



**Calhoun: The NPS Institutional Archive**  
**DSpace Repository**

---

Faculty and Researchers

Faculty and Researchers' Publications

---

2006

## VMM - Virtual Machine Monitors (archived)

---

<http://hdl.handle.net/10945/49122>

---

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

*Downloaded from NPS Archive: Calhoun*



Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

**Dudley Knox Library / Naval Postgraduate School**  
**411 Dyer Road / 1 University Circle**  
**Monterey, California USA 93943**

<http://www.nps.edu/library>



## Introduction

## Research

Projects  
Laboratories  
Sponsors

## Academics

## Scholarships

## Publications

## News and Events

## Employment

## Contact

## The Center for Information Systems Security Studies and Research

RESEARCH: Projects - VMM

### Virtual Machine Monitors

This research addresses the problem of implementing secure Virtual Machine Monitors (VMM) on the Intel Pentium architecture. A VMM allows multiple operating systems to run concurrently under virtual machines on a single workstation. High-assurance VMMs could allow complete isolation of, or data sharing between, virtual machines according to a security policy such as a mandatory secrecy policy.

The Intel architecture was mapped to a set of hardware requirements for VMMs. It was found that the Intel architecture was not virtualizable. However, several techniques are presented that allow the Intel architecture to support a "virtual VMM". A Commercial virtual VMM was studied and found to be unable to support secure VMMs. Therefore; a foundation upon which a secure VMM could be built for the Intel Pentium architecture is presented.

A secure VMM for the Intel architecture offers several benefits. First, PC users could run familiar Commercial of the Shelf (COTS) operating systems and applications. Finally, secure VMMs could save the DoD millions of dollars by eliminating the need for separate systems when both high assurance and COTS operating systems and applications are required.

#### What is a Virtual Machine Monitor?

- A program that creates efficient, isolated duplicates of the real machine
- Mediates these duplicates (virtual machines) and actual computer system resources

#### Motivation

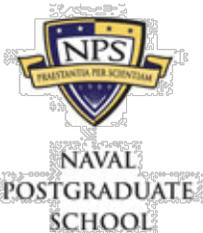
- High assurance VMMs can be used to separate mandatory security classes

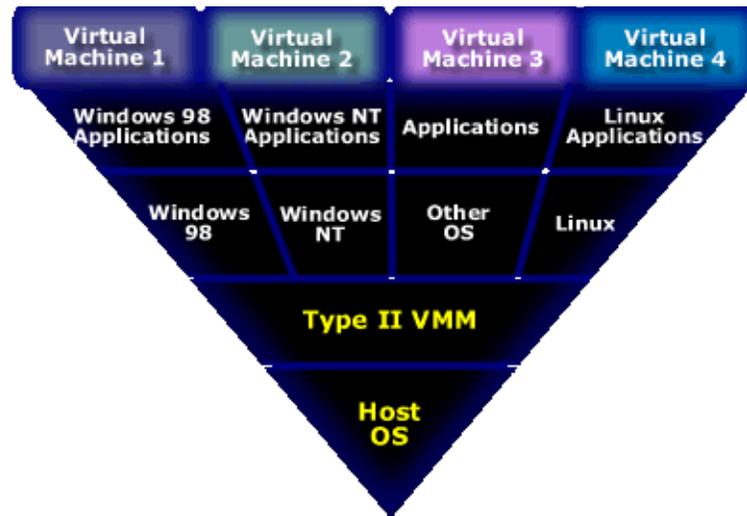
#### Problem

- Can a secure virtual machine monitor be designed for the Intel architecture?

#### Types of Virtual Machine Monitors

- Type I: A VMM that runs on a bare machine
- Type II: A VMM that runs as an application on a host operation system





### VMM Hardware Requirements

- Rough equivalence of a non-privileged instruction execution is user and privileged mode: applies to a large subset of non-privileged instructions
- Protection of real system and other VMs from the active VM: examples are a protection system or address translation system
- Method of automatically signaling VMM when a VM attempts to execute a sensitive instruction : VMM must be able to simulate the instruction

### Sensitive instructions include those that:

- Attempt to change or reference the mode of the VM or state of the machine
- Reference the storage protection system, memory system, or address relocation system
- Look at or change sensitive registers
- Perform I/O

### Issues

**Claim:** "VMware Virtual Platform is both a virtual machine monitor running directly on the hardware and a normal application running on top of the host operating system"

- Intel architecture violates rule 3 of the VMM hardware requirements because:
- Actual machine state is accessible in user mode
- Instructions exist that modify the state of x86 CPUs that can not be trapped

**Claim:** "Even rogue application or operating system is confined to the VMware Virtual Platform sandbox"

*VMware Virtual Platform can not handle documented/undefined features of the PC hardware*

### VMware: A Type II VMM?

- VMware Virtual Platform is "a thin software layer that allows multiple operating system environments to run concurrently using the same hardware resources"

### VMware provides:

- Transparent multiplexing of all hardware resources into multiple virtual machines
- Fault isolation and containment
- File and device sharing via multiple VM-unique network addresses
- Encapsulation and movement of VMs among different physical machines

**VMware supports:**

- MS-DOS 6
- Windows 3.1
- Windows 95
- Windows NT 4.0
- Linux
- FreeBSD
- Windows 2000
- Solaris 7 Intel Edition

**VMM Team****Past Contributors**

- 2LT Scott Robin, USAF

**Thesis Advisors/Principal Investigators**

- Cynthia Irvine, NPS
- Steven Lipner, MitreTek Systems

Limited Access Areas: [SFS Resources](#) / [CISR Resources](#)

Last Modified 03/2006 / [Home](#) / [Webmaster](#) / [Privacy Policy](#) / [Links](#) / [Search](#) / [Sitemap](#) / [NPS](#)