Implementing Protection Domains in JDK 1.2

Li Gong

Java Security Architect

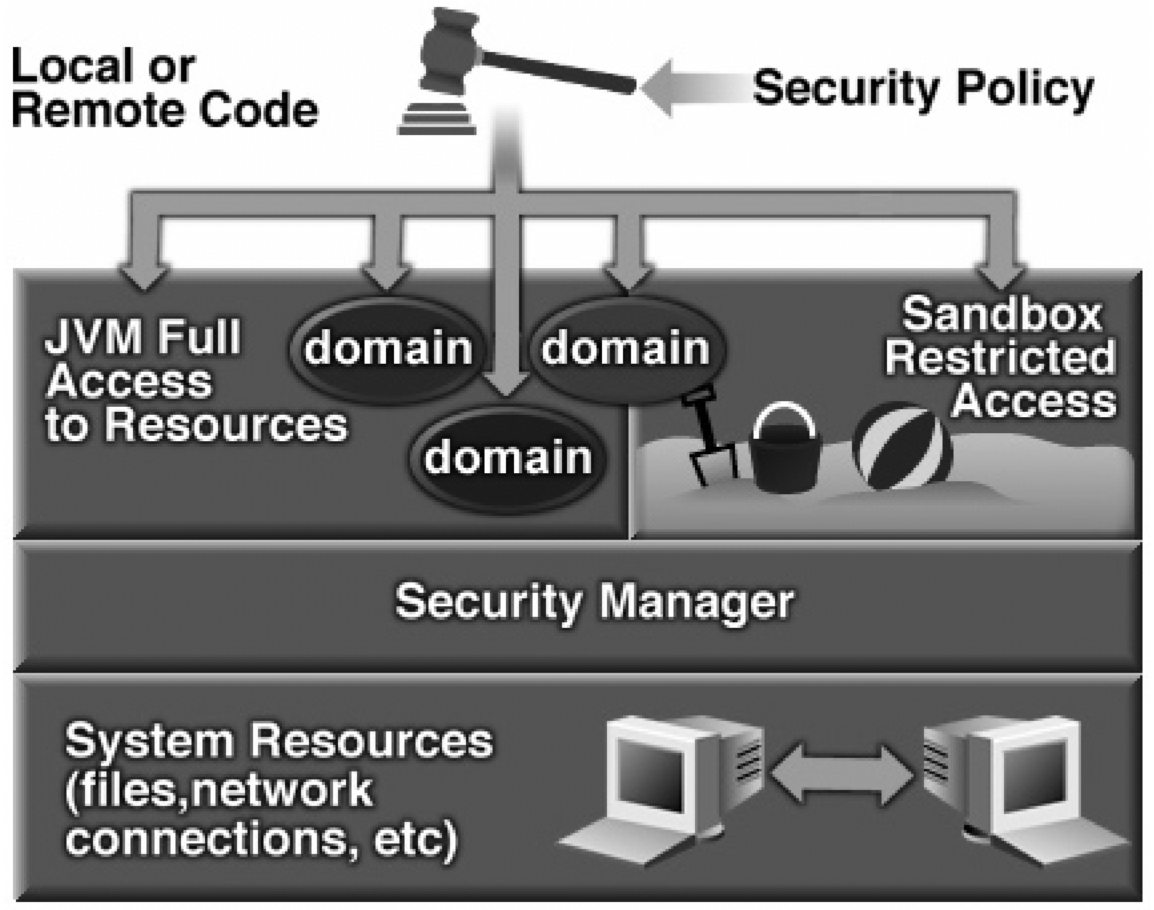
JavaSoft, Sun Microsystems, Inc.

