A Framework for Distributed Intrusion Detection using Interest-Driven Cooperating Agents

Rajeev Gopalakrishna
and
Eugene H. Spafford
Distributed IDS

“a system where the analysis of the data is performed on a number of locations proportional to the number of hosts that are being monitored” – Spafford and Zamboni
## Distributed Communication Models

<table>
<thead>
<tr>
<th>Event-based model</th>
<th>Push-based model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any entity may produce, any entity may consume events</td>
<td>Specific producers and consumers</td>
</tr>
<tr>
<td>Symmetric roles</td>
<td>Asymmetric roles</td>
</tr>
<tr>
<td>Loosely connected</td>
<td>Logical channels</td>
</tr>
<tr>
<td>Higher scalability</td>
<td>Tighter coupling</td>
</tr>
<tr>
<td>Event advertisement, interest specification and event notification</td>
<td>Less scalable</td>
</tr>
</tbody>
</table>
Motivation

• Concept of agents to perform intrusion detection
• Event-based communication model
• Concept of interest propagation
Generic Hierarchical Intrusion Detection Systems

![Generic Hierarchical Intrusion Detection Systems Diagram]
Examples

• DIDS
• GrIDS
• EMERALD
• AAFID
Drawbacks

• Analysis hierarchy
• Data refinement
• Bulky modules at all levels of hierarchy
• Passive interaction
Related Work

- Crosbie and Spafford
- Barrus and Rowe
- Ingram
- Mell and McLarnon
- CARDS
Our Approach

- Agents
- No analysis hierarchy
- Intelligent cooperation using the concept of interests
- Interest propagation
- Active communication
- Lightweight modules at all levels of hierarchy
Interest

“a specification of data that an agent is interested in, but is not available to the agent because of the locality of data collection or because the agent was not primarily intended to observe those data”
Interest Propagation

LEGEND

- Agent
- Domain Propagator
- Local Propagator
- Enterprise Propagator
Types of Interests

• Directed or Propagated Interests
• Local, Domain or Enterprise Level Interests
• Permanent or Temporal Interests
Granularity of Interests

- *Event vs. Alert*
- *Curiosity level*
- Adds dynamism to agents
- Reduces overhead
Data Delivery

Hierarchical delivery  Direct delivery

• Failure of modules
• Scalability
• Data Coalescing
Host

IR - Interest Registry
AR - Agent Registry
Other Considerations

• Security of Agents
• Clock Synchronization
• Redundancy of Propagators
Future Work

- Implementation of the framework
- Explore alternatives for implementing the interest mechanism
- Impact on size of agents and on host and network performance