PB173 Domain specific development: side-channel analysis

Seminar 10: Main goals grading

Łukasz Chmielewski
chmiel@fi.muni.cz,

Consultation: A406 Friday 9:00-11:00

CROCS
Centre for Research on Cryptography and Security

Example

EM SIDE-CHANNEL ANALYSIS: SEMINAR 1 REMINDER

Active Side-Channel

DEMO

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?

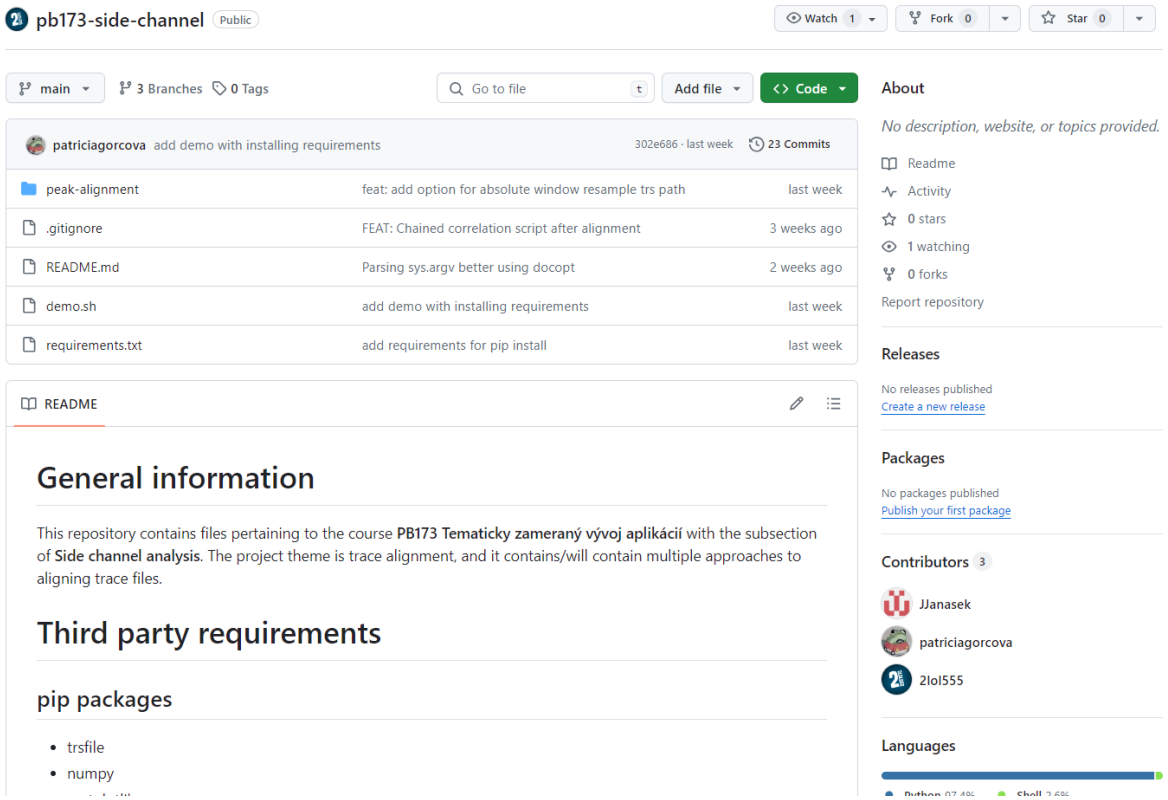
- Later tasks: observe the impact of processing and try to add frequency processing in parallel to the acquisition
- How is it going? Have you used?
  - https://github.com/ikizhvatov/efficient-columnwise-correlation and
  - cpa_aes_evol.py (the corr. traces are also uploaded for Seminar08)

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



pb173-side-channel Public

Watch 1 Fork 0 Star 0

main 3 Branches 0 Tags Go to file t Add file Code

patriciagorcova add demo with installing requirements 302e686 · last week 23 Commits

peak-alignment	feat: add option for absolute window resample trs path	last week
.gitignore	FEAT: Chained correlation script after alignment	3 weeks ago
README.md	Parsing sys.argv better using docopt	2 weeks ago
demo.sh	add demo with installing requirements	last week
requirements.txt	add requirements for pip install	last week

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

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

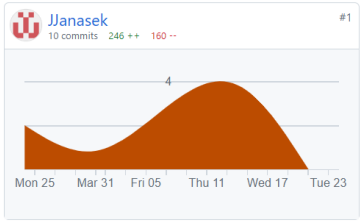
JJanasek
patriciagorcova
2lol555

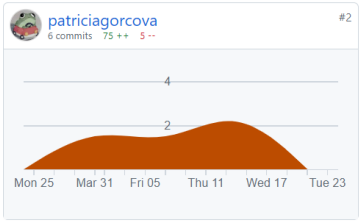
Languages

- Nice!

