PB173 Domain specific development: side-channel analysis

Seminar 7: Progress on First Steps

Łukasz Chmielewski
chmiel@fi.muni.cz,

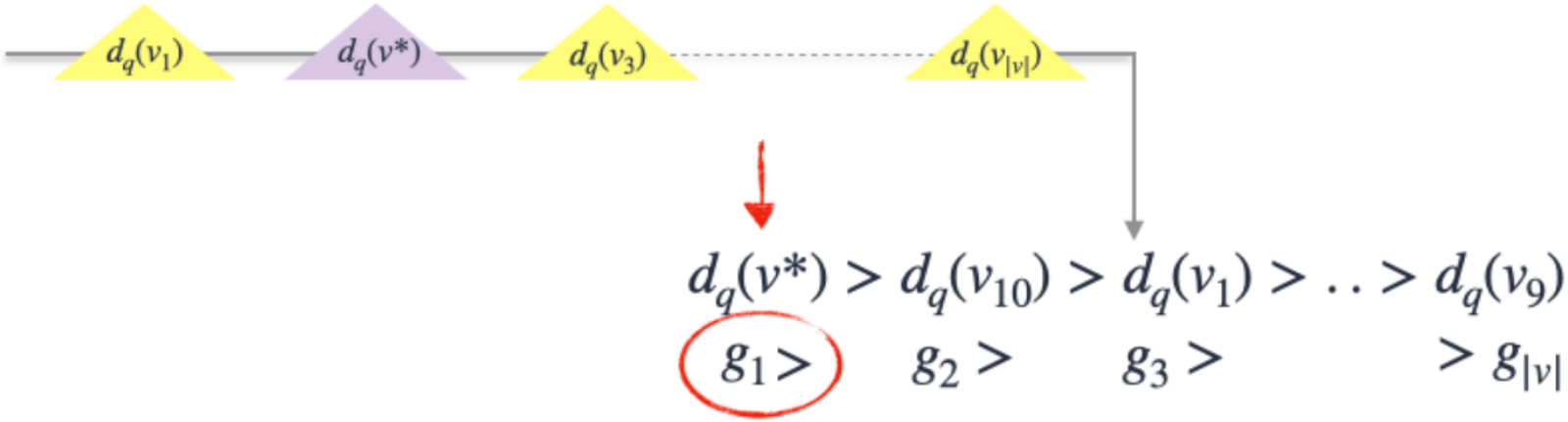
Consultation: A406 Friday 9:00-11:00

CROCS
Centre for Research on Cryptography and Security

USEFUL CONCEPT+ EXAMPLE + EXERCISE

1: Guessing entropy / Key rank

Lets assume we have the results of a key recovery experiment (DPA or CPA) with q queries/traces. We know that the correct value (e.g., a key byte) is v^*:



The result is the guess vector:

Position of the correct key candidate = 1

$$g_q = [g_1, g_2, g_3, \ldots g_{|v|}]$$

1: Guessing entropy in the wild

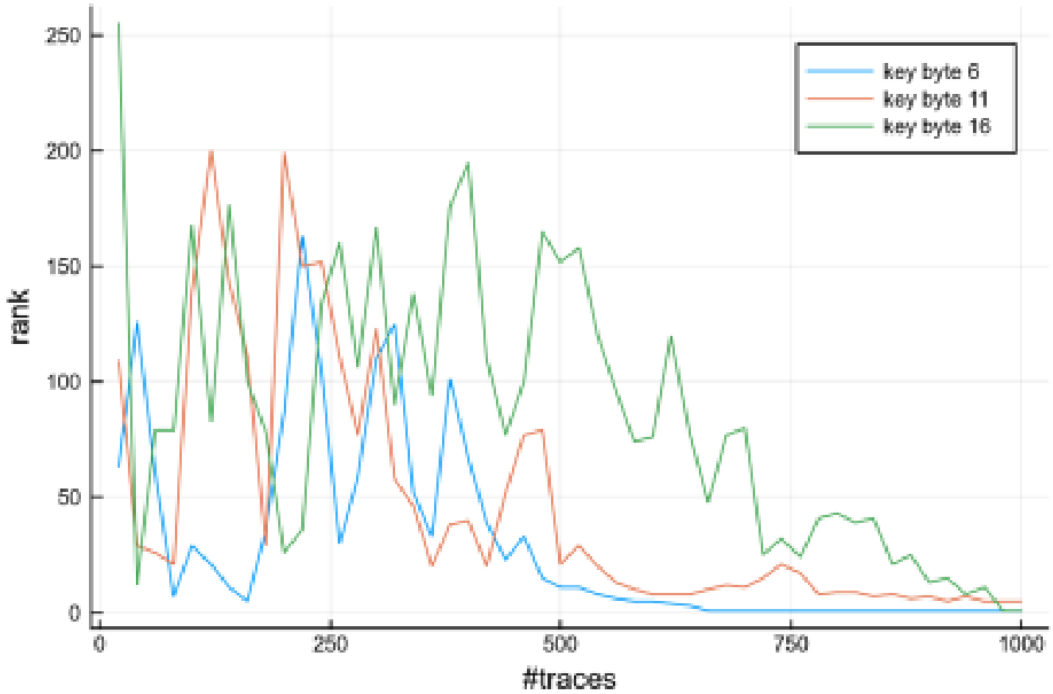


Figure 8: Key rank evolution for hardware AES engine FCA attack.

Source for the figure: Albert Spruyt, Alyssa Milburn, Łukasz Chmielewski, *Fault Injection as an Oscilloscope: Fault Correlation Analysis*, CHES 2020;

2: Reverse engineering of JavaCard bytecode

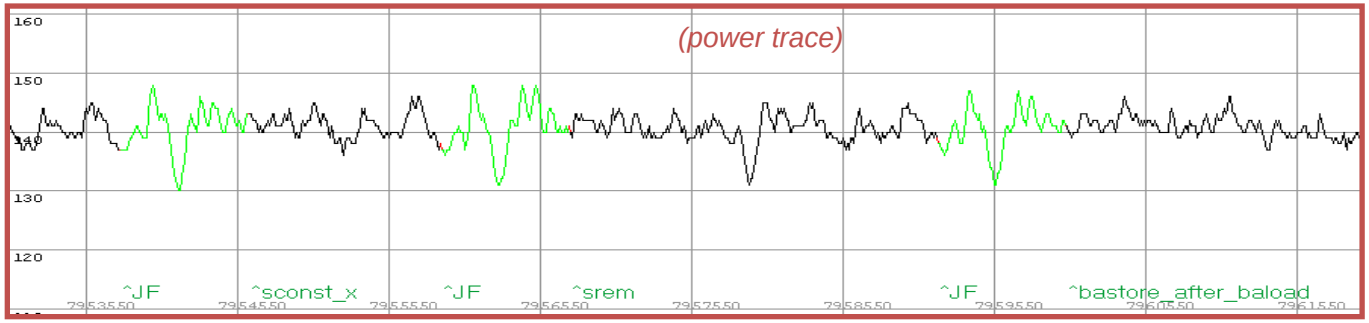
- Goal: obtain code back from smart card
  - JavaCard defines around 140 bytecode instructions
  - JVM fetch instruction and execute it

(source code)
m_ram1[0] = (byte) (m_ram1[0] % 1);

compiler →

(bytecode)
getfield_a_this 0;
sconst_0;
baload;
sconst_1;
srem;
bastore;

oscilloscope →



2: Conditional jumps

- may reveal sensitive info
- keys, internal branches, …

(source code)

```
if (key == 0) m_ram1[0] = 1;
else m_ram1[0] = 0;
```

compiler →

(bytecode)

```
    sload_1;
      ifeq_w L2;
L1: getfield_a_this 0;
      sconst_0;
      sconst_0;
      bastore;
      goto L3;
L2: getfield_a_this 0;
      sconst_0;
      sconst_1;
      bastore;
    goto L3;
L3: …
```

oscilloscope →

Can you use timing attack?

