ADVANCED COMPUTER ARCHITECTURE - HOMEWORK III

Student: Francisco Javier Blázquez Martínez
E-mail: francisco.blazquezmartinez@epfl.ch
Sciper: 331229

Spectre attack.

1.- Training Local and Global Branch Predictors

Following the directions of the homework statement, the branch predictors are trained by both adding long nested deterministic loops (global case) and after these, several invocations to the victim function with a valid value.

2.- Side channel extension

Since it's not allowed to modify the victim's code so that we can artificially make more complex the evaluation of the condition in the if clause (adding the computation of trivial conditions or the evaluation of variables we know are not present in the cache) the only way to make side channel extension is by flushing the cache block where the "malicious_x" is so that we can guarantee a cache miss when reading this for evaluating the condition. However, I don't see if this is really an improvement or if this is a change that doesn't affect since at the end the parameter is passed by value, so it's copied in the stack and therefore in another cache block. This can be the reason behind the lack of estability of my code.

3.- Improving the attack accuracy

This is done thanks to (in order of importance):

1. Adjusting the decission threshold.
2. Randomizing the access to the cache blocks.
3. Increasing the number of repetitions.
4. Adjusting the training of the branch predictors.

4.- Troubleshooting

1. Lack of accuracy, isue solved by readjusting the decision threshold.
2. Making the access random proved to be a requeriment in my computer.
3. Lack of estability, issue not solved.