Group 1: Alignment

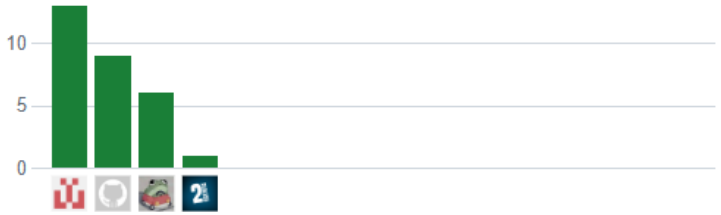
- Main:





- Commits:

Excluding merges, **4 authors** have pushed **23 commits** to main and **29 commits** to all branches. On main, **0 files** have changed and there have been **0 additions** and **0 deletions**.



- Explain work division.

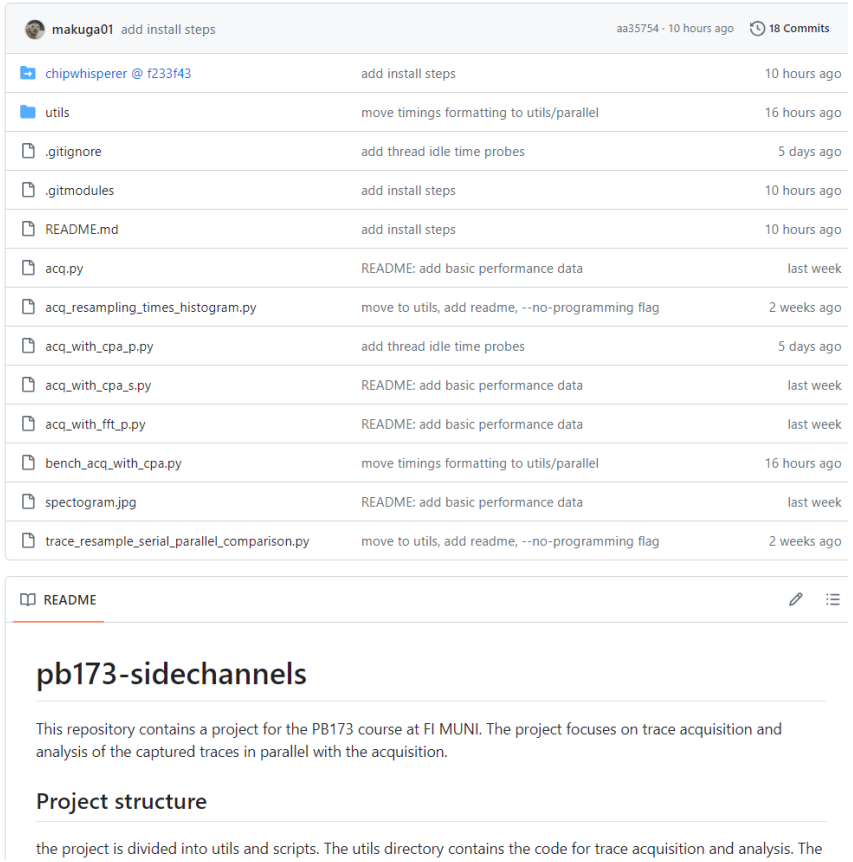
Group 1 Tasks:

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

- Nice!



makuga01 add install steps — aa35754 · 10 hours ago — 18 Commits

chipwhisperer @ f233f43	add install steps	10 hours ago
utils	move timings formatting to utils/parallel	16 hours ago
.gitignore	add thread idle time probes	5 days ago
.gitmodules	add install steps	10 hours ago
README.md	add install steps	10 hours ago
acq.py	README: add basic performance data	last week
acq_resampling_times_histogram.py	move to utils, add readme, --no-programming flag	2 weeks ago
acq_with_cpa_p.py	add thread idle time probes	5 days ago
acq_with_cpa_s.py	README: add basic performance data	last week
acq_with_fft_p.py	README: add basic performance data	last week
bench_acq_with_cpa.py	move timings formatting to utils/parallel	16 hours ago
spectogram.jpg	README: add basic performance data	last week
trace_resample_serial_parallel_comparison.py	move to utils, add readme, --no-programming flag	2 weeks ago

