PURDUE UNIVERSITY

Virtually Secure or Securely Virtual?

Panel, CERIAS Symposium March 18, 2008

Pascal Meunier, Ph.D., M.Sc., CISSP
Purdue University CERIAS

CERIAS®

Virtualization! What Is It Good For?

- Availability
  - Restart a crashed OS or server
- Scalability
  - More or different images as demand changes
- Isolation and compartmentalization
- Better hardware utilization
- Hardware abstraction for OSes
- Support legacy platforms

Operating System Duties

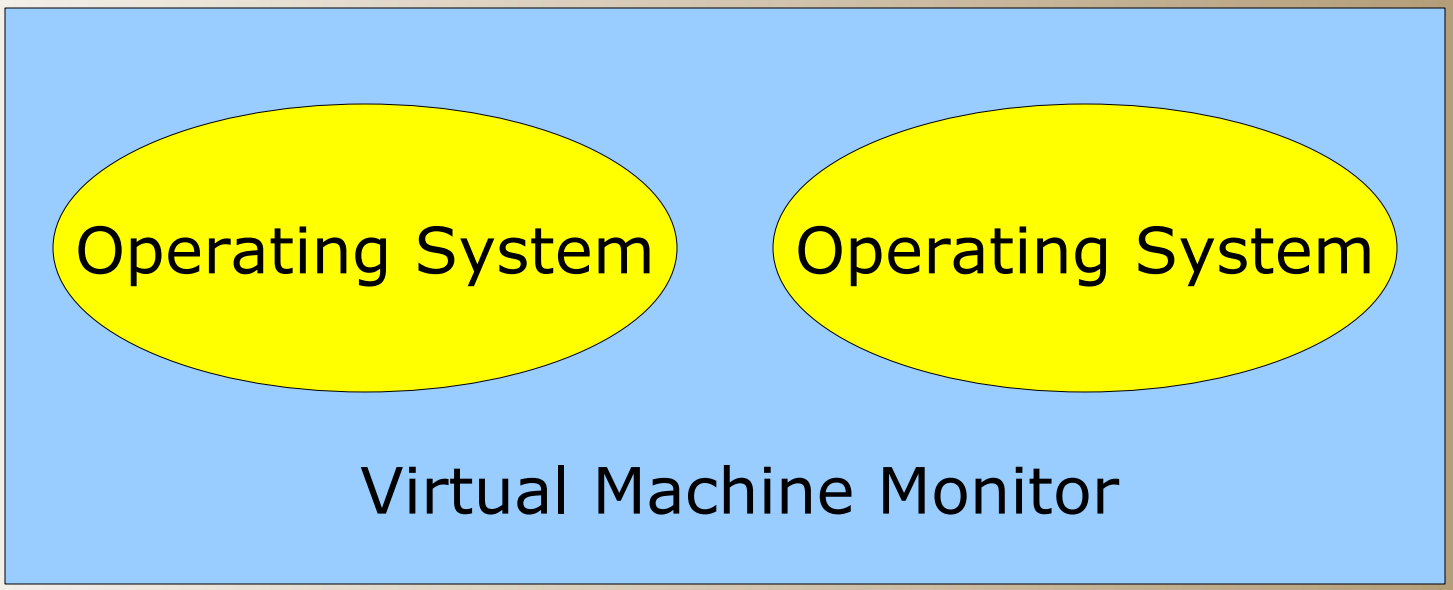
- Availability
  - Restart crashed applications
- Scalability
  - More or different processes as demand changes
- Isolation and compartmentalization
  - Protected memory
  - Accounts, capabilities
- Better hardware utilization
- Hardware abstraction for applications

Virtualization Takes Over Roles of Operating Systems

- Implicit admission that OSes have failed us.
  - Lack of security, reliability, ease of maintenance
    - Drivers
    - Complexity
      - Look at hardening guides
      - SCAP, XCCDF
      - Huge monokernels
    - Intensive, stressful, inefficient maintenance
      - Copying entire VM images is more efficient than copying a binary (?!)
      - Unending vulnerability advisories and patches

