Virtual machine monitors & Secure operation

- **Implementing an Untrusted Operating System on Trusted Hardware** David Lie, Chandramohan A. Thekkath, Mark Horowitz, SOSP 2003
- **Terra: A Virtual-Machine Based Platform for Trusted Computing** Tal Garfinkel, Ben Pfaff, Jim Chow, Mendel Rosenblum, Dan Boneh, SOSP 2003

Related technologies

- Main frames offered virtual machine abstraction
- On a single machine, behaves like many individual, dedicated machines by virtualizing the underlying resources
  - E.g. vmware, jail abstraction in FreeBSD
- Hosting centers: Runs many different customers on the same nodes. Isolate each client from each other while allocating more resources as the need occurs
  - Adaptive infrastructure (HP), autonomous computing (IBM), N1 (Sun) …

XOMOS

- Trusted processor, untrusted OS, external memory
- Use compartments to isolate
- Encryption (with keys inside the processor itself) to let processor access code/data
- Solve issues where the OS does not know the contents for traditional OS operations (restoring registers, paging, process creation, shared libraries etc.)

Terra

- VM based approach
  - attestation: Certificate chains to “prove” whether we can trust the current software was not compromised
  - Root secure: Even root cannot break basic privacy and isolation guarantees
  - Trusted path: Provide trusted path from the user to the application