Scheduler-based Defenses against Cross-VM Side-channels
Venkatanathan Varadarajan, Thomas Ristenpart and Michael M. Swift
University of Wisconsin-Madison

Problem: Cross-VM Side-Channels

Multi-Tenancy in Public IaaS Clouds
Two customers sharing the same physical host managed by a hypervisor is common place.

An Example Control-flow Side-channel
Libgcrypt implements a square multiply algorithm used by many cryptographic functions: RSA, Elgamal, etc.
Leaks secrets via l-cache usage.
Zhang et al. [CCS'12] in a lab setting extracted a 2048 bit usage, funcGons: used by many cryptographic square multiply algorithm
Zhang et al. [CCS'12] in a lab setting extracted a 2048 bit usage.

Solution: Soft-Isolation of VMs

Scheduler-based Defenses against Cross-VM Side-channels

Protection I: MRT Mechanism

Protection II: State-Cleansing

Existing Scenario
Core: VM VM
interrupt & schedule (boost priority)
Minimum RunTime (MRT) Guarantee
Core: VM VM
interrupt schedule
MRT (scheduler parameter)

Makes existing attacks harder

Results
Security
• 5ms MRT increases the mod-exp. bit operations pre-prompted to 386 from 0.096 bit ops with no MRT
Overhead of MRT of 5ms:
  • 0.3% improvement for batch workloads,
  • On average 4% and at worst 7% overhead on 95th percentile latency.
Overhead of State-Cleansing:
  • An average overhead of 10-20µs,
  • A worst case overhead of 80-100µs.

Prior Defenses
2. Specialized Hardware: Problems: high cost, non-commodity.
3. Reduce Resolution of Timers: Problems: Loss of feature or high overhead.

Simple, Secure Scheduler Design
Two protection mechanisms:
• MRT mechanism for securing batch VMs that are involved in involuntary context switches.
• Per-core State-Cleansing for securing interactive VMs involved in voluntary context switches with runtime < MRT.

State-of-the-art CPU schedulers
Interactive VM
Throughput-oriented:
• Benefits from quick wakeups,
• BOOST priority mechanism reduces wakeup latency.

Batch VM
Latency-oriented:
• Benefits from longer scheduler timeslices

Batch
Interactive VM

Prior Defenses
2. Specialized Hardware: Problems: high cost, non-commodity.
3. Reduce Resolution of Timers: Problems: Loss of feature or high overhead.