Verification of a Separation Kernel

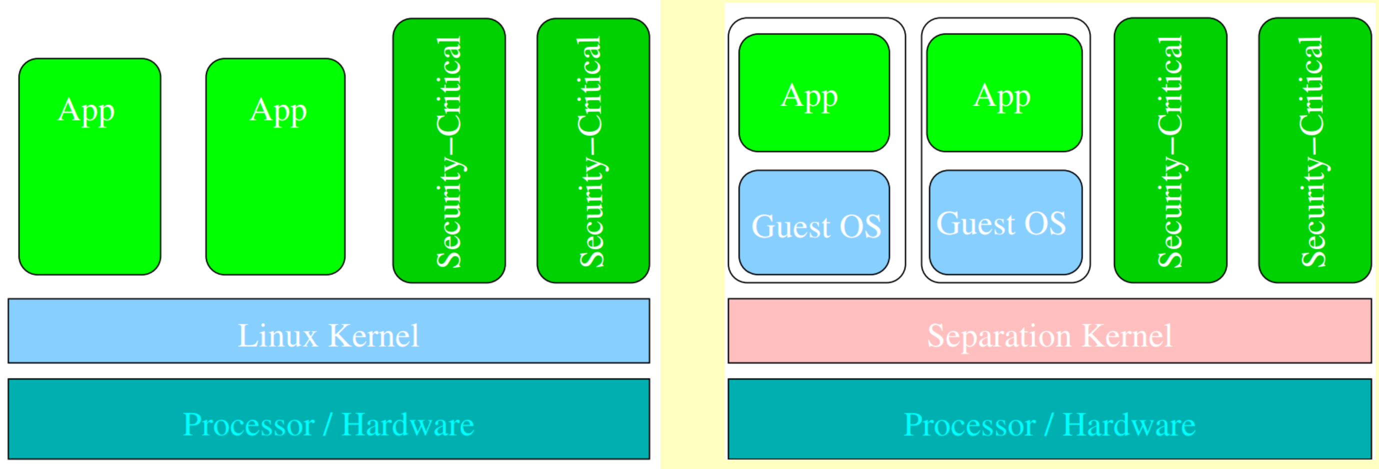
Inzemamul Haque, Habeeb P, Deepak D'Souza

Indian Institute of Science, Bangalore, INDIA

About Separation Kernel

- Separation kernel creates partitions on a machine and ensures no implicit communication.
- Similar to a hypervisor except it provides communication channels between partitions.
- Each partition runs as if it is running on a standalone machine.
- Used in avionics and military systems.

