Techniques for Securing Hosts in Mobile Agent Systems

Will Upchurch
November 21, 2002

Introduction

• Goals and Concerns
• Solutions
• Current Systems:
  • Agent Tcl
  • Telescript
Goals and Concerns

- Authentication
  - Who wrote the script?
  - Has the script been altered?
- Authorization
  - What can the script do?

- The ultimate goal:
  Resource Control

Solutions

- Authentication
  - Digital Certificates
  - Digital Signatures
- Authorization
  - Security Policies
  - Sandboxing
Agent Tcl

- PGP as a separate process
- Based on Safe-Tcl
  - Master Interpreter
  - Safe Interpreter and Aliases
- Resource Managers

Telescript

- Authorities and Permits
- Secure Channels and Regimes
  - identification, registration, fast authentication, re-key and authentication
- Security Mix-Ins control system objects
  - unmoved, uncopied, copyrighted, protected
- Namespace Partitioning
Sources