

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

3

Solutions

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

4

Agent Tcl

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

5

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

6

Sources

- Robert S. Gray. Agent Tcl: A flexible and secure mobile-agent system. 1996
- John K. Ousterhout, Jacob Y. Levy and Brent B. Welch. The Safe-Tcl Security Model. March 1997
- Joseph Tardo and Luis Valente. Mobile Agent Security and Telescript. February 1996