Tyche: Rethinking Trust in Systems

Swiss Joint Research Centre, Spring 2024

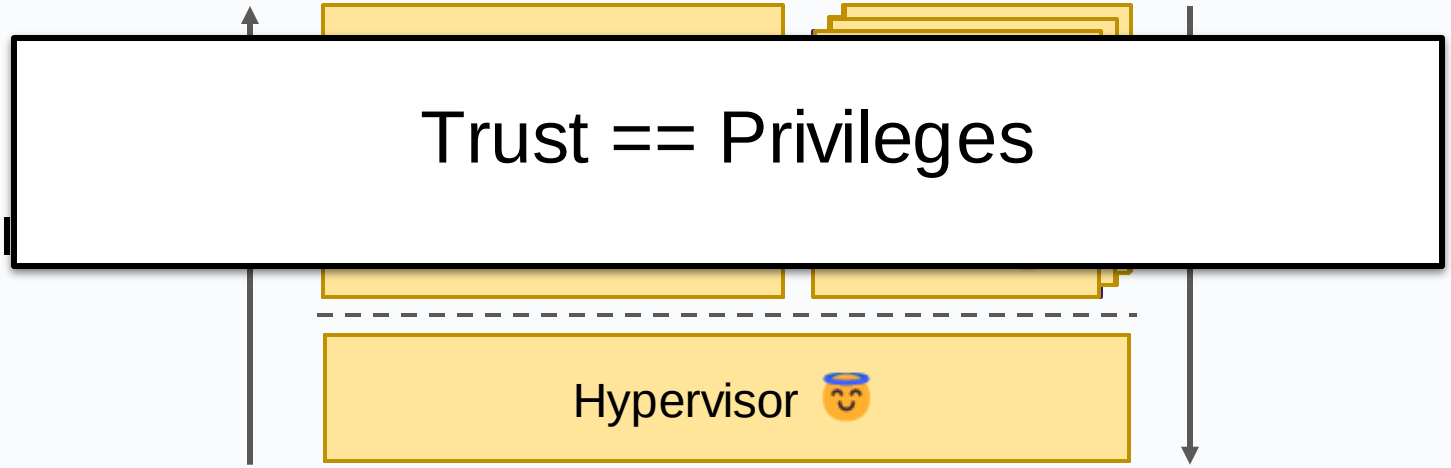
Charly Castes, Adrien Ghosn, Neelu S. Kalani, Yuchen Qian, Edouard Bugnion

First principle approach for creating trust in systems

- Isolation
- Attestation
- Compatibility with existing software
- Compatibility with existing hardware

Software Isolation

Despite growing complexity, software still rely on the privilege hierarchy



Decoupling Trust and Privileges

Other approaches to isolation:

Compartmentalization **Confidential Computing**

Tied to privilege levels

Do not compose

A Zoo of Mechanisms

On Intel x86:

