PB173 Domain specific development: side-channel analysis

Seminar 8: Finalizing on First Steps

Łukasz Chmielewski
chmiel@fi.muni.cz,

Consultation: A406 Friday 9:00-11:00

Centre for Research on Cryptography and Security

Example

USEFUL PLOTS: KEY RANK EVOLUTION

Semi-invasive attacks

- Use cpa_aes_evol.py (from seminar 7) on
- Xoodyak_FVR3000_20240214_124156.npz
- What do you think about the result?

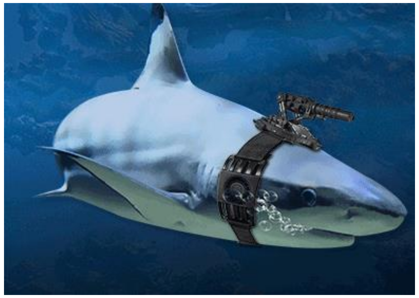
Active Side-Channel

FAULT INJECTION ATTACKS

Passive vs Active Side Channels

Passive: analyze device behavior

Active: change device behavior



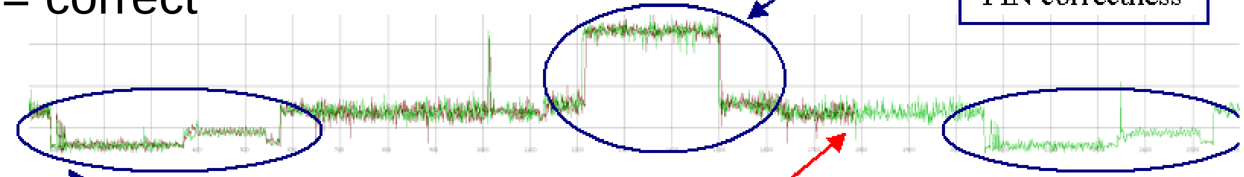
https://escooptics.com/blogs/news/world-space-week-02-lasers

Semi-invasive attacks

- “Physical” manipulation (but card still working)
- Micro probes placed on the bus
  - After removing epoxy layer
- Fault induction
  - liquid nitrogen, power glitches, light flashes…
  - modify memory (RAM, EEPROM), e.g., PIN counter
  - modify instruction, e.g., conditional jump

PIN verification procedure

- [Decrease counter, verify, increase] = correct



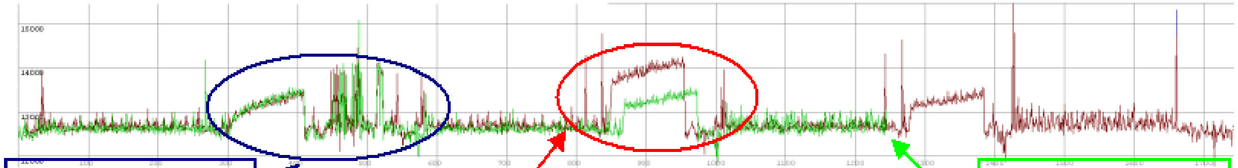
verification of PIN correctness

write to memory (counter decrease)

incorrect PIN trace stops here

write to memory (counter increase)

- [Verify, decrease/increase]

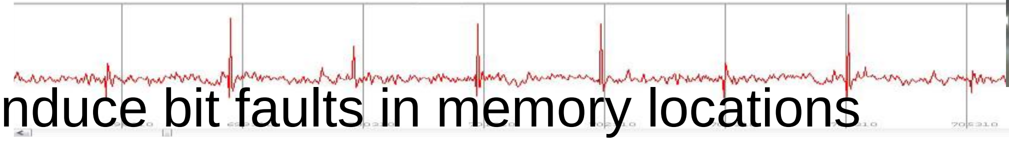


verification of PIN correctness

difference between correct and incorrect trace can be detected and power can be cut off

correct PIN trace stops here

Fault induction



- Attacker can induce bit faults in memory locations
  - power glitch, flash light, radiation...
  - harder to induce targeted then random fault
- Protection with shadow variable
  - every variable has shadow counterpart
  - shadow variable contains inverse value
  - consistency is checked every read/write to memory

