

Mobile Agent Security

Anna Suen

suen@cs.fsu.edu

November 5, 2002

Preview

- Mobile Agent System Model
- Threats
 - Agent-to-Platform
 - Platform-to-Agent
 - Agent-to-Agent
 - Other-to-Agent Platform

My Motivation

- storage jamming detection techniques for mobile agents
 - detection objects
 - Meadows, Catherine. "Detecting Attacks on Mobile Agents."

3

Mobile Agent System Model

- Agent
 - code and state info needed for some computation
 - mobility
 - allows agent to move among agent platforms
- Agent Platform
 - computational environment
 - home platform
 - agent's origin
 - most trusted environment

4

Threats

- Agent-to-Platform
- Platform-to-Agent
- Agent-to-Agent
 - platform agents
- Other-to-Agent Platform
 - external entities attacking platform
 - external agent
 - another agent platform

5

Agent-to-Platform

1. Masquerade
 - as authorized agent to gain access
 - as unauthorized agent to avoid blame
 - damages trust and reputation of legitimate agent
2. Denial of Service
 - run attack scripts
 - unintentional program errors

6

Agent-to-Platform

3. Unauthorized Access

- accessing unauthorized data on platform

7

Platform-to-Agent

1. Masquerade

- platform pretends to be a trusted platform
 - extract private info from agent
- harms visiting agent and assumed platform

2. Denial of Service

- ignore, delay, terminate agent's requests
- can affect other agents that depend on attacked agent → deadlock
- platform keep feeding agent with tasks

8

Platform-to-Agent

3. Eavesdropping

- platform has access to all agent's data and instructions
- ie, agent planning a trip

4. Alteration

- platform can modify agent's code, state, or data

9

Agent-to-Agent

1. Masquerade

- platform agent pretends to be reputable vendor
 - get private info (ie, credit card #)

2. Denial of Service

- spamming agent with messages
- sending useless info

10

Agent-to-Agent

3. Repudiation

- agent claims that transaction/communication never took place
- platforms keep records to resolve disputes

4. Unauthorized Access

- interfere by invoking its public methods
- modify data or code
 - change agent's behavior
- gain info about agent's activities
 - eavesdropping on its communications

11

Other-to-Agent Platform

1. Masquerade

- agent on remote platform requests services and resources
- act in conjunction with malicious platform
- act alone

2. Unauthorized Access

- remote users, processes, and agents accessing platform

12

Other-to-Agent Platform

3. Denial of Service
 - platforms susceptible to common DoS attacks
4. Copy and Replay
 - agents can be cloned and retransmitted
 - ie, interceptor capture agent's "buy order"

13

Review

- Threats to mobile agent system
 - Agent-to-Platform
 - Platform-to-Agent
 - Agent-to-Agent
 - Other-to-Agent Platform

14

Questions?



15

Reference

- Wayne Jansen, Tom Karygiannis, "NIST Special Publication 800-10 – Mobile Agent Security", 2000.
 - section 2

16