Name: Bo Sun(UiB)

Preventing Cross-VM Cache Side-Channel Attacks Through Dynamic Software Diversity

Cloud computing is promising and widely used technology nowadays. Sharing hardware through locating in different virtual machines is the basis for cloud computing. Many security concerns arise from this and one of them is side-channel attacks between different virtual machines. Since different virtual machines share last level cache, so cache side channel attack can't be ignored. There are two categories of cache side-channel attacks. One is networking timing side channel attack and the other is cache-based side channel attacks[1, 2]. Our work focus on the second one. Furthermore, cache timing attack[3] is the most common attack for inferring encryption key from encryption algorithms. Due to core migration[1] feature in the cloud, we will focus on last level cache timing attack.

We propose to use software diversity[4] methods as countermeasure for preventing cross-VM cache timing side-channel attack. Our work will base on [5] and extend it to cloud environment between different VMs.

References

[1] T. Ristenpart, E. Tromer, H. Shacham, S. Savage, Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds, in: Proceedings of the 16th ACM conference on Computer and communications security, ACM, Chicago, Illinois, USA, 2009, pp. 199-212.
[2] Y. Zhang, A. Juels, A. Oprea, M.K. Reiter, HomeAlone: Co-residency Detection in the Cloud via Side-Channel Analysis, in: 2011 IEEE Symposium on Security and Privacy, 2011, pp. 313-328.
[3] H.C.A.v. Tilborg, S. Jajodia, Encyclopedia of cryptography and security, Springer, New York, 2011.
[4] B. Baudry, M. Monperrus, The Multiple Facets of Software Diversity: Recent Developments in Year 2000 and Beyond, Publisher, City, 2015.
[5] S. Crane, A. Homescu, S. Brunthaler, P. Larsen, M. Franz, Thwarting Cache Side-Channel Attacks Through Dynamic Software Diversity, Publisher, City, 2015.