Separation Kernel vs. Normal OS

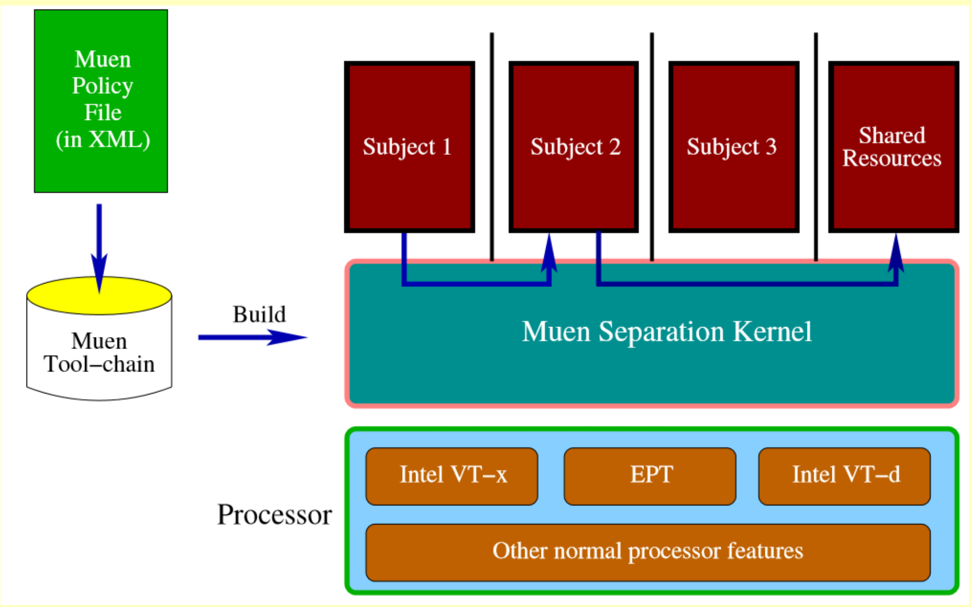


Problem Statement

- To formally specify and prove the correctness of a modern separation kernel like Muen.
- To prove that a separation kernel is obeying the given policy.
- Chose 'Muen' as an exemplar of a modern separation kernel which uses hardware virtualization support.

Muen Separation Kernel

- A separation kernel for Intel x86 platform.
- Written in SPARK, a language based on Ada



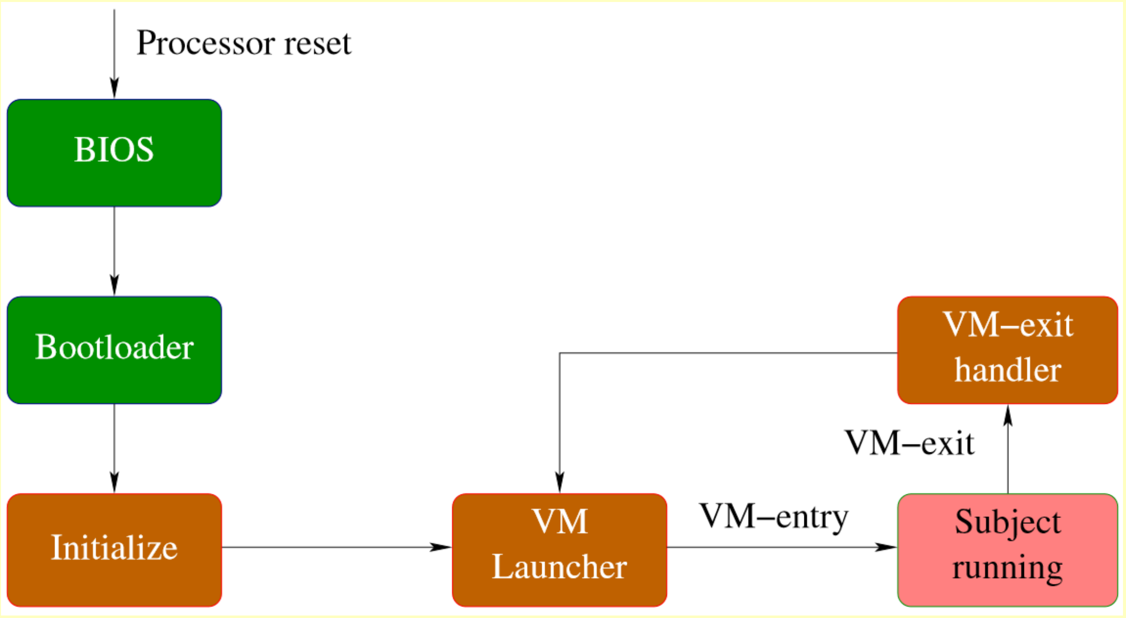


Fig: Overview of working of Muen separation kernel

Approach to Verification

- Define an abstract model which captures the correct behaviour of the separation kernel.
- To show that for every execution in the concrete there exists a corresponding execution in the abstract.
- Inductive proof by defining an abstraction relation.