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

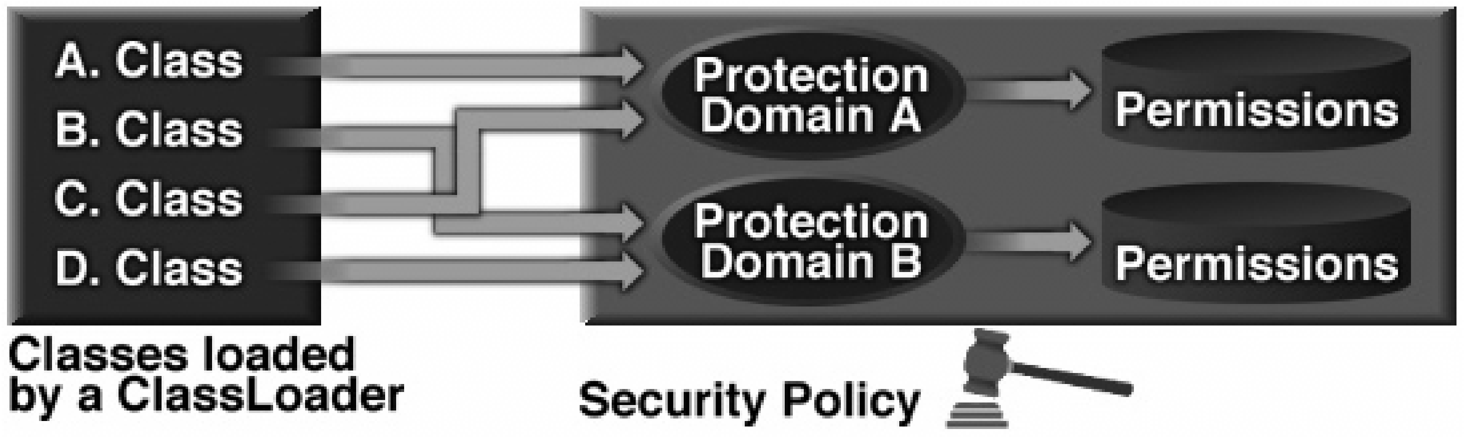


Local or Remote Code
Security Policy
JVM Full Access to Resources
domain
domain
domain
Sandbox Restricted Access
Security Manager
System Resources (files,network connections, etc)

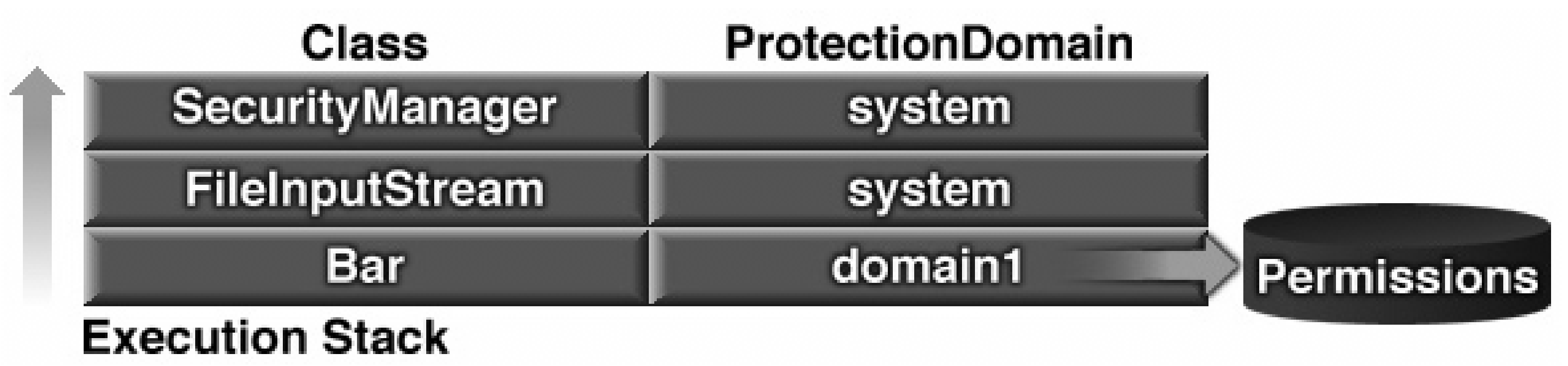
Security Policy in ACL

what code	what permissions
CharlesSchwab applets, signed	read and write /tmp and /home/gong/stock
CharlesSchwab applets, signed and unsigned	connect and accept bankofaemrican.com
...	...

