PB173 Domain specific development: side-channel analysis

Seminar 6: First Steps & CPA and DPA

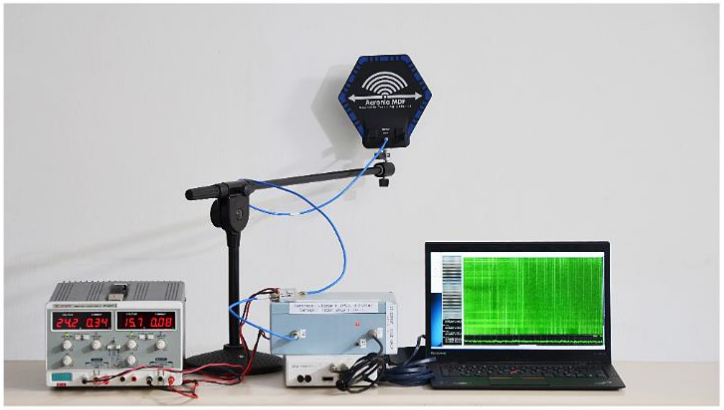
Łukasz Chmielewski
chmiel@fi.muni.cz,

Consultation: A406 Friday 9:30-11:00

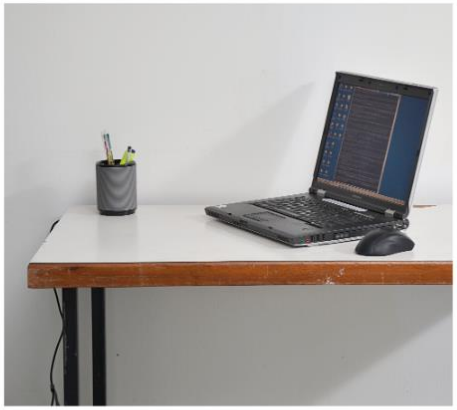
CROCS
Centre for Research on Cryptography and Security

Example: Practical TEMPEST for $3000

- ECDH Key-Extraction via Low-Bandwidth Electromagnetic Attacks on PCs
  - https://eprint.iacr.org/2016/129.pdf
- E-M trace captured (across a wall)



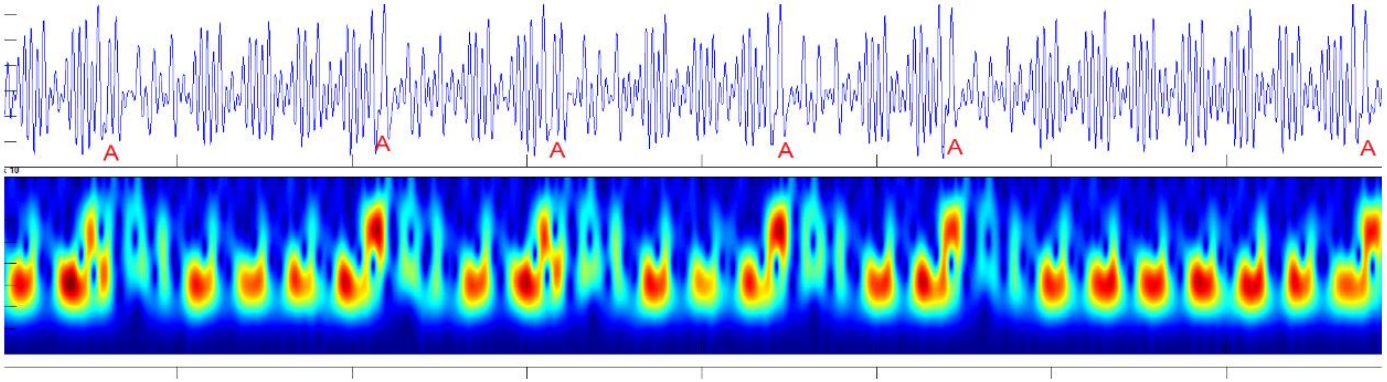
(a) Attacker's setup for capturing EM emanations. Left to right: power supply, antenna on a stand, amplifiers, software defined radio (white box), analysis computer.



(b) Target (Lenovo 3000 N200), performing ECDH decryption operations, on the other side of the wall.

Example: Practical TEMPEST for $3000

- ECDH implemented in latest GnuPG's Libgcrypt
- Single chosen ciphertext – used operands directly visible

