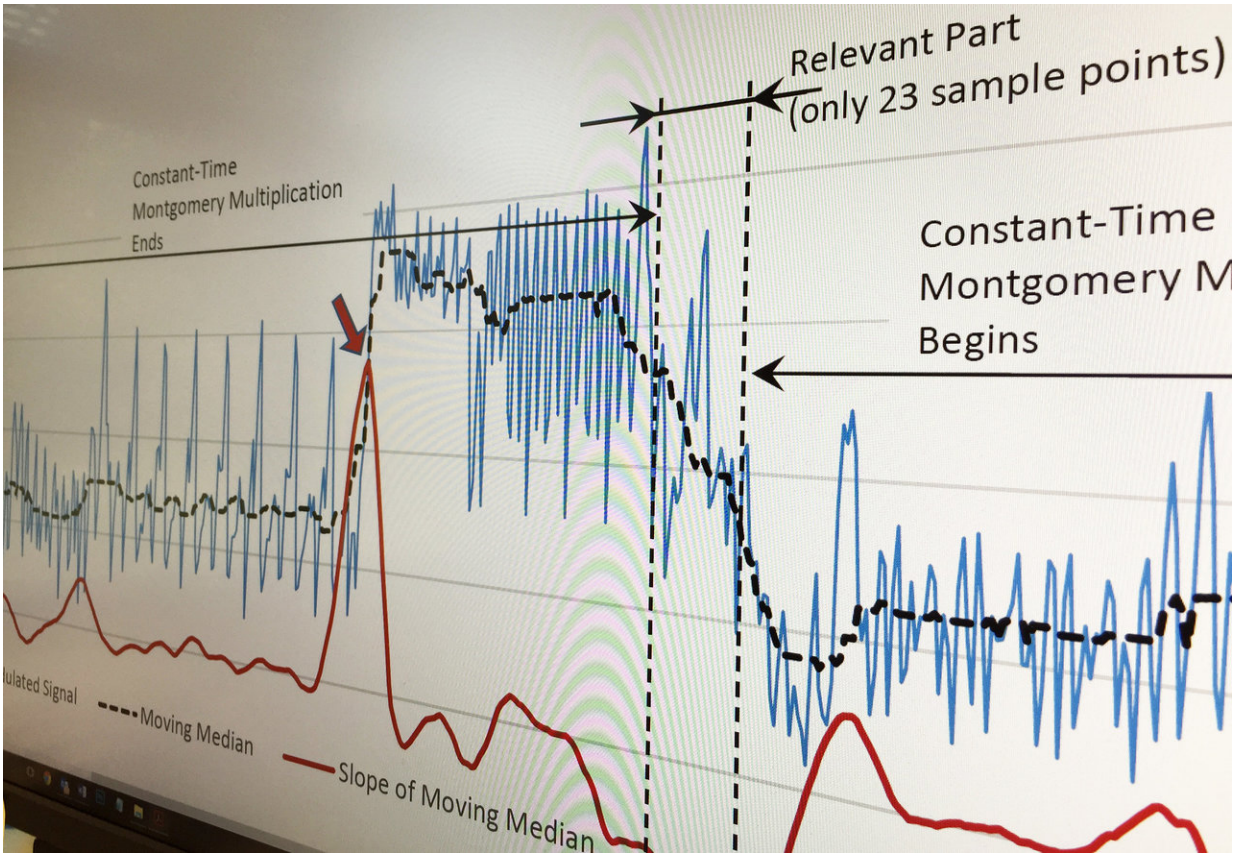
Researchers help close security hole in popular encryption software

August 9 2018



Analysis of the AM-modulated signal showing the portion relevant to the security of the encryption software. Credit: Georgia Tech

Cybersecurity researchers at the Georgia Institute of Technology have helped close a security vulnerability that could have allowed hackers to

steal encryption keys from a popular security package by briefly listening in on unintended "side channel" signals from smartphones.

The attack, which was reported to software developers before it was publicized, took advantage of programming that was, ironically, designed to provide better security. The attack used intercepted electromagnetic signals from the phones that could have been analyzed using a small portable device costing less than a thousand dollars. Unlike earlier intercept attempts that required analyzing many logins, the "One & Done" attack was carried out by eavesdropping on just one decryption cycle.

