3rd URSI AT-AP-RASC, Gran Canaria, 29 May – 3 June 2022

Comparing Intentional Electromagnetic Interference and Electromagnetic Fault Injection for electromagnetic security applications

José Lopes Esteves
National Cybersecurity Agency of France (ANSSI), Paris, France
jose.lopes-esteves@ssi.gouv.fr

The analysis and the management of risks involving the exploitation of EMC phenomena in the framework of information security or functional safety are of fundamental interest. This interest is increasing with the widespread of low power electronics in critical systems, such as autonomous vehicles or unmanned aerial vehicles. Several challenges arise when it comes to characterizing the susceptiblity of an electronic device, determining the exploitability of effects and assessing the impacts on both the processed information and the critical functions [1].

Electromagnetic fault injection, both conducted and radiated, usually target components at a very short distance [2]. Threat models consider a powerful attacker which controls precisely the electromagnetic environment, along with power and/or clock signals. Furthermore, it often is able to both trigger specific processing (e.g. cryptographic operations) and monitor the target activity in order to finely synchronize the injected signals [3]. Fault models are used to analyse the exploitability of effects in a information security perspective.

Intentional electromagnetic interference and high power microwave threats focus usually range from components to complex systems. Threat models cover several scenarios where the attacker can be at a significant distance from the target [4], bringing signal generation, emission and propagation into the attacker profile estimation. Effects are generally considered coarse grain and focused on functional or mission critical impacts [5]. Recent effort has been made to find a characterization method than would be information security oriented [6].

In this study, a thorough comparison of EMFI and IEMI will be presented, with a focus on threat models, attacker profiles and characterization. Then, a reflection will be depicted on potential benefits each approach might bring to the other, especially when it comes to understanding EMC phenomena and assessing relevant impacts for information security. Finally, a discussion on the threat models and potential misconceptions will be proposed.

References

[1] D. Giri, R. Hoad, and F. Sabath, *High-Power Electromagnetic Effects on Electronic Systems*. Artech House, 2020.

[2] P. Maurine, "Techniques for EM Fault Injection: Equipments and Experimental Results," in *FDTC 2012: Fault Diagnosis and Tolerance in Cryptography*, p. 003, 2012.

[3] C. O'Flynn, *A Framework for Embedded Hardware Security Analysis*. PhD thesis, Dalhousie University, Halifax, Nova Scotia, USA, 2017.

[4] M. G. Backstrom and K. G. Lovstrand, "Susceptibility of electronic systems to high-power microwaves: Summary of test experience," *IEEE Transactions on Electromagnetic Compatibility*, vol. 46, no. 3, pp. 396–403, 2004.

[5] F. Sabath, "Classification of electromagnetic effects at system level," in *2008 International Symposium on Electromagnetic Compatibility - EMC Europe*, pp. 1–5, 2008.

[6] J. Lopes Esteves, E. Cottais, and C. Kasmi, "Analysis of Soft Faults induced by IEMI for Elementary Functions and Complex Electronics," in *Radio Science Conference (URSI AP-RASC), 2019 URSI Asia Pacific*, (New Dehli, India), IEEE, 2019.