Classifying and Mitigating Side-Channel Vulnerabilities between VMs

Jinpeng Miao*  Dwight Browne*  Abdulrahman Alaraj*  Tamara Lehman*  Daniel Massey*
* University of Colorado Boulder

Objectives

- Classify VM side-channel vulnerabilities novelly
- Typical corresponding defenses discussion
- Propose an effective mitigation direction
- Minimize performance loss and resource consumption
- Comprehensively suite and protect against possible future attacks
- Encouragement purpose

Status Quo

- Popularity of large-scale cloud services and virtualization technology breeds more powerful remote side-channel attacks.
- The fact that side-channel attacks exploit different properties requires distinct defenses, hence making it difficult to defend against.
- Existing defenses for these vulnerabilities are either limited to a single vulnerability or causing a lot of performance loss.
- Hard to completely solve these problems with small software and hardware patches.
- Failure to consider future related potential attacks and prevent them in advance, which will once again make us vulnerable.

References

- [12] https://www.theregister.co.uk/2018/11/02/portsmash_intel_security_attack/