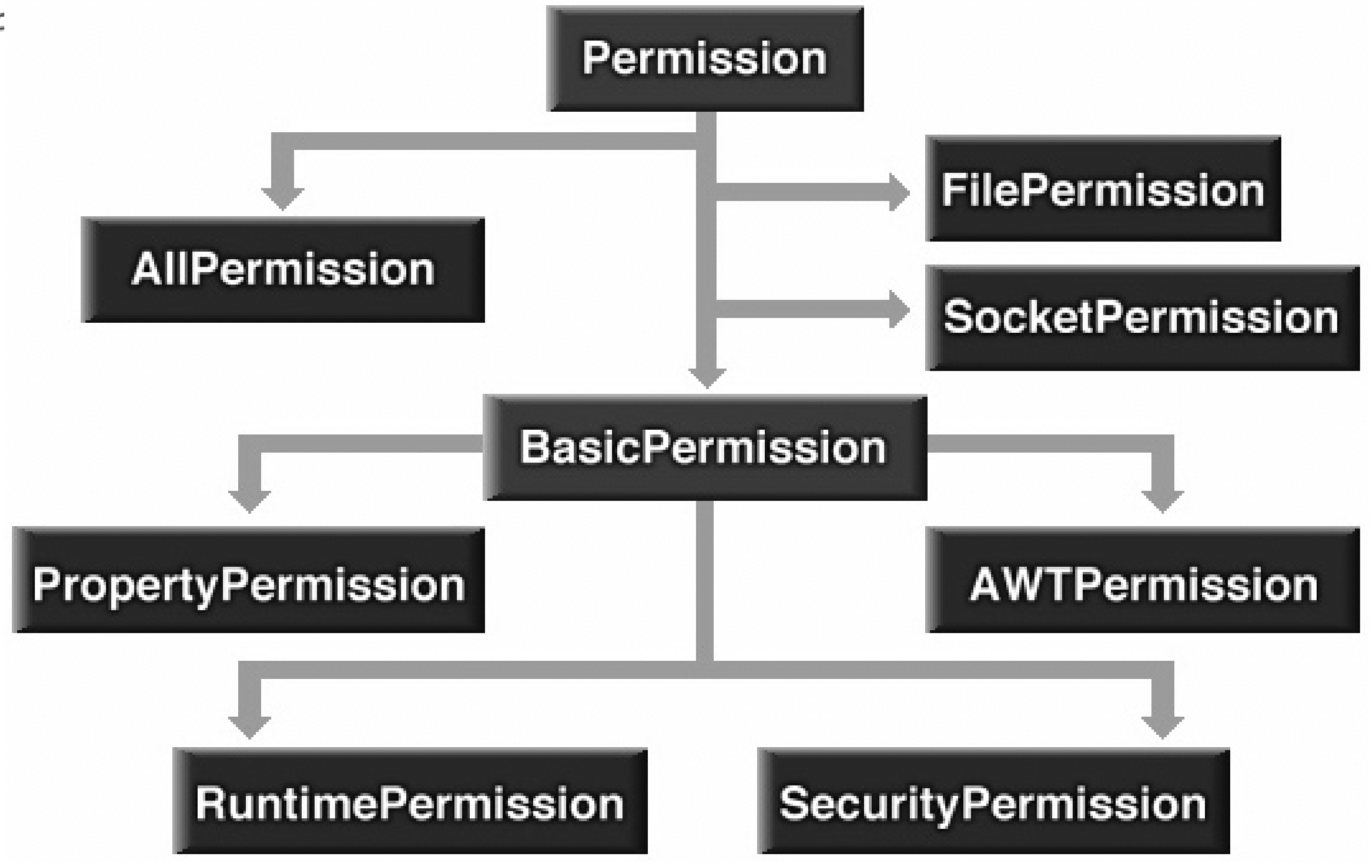
Class->Domain->Permissions



Access Control Mechanism

