Hardware Assisted OS Virtualization

Bhushan Jain, Donald E. Porter

{bpjain, porter} @cs.stonybrook.edu

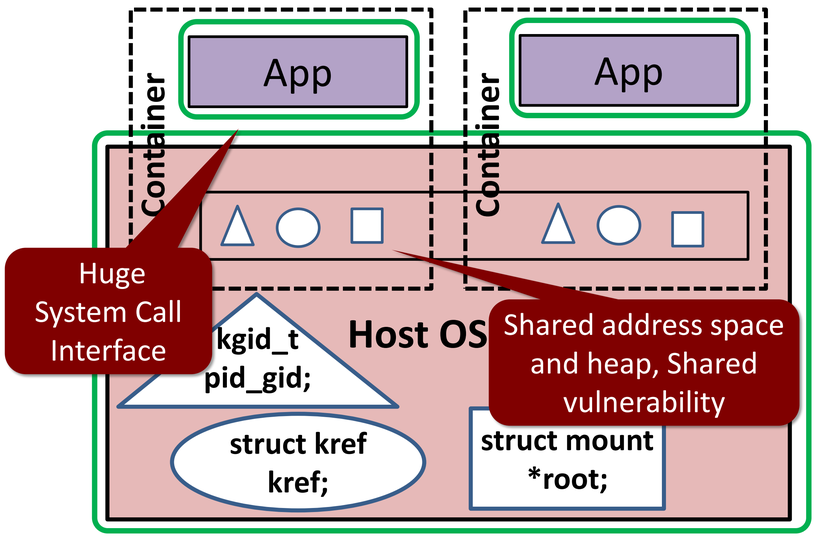
Stony Brook University

OSCAR Operating Systems, Security, Concurrency and Architecture Research

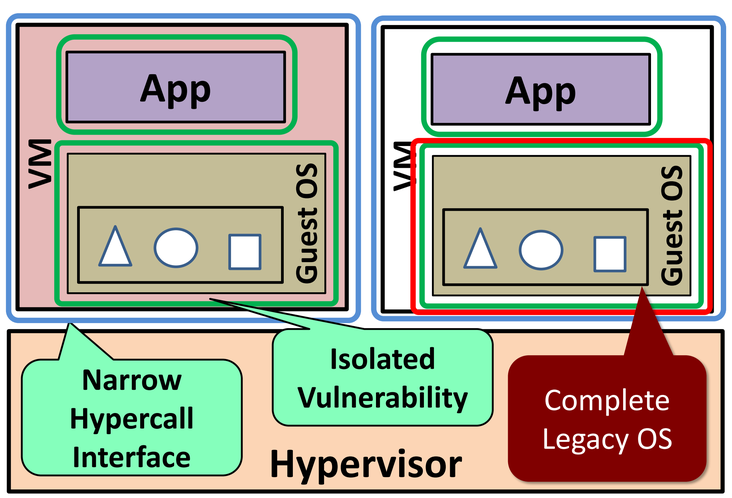
Problem

VMs and Containers make trade-offs between security and overheads

- Containers are a poor security isolation layer
  - Trade efficiency for security risks
  - Shared host OS but shared vulnerability



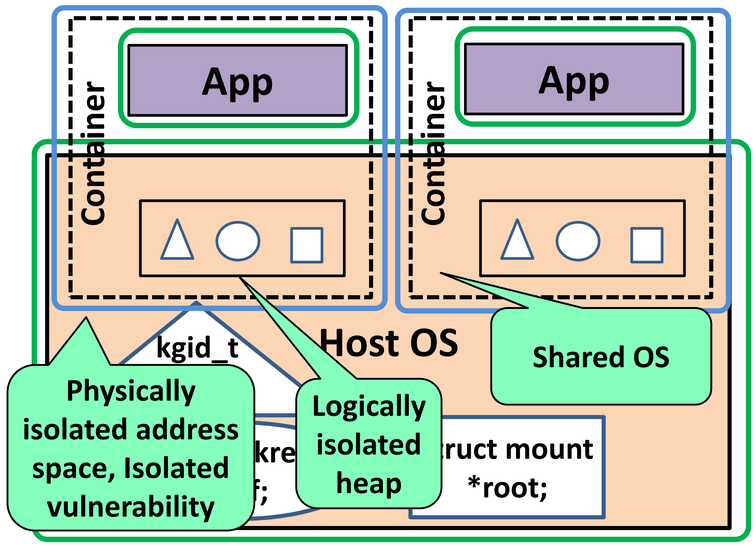
- VMs necessary for security isolation
  - Trade functionality, security for high overhead
  - Isolated vulnerability but new OS instance



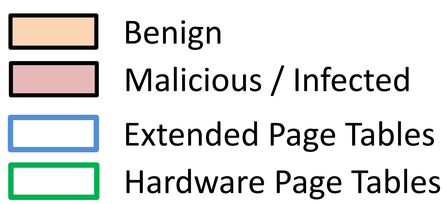
Our Solution

Goal : Get both security and low overheads

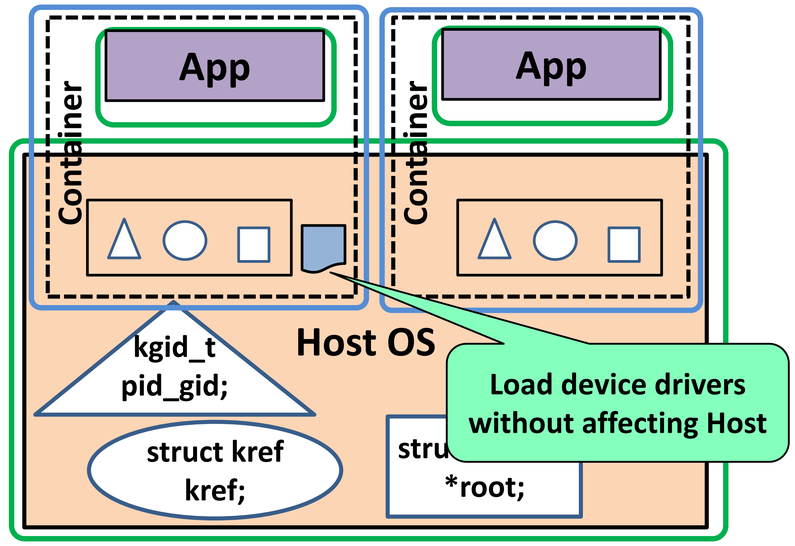
- Create heap's physical and logical isolation



- Isolate Container specific kernel objects
  - Repurpose hardware designed for VMs
  - Redesign the OS to be EPT protection friendly
- Share host OS to keep overheads low
  - Map OS copy-on-write in Container context
  - Map Container objects only in its context
  - Container context OS handles safe interrupts



Our Vision



- Functionality & Security equivalent to VM
  - Insert kernel modules in a Container
  - Contain a rootkit attack
- Overheads equivalent to Containers
  - Small startup time and memory footprint

Conclusion

- VM-like hardware isolation for Containers
  - Make Container a first class kernel object
- Best of both VMs and Containers
  - Efficiency and low overhead of Containers
  - Security and functionality of VMs
- Work in progress
  - Can provide exciting features for Containers