

**Stony Brook University
The Graduate School**

Doctoral Defense Announcement

Abstract

OS-level Virtualization and Its Applications

By

Yang Yu

OS-level virtualization is a technology that partitions operating system to create multiple *Virtual Machines* (VM), each of which is an isolated execution environment that can be forked instantly from the base operating environment. OS-level virtualization is widely used to improve security, manageability and availability in today's complex software environment. A main challenge with OS-level virtualization is how to achieve strong isolation among VMs that share a common base OS. In this dissertation we study major OS components on Windows NT kernel and present a *Feather-weight Virtual Machine* (FVM), an OS-level virtualization implementation on Windows platform. The key idea behind FVM is access redirection and copy-on-write, which allow each VM to read from the base environment but write into the VM's private workspace. In addition, we identify various communication interfaces and confine them in the scope of each individual VM. We demonstrate how to accomplish these tasks to isolate different VMs and evaluate FVM's performance overhead and scalability.

We present five applications on the FVM framework: secure mobile code execution service, vulnerability assessment support engine, scalable web site testing, shared binary service, and distributed display-only file server. To prevent malicious mobile code from compromising desktop's integrity, we confine the execution of untrusted content inside a VM. To isolate adverse side effects on network service during vulnerability scans, we clone the service to be scanned into a VM and invoke vulnerability scanners on the virtualized service. To identify malicious web sites that exploit browser vulnerabilities, we use a web crawler to access untrusted sites, render their pages with browsers running in VMs, and monitor their execution behaviors. To allow Windows desktop to share binaries that are centrally stored, managed and patched, we launch shared binaries in a VM whose runtime environment is imported from a central binary server. To protect confidential files in a file server against information theft, we ensure that file viewing/editing tools run in a client VM, which grants file content display but prevents file content from being saved to the client machine. In this dissertation, we show how to customize the generic FVM framework to accommodate the needs of these applications.

Date: November 21, 2007

Time: 02:15 pm

Place: Computer Science, Room 1310

Program: Computer Science

Dissertation Advisor: Tzi-cker Chiueh