Hardware-enabled AI for Embedded Security: A New Paradigm

Adrien Facon[1;2], Sylvain Guilley[1;2;3], Xuan-Thuy Ngo[1],
Robert Nguyen[1], Thomas Perianin[1], Ritu-Ranjan Shrivastwa[1]

[1] Secure-IC S.A.S., Rennes, France
{firstname.lastname@secure-ic.com}
[2] Ecole Normale Supérieure, Département d'Informatique, Paris, France
[3] LTCI, Télécom ParisTech, Université Paris-Saclay, Paris, France

Abstract.

As chips become more inter-connected, they are more exposed to both network and physical attacks rendering it pertinent to ensure a sufficient protection level to them. In this paper, we explain why it is worthwhile resorting to Artificial Intelligence (AI) for security event handling and present an experimental use-case of a crypto-accelerator protected by a fleet of digital sensors embedded on a FPGA board. The data from this fleet of sensors need to be aggregated and processed fast to produce exploitable information while maintaining a low false positive detection rate. We evaluate different Machine Learning (ML) techniques and conventional method of perturbation detection using sensor threshold. Analysis includes quantitative figures of merit regarding EMFI detection comparing ML-based sensor teaming strategy and threshold-based individual sensor approach to establish significant gain in detection accuracy of the former.

Keywords:
Artificial Intelligence (AI), Machine Learning (ML), Threat Detection, Cyber-Protection, Decision Making Process, Naive Bayes Classifier, Embedded Security, Cyber-Physical Attack