System Security, Solution Lab Report

George Cojocar, Andrin Jenal, Jonas Passerini

October 20, 2015

1 General Hints for the reports

To help you structuring the report on the labs, we provide you with some questions to answer in the report and some **hints** you might need to consider. Please, note that it is not an exhaustive list of questions. Therefore, we advise you to include more information from your hacking experience in the report.

2 Lab Session: Side-channel attack

In the lab session, the goal is to find the secret key used in a RSA operation by analyzing the power consumption.

(a) Explain the setup to measure the power consumption of the sensor node

Solution:

The setup used for power analysis attack consists of a single-board micro-controller, an AC/DC power supply and an oscilloscope (see Figure 1). The micro-controller is powered by the external power supply, and it performs an encryption and a decryption sequence when it is turned on. The power consumption during cryptographic operations is measured by the oscilloscope which is connected to the micro-controller's power pins.

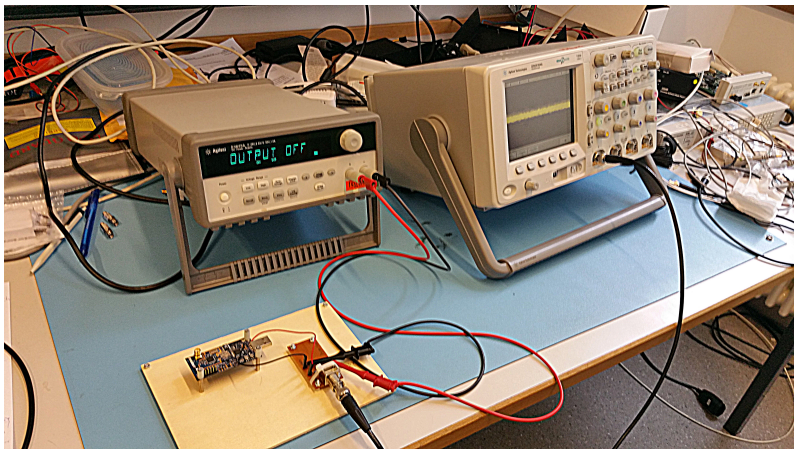
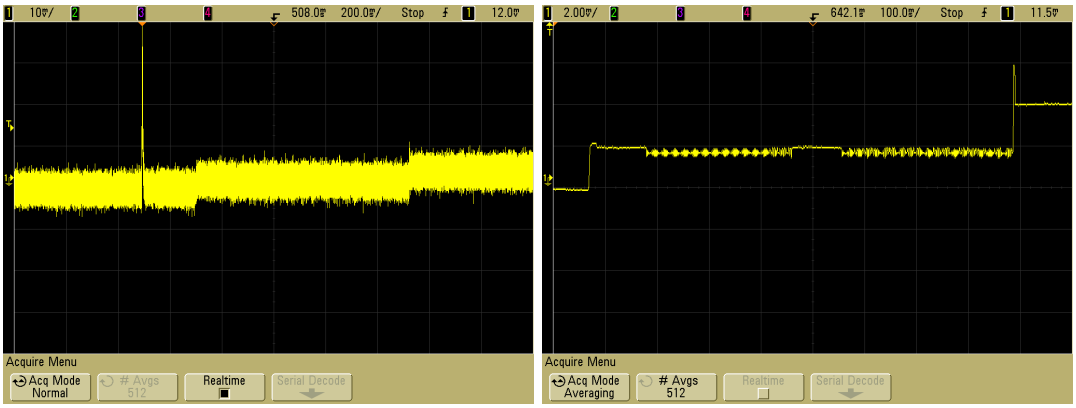


Figure 1: Shows the initial setup with the micro-controller and the oscilloscope.

(b) What technique did you use to improve the measurement noise in the power trace?

Solution:



(a) Power measurement of a single signal using the oscilloscope.

(b) Averaged power measurement of 512 signals using the oscilloscope.

Figure 2: Effect of averaging on the measured signal compared to a single signal measurement.

The method used to reduce the noise on a measured signal was signal averaging. We set up a trigger and acquired the noisy signal 512 times. The oscilloscope added up all acquisitions and divided by 512. This technique significantly reduced the level of noise as one can see when comparing the power measurement of a single signal in Figure 2a to the averaged power measurement in Figure 2b.

(c) To which horizontal resolution did you set the oscilloscope to read out the bits? How did you find this value?

Solution:

The value of horizontal resolution was 2 seconds. We found this value by configuring the maximum resolution available in order to achieve the most accurate period and frequency measurements. Afterwards we adjusted the horizontal scale until the whole signal was visible.

