Assignment – 2

CSE -291

Purvi Agrawal (A59010787)

Discussion Question 3: In our example, the attacker tries to leak the values in the array secret_part2. In a real-world attack, people can use Spectre to leak arbitrary values in the victim's address space. Explain how the attacker can achieve this.

Spectre-based attacks trick a program into accessing arbitrary locations in a program's memory space. As a result an attacker may be able to read the content of the accessed memory, and thus potentially obtain sensitive data.
So as we did earlier in LAB 1 we need to have an idea for victim code. If the secret key is 1, the victim will access that particular address and then the attacker can do timing side-channel attacks and decode the secret key. If the value is 0, the victim won't access any address and the attacker would decode that. In the real-world attack, the attacker poisons the Branch Target Buffer (BTB) to steer the transient execution to a mis-predicted branch target.

Discussion Question 4: Try to tune the training parameters and answer this question: What is the fewest number of times you need to train the branch on line 9 in Listing 3 to make the attack work?

I tried multiple values and found that one time training the brach once works good for the attack.