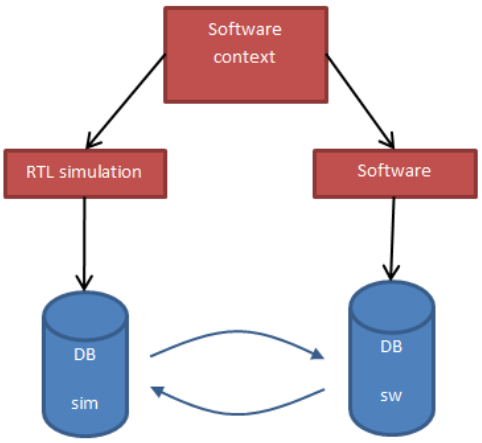
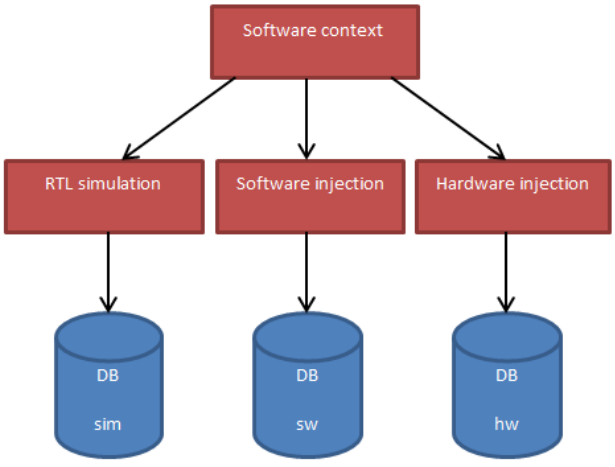
Internship: Fault modeling analysis through experimental attacks

Reference	CYBERINSTITUTE-INT-20013
Description	Fault attacks are a major type of physical attack, which can intrude on the normal and secure behavior of the targeted devices. Regarding this, various security evaluation methods are proposed, which enable the software designers to be aware of existing vulnerabilities against this kind of attacks. A hardware security assessment can be performed either by applying practical techniques such as simulations and emulations or by using mathematical analysis methods [1][2][3]. Today's simulation tools have extensive capabilities, and they can be used as highly accurate, flexible and low-cost appliances in primary evaluation. However, in hardware-based attacks, different environmental parameters are involved, which make it impossible to describe and study any arbitrary attack occurring in the simulation environment [4]. Another considered technique in the hardware security domain is emulation analysis that can provide an experimental platform for investigating and measuring the consequences of possible risks [5]–[7]. Usually, the emulation-based evaluation platforms for FIAs mimic the real fault attacks. The internship takes place in the LCIS laboratory in Valence, France. Two third-year Ph.D. students have developed methodologies to analyze fault injection with different methods: • Johan's thesis (Figure.1) is based on RTL and software fault injection simulation. On one hand, faults are injected in the RTL simulation of a processor running a specific software (e.g. medical IoT application), and on the other hand, a fault is injected in software, under the same conditions. The results are compared to verify that the behaviors described in software correspond to what happens in RTL simulation. As a result, the software fault models are evaluated against a "theoretical" point of view. Comparing models against experimental results (by Elnaz platform) could bring more realism to the methodology. • Zahra's thesis introduces a fault injection evaluation platform with different parameters and capabilities. This platform is injecting precise faults by generating faulty clock/voltage signal with controlling parameters including injection time and glitch properties. These parameters could be defined based on a fault model database generated by Johan's thesis to verify the results of the software level and cover more fault injection scenarios. The objective of this internship is to find convergence points between these two methodologies (Figure.2); for example, to verify the simulation-based fault models with experimental attacks and to extend the domain of emulation based fault results. Regarding this, we can define a 6-month internship, to develop an interface for the experimental hardware attack platform which also covers the simulation-based fault models. This can result in finding the proper setup attack parameters. Finally, the implemented interface could help to have more fault injection scenarios in the Elnaz's evaluation platform and will also verify the simulation fault results from Johan's thesis.  Figure 1. Johan's Thesis  Figure 2 .Evolved methodology • Elnaz's perspective: Find the correct fault injection parameters to reproduce the software fault models in an experimental environment. Cover more vulnerabilities against the fault attacks. • Johan's perspective: Check the efficacy of software fault models in the experimental evaluation platform. Build new

software fault models if necessary.

