

Do you get what you pay for?

**Using Proof-of-Work Functions to
Verify Performance Assertions
in the Cloud**

Falk Köppe
Jörg Schneider

- Classic SLAs doesn't work with VMs
 - No uptime
 - No response time

Every value measurable from the outside may depend on your application

- Solution: Measure with neutral benchmark

Just use a benchmark?

Technology: Internet Explorer 9 Caught Cheating In SunSpider

Posted by [CmdrTaco](#) on Wednesday November 17, @08:43AM
from the well-that's-not-nice dept.

dkd903 writes

"A Mozilla engine
Microsoft – [Intel](#)
The SunSpider,
a very popular c

[Read More...](#)



Technology: More 'Application-Specific' Optimizations in NVidia Drivers

Posted by [michael](#) on Friday June 06 2003, @08:00AM
from the but-it's-not-cheating-so-there dept.

EconolineCrush writes

"Futuremark and NVIDIA have been embroiled in a spat over various cheat/optimizations in 3DMark03 for several weeks now. Last week, the soap opera appeared to be over; Futuremark and NVIDIA [released](#) a joint statement in which Futuremark clarified that NVIDIA was optimizing its drivers for 3DMark03 rather than cheating. This story, however, appears to be far from over. [Tech Report](#) has [uncovered](#) a new series of optimizations in NVIDIA's Detonator FX drivers that affect image quality in even Futuremark's latest 3DMark03 build. What's more, if you rename the 3DMark03 executable, the optimizations disappear."



- Evil cloud operator
 - Can monitor executed code
 - Can modify data in RAM and HD
 - Can change executed code
- Attack vectors
 - Benchmark Skip
 - Pre-calculation
 - Code and data exchange
 - Additional resources

- General idea:
Hard to solve, but easy to check result
- Properties
 - Costs
 - Stability
 - Security
 - Concurrency
 - Advantage
 - Parameterability
 - CPU-bound vs. memory-bound

Example PoW function

- Extracting square roots
 - Find x^2 in the congruence class modulo p
- Forge a digital signature
 - Weakened algorithms
 - Known attacks on old algorithms
- Hash collisions
 - Find a string with a hash starting with x

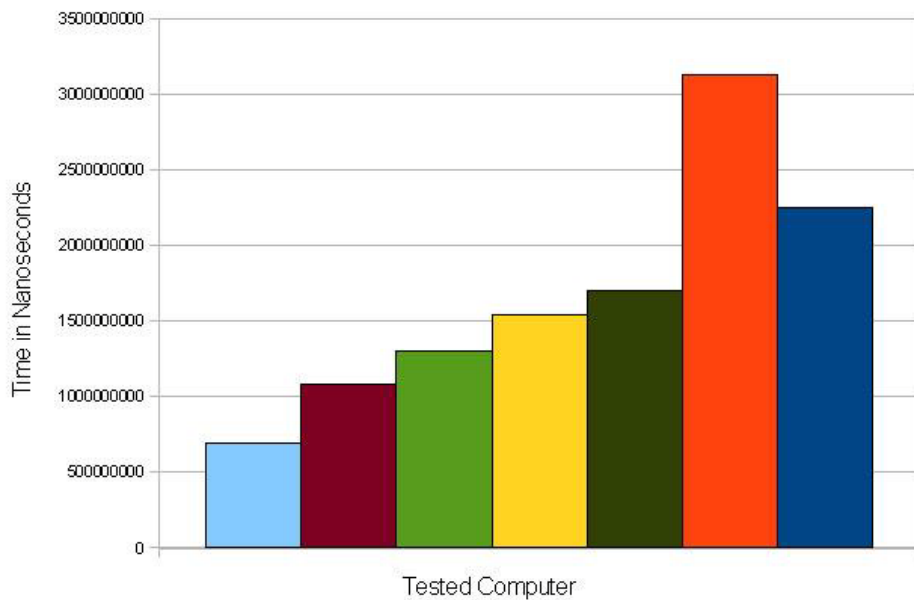
Proof-of-Work function based benchmark

- Cloud-VM solves challenges
- User verifies solution and runtime
- Micro benchmark run on productive VM

