CACHEOMS: About Practical Exploitation of **Cache** Side Channel **O**n **M**ultiprocessor **S**ystems

Aravind Kumar Machiry
machiry@cs.ucsb.edu

Varun Kulkarni Somashekhar
varun_kulkarni@cs.ucsb.edu

April 22, 2015

1 Abstract

Cache side channel is well known attack on cryptographic implementations[3][1][2]. This is primarily based on observation that infrequently used information incurs a large timing penalty, thus revealing some information about the frequency of use of the memory blocks. This attack is straight forward on a single processor system with single level of cache, but current systems (both desktop and mobile) are multiprocessor where each processor has multilevel caches also there are some cache levels which are common to a subset of processors. Moreover, latest ARM processors have TrustZone support[4] which ensures System-On-Chip (SOC) wide security by avoiding shared cache access. In addition to this, there has been lot of work done both on Hardware and Software side to mitigate cache side channel[5][6]. It is high time we revisit and evaluate cache side channel, its bandwidth and implications[7].
We would like to explore this for our project, specifically following are our goals:

- Investigate, understand and report cache side channel with examples. We aim to make the documentation simple enough to be understood by a computer science graduate without much knowledge of cryptography or computer architecture.
- Research on the recent improvements and state of art on cache side channel and clearly report the findings.
- Evaluate the applicability of these attacks on well known protocols on current multiprocessor systems, both on x86 and ARM.
- If time permits, implement one of these attacks and report corresponding result.

References

[1] Onur Aciçmez and Çetin Kaya Koç. Trace-driven cache attacks on aes. 2006.

[2] Sebastian Banescu. Cache timing attacks. 2011.

[3] Daniel J Bernstein. Cache-timing attacks on aes, 2005.

[4] Torsten Frenzel, Adam Lackorzynski, Alexander Warg, and Hermann Härtig. Arm trustzone as a virtualization technique in embedded systems. In *Proceedings of Twelfth Real-Time Linux Workshop, Nairobi, Kenya*, 2010.

[5] Taesoo Kim, Marcus Peinado, and Gloria Mainar-Ruiz. Stealthmem: System-level protection against cache-based side channel attacks in the cloud. In *Presented as part of the 21st USENIX Security Symposium (USENIX Security 12)*, pages 189–204, Bellevue, WA, 2012. USENIX.

[6] Zhenghong Wang and Ruby B Lee. New cache designs for thwarting software cache-based side channel attacks. In *ACM SIGARCH Computer Architecture News*, volume 35, pages 494–505. ACM, 2007.

[7] Yuval Yarom and Katrina Falkner. Flush+reload: A high resolution, low noise, l3 cache side-channel attack. In *23rd USENIX Security Symposium (USENIX Security 14)*, pages 719–732, San Diego, CA, August 2014. USENIX Association.