OSMosis: Modeling & Building OS Isolation

Sidhartha Agrawal, Shaurya Patel, Reto Achermann, Margo Seltzer

Problem

- Modern systems provide myriad **isolation mechanisms**, but it is **difficult to identify** precisely **which software state is shared** between two tasks.
- This **lack of transparency** leads to attacks and opaque performance/security tradeoffs.
- Every new mechanism is a new implementation

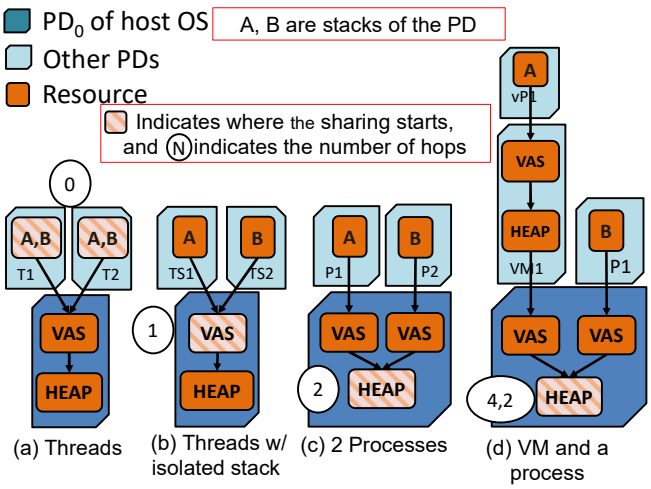
Our Approach

- **Develop a model** to formally describe state sharing.
- **Query the model** to get insights about the extent of sharing between different tasks.
- **Quantify** the degree of isolation.
- **Build a Framework** that creates isolation mechanisms based on the model.

Isolation Model

- Every task is a Protection Domain.
- Every Protection Domain has access to Resources.
  - Resource can be Virtual or Physical.
  - Resource Relation is the dependency relation between resources (→)

Degrees of Isolation



- The higher the number of hops at which sharing happens, the higher the isolation
- As the number of hops to the same resource differs for different PDs, the ability to corrupt the resource also differs.
- Captures degrees of isolation

Querying the Model

Once the system is captured using a model it is easy to query.

- Find all the resources used by a PD
  - Transitive closure of the resource relation
- Find the resources used by the PD at ***N*** hops
  - Traverse the Resource Relation for ***N*** hops
- Find the number of hops at which sharing begins
  - First common resource for the two PDs
- Find if a PD is sufficiently isolated
  - For a given number of hops, check that the set of common resources is empty

Framework

- All resources are capabilities
- Every resource returns a set of resource relations

What else does this enable us to do?

- ✓**Viewing isolation as a *spectrum***
- ✓**Precisely state the extent of sharing**
- ✓**Explore the design space of mechanisms**
- ✓**Build arbitrary isolation mechanisms**

What's next?

- Find a performant way to trace resource relations
- Protype the model and framework on seL4

Paper