Paper Review

Saurabh Mathur

November 19, 2018

Paper Title

The paper is titled "A Comparison of Software and Hardware Techniques for x86 Virtualization". It was written by Keith Adams and Ole Agesen.

Summary

This paper compares virtualization techniques that are fully software based to those that utilize the newly developed (at the time) x86 hardware primitives. Software virtualization was developed out of the lack of availability of hardware primitives to implement classical virtualization. With the support for hardware primitives, hardware virtualization became possible in the x86.

However, in this paper, the authors conclude that the hardware based virtualization fails to perform better than the software based virtualization. They point out some of the issues with the hardware support for virtualization on the x86 and claim that future work on these issues would greatly improve performance of the hardware primitives.

Details

The authors used Popkek and Goldberg's three essential characteristics of a VM (Virtual Machine) Manager-

1. Fidelity: The code is executed in exactly the same way on a VM as it would be executed locally.
2. Performance: Instructions are executed with as little intervention from the VM Manager as possible.
3. Safety: The VM Manager has full control over the resources.

The key techniques in software virtualization described in the paper are as follows-

1. Simple Binary Translation: Binary guest code is translated as and when it is executed, replacing priviledged instructions with their equivalent safe instructions.
2. Adaptive Binary Translation: Detects non-privileged instructions accessing sensitive data that trap frequently and patches them with equivalent simulated instructions.

The primitives that enabled hardware virtualization are as follows:

1. Separate guest and host modes
2. Virtual Machine Control Block
3. `vmrun` instruction to switch to guest mode

The issues with the new hardware primitives pointed out in this paper are as follows-

1. Overhead of maintaining VM state
2. Inefficient implementation of primitives
3. Lack of hardware MMU (Memory Management Unit) support

While the software virtualization performed better in terms of emulation speed and trap elimination, the hardware primitives provided precise exceptions, more efficient system calls and preserved the original code. So, while the software techniques were faster, the hardware primitives made debugging easier.

Positives

This paper was a comprehensive review of virtualization techniques available at the time. VMWare's software virtualization techniques allowed direct virtualization without depending on the underlying hardware architecture to support virtualization. Further, their implementation was so efficient that it outperformed the first hardware primitives.

The authors also pinpointed the exact places where the hardware primitives were lacking. What I especially liked was the variety of simple but informative nanobenchmarks that they wrote for their qualitative comparision to verify their claims.

Significance and Relevance

This paper compared the hardware virtualization with the state of the art in software virtualization. The authors provided insights into improving hardware support for virtualization. The precise feedback in this paper helped the manufacturers develop more efficient hardware to support virtualization. The implementations of the primitives were improved in later releases and support for hardware MMU was provided by Intel's VT-d and AMD's nested paging systems.