PB173 Domain specific development: side-channel analysis

Seminar 9 – Work in progress

Łukasz Chmielewski (chmiel@fi.muni.cz),

Milan Šorf (xsorf@fi.muni.cz)

Consultation: in A406 on Fridays 9:30-11:00
(please email Łukasz before coming)

CRoCS
Centre for Research on
Cryptography and Security

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.

Differential Fault Analysis

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

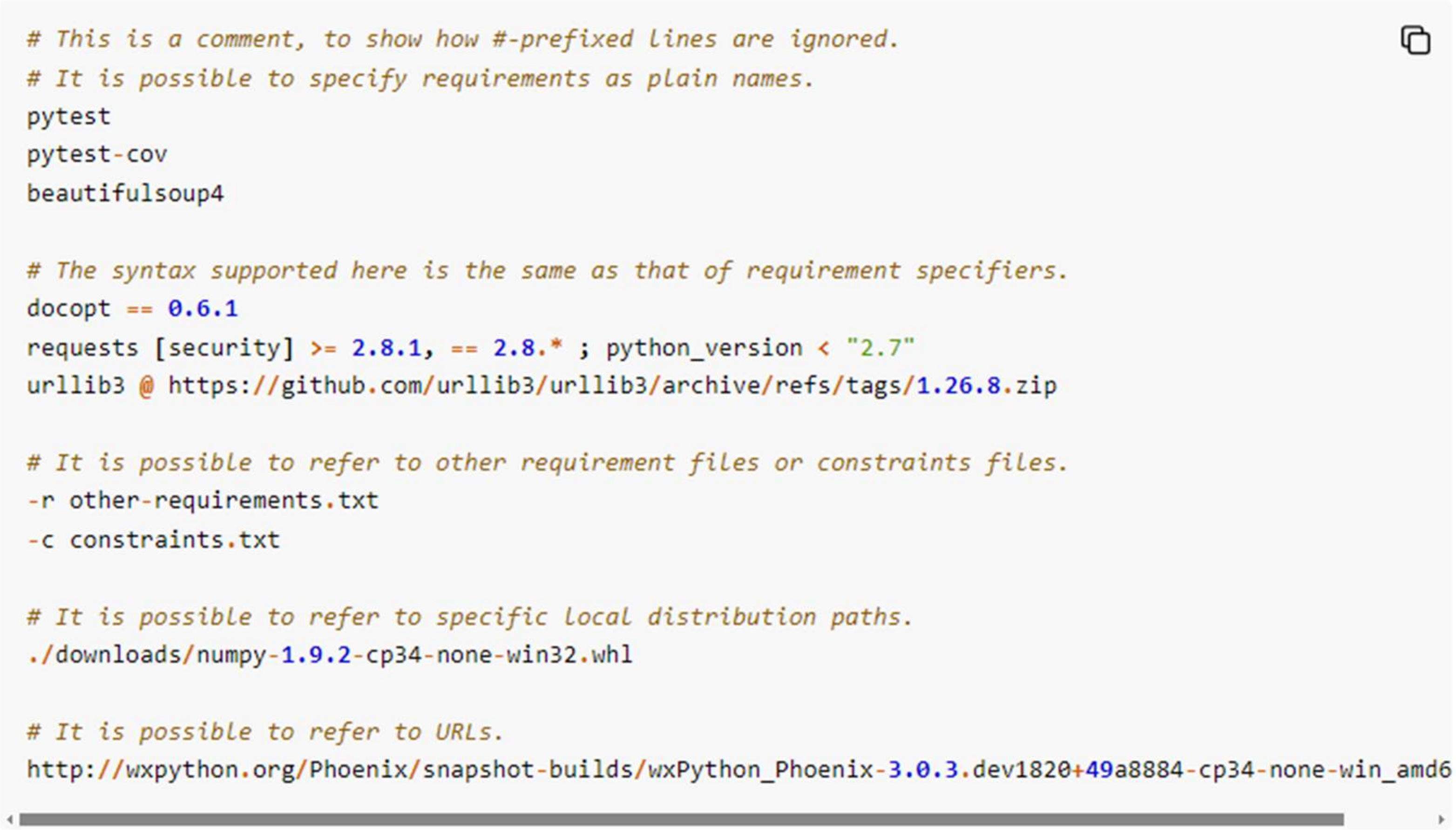
Requirements.txt

Requirements.txt

- Simple way of sharing dependencies
- https://pip.pypa.io/en/stable/reference/requirements-file-format/