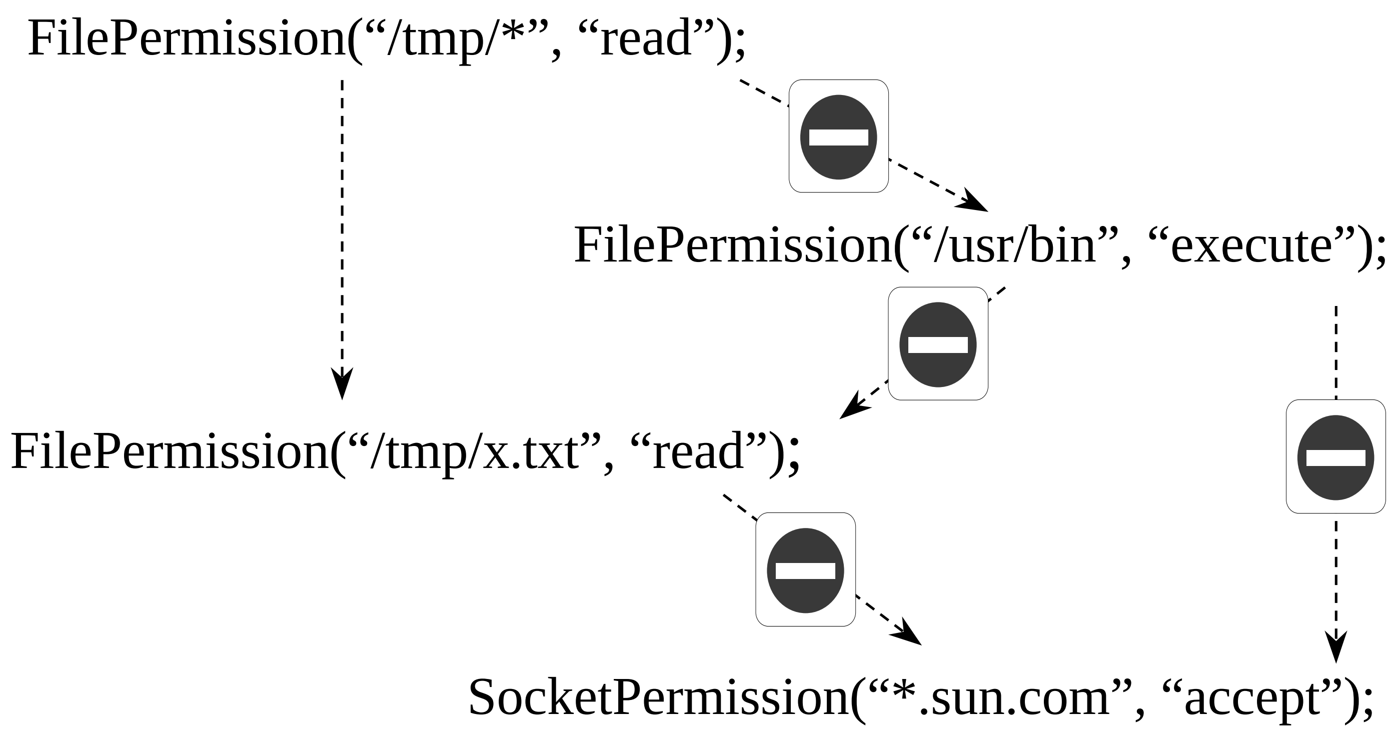


Permission Classes

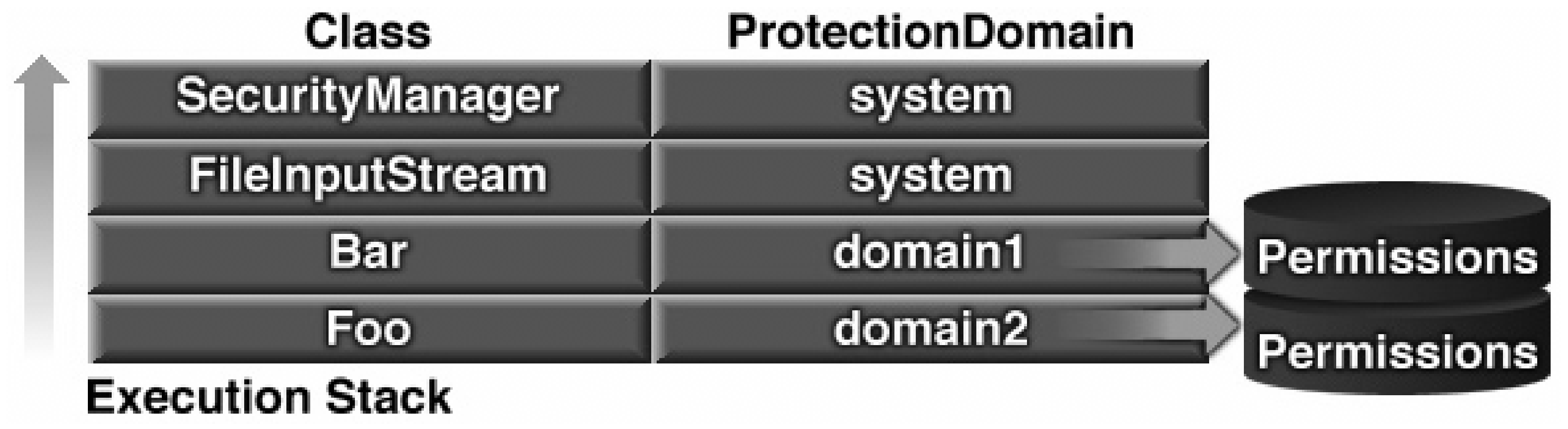


