When Virtual Is Better Than Real

Peter M. Chen, Brian D. Noble
Advantages

• provide services below the most code running on the system
• need not trust the OS
• useful for enhancing security and mobility
• functionally equivalent to modifying the physical machine, but way easier
• fast connection to „another computer“
Challenges

- virtualization and its overhead
- semantic gap, consistency problems
- leaky abstraction
  - real-time guarantees within the OS?
  - direct hardware access (think GPUs)
Secure Logging

- logging in OS: easily turned off by attacker
- paper proposes checkpointing approach
  - replay attacks to analyze them
- reduce data to log by trusting other machines
- seems only applicable for the datacenter
Intrusion Detection

- detect and prevent attacks by observing the OS from the outside
- cannot detect today’s web-based attacks
- adds another attack vector
Migration

- motivated as a non-server use-case here
- virtual machines travel with the user
- trust issue with encrypted data
- What about the data on the disk?
- What’s wrong with notebooks?
Alternative

- implement such services in the OS
- it has all the required knowledge
- it is just one level of abstraction away from the hardware
- can use all features offered by the hardware
- minimal design
Security

- 7.11.2008: Bug in VMware’s CPU emulation grants elevated privileges
- 31.10.2008: VMware patches ESX server to close security holes
- 6.10.2008: VMware patches various vulnerabilities
- 19.9.2008: security update for VMware ESX
Be Afraid

- Hardware
- Cloud Computing Layer
  - Applications
  - Webbrowser
  - Managed Runtime
  - Virtual Machine
What I do believe in

- virtualization as an application on top of the OS
- hosted VMM architecture
- running the occasional windows app
- nice for developers
- virtualization only as needed
What I do not believe in

- virtualization to solve problems of the OS
- virtualization purely for isolation
  - that’s what OSes and address spaces were invented for
- virtualization as an additional layer for everything
  - brings more complexity
Discussion

• Is the recent hype of virtualization primarily an artifact of the flaws in Windows?
• Will the trend of adding layers ultimately make the systems unmanageable?
• Or should we give up on transparency?
• Will VMMs inherit today’s OS problems? (monolithic, insecure, hard to restructure)
• Name one use-case that requires pervasive virtualization on mobile phones.