Requirements.txt

- Simple way of sharing dependencies
- https://pip.pypa.io/en/stable/reference/requirements-file-format/



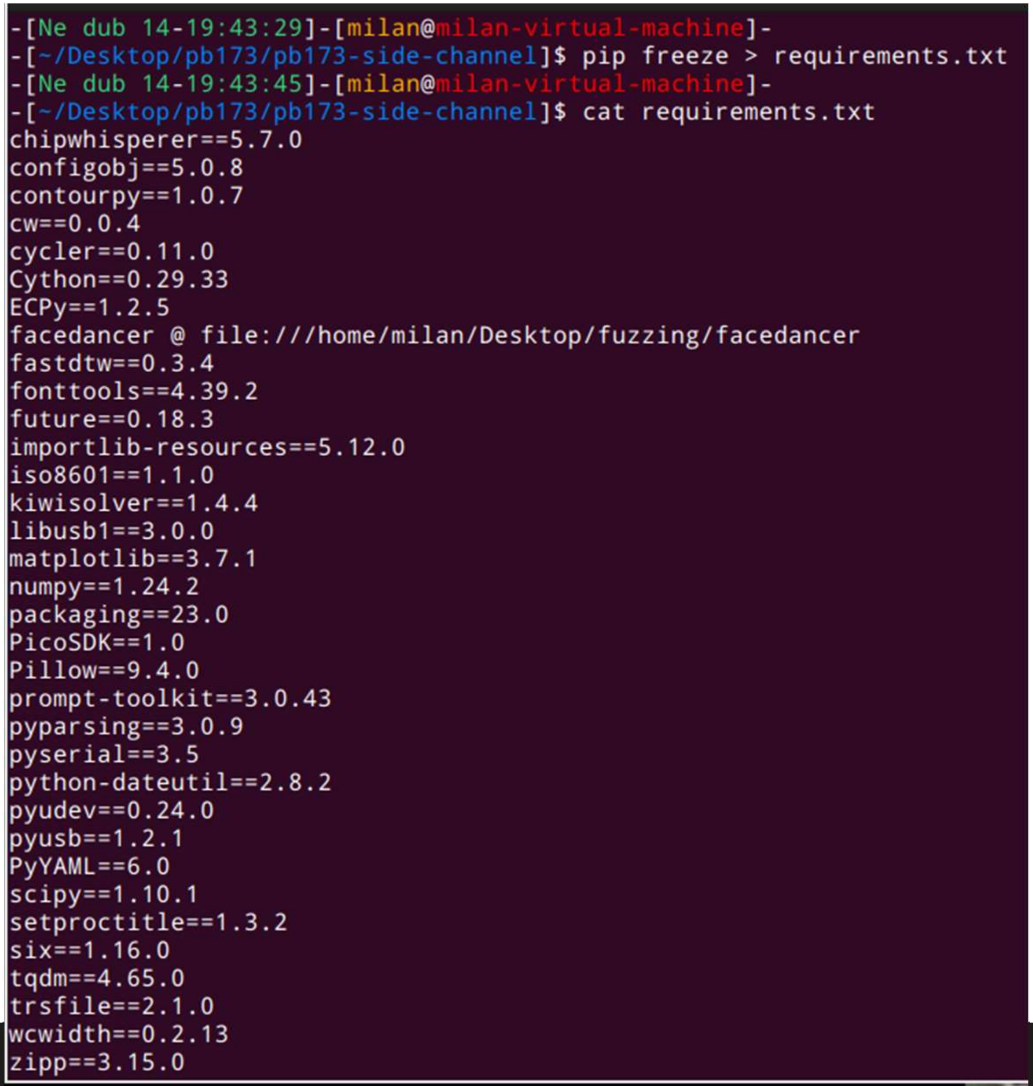
```
# This is a comment, to show how #-prefixed lines are ignored.
# It is possible to specify requirements as plain names.
pytest
pytest-cov
beautifulsoup4

# The syntax supported here is the same as that of requirement specifiers.
docopt == 0.6.1
requests [security] >= 2.8.1, == 2.8.* ; python_version < "2.7"
urllib3 @ https://github.com/urllib3/urllib3/archive/refs/tags/1.26.8.zip

# It is possible to refer to other requirement files or constraints files.
-r other-requirements.txt
-c constraints.txt

# It is possible to refer to specific local distribution paths.
./downloads/numpy-1.9.2-cp34-none-win32.whl

# It is possible to refer to URLs.
http://wxpython.org/Phoenix/snapshot-builds/wxPython_Phoenix-3.0.3.dev1820+49a8884-cp34-none-win_amd6
```

