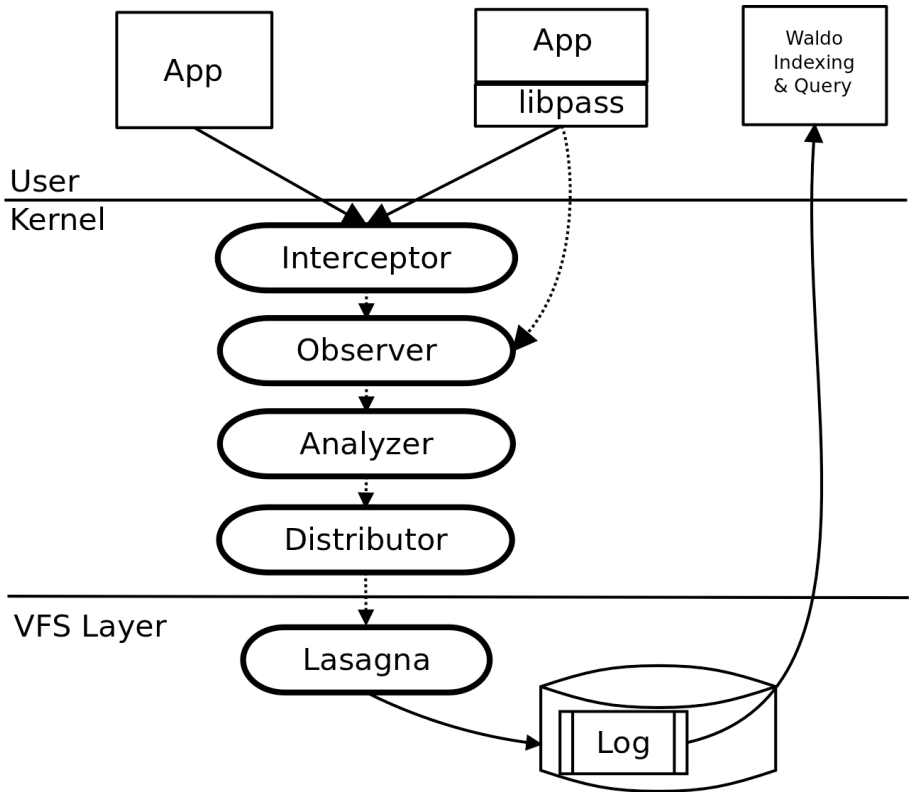
Collecting Provenance via the Xen Hypervisor

Peter Macko, Marc Chiarini, Margo Seltzer
Harvard SEAS

TaPP '11

What We're Doing

- Provenance-Aware Storage Systems Group
- Modified Linux Kernel
- Captures rich relationships between files, pipes, processes.

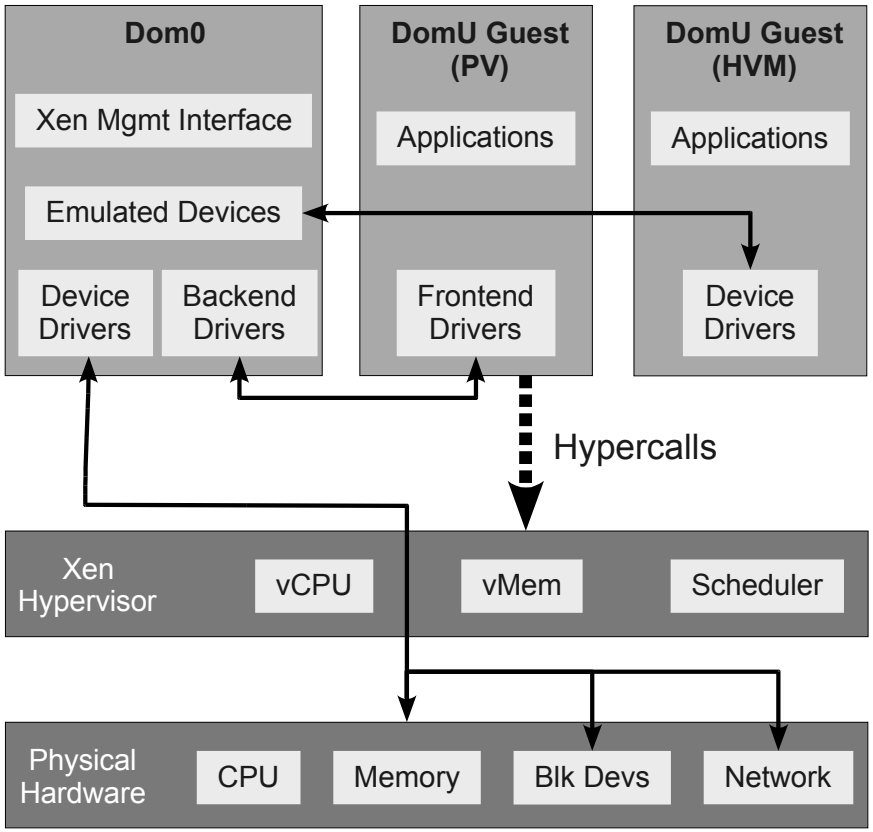


A Problem

- Maintaining the provenance *interceptor* is unsustainable.
- Need a way of collecting system-level provenance that is:
  - easier to maintain.
  - more portable.
  - more likely to be adopted.
    - Helps the development effort (find bugs, etc)!

Our Approach

- Collect the same kind of system-level provenance from virtual machines running under the Xen Hypervisor.



Challenges

- Potential performance impact?
- Where to store provenance?
- How to extract provenance that is not available via system call from guest memory?
- How to extend to other guest OSes?

Questions?

Prototype will be available in late summer 2011.

http://www.eecs.harvard.edu/syrah/pass/

chiarini@seas.harvard.edu