

Meltdown Lab

ENEE 457

1. What is a side-channel attack?
2. What is a cache timing channel?
3. What is the Flush+Reload Technique?
4. What is exception handling?
5. What is out-of-order execution?
6. How can one check that out-of-order execution indeed occurred using the Flush+Reload technique?
7. How can one learn secret information by leveraging out-of-order execution and the Flush+Reload technique (as in the Meltdown attack)?