3: PIN Checking simple_pin.c: find two problems

```c
char realPukPin[] = { ... };
short counter;//variable to store the current counter value; it is being read and stored from / to flash

bool checkPin(char[] pin, short offset, short length) {
    if (cardState == BLOCKED)
        return false;

    readCounterFromFlash(&counter);//read counter value from flash
    //realPukPin+PUK_LENGTH points to the PIN
    if ((counter > 0) && (! memcmp(pin+offset, realPin, length)))
    {
        counter = counterLimit;
        writeCounterToFlash(counter);//program counter value to flash
        return true;
    }
    counter--;
    writeCounterToFlash(counter);
    return false;
}

void memcpy(void *dest, void *src, size_t n)
{
    // Typecast src and dest addresses to (char *)
    char *csrc = (char *)src;
    char *cdest = (char *)dest;

    // Copy contents of src[] to dest[]
    for (int i=0; i<n; i++)
        cdest[i] = csrc[i];
}
```

ORGANIZATIONAL

Organization

- Group 1: Alignment
  - https://github.com/2lol555/pb173-side-channel/tree/main
  - Progress: ?
- Group 2: Parallel computations with acquisition
  - https://github.com/makuga01/pb173-sidechannels
  - Progress: ?

Register in IS – thank you!

Side-Channel Topics

details, instructions

Order topics by: names | last modification | **supervisor**
Display topics: **my current ones** | currently available ones | all current ones | which have not been made public | awaiting approval | by selection in Teacher's Notebook | advanced selection

Lukasz Michal Chmielewski, PhD

1. Alignment

Supervisor: Lukasz Michal Chmielewski, PhD, učo 247858

Students (max. 3):

1. Patrícia Gorcová, učo 525287, **FI** B-CS BCS [sem 6, year 3]
2. Jan Janásek, učo 536539, **FI** B-INF IN [sem 4, year 2]
3. Samuel Polakovič, učo 536299, **FI** B-INF IN [sem 4, year 2]

Display operations

2. Parallel computations with acquisition

Supervisor: Lukasz Michal Chmielewski, PhD, učo 247858

Students (max. 3):

1. Marek Geleta, učo 536451, **FI** B-CS BCS [sem 4, year 2]
2. Oliver Šimoník, učo 536671, **FI** B-PVA PVA [sem 4, year 2]

Display operations

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
- Prepared: more traces for you – see IS ☺

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
- Prepared for you: see
  - https://github.com/ikizhvatov/efficient-columnwise-correlation and
  - cpa_aes_evol.py (see IS)

Reminder: Colloquium

- To get the colloquium
  - You must be present at seminars (2 absences OK)
  - You must be active at seminars (+2 points given by me at the end)
  - You must submit and get:
    - 50%: 7 points in total

      (projects + presentation + activity = 14 points)

Remaining Seminars Plan

- 7: evaluation of progress on first steps: 1 point per person per work done till today also based on the commits in GIT
- 8: evaluation of finished first steps : 3 points per group (personalized per person based on the Github) + giving the next tasks
  9: work in progress
- 10: 4 points per group (personalized per person based on the GitHub) + what would say about showing a more official progress presentations?
- 11/12: national holiday / online consultation
- 13: final 2 points for work + 2 points for presentations + 2 points for activity, grading.

WORK

Group 1: Alignment

March 2, 2024 – April 2, 2024

Period: 1 month

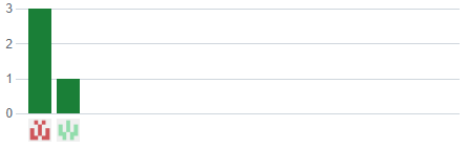
Overview

0 Active pull requests

0 Active issues

0 Merged pull requests	0 Open pull requests	0 Closed issues	0 New issues

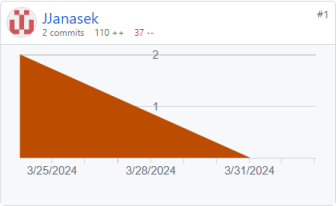
Excluding merges, **2 authors** have pushed **3 commits** to main and **4 commits** to all branches. On main, **0 files** have changed and there have been 0 additions and 0 deletions.