Requirements.txt

- List everything (use in a virtual environment)
  - pip freeze > requirements.txt
  - pip install -r requirements.txt

Requirements.txt

- List everything (use in a virtual environment)
  - pip freeze > requirements.txt
  - pip install -r requirements.txt



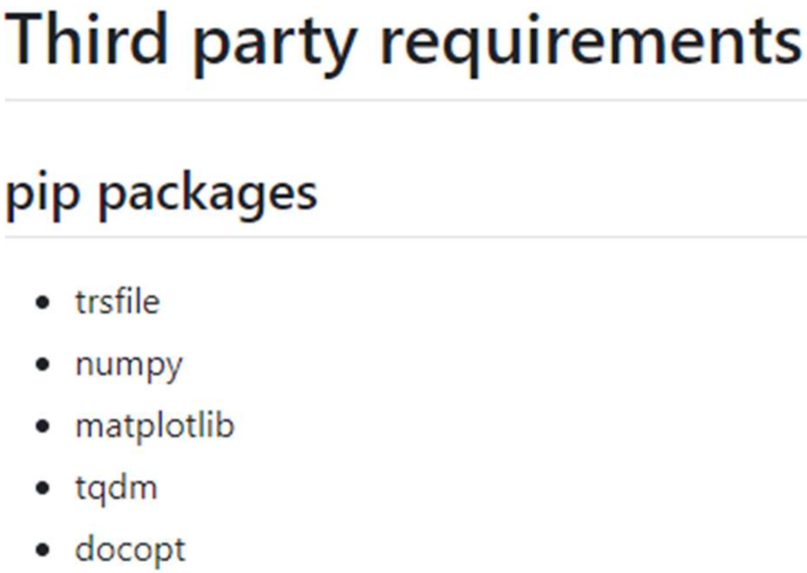
```
-[Ne dub 14-19:43:29]-[milan@milan-virtual-machine]-
-[~/Desktop/pb173/pb173-side-channel]$ pip freeze > requirements.txt
-[Ne dub 14-19:43:45]-[milan@milan-virtual-machine]-
-[~/Desktop/pb173/pb173-side-channel]$ cat requirements.txt
chipwhisperer==5.7.0
configobj==5.0.8
contourpy==1.0.7
cw==0.0.4
cycler==0.11.0
Cython==0.29.33
ECPy==1.2.5
facedancer @ file:///home/milan/Desktop/fuzzing/facedancer
fastdtw==0.3.4
fonttools==4.39.2
future==0.18.3
importlib-resources==5.12.0
iso8601==1.1.0
kiwisolver==1.4.4
libusb1==3.0.0
matplotlib==3.7.1
numpy==1.24.2
packaging==23.0
PicoSDK==1.0
Pillow==9.4.0
prompt-toolkit==3.0.43
pyparsing==3.0.9
pyserial==3.5
python-dateutil==2.8.2
pyudev==0.24.0
pyusb==1.2.1
PyYAML==6.0
scipy==1.10.1
setproctitle==1.3.2
six==1.16.0
tqdm==4.65.0
trsfile==2.1.0
wcwidth==0.2.13
zipp==3.15.0
```

