Now, Smart Cards Can Leak Secrets A New Breed of Crypto Attack on "Tamperproof" Tokens Cracks Even the Strongest RSA Code

SEPTEMBER 25, 1996. Security research findings do not usually cause dramatic changes in the marketplace. This one will. It's such a novel approach to breaking cryptographic security systems that it is considered a new threat model. The work is formally called "Cryptanalysis in the Presence of Hardware Faults," and it exposes a serious flaw in the assumptions made by manufacturers of smart cards, secure ID cards, and other "tamperproof" hardware tokens that are used for secure networked transactions.

The attack targets public key cryptography schemes-such as the well-known RSA authentication and digital signature algorithms-when they are implemented in tamperproof devices. RSA public key cryptography has been licensed to a wide range of companies for inclusion in their products and services. Indeed, faith in the strength of this code underlies much of the market optimism for electronic commerce.

Of all the challenges facing electronic commerce-billing logistics, Internet congestion, lack of privacy, and so forth-the new attack on tamperproof devices may be the most debilitating. It diminishes confidence in smart cards that are used for stored value, such as some forms of electronic money; and in cards that personalize cellular phones, generate digital signatures, or authenticate users for remote login to corporate networks. The security risks in each of these examples are impersonation and fraudulent use of data.

"Designers of cryptography systems have a new constraint to worry about," says Dan Boneh, a Bellcore research scientist and co-developer of the new threat model along with Richard Lipton, a professor of computer science at Princeton University and a Bellcore chief scientist, and Richard DeMillo, a Bellcore vice president and head of Bellcore's Information Sciences and Technologies Research laboratory. "Our attack," Boneh explains, "is basically a creative use of a device's miscalculations, or, faults. Now, tamperproof devices must not only conceal the unit's inner circuitry but also be fault resistant."

In light of the new threat model, it is dangerous to assume that secret information stored in a tamperproof device cannot be discovered by an adversary. Moreover, according to DeMillo, "designers of tamperproof devices can no longer claim with impunity that their products are secure. An external testing organization, such as Bellcore, must determine to what extent the device is vulnerable to the new attack-by analyzing the design and manufacture of the device and playing the results against the new mathematical methodology."

How The New Attack Works

Lipton is given credit for making the crucial observation on which the new threat model is based. He noted that once a device performs a faulty computation, it may well leak information that can be used for cryptanalysis. This is a new way of looking at the fact, widely acknowledged in the computer industry, that no computing system can be perfectly fault free.

The attack uses an algorithm that, first, compares the faulty values generated by a device against correct values and, second, infers the cryptographic code stored inside the device. Next, in the case of some RSA implementations, the algorithm efficiently factors the RSA modulus. It is not difficult to then derive the private key of the private/public key pair.

Perhaps the most powerful and surprising aspect of the new threat model is that it avoids directly factoring the RSA modulus. Therefore, it is equally effective against moduli of any length. In contrast, the Number Field Sieve factoring technique developed by former Bellcore research scientist Arjen Lenstra and others has, so far, broken RSA implementations using moduli that are 130 digits (i.e., 431 bits) long but has not succeeded against 512-bit implementations, which are used in products worldwide.

"Even if all of the products currently using RSA authentication or digital signatures were upgraded to use 1024-bit moduli, we could still break the code with the new threat model," says Boneh. But, he adds, the algorithm used in the new threat model is not effective against symmetric or, secret key cryptographic techniques, such as the Data Encryption Standard (DES) and Bellcore's Video Rate Algorithm (VRA). "The algorithm that we apply to the device's faulty computations works against the algebraic structure used in public key cryptography," Boneh explains. "Another algorithm will have to be devised to work against the nonalgebraic operations that are used in secret key techniques."

Creating Faults

The new threat model hypothesizes that a tamperproof device can be easily subjected to physical stresses that cause it to generate faulty computations at rare and unpredictable rates. It is reasonable to assume that an adversary could easily gain full control over a smart card and card-reading device while the processor is performing security-related calculations. Certain levels of radiation or atypical voltage could then be applied, or for brief periods of time the device might be given a higher clock rate that it was designed to accommodate.

It would be more difficult to gain this type of control over a larger computing device housed inside a secure environment. So far, therefore, it seems that the new threat model is most acute against such tamperproof devices as smart cards because we can cause them to make faults. However, there is a substantial threat even in the case of servers that operate behind locked doors. Lipton notes that since all computers make errors from time to time, "even servers are not safe from our attack. Our methods work even against machines that we cannot actively tamper with. As long as they are not perfect, we can use our methods to break their security code."

The new model has been tested using hypothetical calculations, but the physical phase of the research has not been carried out. It is not, however, necessary to mount the attack in order to emphasize its seriousness. In the security community, it is universally accepted that the mere possibility of an attack's existence is a sign of great danger. Now that the model called "Cryptanalysis in the Presence of Hardware Faults" has been proven to work theoretically, security experts must assume that attackers exist who have the means of carrying it out.

One way to protect devices against the new attack is to ensure that the computing device verifies the computed value by, for example, repeating the computation and checking that the same answer is obtained both times. Unfortunately, in some systems, this form of protection usually slows down the computation by a factor of 2. For some applications, this drag on performance is not acceptable.

Lipton points out that "checking the computation in this way may not stop all our attacks." A better way to protect a tamperproof device is to use protocols that are fault-resistant. Lipton believes that it may be possible to create such protocols.