Permission Relationship

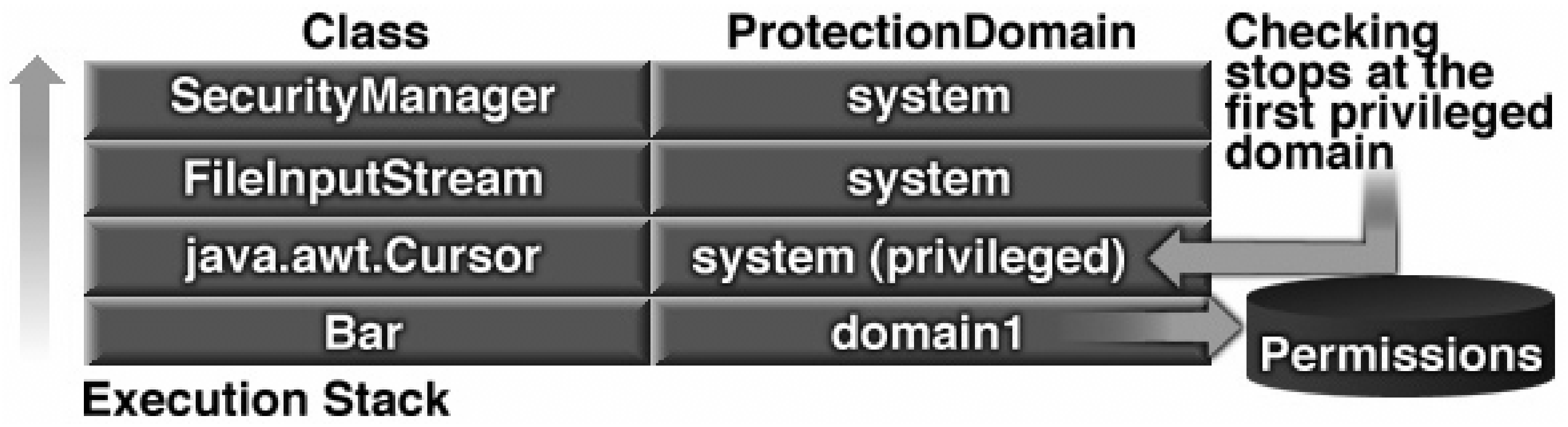
PermissionA.implies(PermissionB) = true?