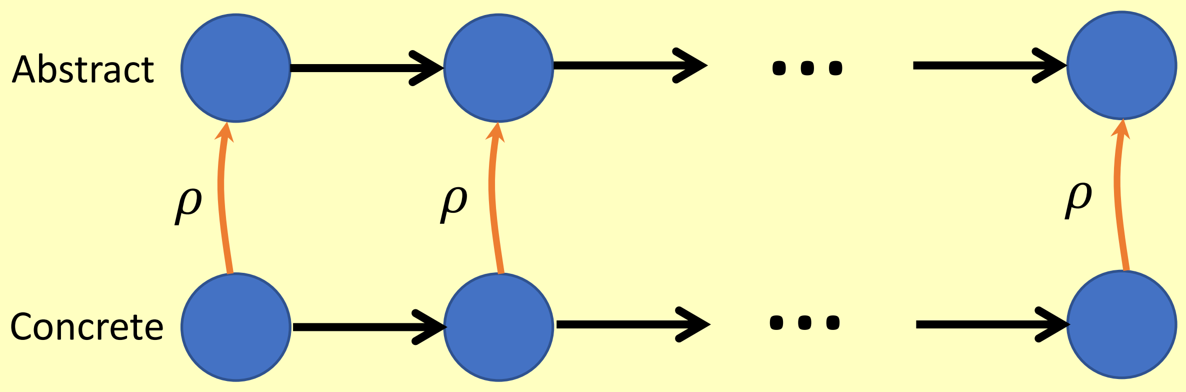


Fig: Correctness condition – For every concrete execution there is a corresponding abstract execution

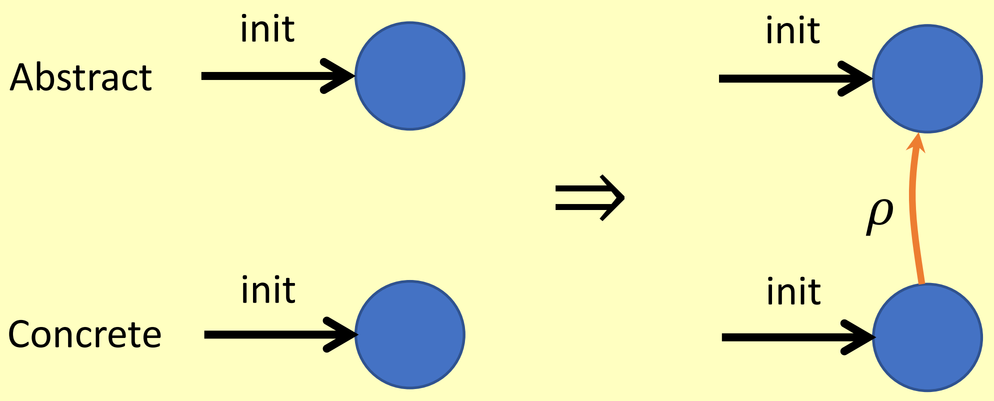


Fig: Inductive proof – Initial step

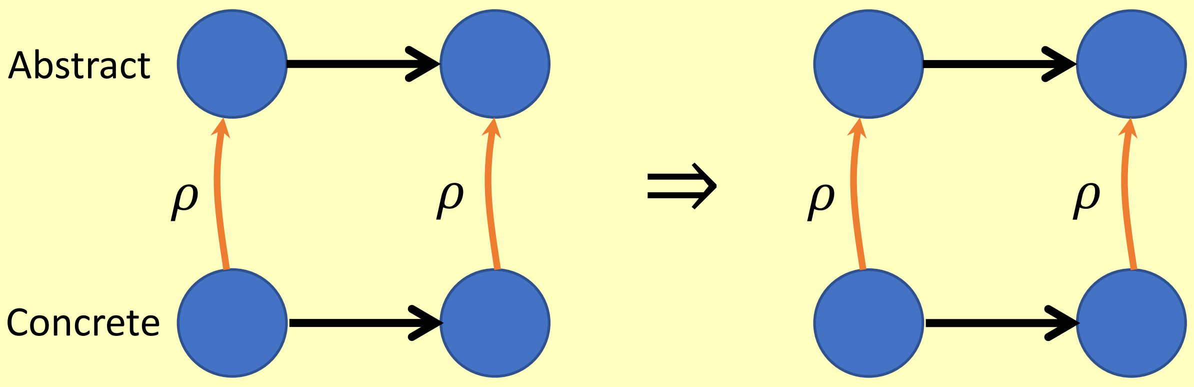


Fig: Inductive proof – Induction step

Experiments

- Carried out a small exercise to verify virtual memory translator
- Translating assembly code in Ada to verify it using AdaCore SPARK
- Working on a fixed policy

References

- John Rushby, Design and verification of secure systems, 1981
- Muen Report - https://muen.codelabs.ch/muen-report.pdf