01011010

10100101

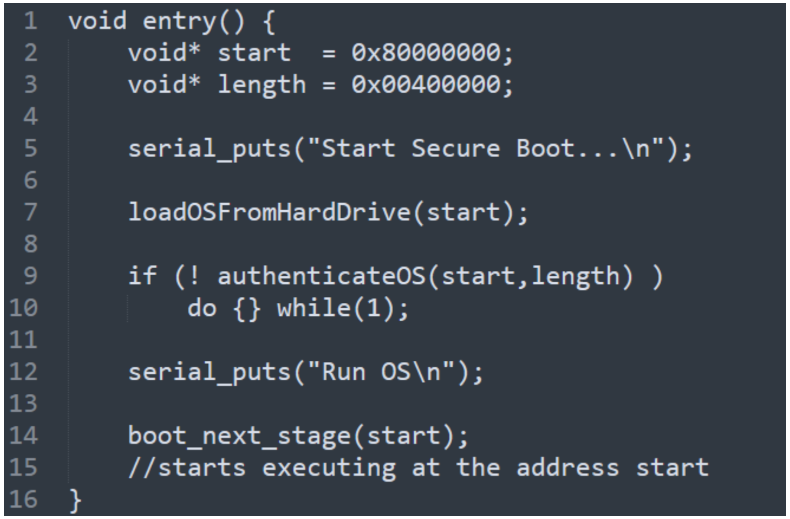
More in **PV286/PA193** or https://riscureprodstorage.blob.core.windows.net/production/2017/08/Riscure_Whitepaper_Side_Channel_Patterns.pdf

a	01011010	*if (a != ~a_inv) Exception();*
		a = 0x55;
		a_inv = ~0x55;
			01010000	*if (a != ~a_inv) Exception();*
				a = 0x13;

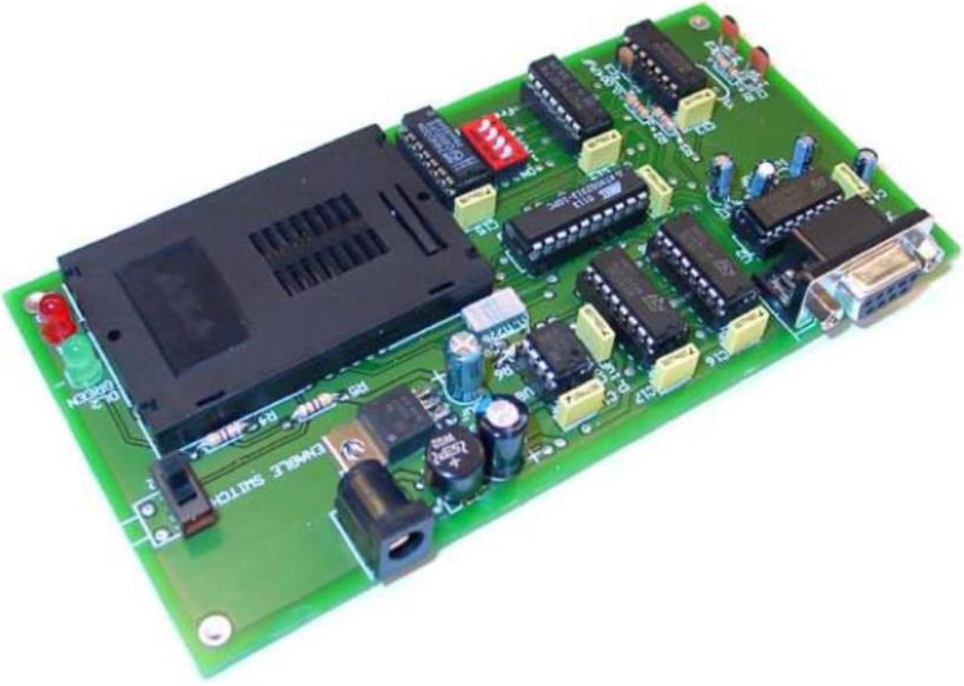
a_inv	10100101		10101010	

- Robust protection, but cumbersome for developer

“Commercial” Example: the “unlooper” device



```
void entry() {
    void* start  = 0x80000000;
    void* length = 0x00400000;

    serial_puts("Start Secure Boot...\n");

    loadOSFromHardDrive(start);

    if (! authenticateOS(start,length) )
        do {} while(1);

    serial_puts("Run OS\n");

    boot_next_stage(start);
    //starts executing at the address start
}
```



Differential Fault Analysis

- Would you like me to present that?
- Or do you prefer to see a real setup? Hard to fit both together.

