A Distributed Multi-Agent Intrusion Detection and Response Framework

Patrick Miller
patrick@spider.doriathproject.com
Overview
Goals

- Utilize new and existing sensors collaboratively to generate threat analysis.
- Increased classification rate
- Reduced false positives
Heterogeneity

- Harder to fool
  - Artificial immune systems

- Many heads are better than one
  - Diverse computational models are appropriate when both the data and patterns are widely different.
Related Works

- EMERALD
- Contego
- Tivoli
  - http://www.tivoli.com
- Ect.
Architecture

- BB
  - Storage & Collection
- BBM
  - Response System
- UI
  - Configuration Center
- IDA
  - Intrusion Detection Agents
Network Utilization

- Low communication between agents
  - Response
  - Reinforcement signal
- Run on a dedicated network
  - VPN
  - Physical
IDAs

- Intrusion Detection Agents
  - Distributed throughout network
  - Monitor diverse data sets

- Use heterogeneous soft-computing methods
  - Reply with diverse decisions
  - Incremental Machine Learning
Result Correlation

- Different computational models may generate different decision types.
  - Crisp
  - Probability
  - Probability Interval
  - Fuzzy Set
MAT

- Allows integration of various decision types
- Manages consistencies between a probability distribution and a fuzzy set
## Team Decision Process

<table>
<thead>
<tr>
<th>IDA\Decisions</th>
<th>X1</th>
<th>..</th>
<th>Xi</th>
<th>...</th>
<th>Xn</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDA1 (C):w1</td>
<td>0</td>
<td>..</td>
<td>1</td>
<td>..0..</td>
<td>0</td>
</tr>
<tr>
<td>IDA2 (P):w2</td>
<td>0.5</td>
<td>..</td>
<td>0.2</td>
<td>..0..</td>
<td>0.3</td>
</tr>
<tr>
<td>IDA3 (S):w3</td>
<td>( )</td>
<td></td>
<td>(0.2,0.3)</td>
<td>...</td>
<td>( , )</td>
</tr>
<tr>
<td>IDA4 (F):w4</td>
<td>Mid</td>
<td></td>
<td>High</td>
<td>...</td>
<td>Low</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IDAm (..): wm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**MAT (with controls on bias)**

<table>
<thead>
<tr>
<th>Team: 1</th>
<th>P1</th>
<th>...</th>
<th>Pi</th>
<th>...</th>
<th>Pn</th>
</tr>
</thead>
</table>
Decision Support

- Response generated -> decision made.
- Response can be adjusted based on
  - Detection confidence
  - Attack type
- Responses configured by administrator
- Response to new attacks
  - Learning algorithm to make best guess
  - User defined defaults
Detection Methods
Signature Detection

• Useful for detecting
  – Well known attacks
  – Attacks which can be defined by regular expressions

• Quick filtering
  – Regular expressions
    • If-Else rules
  – Good for exception cases as well

• Decision most likely crisp
Anomaly Detection

• Pros
  – Zero-day attacks
  – Privilege abuse
  – Account hi-jacking

• Cons
  – Can be trained to accept malicious use
  – Memory intensive
Anomaly Detection

- Defined in linguistic terms.
  - Normal/strange/whoa!
  - Well suited for fuzzy logic

- Most likely decision output types.
  - Fuzzy, Probability
Event Classification

- Useful for
  - Determining a attack type
  - Detecting semi-known patterns of attack.
- Variety of methods
  - Self Organizing Maps
  - Rule-based systems
- Decision may be
  - Fuzzy, Probability
IDAs

- Single IDA can be a miniature multi-agent system.
  - Signature detection
  - Anomaly detector
  - Attack classifier
  - Decision Correlation
Classification Methods
## Soft Computing

- **Computational models**
  - Fuzzy Logic
  - Decision Tree
  - Neural Network
  - Self Organizing Map
  - Genetic Algorithm

<table>
<thead>
<tr>
<th></th>
<th>Classification</th>
<th>Speed</th>
<th>Adaptability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anomaly</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Good</td>
<td>Avg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Best</td>
<td>Poor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avg</td>
<td>Good</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avg</td>
<td>Best</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Poor</td>
<td>Good</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ID3 Trees

