Implementation and Security Respectively Performance Evaluation of a Cache Covert Channel Cloud Scheduler

Luthfi Idris
Supervisor: Prof. Dr. Dirk Westhoff and M. Sc. Johann Betz
University of Applied Sciences Offenburg

Introduction

In Virtualization, scheduler effects on many parts of a cloud infrastructure. So that, selecting the right scheduler can optimize speed or increase security. Local scheduler defines access to the given resources from VMs on single physical machine while global scheduler defines the target physical machine on which VM should be started or migrated.

C3 scheduler intention is to mitigate the threat of leakage of information via cache covert channels by preventing processes to access cache lines alternately[1].

Attack scenario

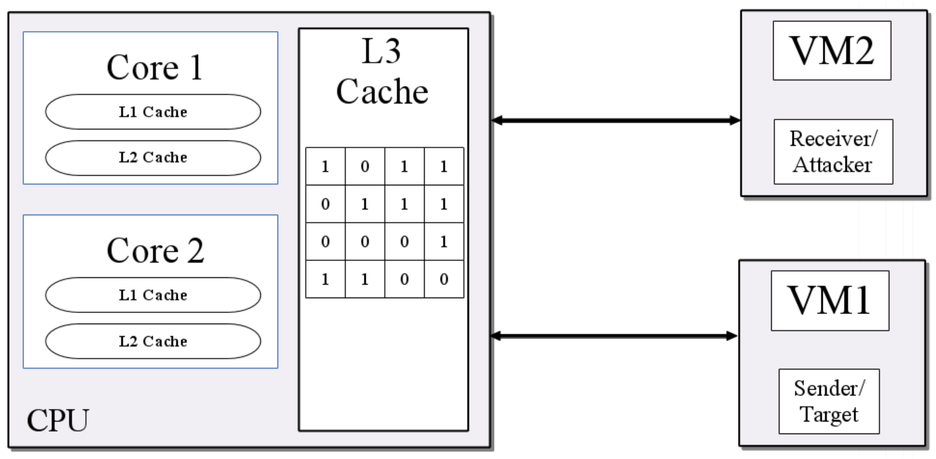

Figure: CPU Cache Overview

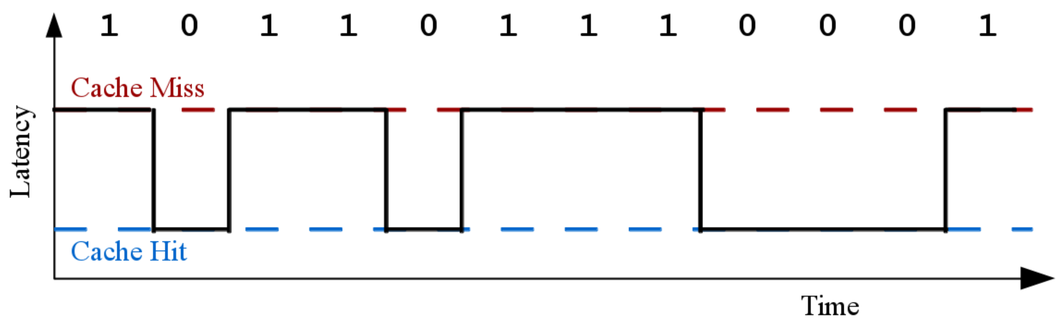

Figure: Timing Modulation Pattern [3]

Architecture

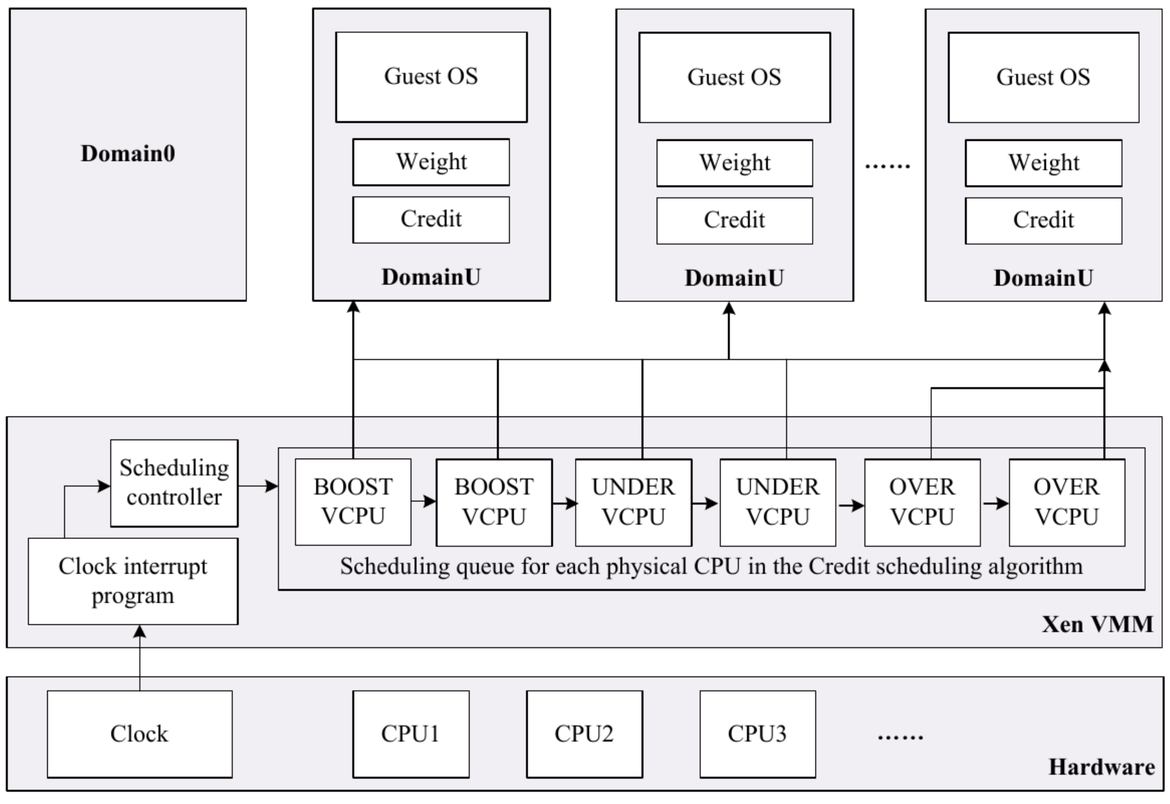

Figure: High Level Credit Scheduler[2]

