Lecture 5:
Mobile Agents Security

Subjects / Topics:
1. Introduction and basic principles
2. Mobile agent’s computing cycle
3. Authorization and trust
4. Security scenarios
5. Secure Mobile Agent Applications
6. Conclusions

What is a mobile agent

Properties:
• A program acting on behalf of
  - Human user or Organization
  - Another Agent or System
• Migrate autonomously from host to host
• Communicate with its user and other agents

Terms:
• Agent Owner
• Agent Server (Agent Engine, Agency, Platform)
  – communication, registration, management, transport, Security

Attractive features

- Asynchronously and Autonomously
- Adapting dynamically (i.e. configuration, state and functions, environment customization(e.g. IDS), Exception condition etc)
- Operate in heterogeneous environment
- Robust and fault-tolerant behavior for distributed system

By moving program to resources:
• Network traffic reduced
• Resource access more efficient and flexible
• Mobile users well supported
Potential Applications

- Distributed Information Gathering
- Networking Monitoring (distributed surveillance sensor network)
- Secure Information Retrieval
- Secure Network Management (updates etc.)
- Secure Service Provisioning support

Mobile Agent System Architecture

1. Mobile Agents
   - Mobile agents are self-contained modules of software, various credentials and accumulated data.
     - Associated credentials
     - Baggage
     - Routing information
2. Mobile Agents Platform
3. MAS Management Station
4. Agent Servers (accept, execute & launch agents)
5. MAS Execution Logs:
6. MAS Infrastructure Servers: (directory server, state server, lookup server, data backup etc.)

Security aspects

Agent Owner

Agent Server Operator

Malicious agent server? Malicious agent?
My agent damaged? Local security compromised?

Threat Categories

- Agent to Platform
- Platform/Agent Server to Agent
- Agent to Agent

Examples of applications:
- Airline Tickets (Shopping)
- Multi-Media Services (Searching)

Threats from Mobile Agents to Agent Server

- Masquerade (identity of another agent)
  - Illegal access to services and resources
  - Steal/reveal secret information
  - Exhaust resources
- Malfunction
  - Program errors
  - Viruses or worms
  - Trojan horses, backdoor programs
- Action repudiation

Threats from Agent Servers to Agents

- Masquerade (identity of another Server or Platform)
  - Illegal access to mobile agent's resources
  - Steal code, valuable information carried by agent ("baggage")
  - Reveal private or sensitive actions performed by agent
- Illegal manipulation of mobile agents
  - Execute agent's code incorrectly
  - Send agent to unintended destination
  - Cheat agent with false information
  - "Kidnap" agent
- Information/action repudiation
Threats from Agents to Agents

- Masquerade (identity of another agent)
  - During Agent communication
  - Steal information
- Denial of Service
  - Extra messages
  - Change CPU time
  - Convey false information
- Information/Action Repudiation
  - Agent to Agent Communication
  - Unauthorized Access

Security Requirements

- Protection of mobile agents from malicious agents
  - Authentication of agent server
  - Non-replay
  - Confidentiality of agent's secrets
  - Integrity of agent's code, "baggage"
  - Detection of server's illegal manipulation
  - Non-repudiation of information/action by server
  - Disaster recovery

Lecture 5:
Mobile Agents Security

Subjects / Topics:
1. Introduction and basic principles
2. Mobile agent's computing cycle
3. Authorization and trust
4. Security scenarios
5. Secure Mobile Agent Applications
6. Evaluations and conclusions
Mobile agents computing cycle

**Components:**
- Agent author
- Agent owner
- Agent home
- Mobile agent
- Agent server

**Agent life cycle:**
- Agent creation
- Agent owning
- Agent launching
- Agent hosting
- Agent traversing
- Agent return

**Communication Links:**
- Agent – Agent Owner
- Agent – Agent

**Two cases:**
- Single-step case ("weak" mobility)
  - "client–server" paradigm
  - e.g. Java applet, active mail
- Multi-step case
  - e.g. information searching agent, shopping agent, etc.

Lecture 5:
Mobile Agents Security

**Subjects / Topics:**
1. Introduction and basic principles
2. Mobile agent’s computing cycle
3. Authorization and trust
4. Security scenarios
5. Secure Mobile Agent Applications
6. Evaluations and conclusions

**Agent creation**

**Agent Privileges**

**Authorization and trust**
Agent owning

Verify Signature

OK

Trust Level

OK

Agent Author

Agent Owner

Agent Launching

Agent hosting

Agent traversing

Agent return
Lecture 5:
Mobile Agents Security

Subjects / Topics:
1. Introduction and basic principles
2. Mobile agent’s computing cycle
3. Authorization and trust
4. Security scenarios
5. Secure Mobile Agent Applications
6. Conclusions

Intrusion Detection and Prevention System based on Secure Mobile Agents

Available Solutions weaknesses
- Firewalls, Spy-ware, Authentication mechanisms, Anti virus

IDS Shortcomings
- Lack of efficiency
- Limited flexibility
- Vulnerable to direct attack
- High number of false positives
- High maintenance required
- Limited response capability
- Analysis of huge log: system admin report

IRS - Automatic Responses

Security evaluations

Achieved security properties:
- Unique identification of mobile agents
- Authentication between agents and agent servers
- Integrity of agent’s code, attributes and “baggage”
- Trust evaluation of agent code
- Access control imposed on mobile agents
- Protection against replay and re-launch
- Error detection and recovery
- Non-repudiation
Open issues:

- Privacy of actions of mobile agents
- Trust schemes for agent’s code
- Specification and enforcement of various security policies
- Implementation details and specifications
- Dynamic configuration of Access Control
- Security issues in agent reproduction/ cloning
- Security issues in case of strong mobility
- Security issues in case of Interoperability among Agent Platforms.