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: ?

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
- How is it going?

Group 2: Parallel computations with acquisition

- Implement multithreaded Acquisition + Processing
- Measure Efficiency
- First Task: measure the efficiency of the acquisition (done?) Do you have some graphs?

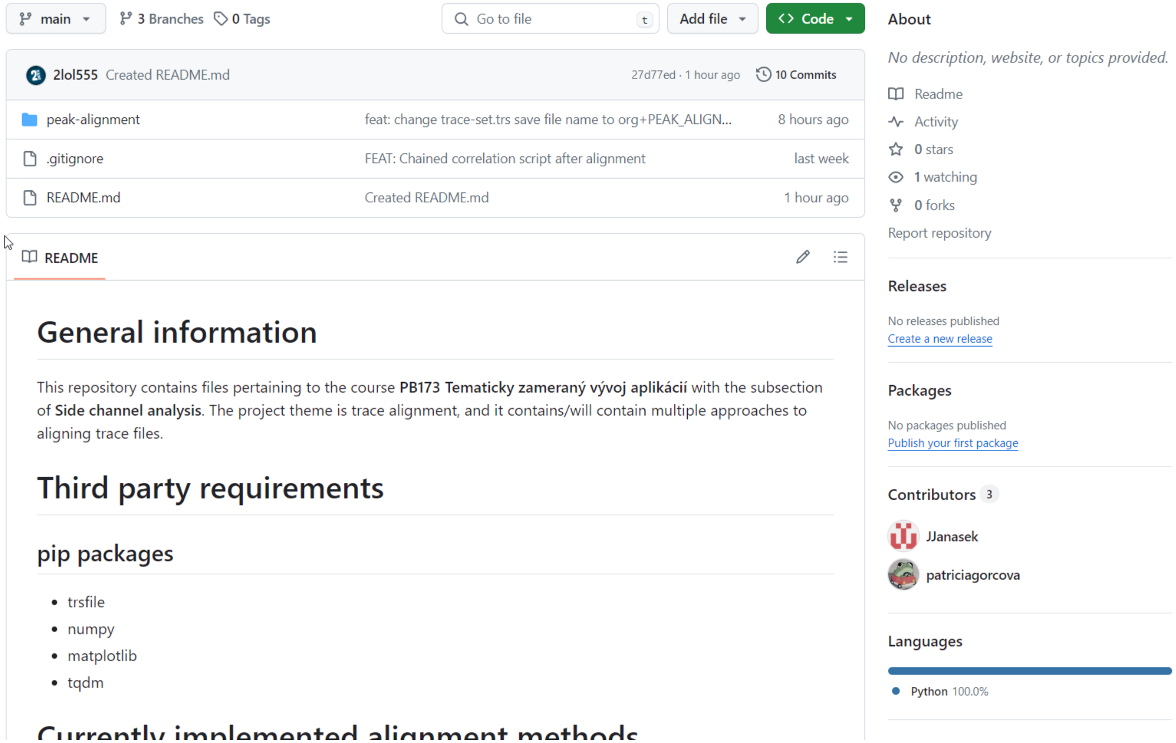
- Later tasks: observe the impact of processing and try to add frequency processing in parallel to the acquisition
- How is it going? Have you used?
  - https://github.com/ikizhvatov/efficient-columnwise-correlation and
  - cpa_aes_evol.py (the corr. traces are also uploaded for Seminar08)

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 **(I will join online for some time)**
- 10: 4 points per group (personalized per person based on the GitHub) + what would say about showing a more official progress presentations? **Decide today.**
  This seminar: real SCA setup
- 11/12: national holiday / online consultation
- 13: final 2 points for work + 2 points for presentations + 2 points for activity, grading.

WHAT WAS DONE + GIVING NEW TASKS

Group 1: Alignment



2lol555 Created README.md 27d77ed · 1 hour ago 10 Commits

peak-alignment	feat: change trace-set.trs save file name to org+PEAK_ALIGN...	8 hours ago
.gitignore	FEAT: Chained correlation script after alignment	last week
README.md	Created README.md	1 hour ago

README

General information

This repository contains files pertaining to the course **PB173 Tematicky zameraný vývoj aplikácií** with the subsection of **Side channel analysis**. The project theme is trace alignment, and it contains/will contain multiple approaches to aligning trace files.

