Statistical Anomaly Intrusion Detection System

-Midterm Project
By Sheng Li

Presentation Outline

• What is statistical anomaly IDS?
• Methods
• Evaluating – Benchmarking
• Case-studies – NIDES, AAFID, JiNao
• Conclusions and Future Works
Intrusion Detection Techniques

- Misuse Detection
  - Seeking for matches
  - Known attack recognition only

- Anomaly Detection
  - Assumption: Deviation
  - Capable to detect new threats

Solution in most IDS:
Combine the two techniques to achieve higher performance and higher precision

Types of Threats and SAIDS
Benchmarking SAID

- **Event outcomes**
  Determining hits, misses, and false alarms
- **Ground truth**
  Positions and types of test
- **Threshold**
  Level of triggering alarms
- **Scope**
  Range of data the detector takes into account

Case Studies

- **NIDES** (Next-generation Intrusion Detection Expert System)
  – Developed by SRI/CSL lab, concluded in 1995
  – Provided the most fundamental and developed algorithm models
- **AAFID** (Autonomous Agents For Intrusion Detection)
  – Developed by COAST Laboratory at Purdue University
  – Most recent release of AAFID2 in Sep 1999
- **JiNao**
  – Developed jointly by Microelectronics Center of North Carolina (MCNC) and North Carolina State University
  – Most recent modification on June 2000
NIDES Architecture:

• Auditing data collected from hosts being monitored
• NIDES runs on its own station to detect intrusions
• ID component uses both rule-based analysis and statistical analysis

NIDES statistical analysis Algorithm

• Measures - $S$:
  \[ S = \Phi^{-1}(1 - TPROB/2) \]

• $T^2$ Statistics:
  \[ T^2 = \left( S_1^2 + S_2^2 + \ldots + S_n^2 \right) / n \]

• Warning flags raised when either $S$ or $T^2$ is high
Physical view of a Possible AAFID architecture

Logical view of the same AAFID architecture
JiNao

- OSPF routing protocol
- Attacks to OSPF
  - Seq++
  - MaxAge
  - MaxSeq#
- JiNao’s solution:
  Distributed agents on routers
- Uses modified NIDES statistical algorithm in anomaly detection

JiNao Architecture
Conclusion

<table>
<thead>
<tr>
<th>Feature</th>
<th>NIDES</th>
<th>NiJao</th>
<th>IDIP</th>
<th>AAFID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real-time</td>
<td>v</td>
<td>v</td>
<td>v</td>
<td>v</td>
</tr>
<tr>
<td>Off-line</td>
<td>v</td>
<td>v</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detection</td>
<td>Hybrid</td>
<td>Hybrid</td>
<td>Hybrid</td>
<td>Hybrid</td>
</tr>
<tr>
<td>Data Collection</td>
<td>Centralized</td>
<td>Distributed</td>
<td>Distributed</td>
<td>Distributed</td>
</tr>
<tr>
<td>Data Process</td>
<td>Centralized</td>
<td>Centralized</td>
<td>Distributed</td>
<td>Distributed</td>
</tr>
<tr>
<td>Decision Making</td>
<td>Centralized</td>
<td>Centralized</td>
<td>Distributed</td>
<td>Distributed</td>
</tr>
<tr>
<td>Intrusion</td>
<td>Components</td>
<td>monitored</td>
<td>Hosts, Routers</td>
<td>Hosts, Gateways</td>
</tr>
<tr>
<td>Response</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Reliability: Low, Medium, High
Scalability: Low, High, High, High

Decision Making Entities: Single, Multiple, Multi-leveled

Future Works

- Collecting appropriate training data
- How to prevent being fooled
- Selecting proper threshold level for warnings, optimum size of scope, etc.
Thank you for attending my presentation!