Last-Level Cache Side-Channel Attacks are Practical

Kalind Karia

(213076001)

1 Summary

In this paper, the authors present an effective implementation of Prime + Probe side-channel attack on LLC. They have demonstrated the attack on cross-core, cross-VM and measured the capacity of the covert channel created. Their technique relies only on cache inclusiveness and large-page mappings used by VMM.

2 Details

The work presented in the paper adapts the PRIME + PROBE technique for practical LLC attacks by exploiting hardware features such as:

1. inclusive caches (outside control of the cloud provider)
2. large page mappings (controllable and usually enabled in VMM for better performance)

Only other assumption made is that the attacker and victim are co-hosted on the same processor.

Major contributions of the work:

1. asynchronous PRIME + PROBE attack on LLC that does not require sharing of cores or memory between attacker and victim and does not exploit VMM weaknesses.
2. develops two techniques for efficient attack:
   - algorithm for attacker to probe exactly one cache set without the knowledge of virtual-address mapping
   - use temporal access patterns to identify victim's security-critical accesses.
3. achieves the measurable bandwidth of cross-VM covert timing channel as high as 1.2 Mb/s.

`rest sections I will fill as I complete the remaining sections for review`

3 Strengths

4 Weakness

5 Extensions