statistical sampling. It was one of the key issues we went through when we went through acquiring the company."

Steve Schapp, an executive vice-president of Visa, said in a telephone interview that the company is well aware of the vulnerability and developing solutions that will be incorporated in future cards.

He said: "I think you need to put this in perspective. There are only a handful of people around the world who have the expertise to actually apply this type of hardware approach. We don't think there is any reason whatsoever to slow down or stop any of our programs. We have implemented one change and are planning to make future changes as well."

Schapp also pointed out that the Visa system uses a different architecture than Mondex. The corporation maintains a central database that keeps track of the balance on any of the cards in circulation. Each transaction with a merchant is recorded at the end of the day when the merchant terminal sends a batch of transactions for settling. This allows Visa to keep better track of fraud by noticing cards with balances that jump up without reason. The cost of this advance, however, is flexibility. Visa does not allow card-to-card transactions. Mondex users can give a few dollars to their neighbor with the system, but Visa users can only spend their money at merchants.

Some other industries could also be affected. Smart cards are often used as access devices to buildings and computer systems. Some of the modern digital cellular phones use smart cards to hold the account number and

these are made tamper-resistant to try and restrict cloning. Some digital satellite television systems distribute keys on smart cards to their customers to reduce piracy.

In the long run, the discovery casts doubt on the ability of the industry to create tamper-resistant devices that will guard secret values and not be cloned. The industry has long relied on special plastics and circuit designs to ensure that no information could be extracted by people using physical attacks against the devices. Very little work has been done on techniques for blocking the chips' ability to leak information.

Bruce Schneier, the author of the book "Applied Cryptography", said, "The fundamental flaw in the smart card paradigm is that the owner of the card and the owner of the secrets on the card aren't the same." So, a person with a cash card in hand has an incentive to break into the card and arrange for it to automatically refill with cash.

Briceno of the Smartcard Developer's Association said that cards are still useful for identification. "For these types of applications, smart cards are ideal. If you lose the card, you can revoke it" he said in an interview. "For electronic banking application where the issuer is providing a large number of hostile users which have a clear incentive to break them, smart cards are not necessarily sufficiently secure."

David Kahn, author of the bestseller "The Codebreakers", said that there are many different stories from the history of cryptography. He said in one version, a U.S. Intelligence agency bugged an embassy and listened to the rotors shift in a mechanical enciphering machine manufactured by the Hagelin corporation.

He said: "As the wheels move they strike pins which in effect create a variable gear which is the enciphering key to the whole thing. If you were able to listen to these noises as these lugs strike these arms, you could reconstruct the shift of this variable gear. You know that the first letter is shifting fifteen because you hear fifteen little blows against this little arm."

Stories like this have made their impression at Mondex.

Keegan said: "We assume that there are people out there who are smarter than us. We want to introduce as many enhancements that you can. It's kind of an arms race. We would make no claim to having absolute security. What you've got to try to do is keep ahead of technological advances. That's a continual process and you'll never stop it. It's part of the price of being in the business."

Possible solutions

To address the newly revealed security problem with smart cards, scientists at Cryptography Research have been examining and patenting several general approaches for reducing the flow of information through power consumption and electromagnetic radiation.

This might be accomplished by adding a secondary circuit to the chip that would do calculations on random numbers. This could mask the power consumed by the other part of the chip handling the encryption. But it is unclear whether enough randomness could be created to resist the more thorough statistical techniques used to break the cards' codes. Random calculations tend to average out over time and are easy for differential power analysis to remove.

Another solution is to add parallel circuits to the chip that would mirror the real encryption calculations. For instance, if the real circuit is multiplying by the binary number 101, then the mirror circuit might multiply by 010. This would smooth out the power consumption because the power consumed by both parts together should be more constant. Still, it is unclear whether all information can be blocked by this solution, because the mirroring is not perfect.

A third approach is to modify the software running on these chips. For instance, the traditional encryption algorithms like DES or RSA might be modified to use different sequences of computations to make it more difficult to recover the solution from watching power consumption.