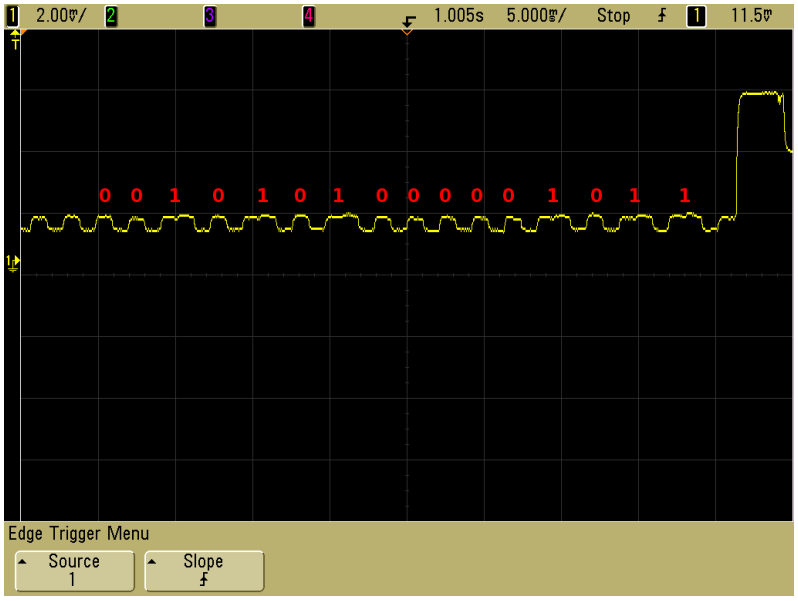
(d) What is the key that you could see? Explain how you are able to see the key and what leads to differences in the power consumption. Mark the different bits in a picture.

Solution:

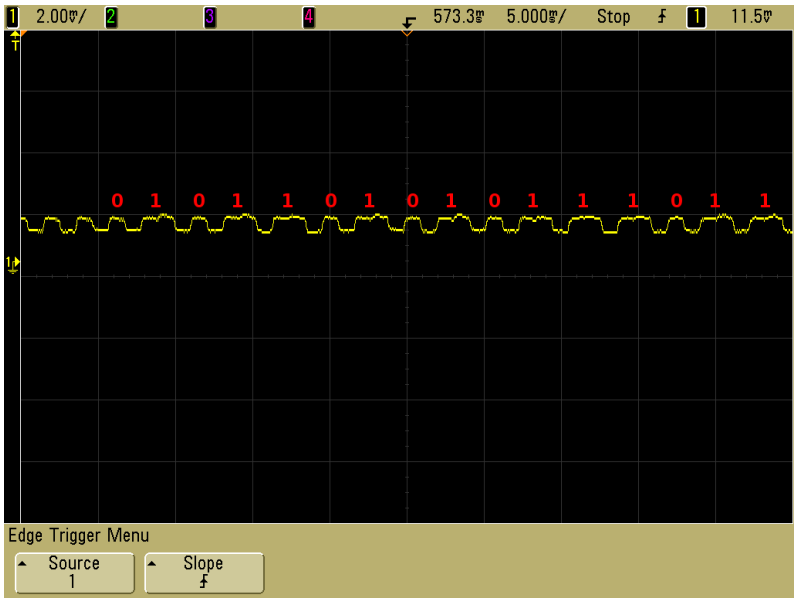
The RSA decryption is implemented by using the square and multiply exponentiation algorithm. Each of the two operations has a different power consumption pattern, that can be observed on an oscilloscope. For this reason, one can apply simple power analysis and extract the private key bit by bit as follows:

- If the squaring is followed by a multiplication, this bit of the exponent is one
- If the squaring is followed by another squaring, this bit of the exponent is zero

A shorter operation consists only of squaring and therefore represents a zero while a longer operation both consists of squaring and multiplication and accordingly represents a one. This information can be used to directly read the key from the power measurement as one can clearly distinguish between shorter and longer operations. Figure 3 shows the extraction of the public and private key based on the power measurements. In our experiment, the last 16 bits of the private key are 0x2A0B as shown in Figure 3a and the last 16 bits of the public key are 0x5ABB as shown in Figure 3b.



(a) Extraction of the last 16 bits of the private key (0x2A0B).



(b) Extraction of the last 16 bits of the public key (0x5ABB).

Figure 3: Key extraction based on the averaged measurement while performing the encryption and decryption. Bit 1 is represented by a larger working cycle and bit 0 by a smaller one.

References

[1] Srdjan Capkun, Adrian Perrig, *System Security*, ETH, AS 2015