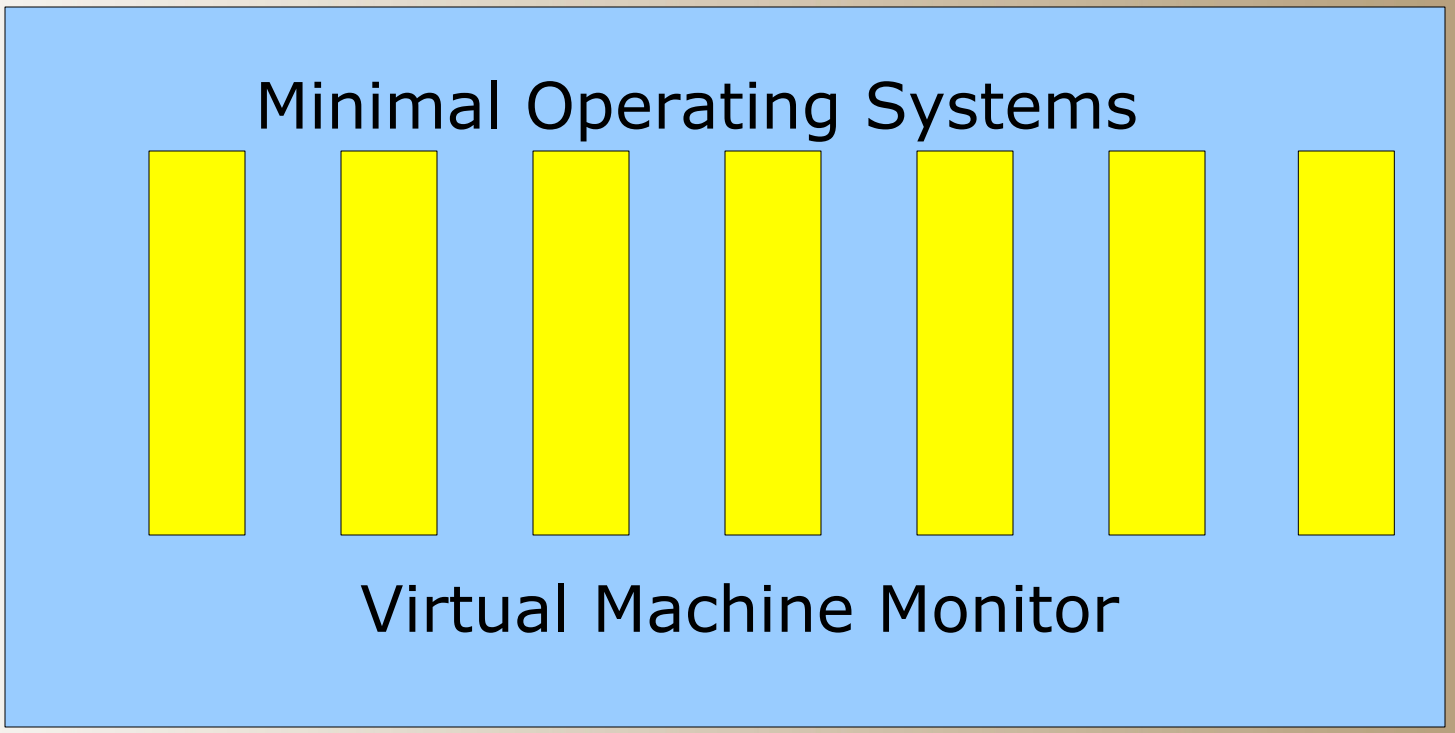
Dysfunctional Approach

- Boats are sinking
  - Put them inside another, bigger boat
    - Get bloat



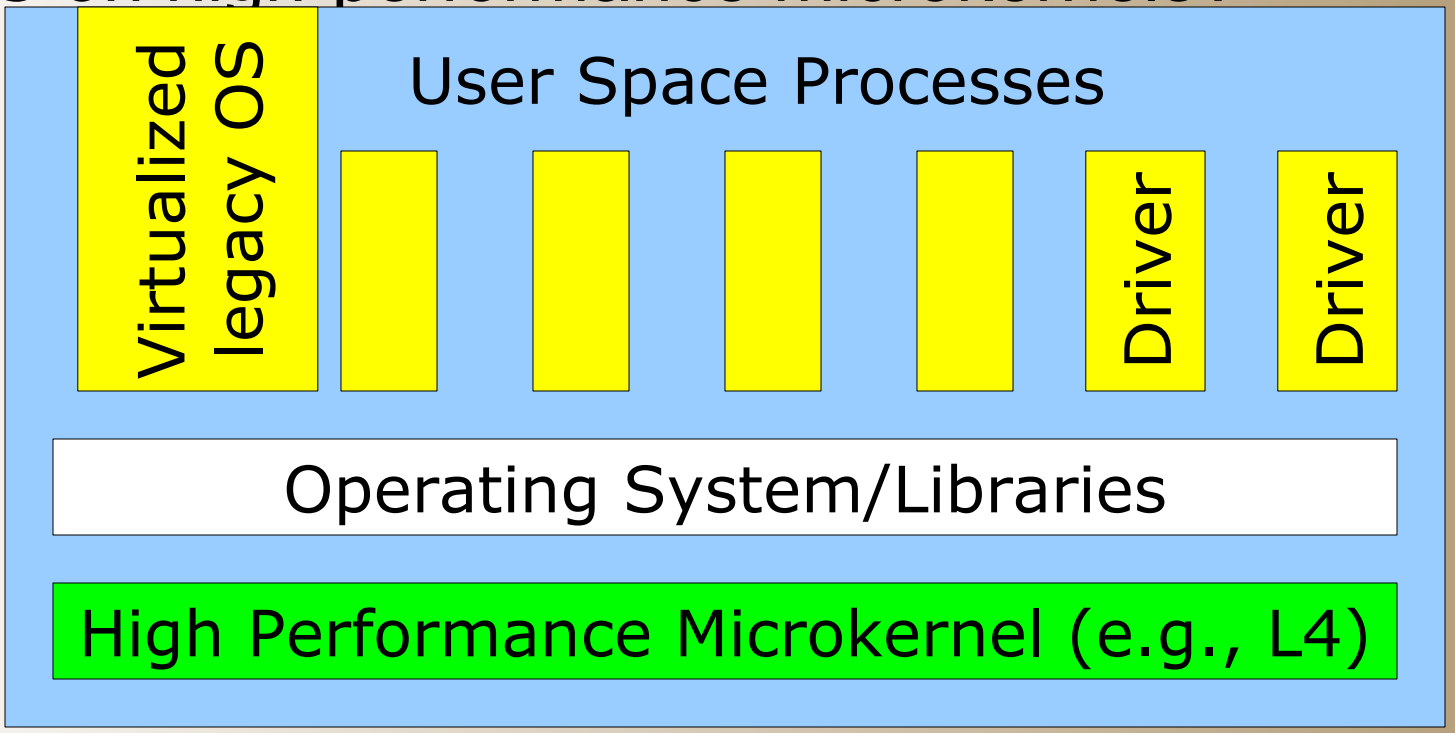
How can we make things better?

