1 ExfilState Sheet

This document lists all setup steps, links, and commands used during the interactive exercises.

2 Setup

- Install Termux via GitHub (**Not from Play Store**): `https://github.com/termux/termux-app/releases/tag/v0.118.3`
- Then in Termux:

  ```
  pkg update && pkg upgrade
  pkg install croc wget
  ```

- You can transfer files from/to device via croc: `croc send <file>`

3 Downloading ExfilState

- Download the prebuilt binaries:
  `https://github.com/cispa/ExfilState/releases/download/ccs-2025/exfilstate`
  `https://github.com/cispa/ExfilState/releases/download/ccs-2025/repro-runner`
- `wget` and `chmod +x`
- `exfilstate`: Fuzzer, discovering timer-less side channels
- `repro-runner`: Reproduce discovered primitives
- Both **static** binaries (no dependencies required)

4 Running ExfilState

- Run as: `./exfilstate`
- Backup Reproducers: `https://github.com/cispa/ExfilState-artifacts/tree/main/framework_evaluation/side_channel_discovery/reproducers`

4.1 Questions

- How many cores are detected?
- Which core types (microarchitectures) are detected?
- How many memory instructions are detected?

5 Inspecting Results

- Reproducers are YAML files generated by the fuzzer
- Run (a few) reproducers with: `./repro-runner <repro-file>`
  - Does it reproduce nicely?
  - How are the evaluation scores?
- Inspect (a few) reproducers:
  - Which core was the reproducer discovered on?
  - Inspect the instruction sequence.
  - How long is it?
  - What do the instructions do? (e.g., search for `<instruction> site:developer.arm.com`)
  - Inspect the architectural states.
  - What is the difference?
  - Do both results comply with the ISA?

6 Other Resources

- ExfilState repository:
  `https://github.com/cispa/ExfilState`
- ExfilState paper:
  `https://fabianthomas.de/thomas_exfilstate.pdf`
- ExfilState artifacts repository:
  `https://github.com/cispa/ExfilState-artifacts`
- Backup Reproducers:
  `https://github.com/cispa/ExfilState-artifacts/tree/main/framework_evaluation/side_channel_discovery/reproducers`

7 (Optional) Building ExfilState

Repository: `https://github.com/cispa/exfilstate`

7.1 Nix

Follow the Readme.

7.2 Docker

Launch the Docker container with the prebuilt cross-compilation environment. Follow the Readme.

```
docker pull fabianthomas/exfilstate-artifact-prebuilt:latest

docker run -dit -v .:/mnt --name exfilstate-artifact-prebuilt \
  fabianthomas/exfilstate-artifact-prebuilt

docker exec -it exfilstate-artifact-prebuilt bash
```