CS6630 : Assignment 4

Micro-architectural Attacks : 100 Marks

Deadline: October 14th

After his recent success with injecting faults, Luther Stickell wants to try his hands with micro-architectural attacks. Like all his fellow researchers, he started this new research with something he does best …. Googling!!! and was able to find a time-driven cache attack on AES over here: https://bitbucket.org/casl/sidechannels/src/master/MicroarchAttacks/

Now that he has found code, he does something he does 2nd best … Post the question on stackexchange. But that didn't work !! :(So he finally comes to you.

Your job is to
(a) help him understand the source code of the time-driven attack
(b) demonstrate the success / failure of the attack in terms of Guessing Entropy
(c) convert the attack into an Evict+Time attack.

Hints:

- Average Guessing Entropy (GE) for an 8-bit secret key is a number between 1 and 256, which tells the number of guesses the attacker would need in order to get the secret key. If the attack works, the correct key would be easily distinguished, then the GE is 1. If a random guess is made about the secret key, then GE is 128.
- To measure GE, take an average of 100 experiments.
- To convert the attack into a Evict+Time, prefer to use an SMT machine.

To be Answered:

1. Provide a document on the time-driven attack works. **(5 marks)**
2. Provide details about the CPU used for the experiments. **(5 marks)**
    a. How many CPU cores?
    b. L1 cache size, associativity, sets?
    c. Which SMT threads (if available) share the same CPU core?
3. Plot a graph of Average GE (Y-axis) vs number of encryptions (X-axis) for the time-driven attack. Use log scale for the X-axis. **(10 marks)**
4. Add a section in the document to describe how you converted the time-driven attack to an Evict+Time attack. **(10 marks)**
5. Code for the Evict+Time attack **(60 marks)**
6. Plot a graph of Average GE (Y-axis) vs number of encryptions (X-axis) for the time-driven attack. Use a log scale for the X-axis. **(10 marks)**

7. Bonus Question :
    a. Extend the attack to a second round attack on AES, to show how more bits of the can be obtained. **(no marks here but may help change grades later)**

Submission Format:
Folder rollnum1_rollnum2 should contain the following files

1. Directory with code
2. Report and results (in PDF)