University of Southern California

Department of Electrical Engineering

EE653 Fall 2024

Instructor: Murali Annavaram

Project #3 Cache Side Channel Attacks, Due Nov 27th, 2024

We use the Cache Side Channel Attacks Lab (Prof. Mengjia Yan)

from MIT course Secure Hardware Design.

Overview:

In this project, you are writing an attack program that uses cache side channels to obtain the information you should not get.

Use the same machine as the last project:

You must be connected to USC VPN or connected to USC secure wireless.

$ ssh teamX@education1-scip.usc.edu
, where X is your team number.

Password: **!makababka@359**

passwd
Change your password

Setting up the environment:

$ python3 -m venv ~/myPython
$ source ~/myPython/bin/activate
$ python3 -m pip install matplotlib tqdm
, where X is your team member.

Procedure every time you login:

$ source ~/myPython/bin/activate

Getting the source code:

Download your starter code here.

Assigned cores;

In this lab, you will be assigned 2 cores in the sgx machine. One acting as a sender and another acting as a receiver. Your 2 core numbers are calculated as follows:

[2*(x-1)]%8 and [2*(x-1)+1]%8, where x is your team number. For example if your team number is 3, your core numbers will be 4 and 5. You need to edit cpu.mk accordingly.

Detailed instruction:

For detailed instruction please refer to the original MIT course website in this link.

Your Responsibility

You are responsible for finishing part 1 Gathering information, and part 2 (Capture the Flag with Flush+Reload)
Part 3 (prime and probe) will be extra credit. The code for prime and prob is not difficult to write. However, due to noise in the system, prime and probe attacks's result can be very inconsistent leading to prolonged development time. Thus, we make it extra credit.

Submission:

Instead of submitting to GitHub as stated on their website, submit the required materials to BrightSpace.