Third party requirements

pip packages

- trsfile
- numpy
- matplotlib
- tqdm

Currently implemented alignment methods

About

No description, website, or topics provided.

Readme
Activity
0 stars
1 watching
0 forks
Report repository

Releases

No releases published
Create a new release

Packages

No packages published
Publish your first package

Contributors 3

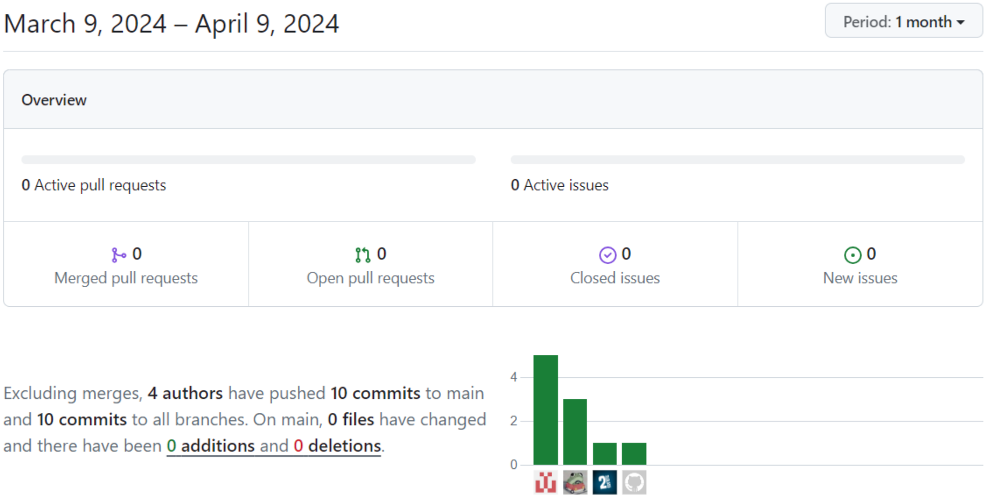
JJanasek
patriciagorcova

Languages

● Python 100.0%

- How reproducible are the installation information?

Group 1: Alignment



March 9, 2024 – April 9, 2024

Period: 1 month ▾

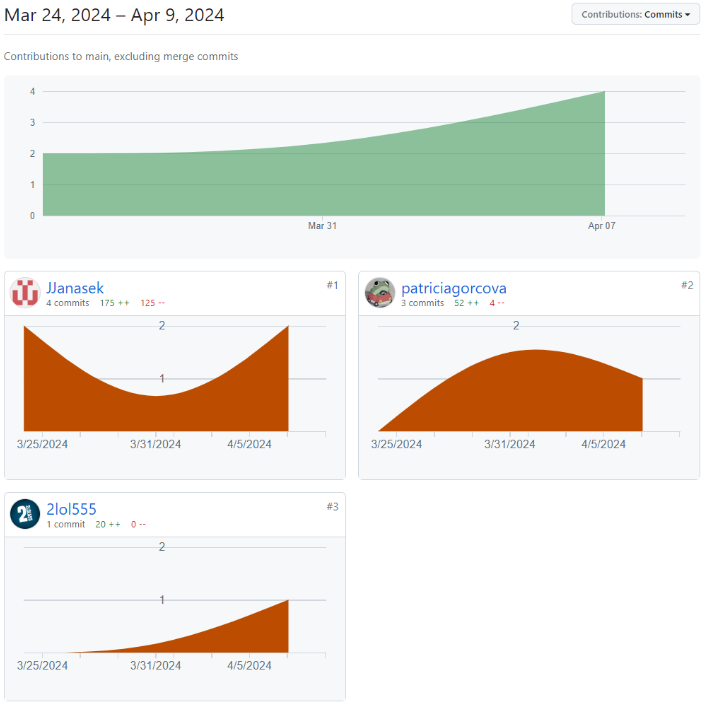
Overview

0 Active pull requests

0 Active issues

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

Excluding merges, **4 authors** have pushed **10 commits** to main and **10 commits** to all branches. On main, **0 files** have changed and there have been **0 additions** and **0 deletions**.



