REPRODUCING SPECTRE ATTACK WITH GEM5

PIERRE AYOUB - EURECOM

PIERRE.AYOUB@EURECOM.FR

CLÉMENTINE MAURICE - UNIV LILLE, CNRS, INRIA

CLEMENTINE.MAURICE@INRIA.FR

ICHSA'21

01 JUNE, 2021

PROCESSOR'S MICROARCHITECTURE IS A BLACK BOX

Consequence: Micro-architectural security is **hard**

Transient Instruction

⇒ Affects the processor **micro-architectural state** – leaving its architectural state as prior the execution

Spectre

⇒ Execute malicious transient instructions exploiting the **branch predictor**

SIMULATION CAN BREAK THIS BLACK BOX

How: Allowing the user to view the micro-architecture's behavior

GEM5

Cycle-accurate simulator

⇒ Simulate very precisely **hardware** entirely **in software**

Build a system

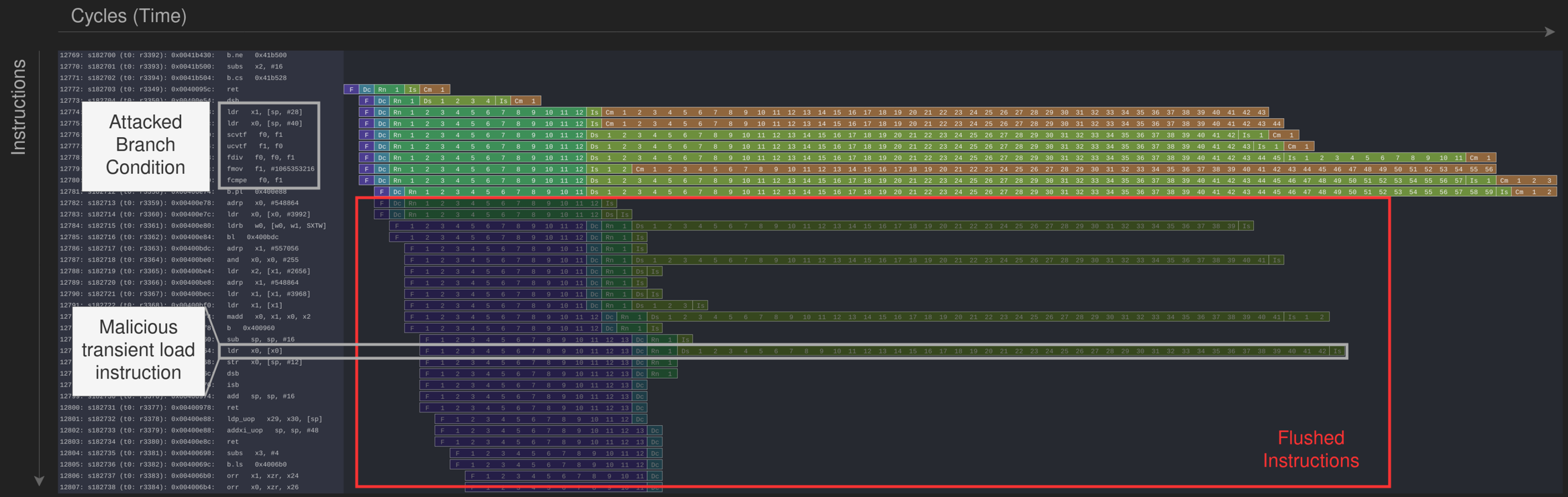
⇒ Instantiate and parameterize **Python objects**

Run a system

⇒ Launch the Python script, then **view and inspect** the running system!