- Build decision tree to make evaluations
  - Use information gain, derived from entropy
- Binary or N-ary classifier
- Slow to train
- Fast to execute
- Does not support reinforcement learning
Self-Organizing Maps

- Build decision map based on input values
  - Correlates input to a map index indicating a classification type.
  - Updates map during train and execution.
  - Resulting map generated based on initial configuration values.
- Binary or N-ary classifier
- Moderately slow to train
- Moderate execution time
- Highly reinforceable
Fuzzy Logic

- Description
  - Expresses responses linguistically

- Strengths
  - Intuitive human interface
  - More human response, harder to detect

- Weaknesses
  - Response may be incorrectly interpreted
Genetic Algorithms

- **Description**
  - Simulate evolutionary process
    - Copy genes from both parents
    - Allow some random mutations
    - Test child for fitness
    - Use fitness to determine number of offspring

- **Strengths**
  - Highly scaleable
  - Determine optimal configurations
    - Useful for determining optimal initialization values

- **Weaknesses**
  - Can be very slow
Reinforcement Learning

- Rule updates
  - Internal decision process is self modifying based on live traffic data.
  - Varies with different computational models
- Trust bias
  - Used to weight the response from specific sensors with regard to past performance.
Trust Bias

- Rewards/penalty distributed among IDAs
  - Team adjusts trust of individual IDAs

- Adaptive IDAs
  - React to reward/penalty
  - Notify team of their improvement
  - Team may choose to readjust trust
### Bias Distribution

<table>
<thead>
<tr>
<th>IDA\Decisions</th>
<th>X1</th>
<th>..</th>
<th>Xi</th>
<th>...</th>
<th>Xn</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDA1 (C):w1</td>
<td>0</td>
<td>..0..</td>
<td>1</td>
<td>...0...</td>
<td>0</td>
</tr>
<tr>
<td>IDA2 (P):w2</td>
<td>0.5</td>
<td>..0..</td>
<td>..0.2..</td>
<td>..0..</td>
<td>0.3</td>
</tr>
<tr>
<td>IDA3 (S):w3</td>
<td>(,)</td>
<td>...</td>
<td>(0.2,0.3)</td>
<td>...</td>
<td>(,)</td>
</tr>
<tr>
<td>IDA4 (F):w4</td>
<td>Mid</td>
<td>...</td>
<td>High</td>
<td>...</td>
<td>Low</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IDAm (..):wm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**MAT (with controls on bias)**

<table>
<thead>
<tr>
<th>Team:</th>
<th>1</th>
<th>P1</th>
<th>...</th>
<th>Pi</th>
<th>...</th>
<th>Pn</th>
</tr>
</thead>
</table>
Incremental Machine Learning

- Detection and response systems adapt to changing environment.
  - Normal use changes over time
  - New variations of known attack types
  - Response type may change over time
Dynamic IDA Generation

Improve Accuracy

• If:
  – Low confidence decision
  – Anomalies are disproportionate to classified attacks

• Then:
  – Build new sensor
Dynamic IDA trimming

Improve Efficiency

- **If:**
  - IDA drops below a trust threshold
  - IDA uses too much processing time
    - determined by the administrator

- **Then:**
  - Refactor decision process
  - Remove IDA
Prototype

- Multiple SOMs
  - Each SOM has different initial values.
  - SOMs trained with a supervised data set
  - KDD Cup ’99 Data set
Results

- Current results available at
  - http://spider.doriathproject.com/results/
Experiment Conclusions

- Increase in accuracy
  - Decrease in false attacks
  - Decrease in false normals

- Increase in consistency
  - System reliability increases

- Increase in time
  - Multiple systems take longer to classify
  - Code not optimized for speed
Conclusions
Pros

- Increased effectiveness of attack detection and classification.
- Reduced false positives
- Increased ability to detect IDS avoidance methods.
- Able to integrate with existing devices
Cons

- Increased time to process inputs
- Requires dedicated systems
- Secondary network to secure communication
Current work

- **SPIDeR-NeST**
  - Live implementation
    - IP traffic
    - Firewall Logs
  - VP-Net
    - High bandwidth WAN
Contact Info

- Patrick Miller
  patrick@spider.doriathproject.com
- Atsushi Inoue
  atsushi.inoue@ewu.edu
- Web Site
  http://spider.doriathproject.com
References