Requirements.txt

- List imports only
  - pip install pipreqs
  - pipreqs project_path

Requirements.txt

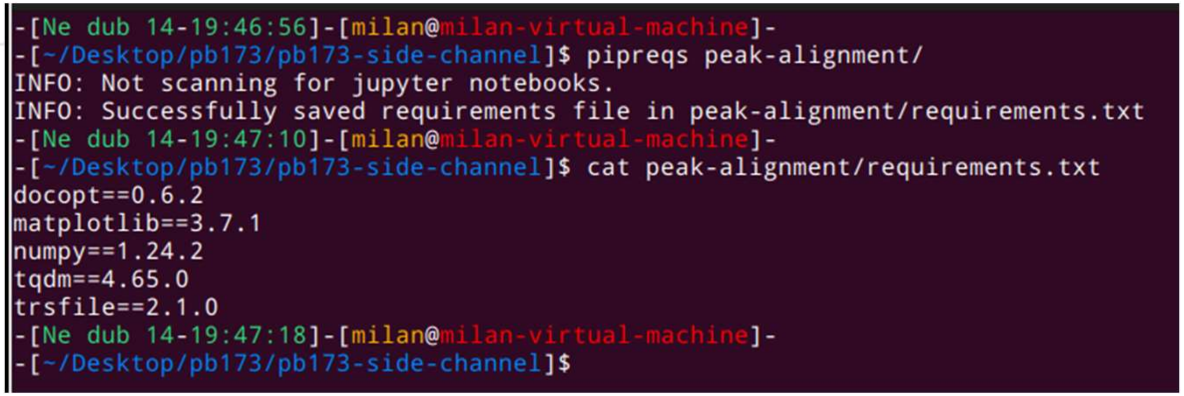
- List imports only
  - pip install pipreqs
  - pipreqs project_path



Third party requirements

pip packages

- trsfile
- numpy
- matplotlib
- tqdm
- docopt



```
-[Ne dub 14-19:46:56]-[milan@milan-virtual-machine]-
-[~/Desktop/pb173/pb173-side-channel]$ pipreqs peak-alignment/
INFO: Not scanning for jupyter notebooks.
INFO: Successfully saved requirements file in peak-alignment/requirements.txt
-[Ne dub 14-19:47:10]-[milan@milan-virtual-machine]-
-[~/Desktop/pb173/pb173-side-channel]$ cat peak-alignment/requirements.txt
docopt==0.6.2
matplotlib==3.7.1
numpy==1.24.2
tqdm==4.65.0
trsfile==2.1.0
-[Ne dub 14-19:47:18]-[milan@milan-virtual-machine]-
-[~/Desktop/pb173/pb173-side-channel]$
```

Unusual side-channels

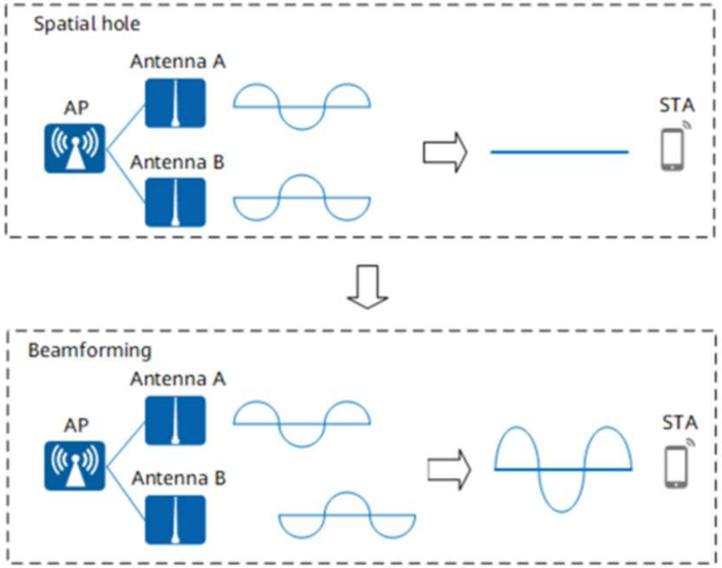
Centre for Research on
Cryptography and Security