"This is something that could be done at an airport to steal people's information without arousing suspicion and makes the so-called 'coffee shop attack' much more realistic," said Milos Prvulovic, associate chair of Georgia Tech's School of Computer Science. "The designers of encryption software now have another issue that they need to take into account because continuous snooping over long periods of time would no longer be required to steal this information."

The side channel attack is believed to be the first to retrieve the secret exponent of an encryption key in a modern version of OpenSSL without relying on the cache organization and/or timing. OpenSSL is a popular encryption program used for secure interactions on websites and for signature authentication. The attack showed that a single recording of a cryptography key trace was sufficient to break 2048 bits of a private RSA key.

Results of the research, which was supported in part by the National Science Foundation, the Defense Advanced Research Projects Agency (DARPA), and the Air Force Research Laboratory (AFRL) will be presented at the 27th USENIX Security Symposium August 16th in Baltimore.

After successfully attacking the phones and an embedded system board—which all used ARM processors—the researchers proposed a fix for the vulnerability, which was adopted in versions of the software made available in May.

Side channel attacks extract sensitive information from signals created by electronic activity within computing devices during normal operation. The signals include electromagnetic emanations created by current flows within the devices computational and power-delivery circuitry, variation in power consumption, and also sound, temperature and chassis potential variation. These emanations are very different from communications signals the devices are designed to produce.

Milos Prvulovic and Alenka Zajic use tiny probe near the phone to captures the

signal that is digitized by a radio receiver to accomplish the side channel attack. Credit: Allison Carter, Georgia Tech

In their demonstration, Prvulovic and collaborator Alenka Zajic listened in on two different Android phones using probes located near, but not touching the devices. In a real attack, signals could be received from phones or other mobile devices by antennas located beneath tables or hidden in nearby furniture.

The "One & Done" attack analyzed signals in a relatively narrow (40 MHz wide) band around the phones' processor clock frequencies, which are close to 1 GHz (1,000 MHz). The researchers took advantage of a uniformity in programming that had been designed to overcome earlier vulnerabilities involving variations in how the programs operate.

"Any variation is essentially leaking information about what the program is doing, but the constancy allowed us to pinpoint where we needed to look," said Prvulovic. "Once we got the attack to work, we were able to suggest a fix for it fairly quickly. Programmers need to understand that portions of the code that are working on secret bits need to be written in a very particular way to avoid having them leak."

The researchers are now looking at other software that may have similar vulnerabilities, and expect to develop a program that would allow automated analysis of security vulnerabilities.

"Our goal is to automate this process so it can be used on any code," said Zajic, an associate professor in Georgia Tech's School of Electrical and Computer Engineering. "We'd like to be able to identify portions of code that could be leaky and require a fix. Right now, finding these portions requires considerable expertise and manual examination."

Side channel attacks are still relatively rare, but Prvulovic says the success of "One & Done" demonstrates an unexpected vulnerability. The availability of low-cost signal processing devices small enough to use in coffee shops or airports could make the attacks more practical.

"We now have relatively cheap and compact devices—smaller than a USB drive—that are capable of analyzing these signals," said Prvulovic. "Ten years ago, the analysis of this signal would have taken days. Now it takes just seconds, and can be done anywhere—not just in a lab setting."

Producers of mobile devices are becoming more aware of the need to protect electromagnetic signals of phones, tablets and laptops from interception by shielding their side channel emissions. Improving the software running on the devices is also important, but Prvulovic suggests that users of mobile devices must also play a security role.

"This is something that needs to be addressed at all levels," he said. "A combination of factors—better hardware, better software and cautious computer hygiene—make you safer. You should not be paranoid about using your devices in public locations, but you should be cautious about accessing banking systems or plugging your device into unprotected USB chargers."

In addition to those already mentioned, the research involved Monjur M. Alam, Haider A. Khan, Moutmita Dey, Nishith Sinha and Robert Callen, all of Georgia Tech.

More information: Monjur M. Alam, et. al., "One&Done: A Single-Decryption EM-Based Attack on OpenSSL's Constant-Time Blinded RSA," Proceedings of the 27th USENIX Security Symposium.