MARCH 21, 2014

Unexpected information leakage from side channel

by University of Electro Communications

Sakiyama Laboratory from the University of Electro-Communications discovered a weakness in the threshold of normal and abnormal behaviour during overclocking (CLK, above) in cryptographic device. This weakness could be used to reveal the secret key, the parameter used to change ciphertext to plaintext, allowing attackers to decipher a code.

In this high-technology age, finding ways to prevent information leakage via device hacking is increasingly important. In order to pre-empt attacks, researchers carry out false attacks on encrypted devices to find weaknesses that may be exploited in order to implement safeguards.

In particular, so-called "side-channel attacks" are used to collect data on emissions from circuits such as heat and electromagnetic waves, to analyse information about the circuit and the devices.

Kazuo Sakiyama and his group at the University of Electro-Communications in Tokyo has uncovered a previously unknown target they refer to as 'fault sensitivity' that can be exploited in devices to retrieve sensitive data such as secret information (cryptographic key). The target lies on the threshold between a device's normal behaviour and any abnormal behaviour triggered when a device is attacked.

In certain attacks, a fault of some kind is deliberately introduced into the device environment - for example inducing strong magnetic field, or forcing the internal electronics to work faster than the device expects ('overclocking'). These cause the device processor to output incorrect results, potentially allowing attackers to decipher encrypted information.

In a series of attacks on three different hardware implementations, Sakiyama and his team found that, during overclocking in one of the three implementations, the fault sensitivity threshold could be used to extract the secret key - the parameter that transforms ciphertext into plaintext. This was in spite of previous error safeguards in programs which stop working once the device is forced into abnormal behaviour.

The researchers believe that a specialized 'S-box', a component used to hide the relationship between the key and the ciphertext, incorporated into devices specifically to respond to timing abnormalities may lessen the chances of sensitive data leakage during the fault sensitivity attack.

More information: Yang Li, Kazuo Ohta, & Kazuo Sakiyama." New fault-based side-channel attack using fault sensitivity." *IEEE Transactions on Information Forensics and Security* 7 (1) (2012).