Access Control in SPIN

Robert Grimm and Brian N. Bershad
University of Washington, Seattle
SPIN Overview

- Minimal core of trusted services
- Infrastructure for extensions
  - Written in Modula-3
- Extensions interact in two ways
  - Call upon existing services
  - Called by other services
Problem

- Extensions form *one* integral system
- Extensions generally untrusted
- Need a way to express and enforce security policies
Domain and Type Enforcement

- Flexible
- Access modes are explicit
- Allows for controlled change of privilege
- Formalizable
DTE in Extensible Systems

• Subjects
  – Traditionally: processes executing for user
  – In extensible systems
    • Extensions
    • Threads of control

• Two fundamental access modes
  – Execute mode
  – Extend mode
Implementation

• Part of trusted SPIN core
• Access checks performed at
  – Link time
  – Call time (if necessary)
• Mostly transparent to extensions
End-to-End Performance

- Protected Transaction System

- Alpha 3000/400 with HP 1Gbyte disk
Micro-Benchmarks

![Bar chart showing micro-benchmarks for Hot and Cold conditions.](chart.png)

- **Hot** and **Cold** states are compared across different operations:
  - **Null Call** shows minimal cost.
  - **+ Access Check** introduces a notable increase in cost.
  - **+ Domain Transfer** has the highest cost among all operations.

The y-axis represents time in microseconds, ranging from 0 to 10.
Summary

- Extensions in SPIN tightly integrated
- Need to enforce security policies
- DTE a flexible solution with low overhead