Computer Architecture III Study Guide Additional Topics

Maximillien Courchesne-Mackie (mcour010@uottawa.ca)

I. Virtualization

Virtualization is the process of running multiple operating systems on one physical machine. This involves using a hypervisor to dictate the sharing of resources. Virtualization is attractive because it allows proper hardware utilization and reduces the number of machines needed for a multi-user multi-operating system environment.

A. Hypervisors

There are two kinds of hypervisors: Type 1 (also known as bare-metal) and Type 2 (known as hosted).

- **Type 1:** A bare-metal hypervisor sits in between the machine's hardware resources and the virtualized operating systems. A popular bare-metal hypervisor is Xen.
- **Type 2:** A hosted hypervisor requires a host operating system to be installed on the machine to be able to run. The host provides the interface to the hardware. Notable examples of hosted hypervisors are VMware, KVM and VirtualBox.

B. Type of Virtualization

- **Full Virtualization:** A complete simulation of the actual machine's actual hardware which allows a guest operating system to run unmodified.
- **Paravirtualization:** Guest operating systems operate in their own domains and request privileged operations from the hypervisor using an API. The virtual operating systems need to be modified to work with this type of virtualization.
- **Hardware-Assisted Virtualization:** Ring 0 is split into two subrings. The *root* subring is where the hypervisor runs and has access to all privileged operations. The *non-root* subring is where the guest operating system resides.

C. Xen Hypervisor

The Xen hypervisor supports paravirtualization and hardware-assisted virtualization. It divides guest operating systems into domains (denoted as *DomU* domains) with no driver support. These domains communicate through a master domain (called *Dom0*) to access external devices (except in the case of passthrough).

Xenstore is the memory shared between Dom0 and the DomU domains.

Xen also handles interrupts destined to guest operating systems. The IDT redirects interrupts (called events in Xen) to the relevant DomU over the event channel.

Xen uses a scheduler to assure processes from each operating system get fair access to the system's resources. This system is credit-based (according to the weight of the process) and credits are debited from processes every 10ms. Scheduling decisions are made every 30ms and under or over debited processes are moved into specialized FIFO buffers.

II. Cloud Computing

A. Architectures

- **Grid:** In a grid, grid nodes are connected through a network to a controller which gives out work units. Grids are more specialized than cloud-based architectures.
- **Cloud:** A cloud architecture is not as focused as a grid architecture and generally has more uses.
- **Supercomputing:** A supercomputing architecture consists of clusters of local computers connected via a high speed interconnection network. Each cluster works within a common problem space.

B. Services

- **Software-as-a-Service (SaaS):** The client is can use a piece of software (or a software suite) running through the cloud without the need to service or install it. Notable examples are Gmail and Dropbox.
- **Platform-as-a-Service (PaaS):** The client gets access to a system on which he or she can install and configure software at will. This category is especially used as web app environments and deployments.
- **Infrastructure-as-a-Service (IaaS):** The client is given a complete environment to customize. This includes access to external resources.

C. Virtualization

Virtualization is a key component in cloud computing. Cloud service providers can invest smaller amounts of money in large servers which can be virtualized and rented to clients (instead of buying custom machines for each new client). Virtualization also allows individual isolation from other clients.