April 27, 2009

[PERFORMANCE AND SECURITY LESSONS LEARNED FROM VIRTUALIZING THE ALPHA PROCESSOR]

Paul A. Karger – IBM Thomas J. Watson Research Center
International Symposium on Computer Architecture
Proceedings of the 34th annual international symposium on Computer architecture. ISBN: 978-1-59593-706-3. Published by ACM.
San Diego, California, USA; pages 392 – 401, 2007.

By: André Ricardo Abed Grégio, R.A.: 079779

This paper examines the features of Digital Equipment Corporation's (DEC's) Alpha processor that are designed to support virtual machine monitors (VMMs), highlighting how this processor use of PALcode (Privileged Architecture Library code) and its handling of UNPREDICTABLE results can make the Alpha architecture adequate to support secure hypervisors, and compares Alpha's virtual architecture to other approaches (Intel, AMD, IBM, Sun). A hypervisor (VMM) is a special kind of operating system that emulates multiple virtual machines on a single system as an individual computer. PALcode instructions allow implementing new or complex instructions from VAX on the RISC processor without using microcode. To be virtualizable, all CPU architecture sensitive instructions (i.e., that reveals or modifies the privileged state of the processor) must trap to the VMM, causing performance problems. In Alpha processors they are implemented in PALcode, transferring the basic trapping overhead to the machine architecture instead of the VMM.

Concerning about the performance and security of a virtual-memory operating system/ hypervisor, it is extremely critical the handling of the translation buffer. Alpha architecture doesn't specify a page table structure, unlike more recent virtual memory systems. It has only one translation buffer for which all misses are trapped to PALcode routines, simplifying the processor hardware (less circuitry). Most virtual memory machines have both used and modified bits in the PTEs that are set by the hardware whenever a particular page is used or modified, which are eliminated in the Alpha processor, reducing the need for circuitry to set those bits and the amount of memory needed for the translation buffer. Many CPU specifications include operations whose results may be unpredictable or undefined. Unpredictable results permit security violations – CPU has access to data to which the currently running process should not have access. The Alpha architecture defines UNPREDICTABLE to solve it, saying that security holes created by an unpredictable result are violations to the architecture, requiring them to be fixed in the CPU in order to be a legal Alpha processor. Only software running in kernel mode (privileged) can cause UNDEFINED results, which don't have security concerns as unprivileged software can never cause a result like this.

Comparing with other processors, IBM zSeries architecture approach to implement more complex instructions (Millicode) is very similar to PALcode, turning it well suited for virtualization. However, zSeries architecture is more complex than the Alpha, making it more difficult to pass a high assurance security evaluation. Intel specified a virtual-machine control data structure (VMCS) in order to support x86 virtualization, to store the state of each virtual processor. This requires a large number of extra registers. The Alpha virtual machine let the hypervisor decide how much state information must be saved, avoiding dedicating a large number of registers to store it. AMD Secure Virtual Machine Technology is very similar to Intel's VT, the difference being that AMD already supports ASNs in the translation buffer, improving their processor performance. Intel Itanium has a processor abstraction layer (PAL) closer to Alpha processor's PALcode. IBM POWER5 virtualization features are implemented in firmware and its hypervisor makes use of paravirtualization techniques, requiring little or no need for PALcode, but also requiring changes to the guest operating systems, what can be more difficult if there is no access to modify the guest operating system. Sun UltraSPARC hypervisor optimizes subroutine calls by maintaining a large set of register windows, what led to performance problems on process switches (save and restore windows) and security problems in protecting register windows between contexts, being vulnerable to covert channel issues (information leakage).

The virtualization properties and special features of Alpha architecture can help designers of virtualization support on other processor architectures to improve the performance and security of hypervisors, learning from the lessons of specifying and implementing the Alpha processor.