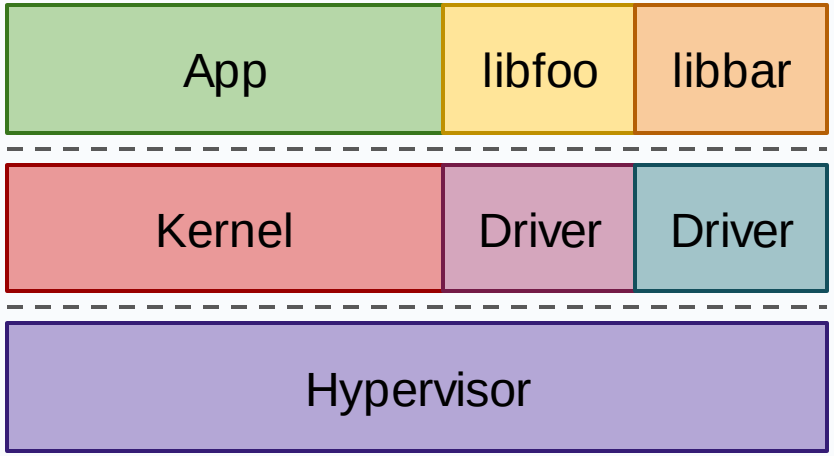
Confidential Process ⟶ SGX

Proliferation of mechanisms to handle specific use cases

Kernel Compartment ⟶ VT-x

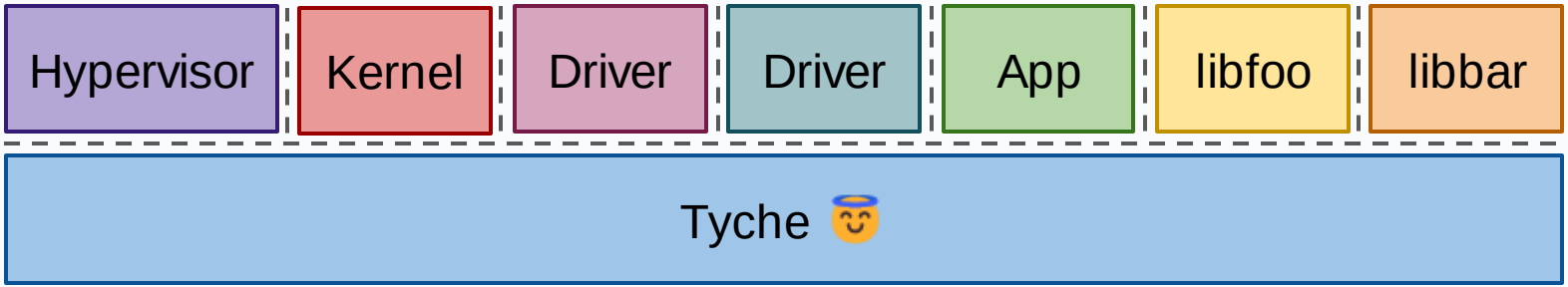
Abolishing the Hierarchy

Let’s tackle the root of the problem…



Abolishing the Hierarchy

and **Abolish the Hierarchy**



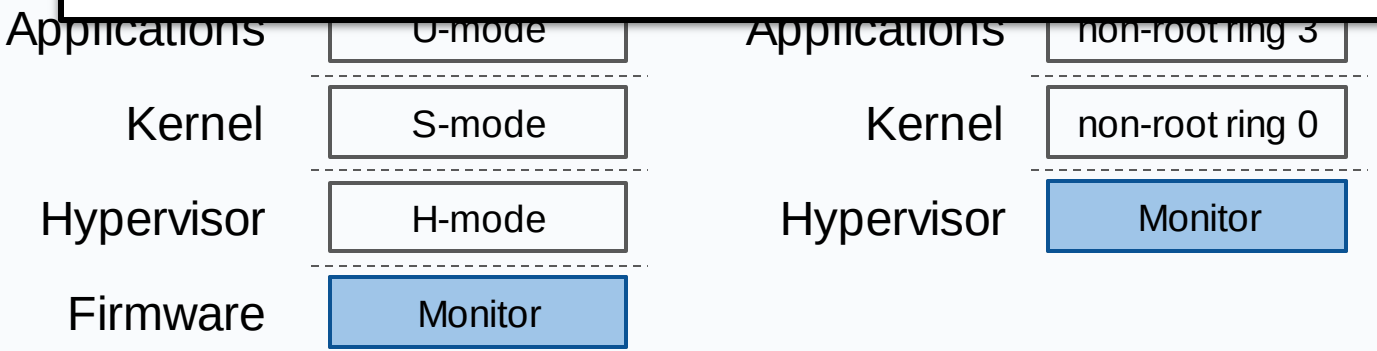
Tyche

A design for restoring trust in systems

A New Kind of Security Monitor

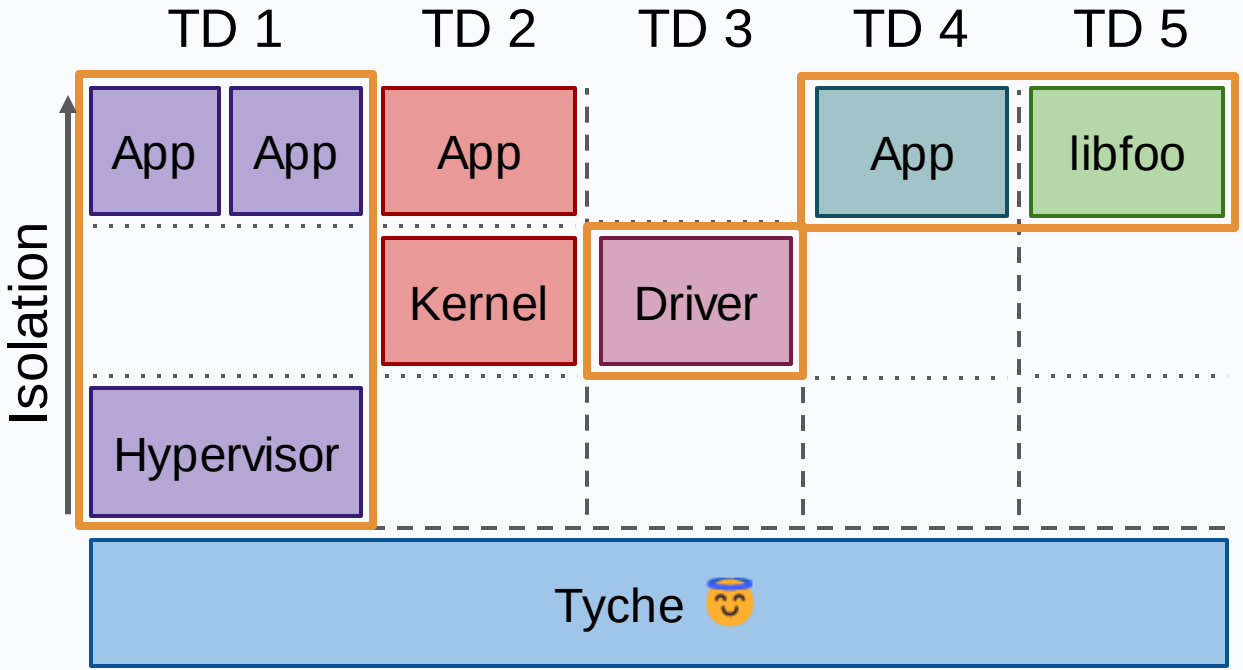
Executes as a **security monitor**, below existing OS and hypervisors

