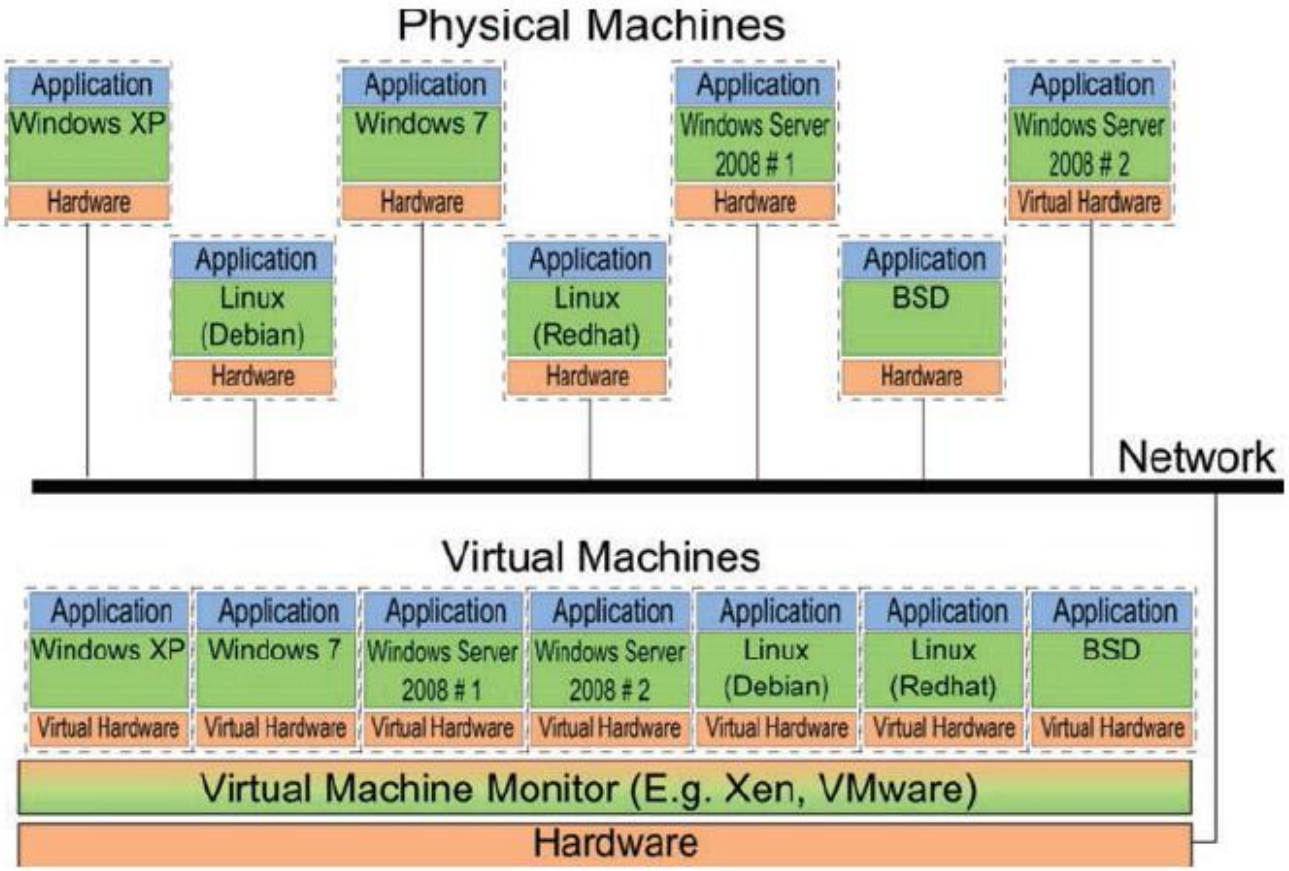
Security Through Virtualization

Tim Peters

Dr. Peterson & Dr. Nico

What is a Virtual Machine Monitor?



Source: Popek, Goldberg. Virtualization: Issues, security threats, and solutions

VMM Security Issues

- Detection and Transparency
  - The VMM is detected from the VM
- Control Breaches / Privilege Escalation
  - Information leakage
  - VM Escape
- Compromise
  - Denial-of-Service
  - Alteration

Why Use a VMM?

- Management
  - Shares expensive hardware
  - Decouples hardware and operating systems
- Security
  - Has a smaller attack surface than a typical OS
    - Massively reduced code size
  - Can observe everything about guest OS
    - Intrusion detection systems
    - Malware analysis
    - Software testing/debugging