Password-Stealing without Hacking: Wi-Fi Enabled Practical Keystroke Eavesdroppiong

- https://arxiv.org/abs/2309.03492
- Detecting keypresses on smartphone from disturbances in BFI caused by shaking the phone

Password-Stealing without Hacking: Wi-Fi Enabled Practical Keystroke Eavesdroppiong

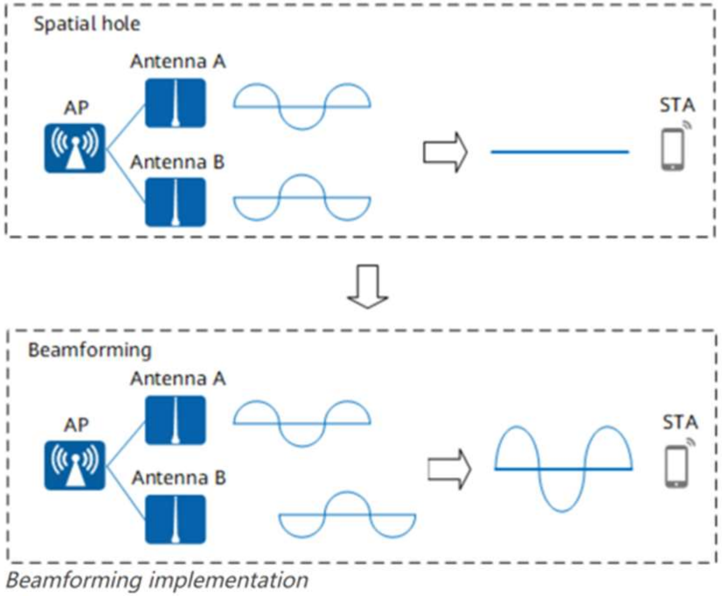
- https://arxiv.org/abs/2309.03492
- Detecting keypresses on smartphone from disturbances in BFI caused by shaking the phone

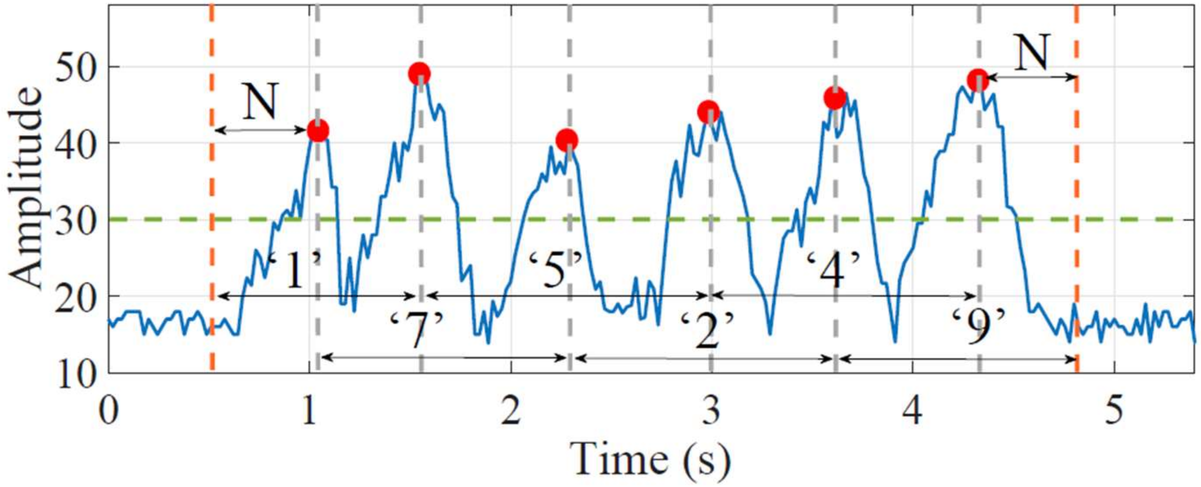


Beamforming implementation

Password-Stealing without Hacking: Wi-Fi Enabled Practical Keystroke Eavesdroppiong

