Fault injection effectiveness compared to reflection coefficient of antenna/target couple

Guillaume Bouffard(1)(2), Valentin Houchouas(1), José Lopes-Esteves(1) and Thomas Trouchkine(1)
(1) National Cybersecurity Agency of France (ANSSI), Paris, France
(2) DIENS, École Normale Supérieure, CNRS, PSL University, Paris, France
firstname.name@ssi.gouv.fr

Most of our daily electronic objects store our personal data. One method used by attackers to retrieve this data consists in disrupting the operation of the component during the execution of a sensitive program [2]. For example, electromagnetic perturbation can disturb the electronic of a component and infer errors during the execution of the program and thus leak or modify sensitive information, which can jeopardize the system security [5].

To generate effective electromagnetic perturbations, the state-of-the-art fault injection community uses small handmade antennas placed within a few millimeters to the target component [1]. These antennas are connected to a pulse generator of several hundred volts and tens of nanoseconds pulse. By moving the antenna over the component, an attacker goal is to determine the parameters (*i.e.* (x, y) positions and pulse amplitude) that maximize the probability of obtaining exploitable faults.

The fact that these antennas are handmade [4, 3] complicates the reproducibility of studies due to the geometry and the constitutive material variability. Furthermore, the input impedance of antennas is never indicated in fault injection related publications.

As antennas are placed in the near vicinity of the component under test (CUT), and because antenna far field properties are different from near field ones, it could be relevant to determine the input impedance of the antenna/target couple which can be computed from the reflection coefficient (S_{11}) measured by a vector network analyzer.

In our work, we aim at comparing the probability to obtain a fault at a given position (x, y) with the frequency dependent absorbed power by the antenna/CUT couple. By doing so, we expect to be able to get information related to the sensitive frequencies of the CUT which might pave the way to narrowband (or continuous wave) injections.

References

[1] Philippe Maurine. Techniques for EM fault injection: Equipments and experimental results. In Guido Bertoni and Benedikt Gierlichs, editors, *2012 Workshop on Fault Diagnosis and Tolerance in Cryptography, Leuven, Belgium, September 9, 2012*, pages 3–4. IEEE Computer Society, 2012.

[2] Niek Timmers, Albert Spruyt, and Marc Witteman. Controlling PC on ARM using fault injection. In *2016 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2016, Santa Barbara, CA, USA, August 16, 2016*, pages 25–35. IEEE Computer Society, 2016.

[3] J. Toulemont, G. Chancel, Jean Marc Gallière, Frédérick Mailly, Pascal Nouet, and Philippe Maurine. On the scaling of EMFI probes. In *18th Workshop on Fault Detection and Tolerance in Cryptography, FDTC 2021, Milan, Italy, September 17, 2021*, pages 67–73. IEEE, 2021.

[4] Thomas Trouchkine, Guillaume Bouffard, and Jessy Clédière. Fault injection characterization on modern CPUs. In Maryline Laurent and Thanassis Giannetsos, editors, *Information Security Theory and Practice - 13th IFIP WG 11.2 International Conference, WISTP 2019, Paris, France, December 11-12, 2019, Proceedings*, volume 12024 of *Lecture Notes in Computer Science*, pages 123–138. Springer, 2019.

[5] Bilgiday Yuce, Patrick Schaumont, and Marc Witteman. Fault attacks on secure embedded software: Threats, design, and evaluation. *Journal of Hardware and Systems Security*, 2(2):111–130, 2018.