Bachelor Thesis Project

Analyzing Timing Side Channels in Embedded Systems

Contact: Ahmed Rezine

Linköping University

Description

Side channel attacks can leverage on micro-architectural behaviors of program execution. Typical side-channel attacks aim to recover sensitive or secret information. The idea is to use non-functional characteristics of the computations in order to recover secret information. Such characteristics can include the time computations may take, their cache behavior, their power consumption or their memory usage. Timing attacks have been mounted against controllers for embedded systems [2, 4] and recent works [1] started analyzing such attacks specifically for embedded systems using symbolic execution frameworks [3]. For this, it is important to analyze what is actually running on the hardware, i.e., machine code. This project aims to identify attacks, to mount some of them on a real platform, and to assess both existing analysis tools and mitigation approaches. For this purpose, the project aims to:

1. Gain familiarity with timing attacks for embedded controllers,
2. Mount some attacks on a real platform (an ARM Cortex M33)
3. Understand and assess existing analysis tools and mitigation approaches.

Qualification

This 16 hp thesis will be carried by one or two bachelor student(s).

- The student should have very good programming skills (assembler, C, Java)
- Compilers and a computer hardware courses is a plus
- Good background in discrete mathematics and logic is a plus

References

1. Sepideh Pouyanrad, Fritz Alder, and Jan Tobias Mühlberg. Automated side-channel analysis of arm trustzone-m programs. In *Computer Security. ESORICS 2024 International Workshops*, pages 494–513, Cham, 2025. Springer Nature Switzerland.
2. Cristiano Rodrigues, Daniel Oliveira, and Sandro Pinto. Busted!!! microarchitectural side-channel attacks on the mcu bus interconnect. In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 3679–3696, 2024.
3. Yan Shoshitaishvili, Ruoyu Wang, Christopher Salls, Nick Stephens, Mario Polino, Audrey Dutcher, Jessie Grosen, Siji Feng, Christophe Hauser, Christopher Kruegel, and Giovanni Vigna. Sok: (state of) the art of war: Offensive techniques in binary analysis. 2016.
4. Jo Van Bulck, Frank Piessens, and Raoul Strackx. Nemesis: Studying microarchitectural timing leaks in rudimentary cpu interrupt logic. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 178–195, 2018.