Mar 24, 2024 – Apr 2, 2024

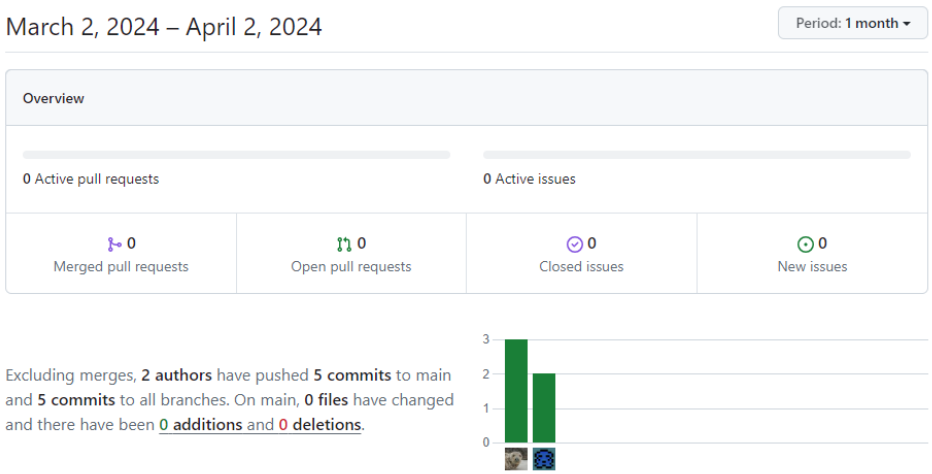
Contributions: Commits

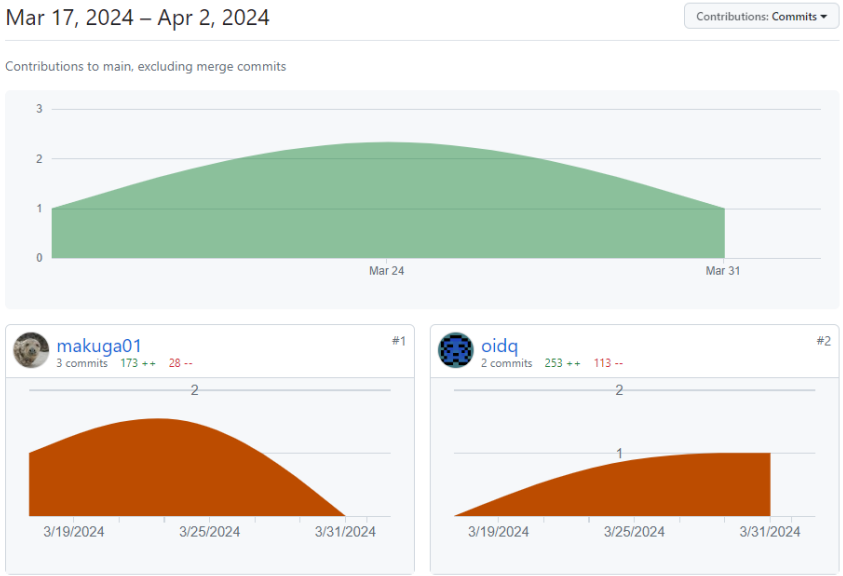
Contributions to main, excluding merge commits



Empty README! Please update so we can test your code.

Group 2: Parallel computations acquisition





Empty README! Please update so we can test your code.

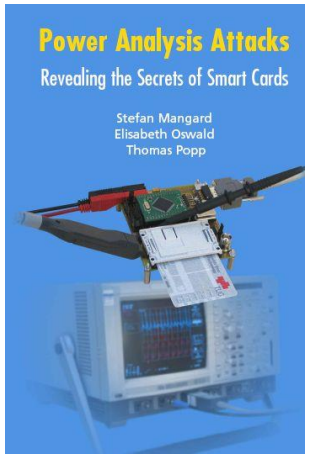
WORK IN GROUPS (60-70 MIN): GRADING (JUST TO TRY, ONLY 1 POINT) DISCUSSING NEXT STEPS AND WHETHER THE FIRST STEPS ARE DONE

Homework

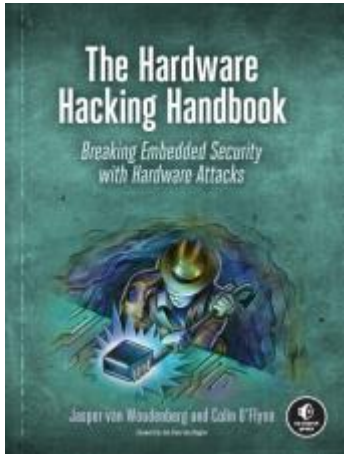
- Finalize the first tasks for your project and start working on new goals.
- Everyone should commit and work on the repository.
- More grading for more points is coming.

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