Combining sources of side-channel information

Christophe Genevey-Metat[1], Benoît Gérard[2;3], Annelie Heuser[1]

[1] Univ Rennes, Inria, CNRS, IRISA, France
[2] Univ Rennes, CNRS, IRISA, France
[3] Direction Générale de l'Armement

Abstract

A few papers relate that multi-channel consideration can be beneficial for side-channel analysis. However, all were conducted using classical attack techniques. In this work, we propose to explore multi-channels approach thanks to machine/deep learning. We investigates three kinds of multi-channel combinations. First, as previous works did, we consider the combination of EM emission and power consumption. Second, we investigate the combination of EM emissions from different locations. We expect that the measurements from these locations will convey complementary information. Eventually, we consider a novel approach that is to combine a classical leaking signal and a measure of the ambient noise. The knowledge of the ambient noise (due to WiFi, GSM,…) may help to remove it from a noisy trace. At the time of submission experiments are ongoing thus we further focus on the state-of-the-art, motivation and the experimental setup. We believe that whatever the results are (combining is improving or is useless) they will be of interest to the community.

Keywords:
Side-channel analysis, profiled attacks, deep learning, power consumption, electromagnetic emanations, multi-channel, neural networks