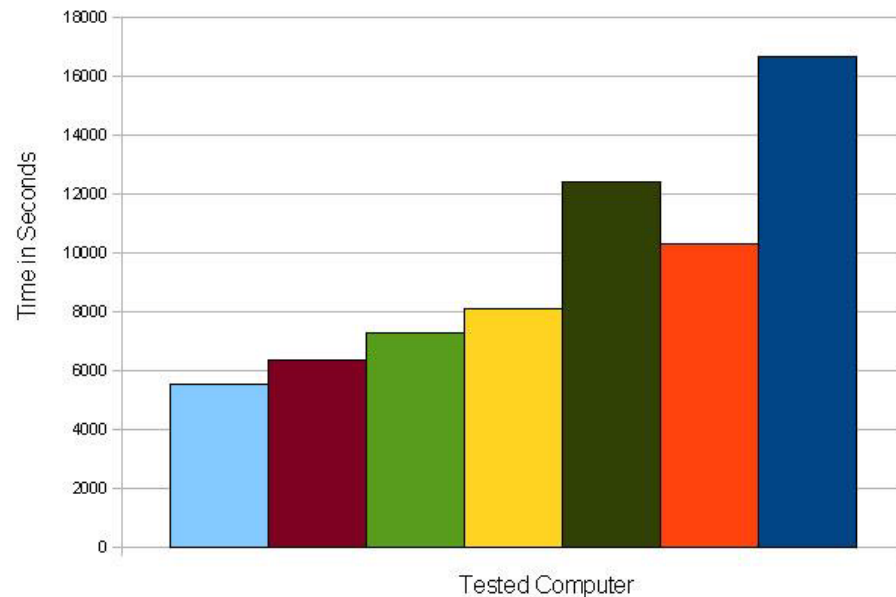
- Attacks blocked:
 - Benchmark Skip ✓
 - Pre-calculation ✓
 - Code and data exchange ✓
 - Additional resources ✗