Mar 24, 2024 – Apr 9, 2024

Contributions: Commits ▾

Contributions to main, excluding merge commits

JJanasek #1
4 commits 175 ++ 125 --

patriciagorcova #2
3 commits 52 ++ 4 --

2lol555 #3
1 commit 20 ++ 0 --

Explain who works on branches and 4 contributors ☺

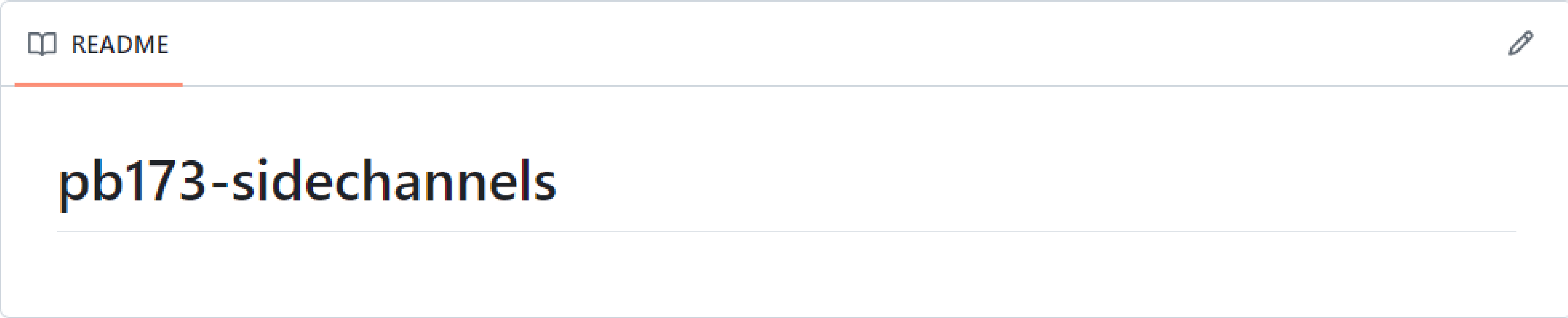
Group 1 New Tasks:

1. Try to misaligned_1000 traces
2. Try alignment on lower peaks (local maximum peaks)
3. Try the Absolute Window Resample + Alignment approach
4. Try pattern matching as explained during the seminar
5. Longer term: Correlation Alignment

- From my side, computing correlation between the traces:

```
from scipy.stats import pearsonr
```

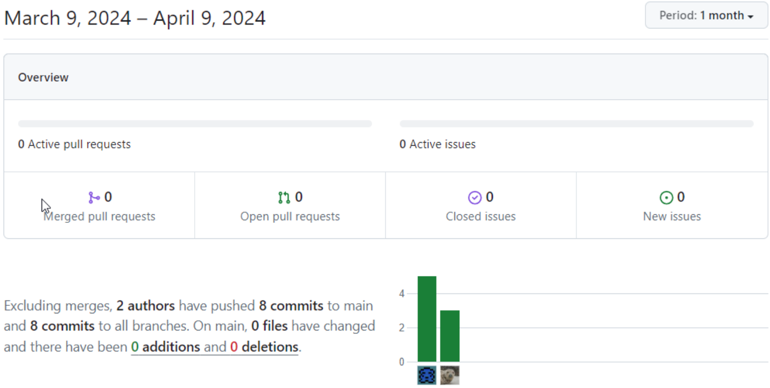
Group 2: Parallel computations with acquisition


README

pb173-sidechannels

☹

Group 2: Parallel computations acquisition



March 9, 2024 – April 9, 2024

Period: **1 month** ▾

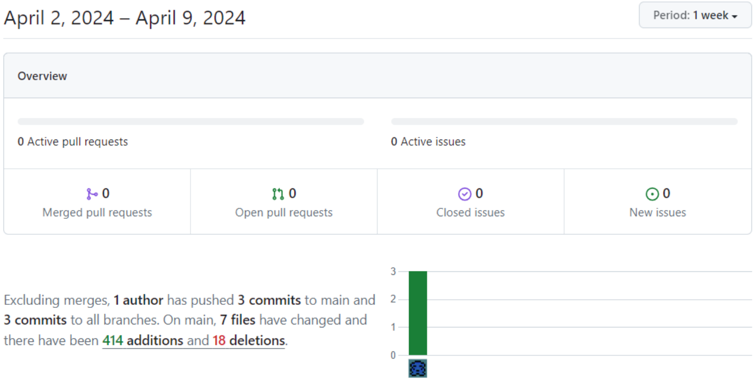
Overview

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 **8 commits** to main and **8 commits** to all branches. On main, **0 files** have changed and there have been 0 additions and 0 deletions.



