Agent-based Intrusion Detection Systems

Xin Li

Computer Science Department
University of Southern California

Outline

- IDSs and Agents
- Current agent-based IDSs
  - AAFID
  - IDA
  - JAM
- Summary
IDSs and Agents

- An Intrusion detection system (IDS) is a real-time computer program that attempts to perform intrusion detection by either misuse or anomaly detection, or a combination of techniques [BALA98].

- Most current IDSs are based on Denning’s hypothesis [DENN87], where she said that security violations could be detected from abnormal patterns of system usage.

- In an IDS, agents are independently-running software entities that perform certain security monitoring functions with the capability to move from place to place.

AAFID

Autonomous Agents For Intrusion Detection (AAFID)

- A distributed IDS based on Autonomous Agents

- Tree-like architecture

- 3 kinds of components: Agents, Transceivers, and Monitors

- Communication between components based on Message Passing.
**AAFID (cont’d)**

Physical layout of an AAFID [BARA98]

---

**Generic behavior of an agent [SPAF98].**

Do initialization

```
loop
  Process input
  if STOP message was received then
    Cleanup and exit
  end if
  Perform checks
  if abnormal condition detected then
    Generate STATUS_UPDATE message with new status information
  end if
  Sleep for a certain amount of time (inter-check period)
end loop
```
IDA
Intrusion Detection Agent system (IDA)

- Agent-based distributed IDS
- Four stages of intrusion patterns
- Intrusion detection based on MLSI (Mark Left by Suspected Intruders)
- Two kinds of mobile agents: Tracing Agents and Information gathering Agents
- Board-based communication mechanism

IDA (cont’d)
Stages of Intrusion patterns [ASAK99a]
IDA (cont’d)

Structure of IDA [ASAK99a]

- Apply data mining programs to the extensively gathered audit data to compute models that accurately capture the behavior of both intrusions and normal activities.
- Two kinds of agents: Learning Agents and Detection Agents.
JAM (cont’d)

The procedure of Meta-learning [PROD00]

An architecture for JAM-based IDS [LEE98]
### Summary

<table>
<thead>
<tr>
<th>IDSs</th>
<th>AAFID</th>
<th>IDA</th>
<th>JAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposed by</td>
<td>Purdue University</td>
<td>IPA, Japan</td>
<td>Columbia University</td>
</tr>
<tr>
<td>Structure</td>
<td>Tree-like</td>
<td>Hybrid</td>
<td>Tree-like</td>
</tr>
<tr>
<td>Components</td>
<td>Agents, Transceivers, Monitors</td>
<td>Managers, Sensors, Bulletin boards, Message boards, Tracing agents, Info-gathering agents</td>
<td>Learning agents, Detection agents</td>
</tr>
</tbody>
</table>

### Summary (cont’d)

<table>
<thead>
<tr>
<th>IDSs</th>
<th>AAFID</th>
<th>IDA</th>
<th>JAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intrusion detection Techniques</td>
<td>Rule-based or Statistical</td>
<td>MLSI</td>
<td>Meta-learning</td>
</tr>
<tr>
<td>Communication mechanism</td>
<td>Message passing</td>
<td>Agent moving</td>
<td>Agent moving</td>
</tr>
<tr>
<td>Mobility</td>
<td>Not yet</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Platform</td>
<td>UNIX</td>
<td>UNIX</td>
<td>JVM</td>
</tr>
<tr>
<td>Programming Language</td>
<td>Perl 5</td>
<td>GNU C/C++ 2.7, Perl 5, D’Agent 2.0</td>
<td>JAVA</td>
</tr>
</tbody>
</table>
## Summary (cont’d)

<table>
<thead>
<tr>
<th>IDSs</th>
<th>AAFID</th>
<th>IDA</th>
<th>JAM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Drawbacks</strong></td>
<td>Monitors are single point of failure, Lack of agent mobility</td>
<td>Managers are single point of failure, Effectiveness needs to be proved</td>
<td>Learning agents are heavy weight, Training data are critical to build a IDS</td>
</tr>
</tbody>
</table>

## Summary (cont’d)

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Rating of degrees to which it is achieved</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run continually</td>
<td>High</td>
</tr>
<tr>
<td>Fault tolerant</td>
<td>Medium</td>
</tr>
<tr>
<td>Resist subversion</td>
<td>Low</td>
</tr>
<tr>
<td>Minimal overhead on the system</td>
<td>Medium</td>
</tr>
<tr>
<td>Easily tailored</td>
<td>High</td>
</tr>
<tr>
<td>Difficult to fool</td>
<td>Low</td>
</tr>
<tr>
<td>Scalability</td>
<td>High</td>
</tr>
<tr>
<td>Dynamic reconfiguration</td>
<td>Medium</td>
</tr>
</tbody>
</table>
Thank you