

Extending a Binary Code Vulnerability Analysis for Fault Injection Attacks

Yanis Sellami Sébastien Bardin
CEA, List 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 contains no such bug, an attacker can still target the hardware on which the program is running to modify the actual execution. An attacker can then bypass security protections that were present in the original code.

However, automated detection procedures for fault injection vulnerabilities are expensive as each fault increases the size of the code to analyze. The binary code analysis platform BINSEC [1] developed at CEA possesses a state of the art analysis for fault attacks detection [2]. Still, this technique suffers from several significant limitations (most notably, permanent faults cannot be handled) that prevents it from detecting some state of art attack scenarios (*e.g.* rowhammer [3]). We are also interested in improvements and/or optimisations of the analysis to increase its efficiency and scalability.

The goal of this project is to produce an implementation of an extension or optimization of the fault analysis technique of BINSEC.

Logistics. The internship will be hosted 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.

Références

- [1] “Plateforme binsec.” <https://binsec.github.io/>.
- [2] S. Ducousso, S. Bardin, and M.-L. Potet, “Adversarial reachability for program-level security analysis,” in *Programming Languages and Systems* (T. Wies, ed.), (Cham), pp. 59–89, Springer Nature Switzerland, 2023.
- [3] Y. Kim, R. Daly, J. Kim, C. Fallin, J. H. Lee, D. Lee, C. Wilkerson, K. Lai, and O. Mutlu, “Flipping bits in memory without accessing them : an experimental study of dram disturbance errors,” in *Proceeding of the 41st Annual*

International Symposium on Computer Architecture, ISCA '14, p. 361–372,
IEEE Press, 2014.