- The common goal: Johan can model faults from the result of the experimental fault injection while Elnaz can obtain the proper parameters in order to inject precise faults (Figure 3).

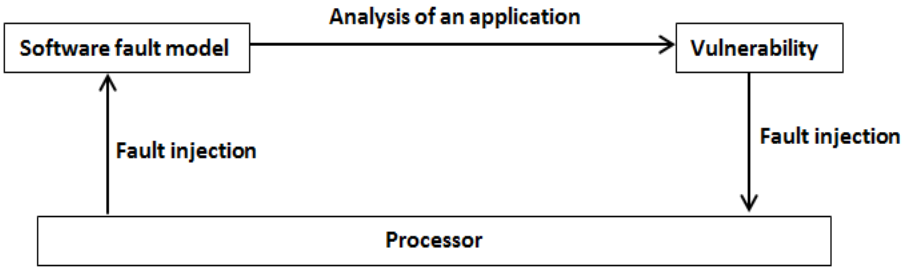


Figure 3. final idea

Context:

The Grenoble Alpes Cybersecurity Institute – in short, Cyber@Alps – is a project selected in 2017 by the Cross-Disciplinary Program (CDP) of the IDEX Univ. Grenoble Alpes and aims at undertaking ground-breaking interdisciplinary research in order to address cybersecurity and privacy protection challenges. Our main technical focus are on cost effective secure elements, security of critical infrastructures all along their life cycle, vulnerability analysis and global challenges in terms of risk analysis and validation of large systems, including practical resilience across the industry and the society. Our approach to cybersecurity is holistic, encompassing technical, legal, law-enforcement, economic, social, diplomatic, military and intelligence-related aspects with strong partnerships with the private sector and robust national and international cooperation with leading institutions in France and abroad (https://cybersecurity.univ-grenoble-alpes.fr)

References

[1] R. Piscitelli and F. Regazzoni, "Fault attacks, injection techniques and tools for simulation," pp. 15–20, 2015.
[2] H. Le Bouder et al., "An Evaluation Tool for Physical Attacks To cite this version : HAL Id : hal-01894517 An Evaluation Tool for Physical Attacks," 2018.
[3] A. Thillard, E. Prouff, and T. Roche, "Success through confidence: Evaluating the effectiveness of a side-channel attack," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 8086 LNCS, pp. 21–36, 2013.
[4] F. E. Potestad-Ordonez, C. J. Jimenez-Fernandez, and M. Valencia-Barrero, "Vulnerability Analysis of Trivium FPGA Implementations," IEEE Trans. Very Large Scale Integr. Syst., vol. 25, no. 12, pp. 3380–3389, 2017.
[5] M. Matsubayashi, A. Satoh, and J. Ishii, "Clock glitch generator on SAKURA-G for fault injection attack against a cryptographic circuit," 2016 IEEE 5th Glob. Conf. Consum. Electron. GCCE 2016, pp. 5–8, 2016.
[6] C. O. Flynn and Z. D. Chen, "chipwhisperer," 2015.
[7] T. Katashita, Y. Hori, H. Sakane, and A. Satoh, "Side-Channel Attack Standard Evaluation Board SASEBO-W Specification Ver 1.1," Niat 2011, p. 36, 2011.

Prerequisites	Programming skills (e.g Python/C/C#/Bash scripting) to design a user-friendly interface that contains different fault injection models. Knowledge of FPGA programming to connect the interface to the evaluation board and to send the configuration parameters to the FPGA .Some knowledge in processor architecture would be a plus A good level in English is required
Tutors	Zahra Kazemi and Johan Laurent
Applications	Please send your resume, application letter with two recommendations (including education director), first year master's degree grades (mandatory) and second year grades (if possible) to cyberalps-contact@univ-grenoble-alpes.fr For more information on the internship, please contact zahra.kazemi at lcis.grenoble-inp.fr or johan.laurent at lcis.grenoble-inp.fr
Location	LCIS, 50 rue Barthélémy de Laffemas, 26000 Valence
Starting date	February-March 2020
Duration	5 to 6 months
Allowance	In accordance with existing regulations (approx. 560€/month). Part of travel expenses can be covered.