Virtual Machine Security Analysis
William Enck and Lisa Johansen

CSE 598c - Spring 2006
Area Overview

• Virtual machines are being used for security purposes because of the isolation that they are designed to provide.

• Problem: The possibility for implementation problems exist in every system.

January 7, 2006:

VMWare Workstation: Vulnerability in NAT networking:

“Malicious guest operating systems using the NAT networking feature or local VMWare Workstation users could exploit this vulnerability to execute arbitrary code on the host system with elevated privileges.”
Idea

• Find threats of possible implementation flaws within Xen
  • examine similarities between an operating system and a virtual machine monitor
Syscalls and Hypercalls

- OS processes use syscalls to the kernel for privileged actions
  - These calls can be malicious
- VM domains use hypercalls to the VMM for privileged actions
Goals

- We hope to:
  - Use security threats within OS to examine possible vulnerabilities within Xen
  - Classify security threats that are posed by the different hypercalls in Xen
  - Examine communication between domains and other software running on the machine.