Cybersecurity Institute
Université Grenoble Alpes

CLAM

Cross-Layer Fault Analysis for Microprocessor Architectures

Better understand fault attacks,
to build more secure embedded systems

What is Fault Analysis?

Fault injection attacks are considered one of the major threats to cyber-physical systems. The increasing complexity of embedded microprocessors involves complicated behavious in presence of such attacks. Realistic fault models are required to study code vulnerabilities and be able to protect digital systems from these attacks. However, inferring fault models using only limited observations of faulty microprocessors is difficult.

We propose a complete approach for fault analysis to build proper fault models at different abstraction levels, which will help in better understanding existing vulnerabilities, and designing suitable countermeasures at reasonable cost at both hardware and software levels.

Application

Digital systems contain sensitive information that can be effectively protected through cryptographic algorithms, often implemented in software on an embedded microprocessor.

Securing components, such as microprocessors and microcontrollers, against fault attacks requires a thorough understanding of the faults: on the one hand, this means characterizing, studying, and analyzing the faults that could lead to exploitable code vulnerabilities. On the other hand, it also requires designing countermeasures at different levels, hardware and software, with an acceptable cost.

PERSYVAL-2 Verimag LCIS Laboratoire de Conception et d'Intégration des Systèmes TIMA

News

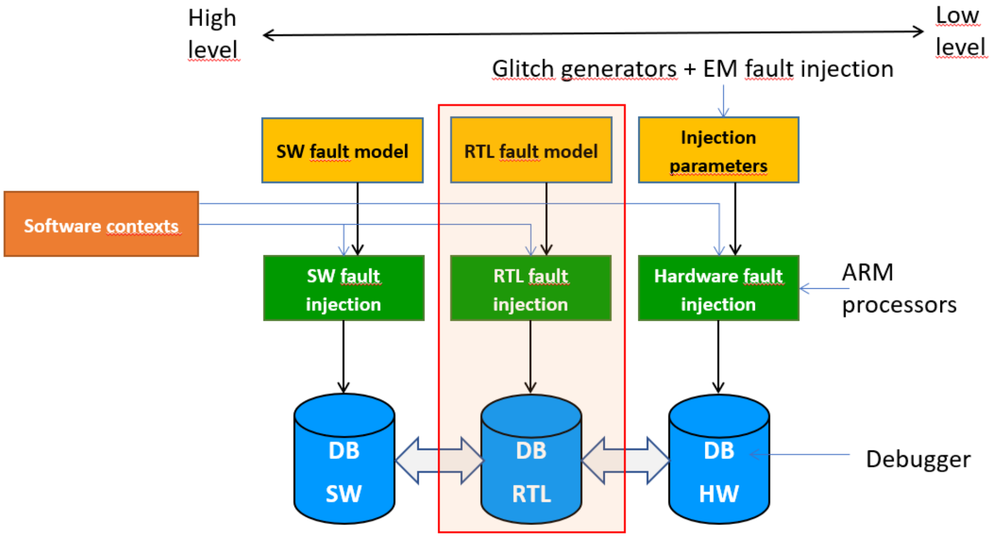
With the increasing complexity of digital applications, the use of variable-length instruction sets became essential, in order to achieve higher code density and thus better performance. However, security aspects must always be considered, in particular with the significant improvement of attack techniques and equipment. Fault injection, in particular, is among the most interesting and promising attack techniques thanks to the recent advancements.

We have provided proper characterization, at the instruction set architecture (ISA) level, for several faulty behaviors that can be obtained when targeting a variable-length instruction set. We take into account the binary encoding of instructions, and show how the obtained behaviors depend on the alignment of the instructions in the memory. Thanks to our approach, we are also able to give a better insight on previous (partially unexplained) results from the literature; and show how they can be exploited in various security contexts.

To find out more

Ihab Alshaer et al.: **Cross-Layer Inference Methodology for Microarchitecture-aware Fault Models.** Microelectronics Reliability, 2022.

Ihab Alshaer et al.: **Variable-Length Instruction Set: Feature or Bug?**. 25th Euromicro Conference on Digital System Design (DSD 2022), 464-471.



Prospects

We have explained and reproduced several experimental faulty behaviors through novel fault models.

Next steps include targeting other architectures, studying compositional methods for countermeasure analysis, extension of software evaluation tools.

Contact

Vincent BEROULLE
Paolo MAISTRI
Marie-Laure POTET

Firstname.Lastname@univ-grenoble-alpes.fr