Targeting several unpipelined instructions with a single electromagnetic pulse on 8-bit microcontroller

Alexandre Menu[1,2], Jean-Luc Danger[2], Jean-Max Dutertre[1], Elias Kharbouche[1], Olivier Potin[1], and Jean-Baptiste Rigaud[1]

[1]*Mines Saint-Etienne, CEA-Tech, Centre CMP, F-13541 Gardanne France , {first.name}@mines-stetienne.fr*
[2]*Institut Mines-Télécom, Télécom ParisTech, Paris France , {first.name}@telecom-paristech.fr*

Abstract

Physical attacks enable an attacker to leverage the side channels of a device hardware implementation to access or retrieve protected resources. They are usually classified in two categories: passive side channel attacks and active fault injection attacks. The former leverage information leakage in side channel emissions to retrieve protected data, while the later aims to disrupt the operating conditions of a target, corrupting data or control instructions. Among fault injection techniques, the choice of electromagnetic fault injection (EMFI) is mainly based on two characteristics. First, access to the die, the clock or the power-ground network is not mandatory, hence little target preparation is required. Second, a price-locality compromise is reached between unexpensive global injection techniques as power glitching, and expensive highly local injection techniques as Laser injection.

This presentation investigates the use of electromagnetic pulse to skip consecutive assembly instructions executed on a microcontroller unit. The dependency between the injection parameters is discussed and an injection methodology is proposed to induce a targeted instruction skip with fine control over the number of faulted instructions. Based on this methodology, several consecutive instruction skips were obtained on a 8-bit microcontroller, which allowed us to bypass compiler-level countermeasures on a verifyPIN algorithm. To the best of the authors' knowledge, this experiment is the first to demonstrates the feasability of a multiple skips electromagnetic fault model, which does not solely rely on microarchitectural aspects. This consideration should be taken into account in designing physical attack countermeasures.