Evaluation: Correlation

HashCashLin
Average Execution Time

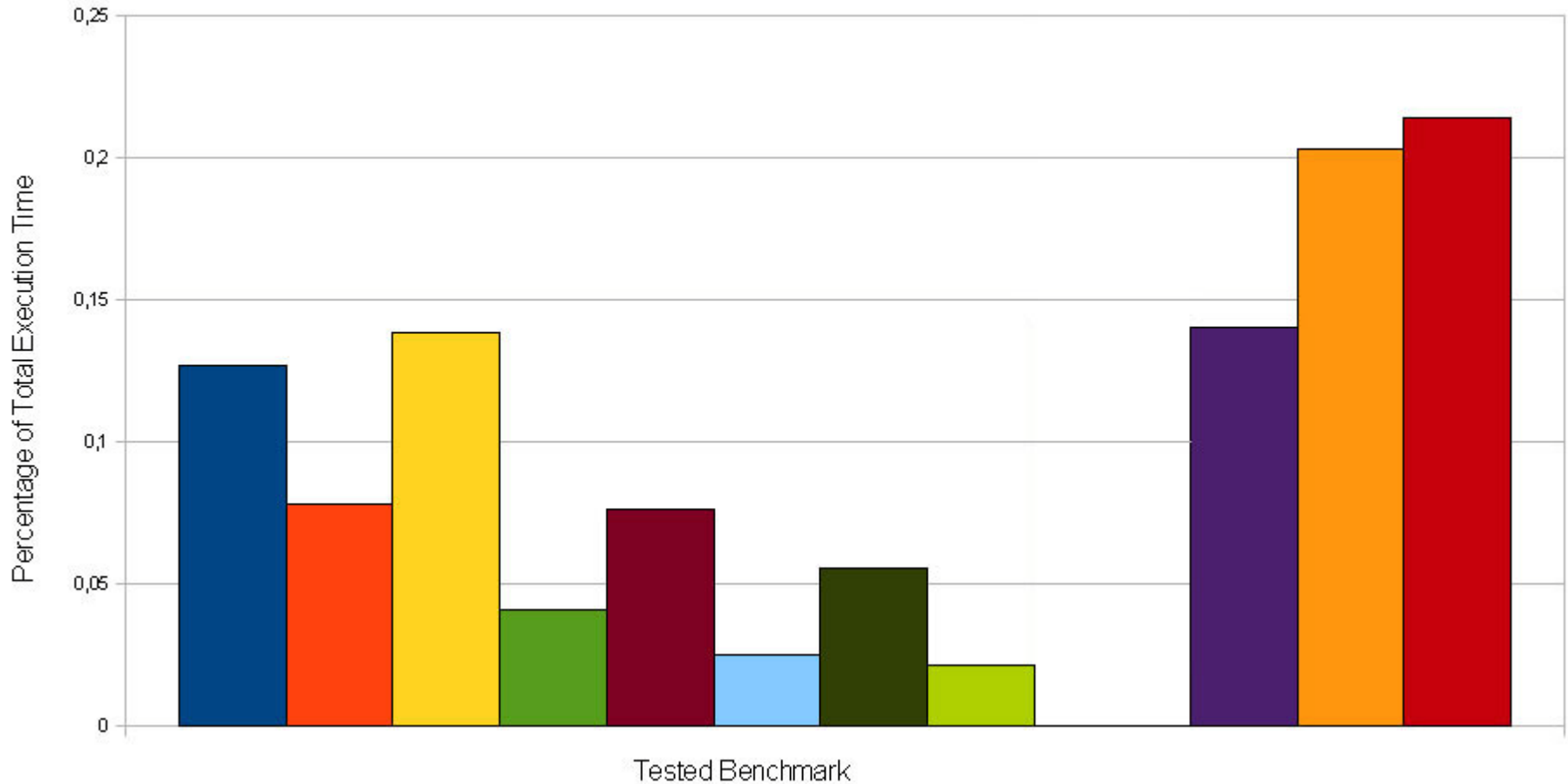


SPEC2006 Benchmark Results
Total Execution Time

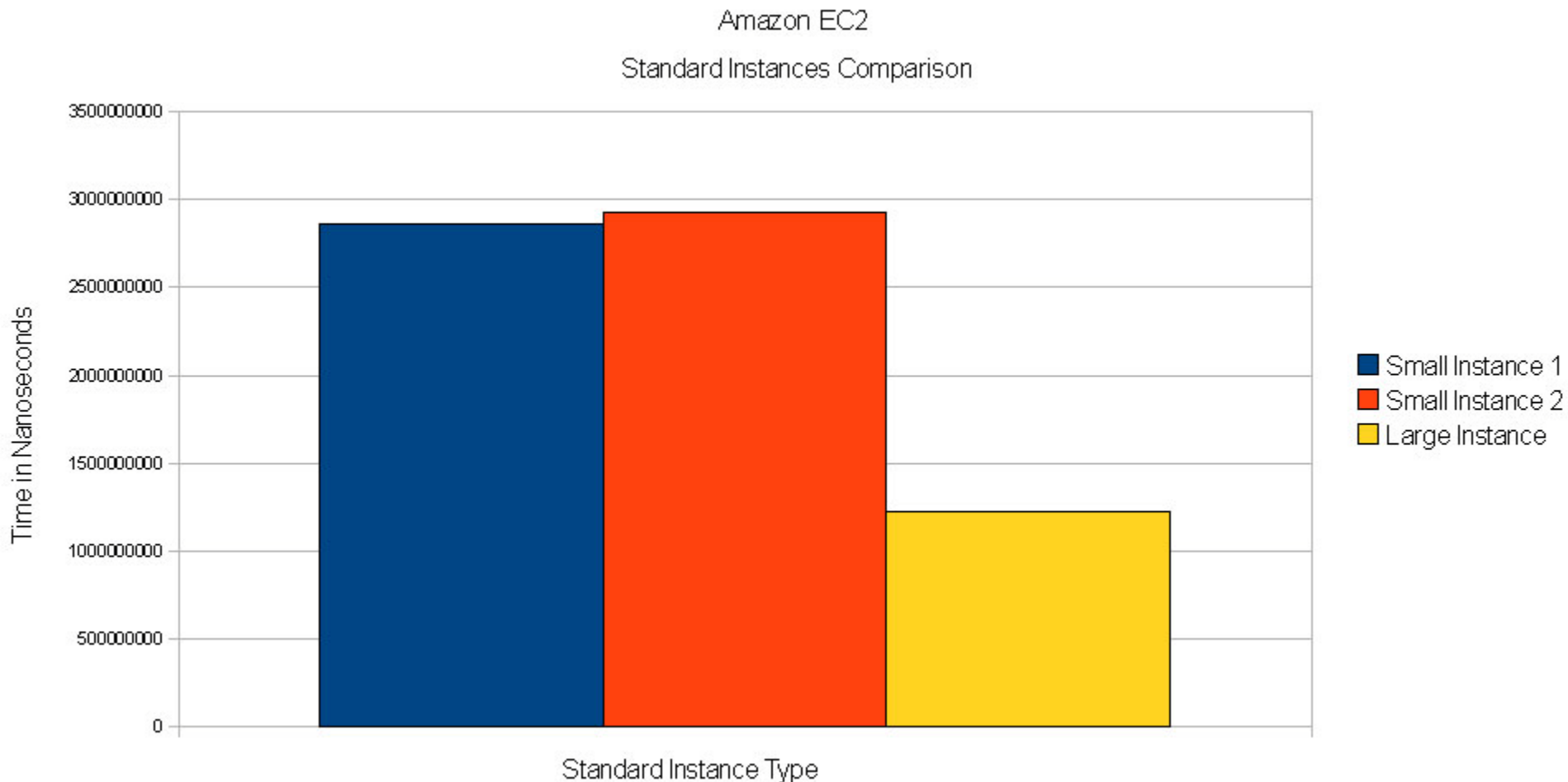


Evaluation: Variance

Standard Deviation Comparison
on Lenovo Tp60 XP



Evaluation: EC2 \neq Evil Cloud



- New micro benchmark to verify performance
- Based on Proof-of-Work functions
 - Hard to solve, easy to check result
- Blocks 3 of 4 attacks
- Sufficient correlation with reference benchmark
- Future work: Weave into application

Do you get what you pay for?

**Using Proof-of-Work Functions to
Verify Performance Assertions
in the Cloud**

Falk Köppe and Jörg Schneider

komm@cs.tu-berlin.de

<http://www.kbs.tu-berlin.de>