Assignment II
Due Date: October 12

1 Objective

To understand and reproduce various microarchitectural attacks including cache attacks, Spectre V1, and another attack of your choice. Additionally, to implement hardware defenses against these attacks.

2 Requirements

- Individual Work: This assignment must be completed individually.
- Submission: Submit a zip file containing your source code, assembly, and a minimum seven-page PDF report to Moodle.
- Deadline: October 12, 11:59 pm.
- Debugging: Note that open-source implementations may have bugs. It's your responsibility to debug if you choose to reuse them.

3 Exercises

3.1 Cache Attack (10 points)

- Reproduce one cache attack on a real machine.
- Include a demo showing successful leakage.
- Explain the functionality of the main region of the attack code line by line in assembly.

3.2 Spectre V1 Attack (20 points)

- Reproduce the Spectre V1 attack on a real machine.
- Include a demo showing successful leakage.
- Explain the functionality of the main region of the attack code line by line in assembly.

3.3 Another Microarchitectural Attack (30 points)

- Choose another microarchitectural attack like LVI or Augury.
- Reproduce the attack on a real machine.
- Include a demo showing successful leakage.
- Explain the functionality of the main region of the attack code line by line in assembly.

3.4 Hardware Defense Implementation (40 points)

- Implement a hardware defense against Spectre, such as InvisiSpec, on a cycle-accurate simulator like Gem5.
- Include a link to a demo (video clip) showing the defense prevents the leakage in your simulator.
- Deliver a minimum three-page report explaining your observations of the leakage and defense functionality, as well as the main implementation section code of the defense in the simulator of your chose.

4 Resources

- PoC Code Collection: Google Drive Link
- InvisiSpec Source Code: GitHub Link
- Gem5 Official Website: Gem5
- Gem5 Tutorial: Learning Gem5
- Visualizing Spectre on Gem5: Visualizing Spectre with Gem5

5 Submission Instructions

1. Include your source code, assembly files, and PDF report in the zip file.
2. Submit to Moodle by October 12. Late submissions will be penalized.

6 Notes

6.1 Fixing Python and GCC Issues for InvisiSpec in Gem5

To fix the Python and GCC issues when building the Gem5 version of InvisiSpec, run the following commands. This assumes that you have Python 2.7 and Python 2-dev installed, as required for Gem5 setup.

```
// This should install gcc7.5
$ sudo apt install gcc-7 g++-7
$ export CC=gcc-7
$ export CXX=g++-7
$ python2.7 $(which scons) build/X86/gem5.opt -j9 --default=X86 PROTOCOL=MESI_Two_Level
```