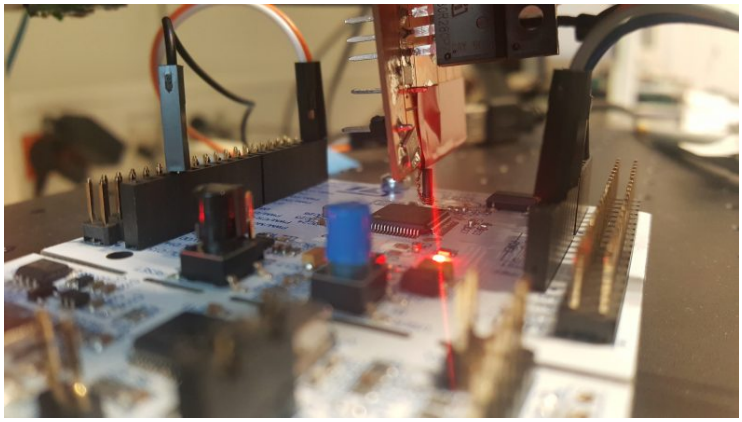
Microcontroller code readout: attacks and countermeasures



Practically all microcontrollers employ some form of read protection to ensure the confidentiality of intellectual property, cryptographic keys, and other secret or sensitive information stored in the device's flash memory. One such method disables the debug interface by using a manufacturer-specific locking mechanism, e.g. a specific 'magic' byte in the device's flash memory. This locking mechanism denies access to the internal nonvolatile memory inside the microcontroller after manufacturing.

However, recent years have seen numerous attacks that bypass this protection. In some chips, the implementation of this lockout mechanism contains logic bugs that render it vulnerable. Others are vulnerable against physical fault injection attacks that try to disable or circumvent the lockout mechanism.

The new generation of microcontrollers thus comes with new countermeasures against the above attacks. While some simply fixed the logic bugs and attempt to make fault injection more difficult, other chips have added fault detectors against such physical attacks, or come with trusted execution environments such as Arm TrustZone-M solely to guard against code readout.

This thesis offers a deep dive in the current state of the field of microcontroller code read protection. After acquiring an understanding of the problem statement and the basic attack methods, the student will evaluate a number of countermeasures in chips marketed as 'secure', and verify whether these marketing claims hold truth.

The thesis has a fairly strong focus on practical work. During the thesis, the student will have the chance to work in COSIC's state-of-the-art lab, equipped to perform a wide range of physical attacks such as side-channel analysis, EM fault injection and laser fault injection. It is strongly encouraged to contact us before making commitments.

Practicalities

Promotor:	Ingrid Verbauwhede		
Daily supervisor:	pcy Sluys	pcy.sluys@esat.kuleuven.be	office 01.20
	Jesse De Meulemeester	jesse.demeulemeester@esat.kuleuven.be	office 01.21
	Lennert Wouters	lennert.wouters@esat.kuleuven.be	office 01.16
Nature of the work:	25% literature, 75% applied work		
Number of students:	1 or 2		

 © 2026 – 2027 COSIC