Agent-based Security System

EE657 Midterm Project
Yuxiang Luo

The benefits of using Mobile Agents

- They reduce the network load
- They overcome network latency
- They encapsulate protocols
- They execute asynchronously and autonomously
- They adapt dynamically
- They are naturally heterogeneous
- They are robust and fault-tolerant
### Security Threats

<table>
<thead>
<tr>
<th>Threats source and target</th>
<th>Categories of Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Agent-to-Host</strong></td>
<td>Masquerading; Denial of Service; Unauthorized Access;</td>
</tr>
<tr>
<td><strong>Agent-to-Agent</strong></td>
<td>Masquerading Denial of Service Repudiation Unauthorized access</td>
</tr>
<tr>
<td><strong>Host-to-Agent</strong></td>
<td>Masquerading Denial of Service Eavesdropping Alteration</td>
</tr>
<tr>
<td><strong>Other-to-Host</strong></td>
<td>Masquerading Unauthorized Access Denial of Service Copy and Replay</td>
</tr>
</tbody>
</table>

### Security countermeasures

(source: Countermeasures for Mobile Agent Security, W. Jansen, NIST 2000)

<table>
<thead>
<tr>
<th>Countermeasure</th>
<th>Category</th>
<th>Security objective</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signed Code</td>
<td>Detection A-P</td>
<td>Old/Easy/Very Popular</td>
<td></td>
</tr>
<tr>
<td>State Appraisal</td>
<td>Detection A-P</td>
<td>New/Hard</td>
<td></td>
</tr>
<tr>
<td>Path Histories</td>
<td>Detection A-P</td>
<td>New/Easy/Popular</td>
<td></td>
</tr>
<tr>
<td>Partial Result Encapsulation</td>
<td>Detection A</td>
<td>New/Hard</td>
<td></td>
</tr>
<tr>
<td>Mutual Itinerary Recording</td>
<td>Detection A</td>
<td>New/Easy</td>
<td></td>
</tr>
<tr>
<td>Itinerary Recording with Replication and voting</td>
<td>Detection A</td>
<td>New/Easy</td>
<td></td>
</tr>
<tr>
<td>Execution Tracing</td>
<td>Detection A</td>
<td>New/Easy</td>
<td></td>
</tr>
<tr>
<td>Software-Based Fault Isolation</td>
<td>Detection A-P</td>
<td>Old/Easy/Very Popular</td>
<td></td>
</tr>
<tr>
<td>Safe Code Interpretation</td>
<td>Prevention A-P</td>
<td>New/Hard</td>
<td></td>
</tr>
<tr>
<td>Proof Carrying Code</td>
<td>Prevention A-P</td>
<td>New/Hard</td>
<td></td>
</tr>
<tr>
<td>Environmental Key Generation</td>
<td>Prevention A</td>
<td>New/Hard</td>
<td></td>
</tr>
<tr>
<td>Computing with Encrypted Functions Obfuscated</td>
<td>Prevention A</td>
<td>New/Hard</td>
<td></td>
</tr>
<tr>
<td>Code</td>
<td>Prevention A</td>
<td>New/Hard</td>
<td></td>
</tr>
</tbody>
</table>
Aglets by IBM Tokyo

Aglets: java-based mobile agents

Context: Aglets’ workplace. Protect host against malicious aglets. Provide aglets with requested public methods and resource.

Focused protection: Host-against-agent
Agent-against-agent

Rule-based security enforcement to protect host and prevent agents interferences:
Both aglet owner and the context master may define security policies. Aglets system implements the overall effect of all security policies involved. The hierarchy of security policies is:
AgletManufacturer<AgletOwner<ContextMaster<DomainAuthority

Transfer Security: Current and destination contexts establish a secure channel between themselves.

Voyager by Objectspace

Voyager has similar security mechanism with aglets. Here are some differences:

Security rules can be defined by
four entities
User can't define its own security preference
Security contexts can't move, only agents move
If in trusted environment, security context can move with agent.
Dynamic security policy management not allowed

Voyager is not designed for open networks, some of its security features are based on this assumption. More authentication by digital signatures or certificates should be introduced to this system before it can be used in open networks.
Concordia by Mitsubishi

- Agent Protection:
  - Transmission Protection
    - Use Secure Sockets Layer (a general-purpose network security protocol) to provide authentication and encryption services so that transmission can be secured
  - Storage Protection
    - All important information is encrypted. Decrypting an agent requires a private key which can be physically secured.
- Agent Platform Protection:
  - Identity-based security enforcement: The access to resources are granted based on the identity of the user who launched the agent.

Ajanta By Univ. Of Minnesota

- Uniform Resource Name model: A name service is provided for mapping URN to the physical locations of the various entities.
- Agent Protection
  - Transmission protection: Ajanta incorporate standard cryptographic mechanisms into its agent transfer protocol
  - Protection against Malicious Host:
    - Read-only state--The programmer can declare parts of the agent state as read-only.
    - Append-only container--The agent can put in data as it executes
    - Selective revealing of agent state--The programmer can specify that certain part should only be made visible to specific agent platforms.
Agent Platform Protection
- Isolated domain for agent execution
- System-level resources access granted based on user URNs, thus by identity.
- Application-defined resources access controlled by a proxy-based mechanism. Each resource can implement its own security policies.
- Communication between agents are allowed and monitored by Ajanta Security Manager.

Comparison and Conclusion