Laser-induced Single-bit Faults in Flash Memory: Instructions Corruption on a 32-bit Microcontroller

Brice Colombier[1], Alexandre Menu[2],
Jean-Max Dutertre[2], Pierre-Alain Moellic[3],
Jean-Baptiste Rigaud[2], Jean-Luc Danger[4]

(1) Laboratoire Hubert Curien, St-Etienne

(2) Ecole des Mines Saint-Etienne

(3) CEA Tech

(4) LTCI, Telecom ParisTech

Abstract

Physical attacks are a known threat posed against secure embedded systems. Notable among these is laser fault injection, which is often considered as the most effective fault injection technique. Indeed, laser fault injection provides a high spatial accuracy, which enables an attacker to induce bit-level faults. However, experience gained from attacking 8-bit targets might not be relevant on more advanced micro-architectures, and these attacks become increasingly challenging on 32-bit microcontrollers. In this article, we show that the flash memory area of a 32-bit microcontroller is sensitive to laser fault injection. These faults occur during the instruction fetch process, hence the stored value remains unaltered. After a thorough characterisation of the induced faults and the associated fault model, we provide detailed examples of bit-level corruption of instructions and demonstrate practical applications in compromising the security of real-life codes. Based on these experimental results, we formulate a hypothesis about the underlying micro-architectural features that explain the observed fault model.