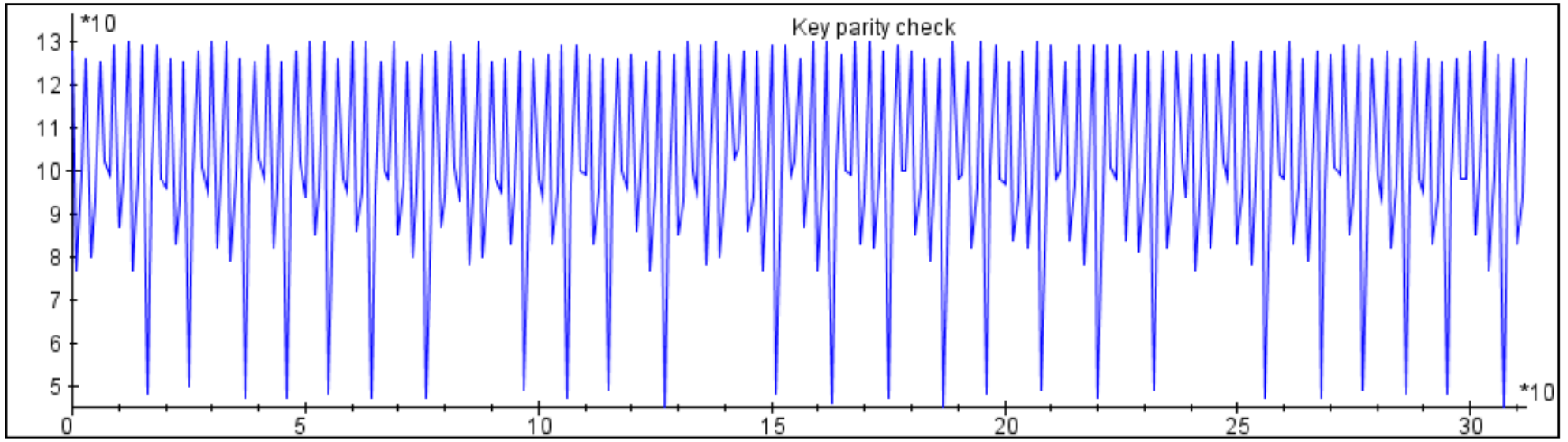


Finishing DES Parity Fail:

What is wrong here?

```
public static boolean checkParity ( byte[]key, int offset) {
     for (int i = 0; i < DES_KEY_LEN; i++) { // for all key bytes
             byte keyByte = key[i + offset];
             int count = 0;
             while (keyByte != 0) { // loop till no '1' bits left
                    if ((keyByte & 0x01) != 0) {
                          count++; // increment for every '1' bit
                    }
                    keyByte >>>= 1; // shift right
             }
             if ((count & 1) == 0) { // not odd
                    return false; // parity not adjusted
             }
     }
     return true; // all bytes were odd
}
```

???


Key parity check
*10
13
12
11
10
9
8
7
6
5
0
5
10
15
20
25
30
*10

???

???

Groups

- Currently 2 groups (3+2)
- Weekly Code Development based on discussions.
  - Uploading code to GitHub. Everyone needs to commit!
  - Languages: Python, Julia, any
- Topics:
  - Alignment
  - Efficient Parallel Acquisition with ChipWhisperer.
- Please enroll in the topics in IS
- I will go through each group topic and discuss what to do.
- Then I will help later on.

Organization

- Group 1:
  - I am added to the repository pb173-side-channel
  - https://github.com/2lol555/pb173-side-channel/tree/main
  - For now, not much, there is a commit by one person
  - Everyone registered for the topic in IS
- Group 2:
  - No repository/invitation?
  - No registration in IS
  - Let’s correct it during today’s seminar.

Group 1: Alignment

- Goals:
  - Peak-Based Alignment
  - Correlation-based Alignment
  - Optional: elastic versions
- Look at:
  - AES_fixed_rand_input_CAFEBABEDEADBEEF0001020304050607+SAVEEVEN(0,1000).trs
  - AES_fixed_rand_input_CAFEBABEDEADBEEF0001020304050607+SAVEEVEN(0,1000)+MIS(100).trs
- First tasks:
  - Try to align the traces mentioned above using peak-based alignment. Note that it might not work for …MIS… traces.
  - See all the uploaded scripts till now
- Later task - Correlation-based Alignment
  - I will explain on the whiteboard. In short – correlation between parts of the traces.

Group 2: Parallel computations with acquisition

- Implement multithreaded Acquisition + Processing
- Measure Efficiency

- First Task: measure the efficiency of the acquisition
- Subsequent tasks: observe the impact of processing and try to add WindowResample in parallel to the acquisition

Affects of misalignment

- Let's look at input correlation for:
  - AES_fixed_rand_input_CAFEBABEDEADBEEF0001020304050607+SAVEEVEN(0,1000).trs
  - AES_fixed_rand_input_CAFEBABEDEADBEEF0001020304050607+SAVEEVEN(0,1000)+MIS(100).trs
  - AES_fixed_rand_input_CAFEBABEDEADBEEF0001020304050607+SAVEEVEN(0,1000)+MIS(1000).trs
- Let's look at correlation scripts.
- correlationIntermediate.py:
  - useIntermediate
  - useHW
- Conclusions?

Parallel: let's go back to the Kyber demo

- Let's finish Points-Of-Interest selection step.

Parallel: let's go back to ChipWhisperer

- Open the progress notebook: Excercise_CPA_DPA_prog3.ipynb
- Let's have a look at CPA and DPA

Let’s discuss your work

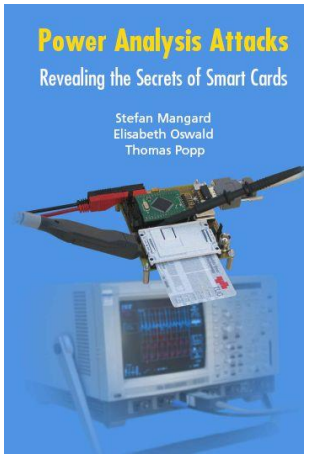
- Work in groups
- Łukasz and Milan will help ☺

Homework

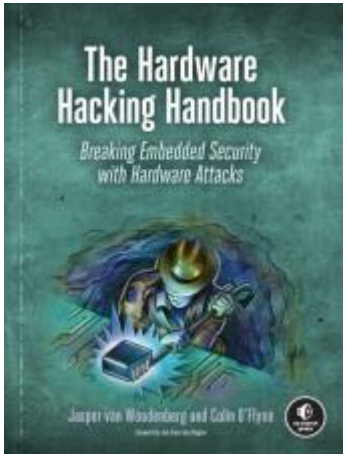
- Try to finalize the first tasks for your project.
- Everyone should commit to the repository.

Reading

- For interested people
- Side-Channel Analysis – blue book:
  - http://dpabook.iaik.tugraz.at/
  - The books is available at the uni.
  - Look online



- The Hardware Hacking Handbook:
  - https://nostarch.com/hardwarehacking
  - I have an epub version.



Questions