README

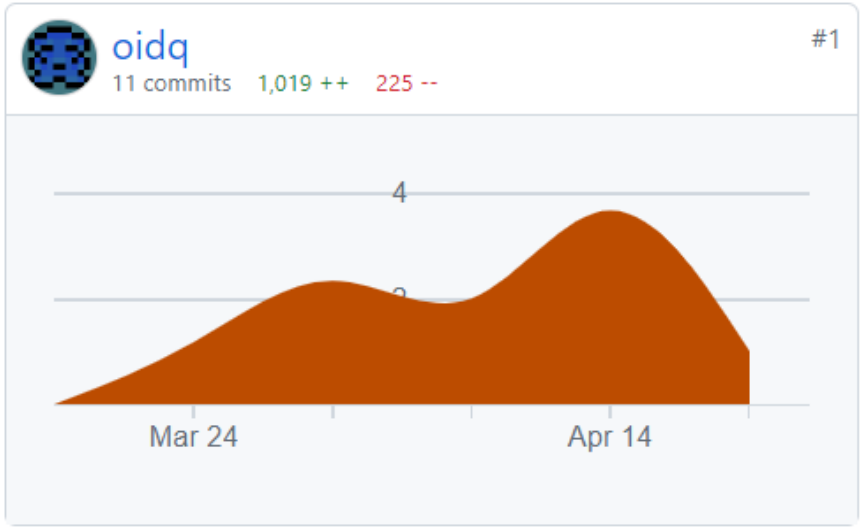
pb173-sidechannels

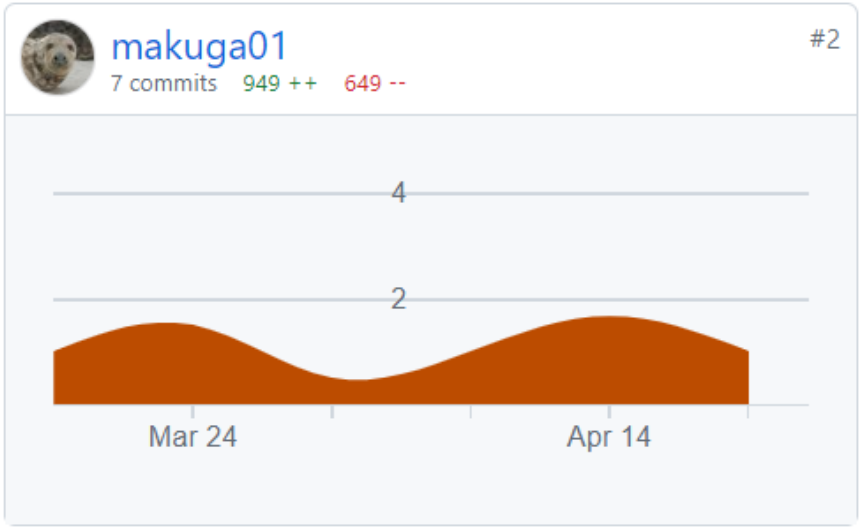
This repository contains a project for the PB173 course at FI MUNI. The project focuses on trace acquisition and analysis of the captured traces in parallel with the acquisition.

Project structure

the project is divided into utils and scripts. The utils directory contains the code for trace acquisition and analysis. The

Group 2: Parallel computations acquisition





It looks evenly distributed, but please describe the division.

Group 2 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 + AGREEING ON FINAL GOALS

Group 1 Final Tasks:

1. Finalize Correlation Alignment on the provided traces.
   - Potentially: investigate optimizations of calculating Normalized Cross Correlation (NCC) between the static reference and target traces. **Lukasz's idea:** find out how it is efficiently done at https://github.com/Riscure/Jlsca. There is an efficient implementation there!
2. Make Peak Correlation + Window Resampling work also for other trace sets:
   - Before 02/05/2024 I will upload two new tracesets to IS.
3. Help Group 2 to incorporate peak alignment into their acquisition pipeline.

Group 2 Final Tasks:

1. Finish comparison of various settings with respect to the number of threads and the amount of traces acquired.
   - Clarify which approach is the best on your system.
   - Possibly use a profiler (e.g., `cProfile`) to identify the most important bottlenecks of your solution.
   - Experiment with various numbers of samples used (or acquired). Does it matter?
2. Add a peak alignment code from Group 1 to your pipeline and perform experiments.
3. **Optional:** add bandpass filtering to your pipeline: https://stackoverflow.com/questions/12093594/how-to-implement-band-pass-butterworth-filter-with-scipy-signal-butter

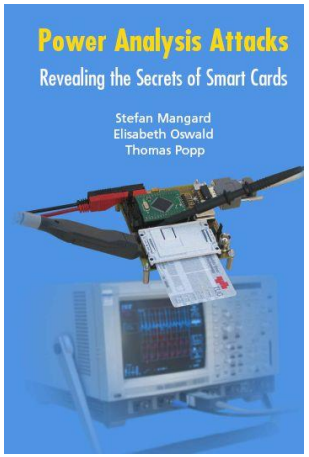
Agree on next two weeks

1. I will prepare a presentation/video about DFA in 2 weeks and publish it online.
2. Online consultation.

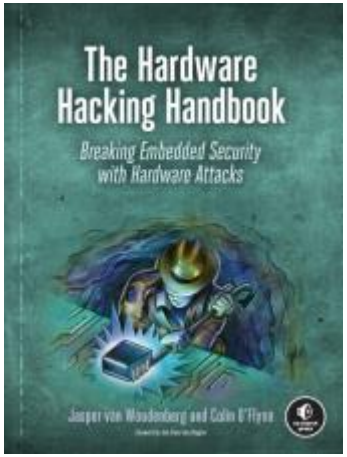
3. Discuss ?

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