System Utilization of Processor Hardware Counters

Kai Shen
Dept. of Computer Science, University of Rochester

Processor Hardware Counters

- Counter registers
  - metrics must map to limited number (2, 4, ... 18) of counter registers for observation

- How to access them?
  - counter register access instructions are privileged (at least on Intel Xeon processors)
  - but OS may choose to expose statistics through system calls

Utilization as Performance Indicators

- Context (hardware resource sharing):
  - on multi-core and multi-threading processors, simultaneous processes compete for shared resources (memory bus, cache, floating point unit)

- Hardware counters indicate execution performance:
  - Case #1: too much competition on floating point unit when processes A/B run simultaneously
    ⇒ schedule them not to run simultaneously.
  - Case #2: inefficient/unfair use of cache - process A misses a lot while process B doesn't miss at all
    ⇒ adjust cache size allocation between them.
Utilization as Workload Signatures

- **Identifying requests for server workloads**

  - On-the-fly: identify a request while it still executes
  - Utilizations:
    - Predicting request properties to guide OS adaptations
    - Classifying requests on-the-fly to detect anomalies

![Graph showing Floating point ops per CPU cycle](image)

4/24/2008 URCS 573 - Spring 2008 5

Utilization:

**Shortest-Job-First Scheduling**

- 15-27% shorter response time than running average
- Perform similar to oracle

![Graphs showing Mean response time and request rate](image)

4/24/2008 URCS 573 - Spring 2008 6

Utilization:

**Request Classification and Anomaly Detection**

- Dots are normal TPC-H requests
- Circles are anomalies (SQL injection attacks)

![Graph showing Trace cache misses per µ-instruction](image)

4/24/2008 URCS 573 - Spring 2008 7

Security Risk:

**Stealing RSA key in OpenSSL**

- In OpenSSL/RSA, $X^d$ is decomposed into a series of square and multiply operations.
  - e.g., $X^{11} = ((X^2)^2*X)^2*X$
- Execution sequence of squares and multiplies can help infer the RSA key d.
- Distinguish square and multiply through hardware counters.

![Graph showing branches per instruction](image)

4/24/2008 URCS 573 - Spring 2008 8
Security Issues

- Side-channel attacks
  - attacks based on machine hardware information collected during the physical execution of a cryptosystem
- Covert-channel attacks
  - a program encodes information into a series of executions with easily recognizable hardware metrics that the collaborator can learn

**Solution:** prevent attackers from reading hardware metrics of targets
- some metrics are reported in a combined fashion on a multi-processor