Lab 1: Cache Side Channels

Securing Processor Architectures - Fall 2022

Purvi Agrawal (A59010787)

Discussion Question 6: Describe your communication protocol. Please refer to Section 2.2 for the components involved in a protocol.

We have two components in this code one is the sender part and the other is the receiver part. The sender will be taking input from the user and receiver will try to retrieve that chat. They run on different threads. The attack which I am trying to demonstrate is Prime and Probe attack. The receiver first tries to prime the L2 cache and sender in the meantime will access some memory address and then receiver will probe the L2 cache. If the latency to access the block is more than the threshold which we have set it will imply that sender has accessed that line. Based on the set index information the receiver will decode the input message.

So first the user will be sending which is 8 bit integer. And the design of algorithm is done in such a way that sender waits for Enter key from user and after that user can enter the number which it wants to send. For 8 bit number we target 8 different set in L2 cache and 64 lines in total. This is the reason we have created an eviction set which has 8 indexes and is of the size of 64 cache line. Also we have allocated a huge page of 2 MB its done so that index bits for virtual address and physical address maps to same cache set.

We also have buffer in sender and receiver which is of the size of L2 cache. In eviction set we calculate the address for which index bits are same as chosen for each bit. We will total have 64 addresses corresponding to 64 cache line of L2. The receiver reads the address stored in eviction set and after that user sends data through sender which gets converted to binary. Now whenever the bit is 1 the sender will access the cache line if its 0 do nothing. The receiver will find the time to access the block. If the access time is greater than threshold corresponding bit is 1 else it is 0. Now receiver has binary coded information.