April 2, 2024 – April 9, 2024

Period: **1 week** ▾

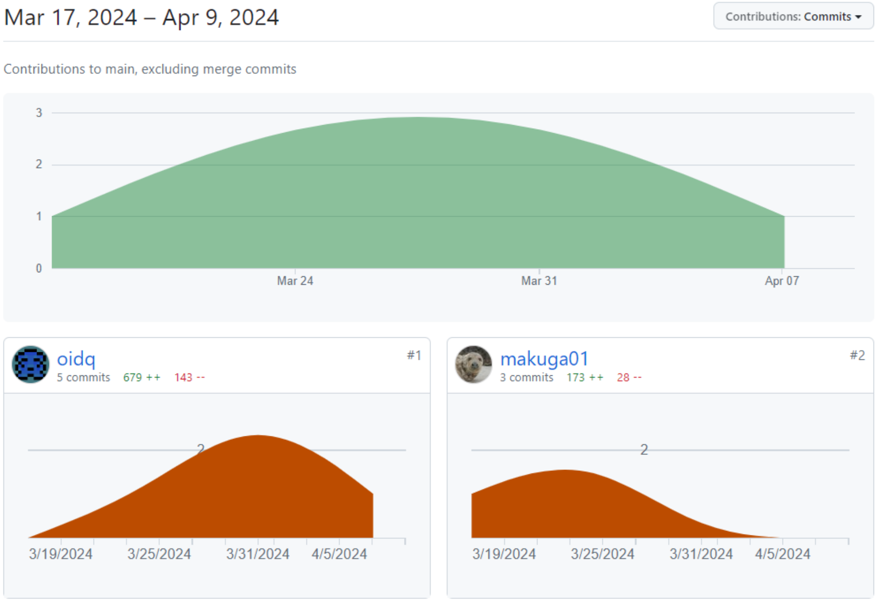
Overview

0 Active pull requests

0 Active issues

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

Excluding merges, **1 author** has pushed **3 commits** to main and **3 commits** to all branches. On main, **7 files** have changed and there have been 414 additions and 18 deletions.



Mar 17, 2024 – Apr 9, 2024

Contributions: **Commits** ▾

Contributions to main, excluding merge commits

oidq #1
5 commits 679 ++ 143 --

makuga01 #2
3 commits 173 ++ 28 --

No input last week from one participant?

Group 2 New Tasks:

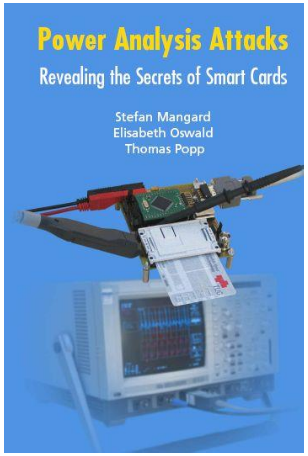
1. Perform analysis with jitter enabled.
2. Try Spectrogram + CPA together
3. Perform evaluation when turning on and off various parallelizations
4. Generate graphs for comparison

- From my side, I will add more ideas for extension for the next seminar. I am considering asking to add an alignment code from Group 1.

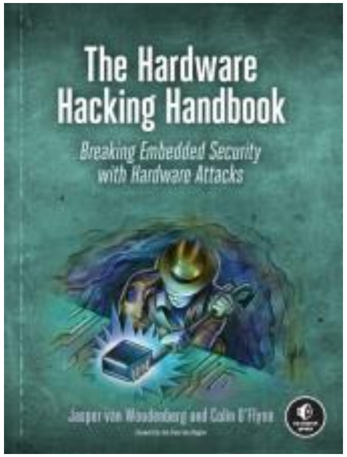
WALK-AROUND + WORKING IN GROUPS

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.


The Hardware Hacking Handbook
Breaking Embedded Security with Hardware Attacks
Jasper van Woudenberg and Colin O'Flynn

Questions