Application Servers
G22.3033-011

Session 6 - Sub-Topic 3
Java 2 Security

Dr. Jean-Claude Franchitti

New York University
Computer Science Department
Courant Institute of Mathematical Sciences

Session Outline

• Java 2 Security
  – Trustworthy Code
  – Sandboxes and Signatures
  – PKI
Java 2 Security - Trustworthy Code

- Cross-platform solution is amenable to cross-platform attacks
- Old security model:
  - Applet code: untrusted & relegated to a security sandbox
  - Application code: treated as fully trusted built-in code
- New model:
  - Levels of trust

Java 2 Security - Sandboxes and Signatures

- Four basic security categories:
  - System modification:
    • Attacker gains complete control of target machine
  - Invasion of privacy
    • Attacker steals sensitive information from target
  - Denial of service
    • Attacker makes a machine unusable
  - Antagonism
    • Attacker interferes with normal machine use
Java 2 Security - Issues

• No such thing as 100% security
• Securing Java involves securing the VM, its supporting classes, and the code that runs on the VM

Java 2 Security - Old Model

• Restrict untrusted code by placing it in a sandbox
  – Sandbox stops untrusted code from doing dangerous things (e.g., some network connections, writing to files, etc.)
• Default Sandbox:
  – Verifier + Class Loader + Security Manager
Java 2 Security - New Model

- Code-signing infrastructure + Access control mechanisms
- Java.security package
  - API including a cryptographic provider interface
  - APIs for common cryptographic mechanisms
- VM can now authenticate signed Java classes (i.e., tell who signed them)

Java 2 Security - New Model (continued)

- Digital signatures are used to put a unique id on arbitrary binary files
- Browser can accept/reject signed code
- Good news: enterprise system designers can setup precise security policies
- Bad news: setting up and managing security policies is a large task
Java 2 Security - PKI

• Code signing relies on a public/private key infrastructure (PKI)
• PKI used to administer keys used to sign code according to some policy
• Problem: few organizations have a PKI in place