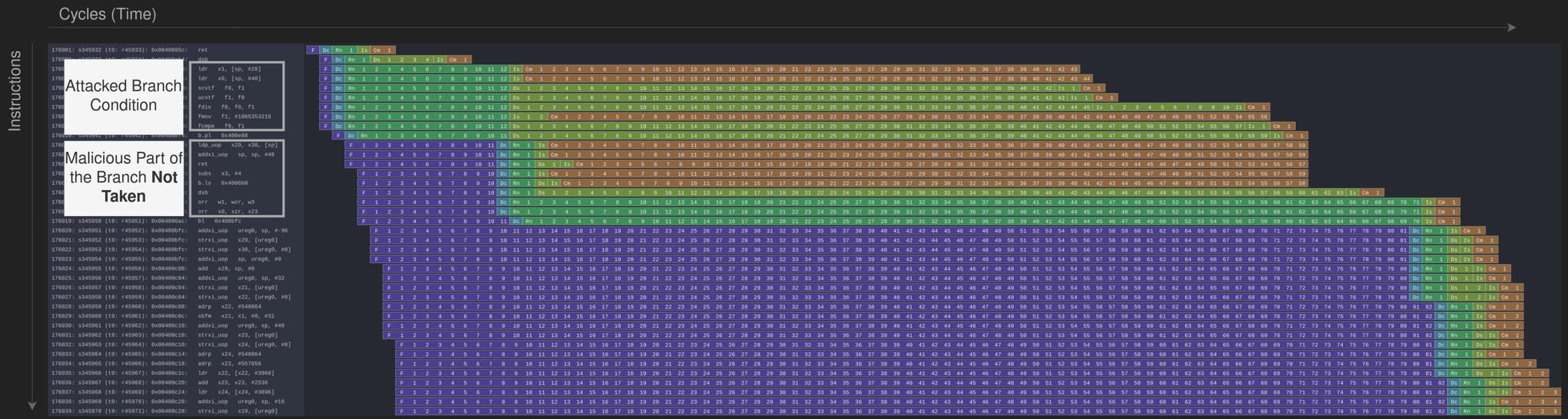
OBSERVING SPECTRE WITH KONATA

SUCCESS SCENARIO



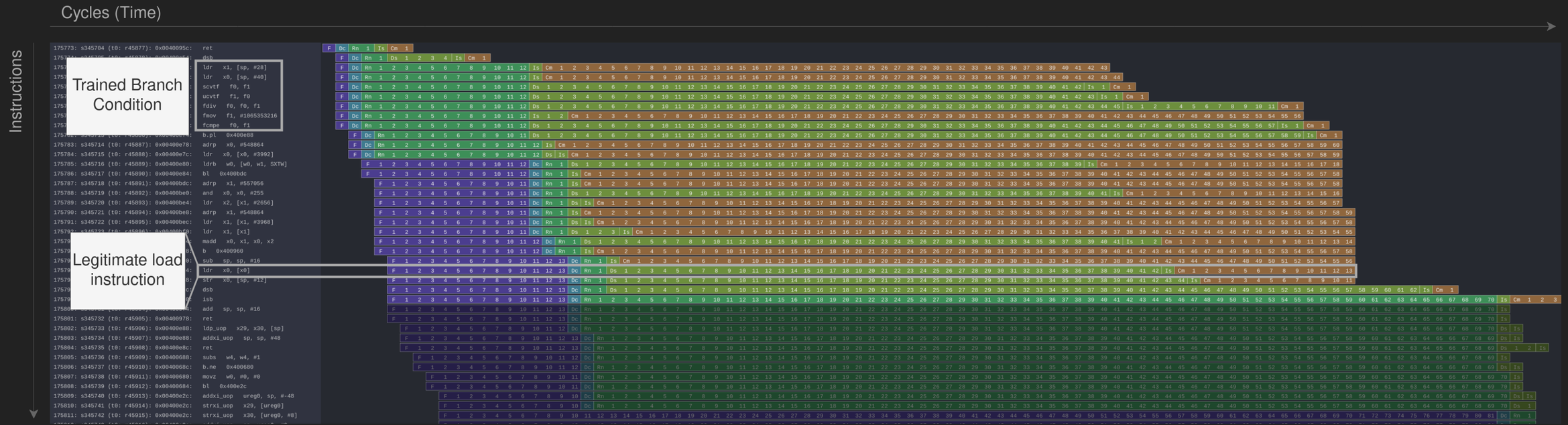
Allows to understand how the attack works

DEFEATED BY THE BRANCH PREDICTOR



Allows to visualize the root cause of a failed attack!

TRAINING SCENARIO



We can even identify more scenarios…

FAITHFULNESS OF THE SIMULATION

Comparing a real system and a simulation

⇒ Very **similar result** of number of **mispredicted branches**

⇒ **Helped** to **implement** the attack on a **real system**

Limitations

⇒ **Slow** simulation, possibly **inaccurate** models

CONCLUSION

PAPER

Reproducing Spectre Attack with gem5

How To Do It Right?

Pierre Ayoub
pierre.ayoub@eurecom.fr
EURECOM
Sophia Antipolis, France

Clémentine Maurice
clementine.maurice@inria.fr
Univ Lille, CNRS, Inria
Lille, France

Pierre Ayoub and Clémentine Maurice. *Reproducing Spectre Attack with gem5: How To Do It Right?* (**EuroSec '21**), April 26, 2021

- **GitHub**: https://pierreay.github.io/reproduce-spectre-gem5/
- **Contact**: pierre.ayoub@eurecom.fr