- https://arxiv.org/abs/2309.03492
- Detecting keypresses on smartphone from disturbances in BFI caused by shaking the phone



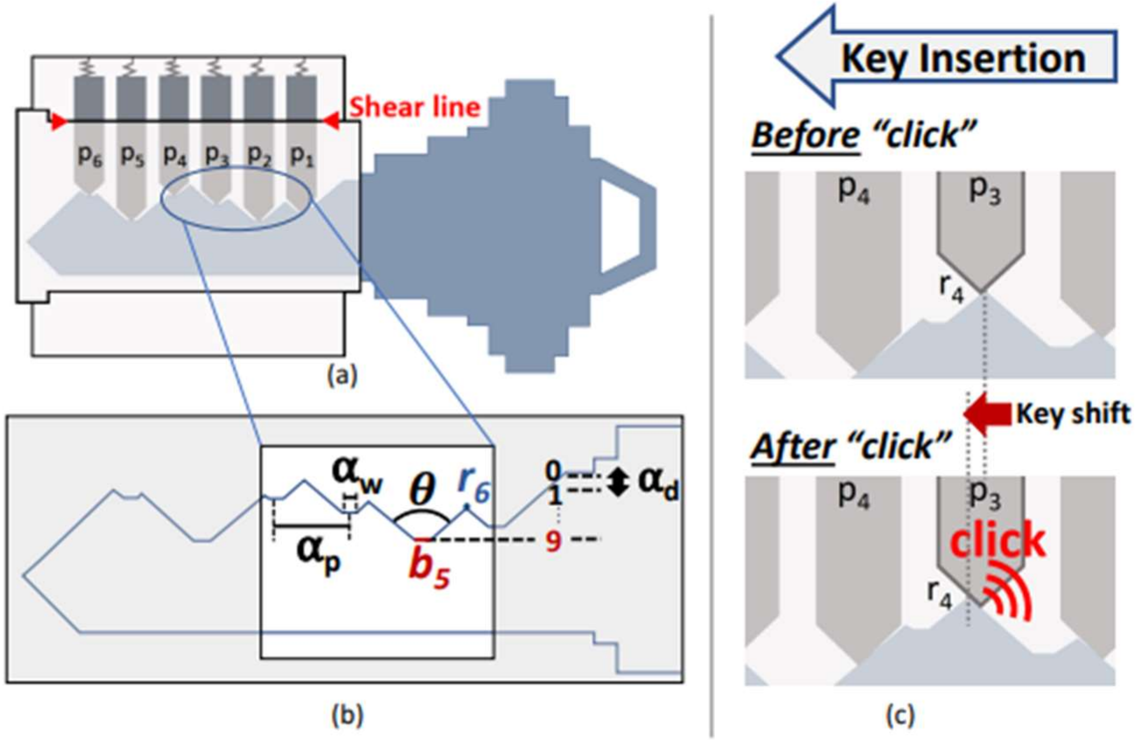


Listen to Your Key: Towards Acoustics-based Physical Key Inference

- https://soundaryaramesh.github.io/papers/spikey_hotmobile.pdf
- 3D printing a key based on audio recording of insertion to a lock

Listen to Your Key: Towards Acoustics-based Physical Key Inference

- https://soundaryaramesh.github.io/papers/spikey_hotmobile.pdf
- 3D printing a key based on audio recording of insertion to a lock



Questions / Team work

CROCS

Centre for Research on
Cryptography and Security