Implementing Protection Domains
in JDK 1.2

Li Gong
Java Security Architect
JavaSoft, Sun Microsystems, Inc.
March, 1998
Outline of Presentation

- Overall security model
- Concept of protection domain
- Tricky details in implementation
  - domain resolution
  - extensibility
  - multi-domain computation
  - performance
- Questions and answers
JDK 1.2 Security Model
## Security Policy in ACL

<table>
<thead>
<tr>
<th>what code</th>
<th>what permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CharlesSchwab applets, signed</td>
<td>read and write /tmp and /home/gong/stock</td>
</tr>
<tr>
<td>CharlesSchwab applets, signed and unsigned</td>
<td>connect and accept bankofaemrican.com</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
Class->Domain->Permissions
Access Control Mechanism
Permission Classes

- Permission
  - AllPermission
  - FilePermission
  - SocketPermission
  - BasicPermission
    - PropertyPermission
    - AWTPermission
      - RuntimePermission
      - SecurityPermission
Permission Relationship

PermissionA.implies(PermissionB) = true?

FilePermission("/tmp/*", "read");

FilePermission("/usr/bin", "execute");

FilePermission("/tmp/x.txt", "read");

SocketPermission("*.sun.com", "accept");
Multi-Domain Computation
Privileged Computation

![Diagram showing execution stack with classes and protection domains]

- SecurityManager: system
- FileInputStream: system
- java.awt.Cursor: system (privileged)
- Bar: domain1

Checking stops at the first privileged domain
Discussion

• Security context inheritance
• Class method inheritance’s impact on security
• Lazy or eager computation
• Performance
Access Control Performance

usecs

0 200 400 600 800 1000 1200 1400 1600

# of domains

* beginPrivileged and endPrivileged add 2 usecs

Li Gong, JavaSoft, March, 1998
JDK 1.2 Security Summary

- Flexible and configurable policy
- Fine-grained access control
- Security for all Java programs
- Security mostly transparent
- Primitives for advanced developers
Security Policy in ACL

grant CodeBase “http://schwab.com”,
    SignedBy “CharlesSchwab” {
        Permission java.io.FilePermission
            “/home/gong/stockbook/*”, “read,write”;
        Permission java.io.FilePermission
            “/tmp/*”, “read,write”;
    };

grant CodeBase “http://schwab.com”,
    SignedBy “*” {
        Permission java.net.SocketPermission
            “bankofamerica.com” “connect,accept”;
    };

Li Gong, JavaSoft, March, 1998