Security for Extensible Systems

Robert Grimm and Brian N. Bershad
University of Washington, Seattle
State of the Art
Security Community
Example
Lattice Model
Domain and Type Enforcement

- Flexible
- Access modes are explicit
- Allows for controlled change of privilege
- Formalizable
- Needs some changes
SPIN

- Good platform to explore security issues
- Implementation of DTE mostly transparent
End-to-End Performance

• Protected Transaction System

• Alpha 3000/400 with HP 1 GByte disk
Micro-Benchmarks

![Bar Chart]

- **Micro-Benchmarks**

- **Null Call**
  - Hot: 0 microseconds
  - Cold: 10 microseconds

- **Null Call + Access Check**
  - Hot: 2 microseconds
  - Cold: 8 microseconds

- **Null Call + Domain Transfer**
  - Hot: 4 microseconds
  - Cold: 10 microseconds
Summary

• Need way to express and enforce security policies
• DTE a flexible solution with low overhead
• http://www.cs.washington.edu/research/projects/spin/www/
Domain and Type Enforcement

- Associates subjects and objects with labels
  - *Domain* for subjects
  - *Type* for objects
- Global DTE matrix defines
  - Legal access modes
  - Valid changes of privilege
## Simple Example (continued)

<table>
<thead>
<tr>
<th></th>
<th>Employee</th>
<th>Outsider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal</td>
<td>rw</td>
<td>--</td>
</tr>
<tr>
<td>Marketing</td>
<td>rw</td>
<td>r-</td>
</tr>
</tbody>
</table>