CS 5153/6053 Network Security, Spring 2023
Project 5: Meltdown Attack

Instructor: Dr. Boyang Wang

Due Date: 4/14/2023 (Friday), 11:59pm.
Format: Please submit a zip file of your code in Canvas.
Total Points: 10 points
Note: This is an individual project. The instructor would like to thank Dr. Wenliang Du from Syracuse University for making the project materials of SEED Labs public and free for students to use.

1 Project Description

In this project, you will need to demonstrate a proof-of-concept Meltdown attack by using the project materials offered by SEED Labs [4]. The description of the Meltdown Attack project offered by SEED Labs can be found at [2]. A copy of the description can also be found in Canvas.

There are several tasks described in the description from SEED Labs. **You need to complete Task 1, Task 2, Task 3, Task 4, Task 5, and Task 6** by following the example we discussed in class. The details of each task are the same as the description from SEED Labs.

- **(Additional Task for CS 6053)**: please complete **Task 7.1** and **Task 7.3** as well.

As before, you do not need to write the code from scratch. The code you need has been discussed during the class and can be found in our slides. You can also download the code directly from `Meltdown_attack.zip` listed on this webpage [2]. Additional information about this project can be found at [2].

To complete the project, you will need to create one VM with with Linux (Ubuntu 16.04-32bit). You can use one of the VMs you have created in previous projects. You can find the instruction regarding how to install VMs and download a copy of the Linux at this webpage [1]. Please read this document [3] from Seed Labs regarding how to install and setup VMs.

Note 1: If your computer **does not have** an Intel CPU, you may not be able to demonstrate the results of the tasks that are related to out-of-order execution. If that is the case, please still complete all these tasks, include your observations, and indicate that your computer does not have an Intel CPU in your report. Failing to show the results that are related to out-of-order execution **will not affect your grade** in this case.

Note 2: The side-channel information from cache is noisy in practice. If you could not obtain correct results in some of these tasks, that is fine. It **will not affect your grade**.

2 Basic Requirements

Program Directory: Please name your project folder in the form of `meltdown_m123456`, where `meltdown` is the name of this project and `m123456` is your UCID. The recommended directories of your program should be organized as follows:

```
./meltdown_m123456/src
./meltdown_m123456/report.pdf
```

Folder `src` should include all the source files that you have completed. In `report.pdf` file, you should describe

- How do you compile the code in each task;
- Please provide a screenshot of the result of each task similar as the ones we have in our lectures.

References

1. Lab enviroment setup, `https://seedsecuritylabs.org/lab_env.html`
2. Meltdown attack lab, `https://seedsecuritylabs.org/Labs_16.04/System/Meltdown_Attack/`
3. Run seed vm on virtualbox, `https://seedsecuritylabs.org/Labs_16.04/Documents/SEEDVM_VirtualBoxManual.pdf`
4. Seed labs (hands-on labs for security education), `https://seedsecuritylabs.org/`