Pseudo Code

INPUT: $P_{sys}, P_{client}, \rho, \gamma, \lambda, |VM|, |CPU|, cache, q$
OUTPUT: $p_i, ..., p_{i+\rho} \in P_{client}, p_j, ..., p_{j+\lambda} \in P_{sys}$

Queue $next$[];
Queue $pollution$[];
Global VM $vm \leftarrow vm_1$;

// $\rho = r \cdot \lambda$
$next \leftarrow$ choose $p_i, ..., p_{i+\rho} \in P_{client}$ as FIFO queue whereas $p_i, ..., p_{i+\rho}$ belong to the same vm_k;
$vm \leftarrow vm_{k+1}$;

// $\lambda = \lfloor \frac{|Psys|}{|VM|} \rfloor$
$pollution \leftarrow$ choose $p_i, ..., p_{i+\lambda} \in P_{sys}$ as FIFO queue whereas $p_i, ..., p_{i+\lambda}$ belong to vm_0;
$\gamma_{achieved} \leftarrow$ sum cache usage of $pollution$;
for $i \leftarrow 0, i < k$ **do**
  // $\gamma = \frac{|VM| \cdot cache}{2 \cdot |P_{sys}|} \cdot |CPU|$
  if $\gamma_{achieved} < \gamma$ **then**
    //increase $q \leftarrow q \cdot i$ by reusing $p_j, ..., p_{j+\lambda}$
    $pollution \leftarrow pollution \,||\, pollution$;
    $\gamma_{achieved} \leftarrow$ sum cache usage of $pollution$;
  end if
  $i \leftarrow i + 1$;
end for
$next \leftarrow next \,||\, pollution$;
if $\gamma_{achieved} > \gamma$ **then**
  return $next$;
else
  return $null$;
end if

Figure: Pseudo Code C3 Scheduler[1]

Design Strategies and Objective

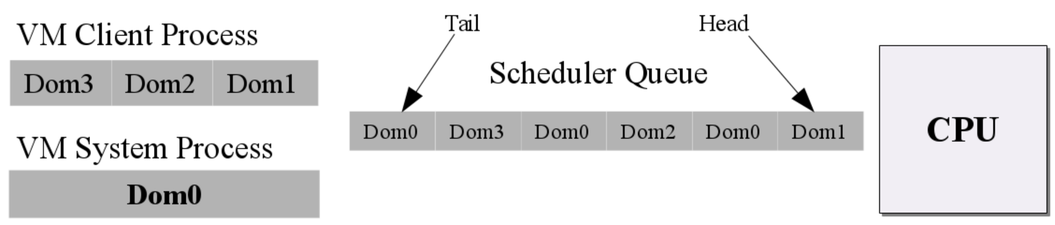

Figure: C3 Scheduler

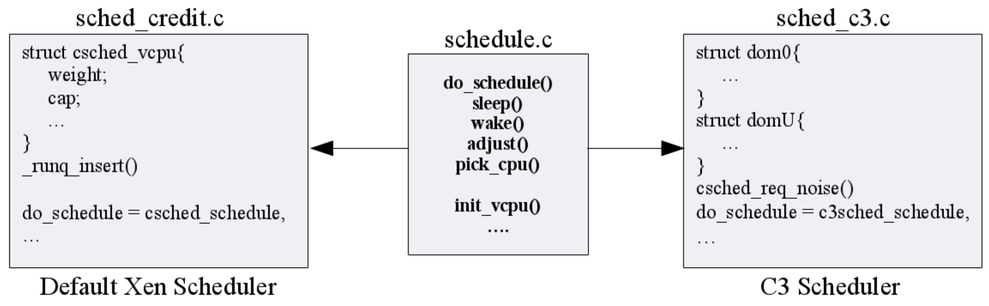

Figure: Xen Scheduler Framework

- Implementing C3 Scheduler
- Integrating to the Xen Hypervisor
- Evaluating performance by simple program with and without using C3 Scheduler

Reference

Betz, Johann and Westhoff, Dirk: C3-Sched - A Cache Covert Channel robust Cloud Computing Scheduler, ICITST, pp. 55-61, Technical Co-Sponsored by IEEE UK/RI Computer Chapter, London, U.K., 2014.

Zeng, L., Wang, Y., Shi, W., and Feng, D. An improved xen credit scheduler for i/o latency-sensitive applications on multicores. In Cloud Computing and Big Data (CloudCom-Asia), 2013 International Conference on (Dec 2013), pp. 267-274.

Wu, Zhenyu, Zhang Xu, and Haining Wang: Whispers in the hyper-space: High-speed covert channel attacks in the cloud. In Proceedings of the 21st USENIX Conference on Security Symposium, Security'12, pages 9–9, Berkeley, CA, USA, 2012. USENIX Association. http://dl.acm.org/citation.cfm?id=2362793.2362802.