Timing Side Channel Attack

This project has been developed as a semester project during our studies at EURECOM, Sophia Antipholis (Fall 2018 - Spring 2019), with the supervision of Prof. Renaud Pacalet.

Goal

Our purpose is to perform a timing side channel attack on an implementation of the RSA algorithm which takes advantage of the Montgomery multiplication. Basically, we will try to cipher different plaintext, and knowing the time needed by our algorithm to encrypt the plain text, we will try to discover the private key. To be successful, we need of course to know the public pair of the key (i.e. N, D). We will try to get the private key, bit by bit, by evaluating the linear correlation of a timing estimate related to a single iteration of the algorithm and the final timing, using `Pearson Correlation Coefficient` as an estimator. As a matter of fact, from a study of the algorithm one may see that the timing will be affected by the value of the bit under evaluation, which means that it could be possible to see a contribution of each iteration with respect to the result.

Analysis

By statistically analyzing the time required by the HW to perform the needed operations, we are likely to retrieve informations regarding the data. As a matter of fact, the timing optimization depends on the data, which means that if we can get information regarding the execution time and/or the power consumption, it should be possible to know the operands with a significant certainty.

Report

To get more precise information about the project development, refer to the REPORT.

Contacts

For any information, you can simply drop an email: * Alberto Anselmo * Simone Alessandro Chiaberto * Fausto Chiatante * Giulio Roggero