MIT Technology Review

How to Break Cryptography With Your Bare Hands

The latest way to snoop on a computer is by measuring subtle changes in electrical potential as data is decrypted.

By David Talbot on August 20, 2014

With enough technical savvy, simply touching a laptop can suffice to extract the cryptographic keys used to secure data stored on it.

The trick is based on the fact that the "ground" electrical potential in many computers fluctuates according to the computation that is being performed by its processor – including the computations that take place when cryptographic software operates to decrypt data using a secret key.

Measuring the electrical potential leaked to your skin when you touch the metal chassis of such laptops, and analyzing that signal using sophisticated software, can be enough to determine the keys stored within, says Eran Tromer, a computer security expert at Tel Aviv University.

The remarkable result is described in this paper due to be presented at a conference in South Korea next month, but it was demonstrated Tuesday at a cryptography conference in Santa Barbara, California.

A signal can be picked up by touching exposed metal on a computer' chassis with a plain wire. Or that wire can make contact anywhere on the body of an attacker touching the computer with a bare hand (sweaty hands work best). The ground signal can also be measured by fastening an alligator clip at the far end of an Ethernet, VGA, or USB cable attached to the computer, or even wirelessly with sensitive voltage-detection equipment. The catch is that contact must be made as data is unlocked with a key – during decryption of a folder or an e-mail message, for instance.

Tromer says his research team has used all those methods to extract encryption keys based on widely used, high-security standards – 4,096-bit RSA keys and 3,072-bit ElGamal keys.

The work contributes to a growing body of evidence that regardless of the software protections people place on computers, there are indirect ways to extract data – so-called "side channel" attacks.

Previous research efforts have found, for example, that analyzing the power consumption of a computer can reveal cryptographic keys. The good news is that analyzing subtle trends in power usage

can also reveal whether a computer is being attacked (see “Tiny Changes in Energy Use Could Mean Your Computer Is Under Attack”).

“Overall, there are likely tens of undiscovered hardware-related side channels – and we are likely going to hear more from these authors and others,” says Radu Sion, a computer security expert at Stony Brook University.

Tromer says he doesn’t know of anybody performing a ground-potential attack to steal real data, but he has notified cryptography software makers. It is possible to avoid such attacks by adding random data to computations. The developers of one popular free cryptographic software package, GnuPG, incorporated such a patch into the latest version of their software.

Credit: Photo courtesy of Tel Aviv University Research

Tagged: Computing, hardware