New Threat Model Breaks Crypto Codes

What End-User Applications Submit to Your Code-Breaking Scheme?

Our research discovery proves that all tamperproof devices--such as smart cards and other hardware security tokens--that use public key cryptography for user authentication are now at risk. For example, smart cards that are used for stored value, such as some forms of electronic money; cards that personalize cellular phones; cards that generate digital signatures; and cards that authenticate users for remote login to corporate networks are all open to the attack that we describe. The underlying crimes in all these cases are impersonation and fraudulent use of data.

How Does Your Research Affect the Security Industry?

Designers of cryptography systems now have a new constraint to worry about. Our attack is basically a creative use of a devices, miscalculations, or, faults. Therefore, tamperproof devices must now not only conceal the device's inner circuitry but also be fault resistant. Being tamperproof is no longer good enough to ensure security.

What is the Business Significance of this Research?

Designers of "tamperproof" devices can no longer claim with impunity that their products are secure. An external organization, such as Bellcore, will have to determine to what extent the devices are vulnerable. Bellcore would analyze the design and manufacture of the device--in effect, test it--and play the results against the mathematical methodology of the new threat model.

What is Your New Threat Model?

We observed that once a computing device performs a faulty computation, it might leak information that can be useful for inferring secret data. This is a novel approach to the widely acknowledged fact that no computing system is safe from faults.
In our theoretical model, which is called Cryptanalysis in the Presence of Hardware Faults, we use an algorithm to compare the faulty values with correct values and then to infer the cryptographic code stored in a tamperproof device.
It can be likened to a person making a Freudian slip; the listener compares the phrase with other observations and certain thinking processes to infer things about the speaker that he might otherwise have wished to keep secret.

What Cryptographic Codes Does This Approach Break?

This model is a threat to authentication systems that use public key cryptography and that are implemented in tamperproof devices. So far, we have shown that the following types of public key cryptography can be broken with our model: RSA, Rabin's Signature Scheme, and the Fiat-Shamir Identification Scheme.

How Does Your Attack on RSA Compare with Factoring Attacks?

Our attack is much more powerful than cryptanalysis that uses factoring. For example, the Number Field Sieve factoring technique developed by Arjen Lenstra and others has so far broken RSA implementations using 130-digit (i.e., 431-bit) moduli. But our attack applies to any length of modulus.
Even if all of the products currently using RSA authentication were upgraded to use 1024-bit moduli, we could still break the code.

Does Your Attack Endanger Secret Key Cryptography, Such as DES?

No. The algorithm that we apply to the device's faulty computations is effective against the algebraic structure used in public key cryptography. Another algorithm will have to be devised to work against the nonalgebraic operations that are used in secret key cryptography. The Data Encryption Standard (DES) and Bellcore's Video Rate Algorithm (VRA) both use secret key cryptography, which is also called symmetric key cryptography.

Why is Your Attack Model Restricted to Tamperproof Devices?

The attack succeeds because it takes advantage of a processor's faulty computations. In our model we hypothesize that tamperproof devices, such as smart cards or any hardware tokens, can be easily subjected to

harmful physical stresses and thereby forced to make faults. The attacker can easily gain full control over a smart card and card-reading device while the processor is performing security-related calculations.
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 our model is best suited for attacking tamperproof devices.

What Kind of Physical Stress Would Be Applied to the Card?

It is reasonable to assume that certain levels of radiation or heat, or incorrect voltage, or atypical clock rates could be imposed on tamperproof devices, which are usually small and portable. These physical stresses can cause the device to malfunction while it is calculating.

How Do You Use the Faulty Computational Values?

We derived an algorithm that makes use of the faulty values in order to recover the factors of the stored cryptographic information. In the case of RSA implementations, our algorithm efficiently factors the RSA modulus. It is not difficult to then derive the public key of the private/public key pair.

What Long-Term Significance Do You Envision for This Work?

Our threat model will spark a new research trend. In addition to focusing on the mathematical properties of the code, researchers may now try to apply the idea of using hardware faults to other cryptographic schemes and perhaps prove that certain schemes are resistant to this type of attack.

How Does This Compare with the Timing Attack on RSA Announced Earlier This Year?

They are similar in that both measure things that are taking place within the processing device. The timing attack described by Paul Kocher compares the discrepancies in time required by certain operations and uses this information to extract the secret information. Our attack is based on using the occurrence of hardware faults to extract the secret data. It may be harder to protect against our attack than to thwart the timing attack.

Have You Tested Your Theoretical Model?

We have tested the algorithm using hypothetical faulty calculations. But we have not carried out the physical phase of the reseach, which would involve using a radiation chamber or high voltage source.
It is not, however, necessary to mount the attack in order to emphasize its seriousness. In the security community, it is widely acknowledged that the mere possibility of an attack existing is a sign of great danger. Now that we have proved that the attack model called Cryptanalysis in the Presence of Hardware Faults works, we must assume that attackers exist who have the means of carrying it out. The fact that our work has not yet been experimented with in the laboratory does not make it a less serious security threat.

How Can Designers Protect Smart Cards from This Attack?

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

Who Are the Researchers Who Developed the New Threat Model?

Richard Lipton, a professor of computer science at Princeton University and a part-time Bellcore research scientist; Rich DeMillo, a Bellcore vice president and head of Bellcore's Information Sciences and Technologies Research laboratory; and Dan Boneh, a Bellcore research scientist. Richard Lipton made the crucial observation that once a device performs a faulty computation, it may well leak information that can be used for cryptanalysis.