Extracting and Synthesizing Cyberattack Behavior Models for Predictive Intelligence

S. Jay Yang
Professor
Computer Engineering
Director of Global Outreach
Center for Cybersecurity

Rochester Institute of Technology
Too many alerts and too little time!
Cyber defense needs to stay ahead!
Never enough expert knowledge!

Let’s transform passive, reactive, catching-up cyber defense into one with

*Actionable Real-time Predictive Intelligence!*
Innovations Needed

• Semi-supervised and dynamic generation of *attack behavior models* without excessive expert knowledge.

• Unique models summarizing *actionable context* presented in spatial and temporal domains for expert analysis.

• Extrapolated *what-if scenarios* reflecting novel adversary and system/network configuration.
**ASSERT Recognizes Unique Attack Behaviors for Prediction**

* Attack models show mix of attack stages used over time.

* Model transition diagram reveals attack tactics/preferences.

* Higher predictability of future actions using attack models.

* High J-S Divergence shows uniqueness of the attack models.

---


CASCADEx Generates Extrapolated What-if Scenarios

* A small misconfiguration leads to change in likelihood and steps needed to succeed the attack.

<table>
<thead>
<tr>
<th></th>
<th>Amateur</th>
<th>Expert</th>
<th>Comprehensive</th>
<th>Random</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Steps</td>
<td>28.76</td>
<td>20.36</td>
<td>36.54</td>
<td>33.57</td>
</tr>
<tr>
<td>Minimum</td>
<td>10</td>
<td>4</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>Maximum</td>
<td>113</td>
<td>72</td>
<td>168</td>
<td>106</td>
</tr>
<tr>
<td>Failure Rate</td>
<td>0.16</td>
<td>0.01</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>% change</td>
<td>4.35</td>
<td>-26.33</td>
<td>-33.41</td>
<td>-29.14</td>
</tr>
</tbody>
</table>

* Rare-event simulation enables what-if analysis even for unlikely events.

Collaboration Opportunities

Option 1:
Provide *feedback* for desired features and ways to use the system.

Option 2:
*Free-trial analysis* with your sample intrusion alerts, with confidential agreement.

Option 3:
*Joint R&D* to advance desired features or apply in your specific contexts.

Contact **Dr. S. Jay Yang** (*Jay.Yang@rit.edu*) for more details!
Acknowledgement

• Contributing students / alumni / collaborators
  • Dr. Ahmet Okutan, Stephen Moskal, Gordon Werner, Shao-Hsuan Su, & To Chen Chang.
  • Profs. Michael Kuhl, Katie McConky, Daryl Johnson, Bill Stackpole, & Aunshul Rege.

• Research supported by NSF Awards 1526383 and 1742789 and NSA/DHS H98230-15-1-0277.