Tyche can run **unmodified OSes**



Trust Domains

Tyche provides a new **trust domain** abstraction

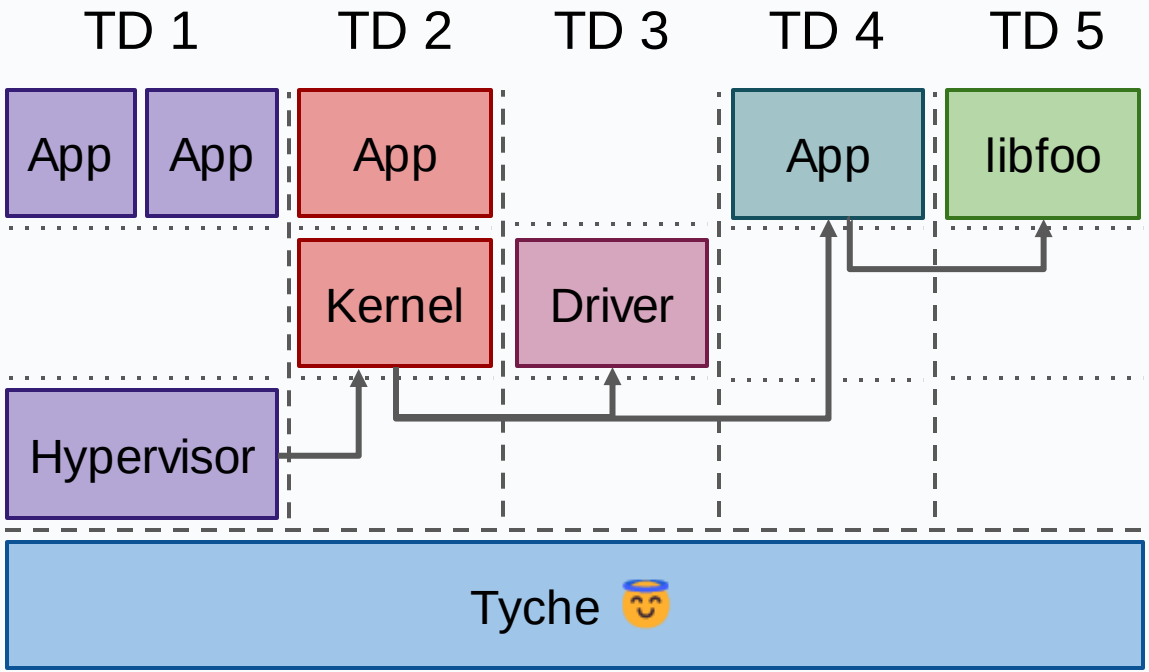


Independent from systems abstractions

Permissions are configured per trust domain

Trust Domains

Tyche provides a new **trust domain** abstraction



There is still a **management hierarchy**

But isolation is enforced by the monitor

Capabilities

On Tyche we use **capabilities** to configure resources

Capabilities for:

- Memory regions
- Cores
- I/O Devices
- Trust Domains

Tyche supports **compartments**, **enclaves**, **confidential VMs,** and **hardware partitioning**