- Option A: Rebuild operating systems without the functionality provided by VMMs, with fewer bugs



How can we make things better?

- Option B: VMMs are similar to microkernels. As we're paying the price anyway, why not build an OS on high-performance microkernels?

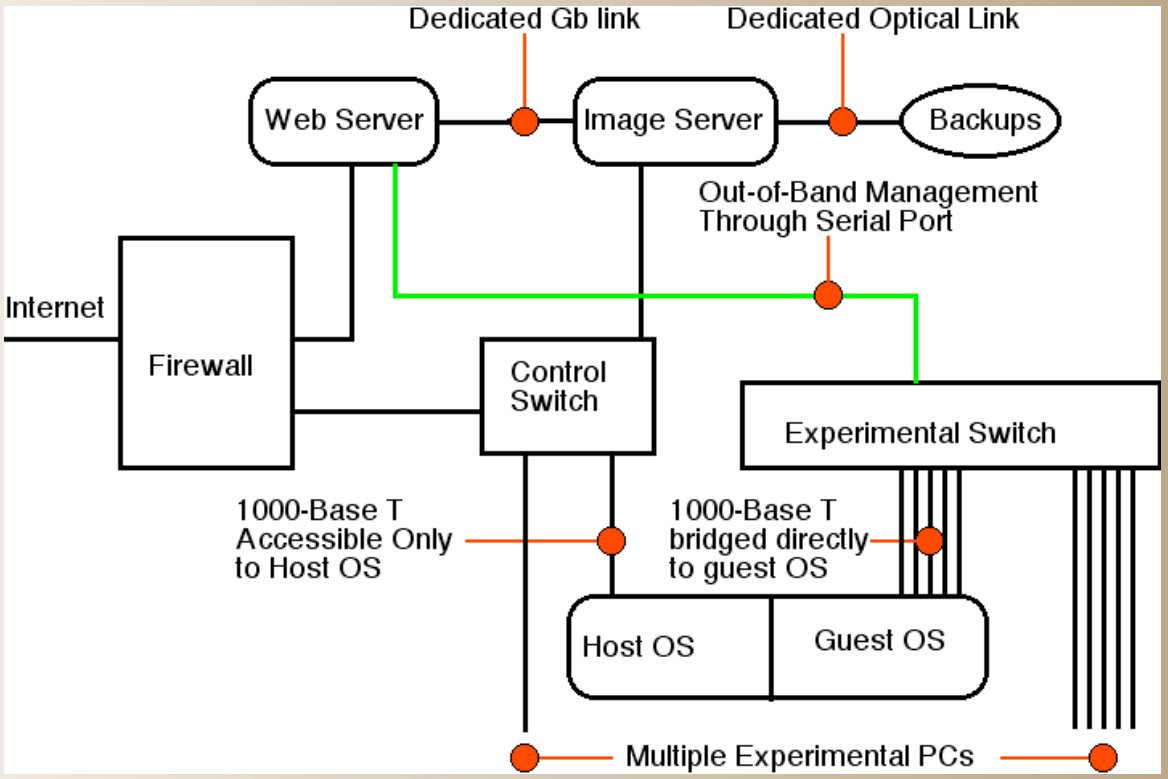


How can we make things better?

- Option C: Install applications by compiling an intermediate form, using formal verification methods, and run that on top of a microkernel
  - e.g., Microsoft's Singularity
    - Software isolated processes

ReAssure: A Virtualized Testbed for Next Generation OSes

- http://projects.cerias.purdue.edu/reassure/



References

- Heiser G et al. (2007) Towards trustworthy computing systems: Taking microkernels to the next level. ACM Operating Systems Review, 41
- Tanenbaum AS, Herder JN and Bos H (2006) Can we make operating systems reliable and secure? Computer, 39