Resource Management for Isolation Enhanced Cloud Services

*Himanshu Raj*, Ripal Nathuji, Abhishek Singh, Paul England
XCG, Microsoft Research
Motivation

• Isolation issues in shared-resource computing infrastructures
Motivation

- Side-channel attacks compromising performance and security
  - DoS, Information leak (key stealing not shown for VMs yet)

Areas lacking:
- SLA specification
- Isolation mechanisms
- Resource management
Proposed Solution

• *Isolation attributes* part of the SLA
• *Mechanisms* for better isolation
• Enhanced *resource management*
  – Include constraints based on isolation attributes
SLA Isolation Attributes

• Degree of hardware fault resistance (n)
  – Type: Integer, e.g., n = 5

• Cache-based side channel attack avoidance
  – For DoS and Information leakage avoidance
  – Type: Boolean
Enforcing Cache Isolation

- Cache hierarchy aware core assignment
- Page-coloring based cache partitioning
Cache Hierarchy Aware Core Assignment
Page-coloring Based Cache Partitioning
Results: No Isolation

- Target VM + Perturbation VM (1 Thread)
- Target VM + Perturbation VM (2 Threads)
- Target VM + Perturbation VM (3 Threads)
- Target VM

Working Set Size:
- 1MB, 1.5MB, 2MB, 2.5MB, 3MB, 3.5MB, 4MB, 4.5MB, 5MB, 5.5MB, 6MB, 6.5MB, 7MB, 7.5MB, 8MB, 8.5MB, 9MB

Execution Time (s):
- 0, 20, 40, 60, 80, 100, 120, 140, 160, 180

Chart shows the execution time for different working set sizes and configurations.
Results: Cache-coloring

![Graph showing results of cache-coloring]

- Target VM + Perturbation VM (1 Thread)
- Target VM + Perturbation VM (2 Threads)
- Target VM + Perturbation VM (3 Threads)
- Target VM

![Diagram showing cache coloring]

- L1D
- L2
- Shared L3
Integration with VM Placement System

- Constraints on resources
  - New isolation constraints
- 4000 blade cloud, <80% utilization, ~30-40 ms for search without backtracking (with high success probability)
- Working on other heuristics for CSP with system dynamism
  - Migration
Conclusions

• Incorporation of isolation attributes in the SLA
• System-level mechanisms to address isolation
• RM enhancements with isolation related constraints