An Infrastructure for Secure Interoperability of Agents

Ramesh Bharadwaj, Judith Froscher, Amit Khashnobish, James Tracy
Center for High Assurance Computer Systems
Naval Research Laboratory

Preview

- Introduction
- Software Agents
- Secure Agents Middleware (SAM)
  - Security Requirements
  - Architecture
**Introduction**

- Building Distributed Applications
  - Difficult
  - Developers’ Tools
    - Remote Procedure Call (RPC)
      - Client-Server Model
      - HTTP
    - Peer-to-Peer (P2P)
      - Security

**Software Agents**

- Key components of distributed applications
- Efficient
  - Only relevant information is passed
- Effective
  - Local control over data distribution and updates is maintained
- Survivable
  - Control is distributed
Software Agents

- Security Vulnerabilities
  - Due to distributed computing
    - Denial of service
    - Information leaks
    - Trojan horses
    - Malicious code
  - Due to agent technology
    - Above vulnerabilities may be intensified

Secure Agents Middleware (SAM)

- Infrastructure designed to meet security requirements in a distributed computing environment
  - Robustness
  - Efficiency
    - Flow of information among hosts is optimized
    - Evaluate emergent behavior
  - Usability
    - Agent Creation Environment (ACE)
      - Agent templates
      - Secure Agent Description Language (SADL)
Secure Agents Middleware (SAM)

- Security Requirements:
  - “Security for Mobile Agents: Issues and Requirements”
    - csrg.nist.gov/nissc/1996/papers/NISSC96/paper033/SWARUP96.PDF
  - Author and sender of agent must be authenticated
  - Correctness of agent's code must be checked
  - Als must ensure privacy of agent during transmission
  - Als must protect themselves (authenticate and authorize)
  - Agents must be created in a "safe" language
  - Sender must have control over agent's flexibility
  - Als must ensure safe state of agent
  - Sender must have control over Als' authority to execute agent

Secure Agents Middleware (SAM)

Architecture

[Diagram showing the Secure Agents Middleware (SAM) architecture with Host, Agent Interpreter (AI), and Agents]
Secure Agents Middleware (SAM)

Architecture:

- Security Agents
  - Monitor other classes of agents (secure agents)
  - Protect against attacks by implementing:
    - Encryption
    - Authorization
    - Virus checking
    - Intrusion detection, etc.

Who will monitor the security agents as they monitor the secure agents?
Secure Agents Middleware (SAM)

Safe and secure behavior of security agents is ensured by:

- creating agents in SADL – a language for high assurance
- using an open source compliance checker (CC)
- implementing an architecture to monitor and coordinate agents' activities

Review

- Difficulty of building distributed applications
- Importance of software agents
- Secure Agents Middleware (SAM)
  - Security Requirements
  - Architecture
?? Questions ??