Controlled Sharing

Isolation is about selectively sharing resources

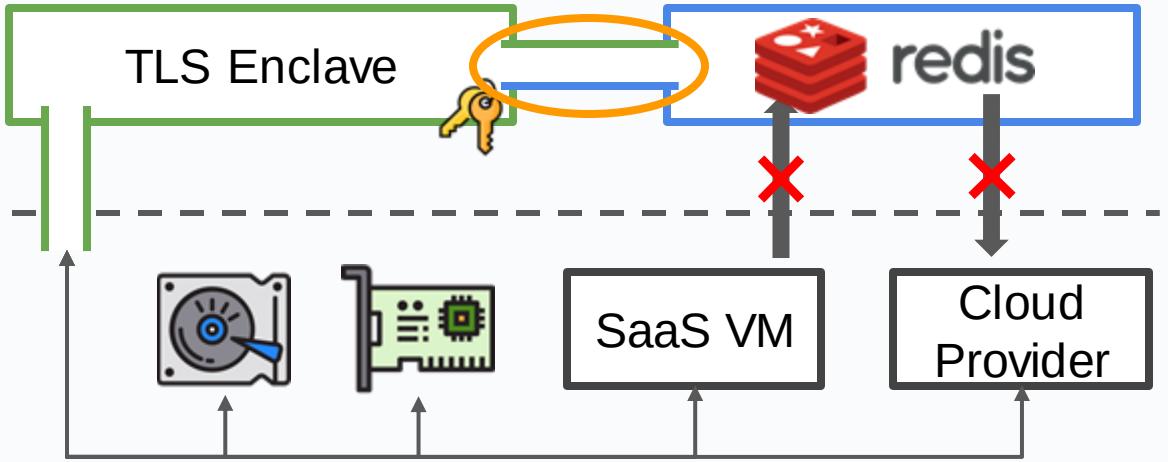
Controlled Sharing

Isolation is not about preventing access to resources

It is about controlling **which resources** are shared, and **with whom**

Example: Confidential SaaS

Confidential data processing through an untrusted SaaS application

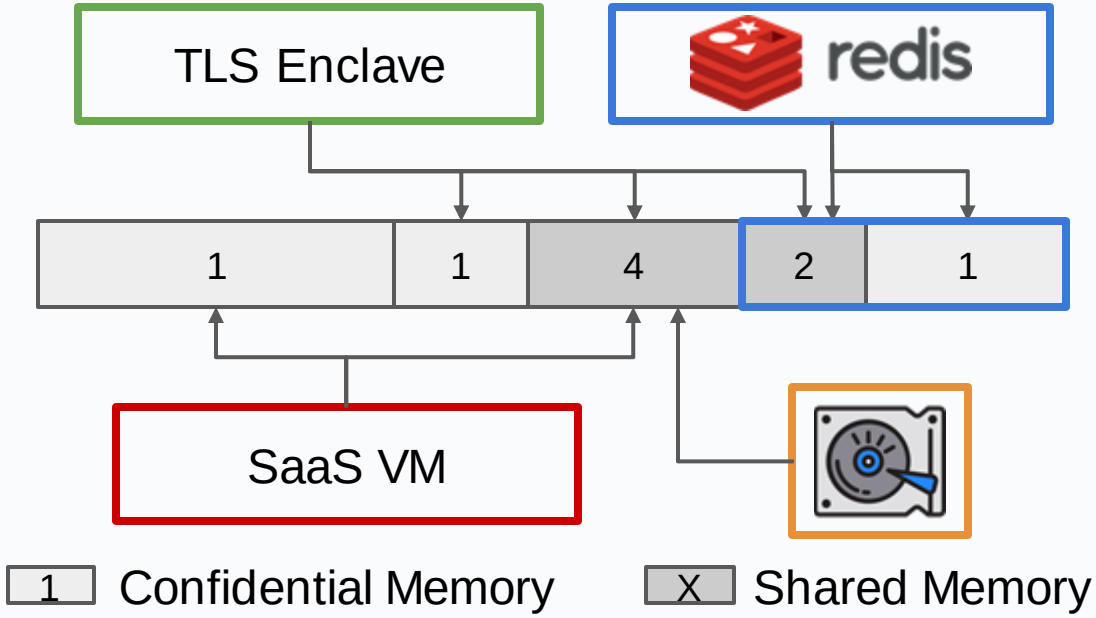


Software needs oversight over sharing

Sharing should be part of the attestation

Sharing on Tyche

Tyche provides a **global view of the system's resources**



Exposes reference count of resources

Ref-counts are part of the attestation

Summary

We introduced **Tyche**

- **A single root of trust**
- **Flexible isolation for all software**
- **Controlled sharing**

Design published at HotOS'23, upcoming full system submission