Hardware and Operating Systems Security, Autumn 2014

Side-channel lab

Session 2: DPA on real-life and protected implementations

Go through this short tutorial and answer the questions. Answer as many questions as you can – there might not be enough time for all of them. Write down the answers per group and hand in/email them to Lejla (lejla@cs.ru.nl) and Barış (b.ege@cs.ru.nl).

Task 1 is about power analysis on real-life AES traces. In Task 2 you will be attacking a protected DES implementation. For Task 3 you have to find out which algorithm is used. The traces are available in C:\Program Files(x86)\Inspector-4.6\data (Also accessible from File -> Open Demo Trace set...). Algorithm descriptions are available at Wikipedia.

1) DPA on AES, real measurements:
   - **a)** Click 'File -> Open Demo Trace set...' and open trace set 'Overview AES.trs'.
   - **b)** It is, as before, required to identify the first or the last round; then you can start with the attack. In order to identify the rounds, run the Autocorrelation module (Analysis -> Autocorrelation) on this trace. You will see 9 repeating patterns and 1 additional pattern looking similar to the others.

   A. Explain why this is the case in autocorrelation output.

   - **c)** Zoom into the first round of computations by selecting the necessary part of the trace and then pressing the return key.

   B. What is the approximate time interval where s-box look-ups are done for the first round? (Hint: Most time consuming operations in AES are SubBytes and MixColumns operations.)

   - **d)** Open demo trace set 'AES_raw_100traces.trs'. This trace is focused on the first round of the AES computation. Select the area where the s-box look-ups for the first round are done, and run 'First-order Analysis' module (Crypto -> First-order Analysis) with parameters: Method: **Correlation**, Criterion: **Peak** to run the attack on the **first** round **S-box output** using Hamming weight (**HW**) model.

   C. What is the key after running First-order Analysis on 'AES_raw_100traces.trs'? Do you think this is the correct key? Why? (Hint: Overlap multiple traces and zoom in.)

   - **e)** Run Static Align module (Align -> Static align) on 266 samples starting from sample 3128, with parameters 'Shift max = 250' and 'Threshold = 0.78'. Now run First-order Analysis on the aligned traces by selecting only the s-box lookup part again.

   D. What is the key after running First-order Analysis on aligned traces? Do you think this is the correct key? Why?

2) Power analysis of a protected implementation of 3DES:

a) Open demo trace set ’2DES_random_delay.trs’. Use the Autocorrelation module to identify repeating patterns. (You will notice that this runs very slowly so after seeing 1st row open a screen shot of the complete graph given in *C:\Program Files(x86)\Inspector-4.6\data* as AutoCorrelation_on_2DES_random_delay.png.)

E. How many repeating patterns can be observed per row/column? Knowing that this is the trace of 3DES what does it mean? (Hint: The card does not have a dedicated random number generator.)

b) Open the ’2Des_randomd_resampled.trs’ trace. This measurement is focused at the end of the process, where the last rounds are computed. It is also statically aligned at the end of the trace. In the trace set select around 150 samples around sample 13000 and zoom into this fragment. Display several traces and overlap them. You will observe that although the traces have been aligned at the end, they are misaligned in this region. This shows that the card is introducing random delays.
Align the traces by using *Elastic align* module (Align -> Elastic align). Select only a small area to speed-up the alignment (last 2 rounds). Run *First-order Analysis* module on the last round. You will need to select DES as the cipher and choose ‘Output -> Input’ as the attack direction.

F. After starting *First-order Analysis* a leakages tab is visible. What are the possibilities and what is computed in different choices of “Target”? Answer the same question for “Model”. What is the round key? (Tip: You can read about all the options in Inspector manual)

c) Run the attack again on 15th round.

G. What is the DES key found after repeating the attacks on round 15?

3) Advanced power analysis:

a) Open ‘2nd_trace1_analysis.trs’ file. Examine the traces and answer the following questions.

H. How many traces are considered in this set? Which algorithm is it?

b) Run first order analysis on it by selecting a round and a module. Repeat the attack for other rounds to check your results.

I. What is the round key for the 5th round?

$Hint_1$: Apply the tricks you learned during this exercise session.
$Hint_2$: Consider how DES key schedule works.