Master 2 Internship proposal

Fault injection attacks on non volatile memories

Keywords: Hardware security, fault injection attack (FIA), non volatile memories (NVM), embedded systems, microcontroller development

Contact: Valentin Egloff (**valentin.egloff@lcis.grenoble-inp.fr**), LCIS laboratory, Valence, France

Context and motivation:

New memory technologies have emerged recently to replace multiple level of the memory hierarchy. These promise high density, low energy and high bandwidth memories into a single type of memory. Moreover, compared to SRAM or DRAM, they are also non volatile, *i.e.* they retain data even when power is cut. However, they present some asymmetries in power depending on the data read or written. As such, it may be possible for an attacker to guess secret information stored within the memory [1].

Fault injection attacks are active attacks in which the attacker has physical access to the device, especially the power supply or the clock generator. Both of these attacks are global attacks (*i.e.* they target the whole chip) while EM fault injection (EMFI) is a powerful local attack which can target limited area of the victim chip. By faulting the normal behavior of the circuit, the attacker can alter the data being stored or read within the memory, or even alter neighboring memory cells [2].

In this internship, we aim to **characterize** the susceptibility of **non volatile memories to fault injection attacks** of different kinds, mainly EMFI, voltage glitch and clock glitch. This exploratory work will be used to target in-memory computing systems in the future [3, 4]. Based on the knowledge of the physical phenomenon used to store the information, we want to propose models to **exploit vulnerabilities** of these new memories.

The intern will perform fault injection attacks on non volatile memories and try to determine fault model that best represent the effect of the injected fault (e.g. bit flip, bit set/reset, etc.)

In this internship, the main tasks will be:

- Implementing basic software to drive the NVM
- Conducting fault injection attacks on different NVM
- Analyzing and determining the best way to fault the NVM
- Eventually, designing basic countermeasures suited to NVM against FIA

Who can apply: Applicants must be enrolled in a Master’s degree or engineering school in cyber security, computer engineering, electrical engineering or embedded systems and have interests in hardware security.

Required skills:

- C and assembly
- Microcontroller development (Arduino, STM32 or ARM)
- Embedded systems
- Basic knowledge of physical phenomenon used in NVM is a plus

Internship duration: 5 to 6 months (starting February 2024)

Internship location: LCIS Laboratory, in CTSYS team (https://lcis.fr/ctsys)

Laboratoire LCIS, 50 Rue Barthélémy de Laffemas, 26902 Valence cedex 9, France

Financing: About 650€ per month.

For more information or in case you are interested:

please contact or send your CV to: valentin.egloff@lcis.grenoble-inp.fr

Bibliography:

[1] M. N. I. Khan, S. Bhasin, B. Liu, A. Yuan, A. Chattopadhyay, et S. Ghosh, « Comprehensive Study of Side-Channel Attack on Emerging Non-Volatile Memories », *Journal of Low Power Electronics and Applications*, vol. 11, nº 4, Art. nº 4, déc. 2021, doi: 10.3390/jlpea11040038.

[2] M. Heidary et B. K. Joardar, « Hardware Attacks on ReRAM-Based AI Accelerators », in *2024 IEEE 17th Dallas Circuits and Systems Conference (DCAS)*, avr. 2024, p. 1‑4. doi: 10.1109/DCAS61159.2024.10539864.

[3] Z. Wang, F.-H. Meng, Y. Park, J. K. Eshraghian, et W. D. Lu, « Side-Channel Attack Analysis on In-Memory Computing Architectures », *IEEE Transactions on Emerging Topics in Computing*, vol. 12, nº 1, p. 109‑121, janv. 2024, doi: 10.1109/TETC.2023.3257684.

[4] M. T. Arafin et Z. Lu, « Security Challenges of Processing-In-Memory Systems », in *Proceedings of the 2020 on Great Lakes Symposium on VLSI*, in GLSVLSI ’20. New York, NY, USA: Association for Computing Machinery, sept. 2020, p. 229‑234. doi: 10.1145/3386263.3411365.