FilePermission("/tmp/*", "read");
FilePermission("/usr/bin", "execute");
FilePermission("/tmp/x.txt", "read");
SocketPermission("*.sun.com", "accept");

Multi-Domain Computation



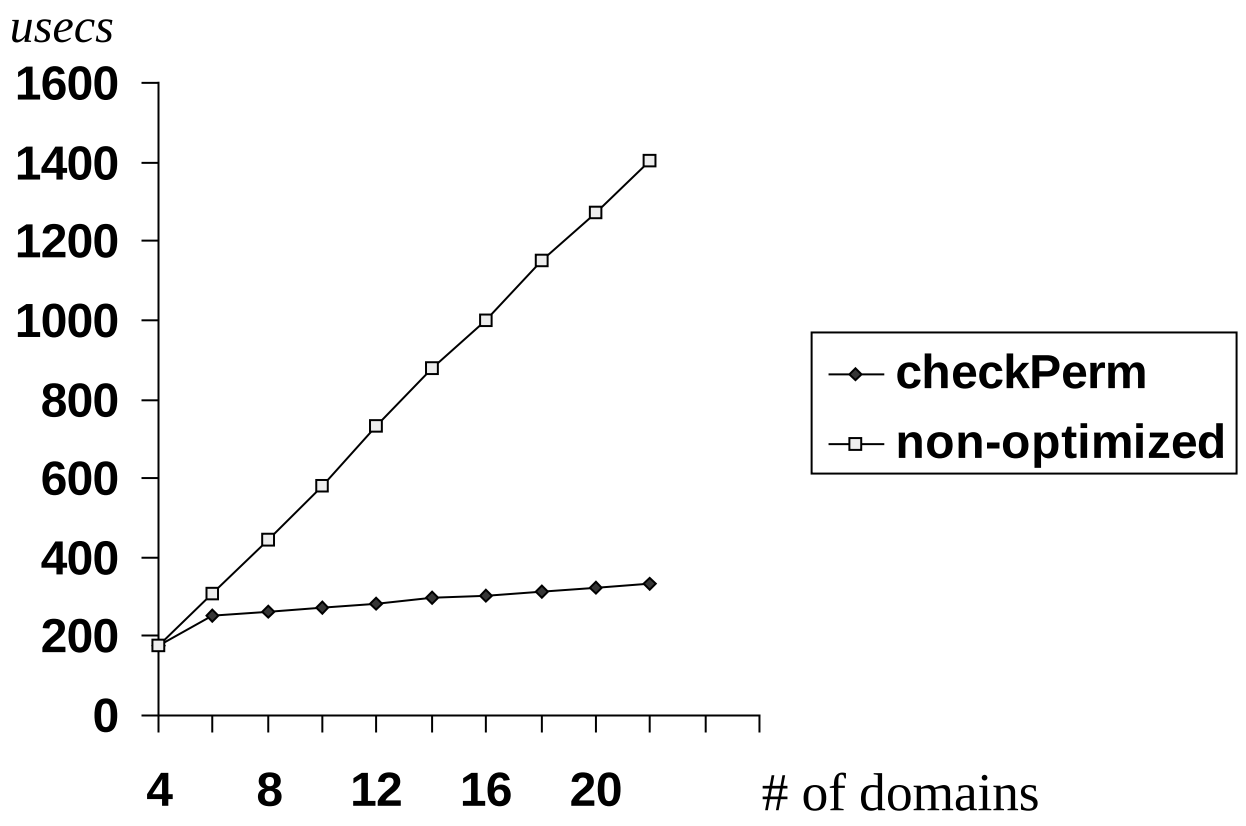
Privileged Computation



Discussion

- Security context inheritance
- Class method inheritance's impact on security
- Lazy or eager computation
- Performance

Access Control Performance



* beginPrivileged and endPrivileged add 2 *usecs*

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”;
};
```