Characterization of Side-Channel Vulnerabilities on Binary Code

Yanis Sellami
CEA, List

Sébastien Bardin
CEA, List

yanis.sellami@cea.fr, sebastien.bardin@cea.fr

Automated program analysis is a research topic that tries to design tools and analyses to detect bugs in programs. Existing techniques typically target memory access vulnerabilities (*e.g.* buffer overflows) and numerical vulnerabilities (*e.g.* zero division) that can corrupt program data or crash the execution. Yet, even when one can prove that a program contain no such bug, an attacker can still exploit some physical properties of program execution (such as execution time, cache values, ...) to understand its behavior and extract secret data. Such attacks are called side-channel attacks.

The binary code analysis platform BINSEC [1] developped at CEA List possesses a relational analysis [2] that can detect some side-channel vulnerabilities, typically when the code is not constant-time. While BINSEC can provide a witness (assignment of the program inputs) alongside the alerts that it raises, this is often insufficient to conclude that the issue will be exploitable in practice.

The goal of this project is to extend a recent work on bug characterization for fault injection attacks [3] to side-channel analysis. The core idea being to provide, instead of a single witness, a logical constraint that describes sets of inputs for which the vulnerability will be triggered. This will require the design of a constraint generation setup adapted to relational symbolic execution, the implementation of a prototype (possibly based on existing prior work) and its experimental evaluation.

Logistics. The internship will be homed at Nano-INNOV in Saclay, co-supervised by Yanis Sellami and Sébastien Bardin.

Candidate. To candidate or obtain additional information, please contact the supervisors by email.

References

[1] "Plateforme binsec." `https://binsec.github.io/`.

[2] L.-A. Daniel, S. Bardin, and T. Rezk, "Binsec/rel: Symbolic binary analyzer for security with applications to constant-time and secret-erasure," *ACM Trans. Priv. Secur.*, vol. 26, apr 2023.

[3] Y. Sellami, G. Girol, F. Recoules, D. Couroussé, and S. Bardin, "Inference of robust reachability constraints," *Proc. ACM Program. Lang.*, vol. 8, Jan. 2024.