Research Directions in Cyber Experimentation

Thomas D. Tarman
tdtarma@sandia.gov
Example: 10/21/2016 distributed denial of service attack on Dyn DNS

- Mirai botnet attack from “10s of millions IP addresses”
  - Internet of things
  - E.g. printers, cameras, and baby monitors
- Affected > 60 services, mostly on the US East Coast

Questions for decision makers:

- Dyn engineers - What fraction of botnet requests can Dyn suppress using its available mitigations?
- Policy makers – How does the map change if x% of ISPs implement Best Common Practice 38 (network ingress filtering)?

Many of the model inputs (form and size of attack, device configurations, etc.) are unknown, or known with some uncertainty. How does this uncertainty propagate to results that a decision maker can use?
The need – confidence in cyber experiment results

- Training, design evaluation, response development, etc. in a safe, offline environment
- Support stakeholders who need to make high consequence decisions based on predicted results from our models
  - Rigorous, quantified, defensible
- Correspondence with real world – V&V
  - Configuration import
  - Modeling human and cyber threats
  - Multi-fidelity modeling – convincing stakeholders that the model is predictive
- CEF report\(^1\) identified need for
  - Experimental methodologies and techniques, especially for complex systems
  - Information sharing and synthesis
  - Advances in experimentation capabilities

Research challenges

- Metrics and measures
- Handling uncertainty
  - How does uncertainty propagate through to the results? (sensitivity analysis)
- Helping the experiment designer produce defensible experiments and results
  - Multi-fidelity modeling (putting high/low fidelity where it is needed and defending the choice)
  - Accessible to non-computer scientists (see CEF report)
- Experimental infrastructure to facilitate experimental rigor
  - Design of experiments (experiment design, but also how to drive the experiments in a computationally feasible, yet defensible way)
  - V&V
  - User and threat models
  - Data sharing and analysis
  - Reproducibility (“runnable papers”\(^1\))

\(^1\)B. Heller, “Reproducible network research with high-fidelity emulation,” Ph.D. dissertation, Stanford University, June 2013.
Workshop format and desired outcomes

- Information sharing
  - Platforms, research directions
- Identify unmet needs and research gaps
- Ideas for addressing gaps
  - Collaborations
- Talks and discussion will go into workshop report, to be distributed in mid-late September.
  - Please provide slides if you would like them included in the report
  - Reminder – Discussion is at Unclassified, Unlimited Release level

How can we leverage this group’s tremendous knowledge and capabilities to drive R&D to help decision makers?
<table>
<thead>
<tr>
<th>Time</th>
<th>Topic</th>
<th>Presenter</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:30</td>
<td>Breakfast</td>
<td></td>
</tr>
<tr>
<td>9:00</td>
<td>Introduction, workshop purpose/format</td>
<td>Tom Tarman, Sandia</td>
</tr>
<tr>
<td>9:15</td>
<td>Cybersecurity Experimentation of the Future (CEF)</td>
<td>David Balenson, SRI</td>
</tr>
<tr>
<td>10:15</td>
<td>Building Beyond DETER: Toward the Future of Cyber Experimentation with Advanced DETERLab Technologies</td>
<td>Terry Benzel, USC ISI</td>
</tr>
<tr>
<td>11:00</td>
<td>Break</td>
<td></td>
</tr>
<tr>
<td>11:15</td>
<td>Infrastructure for building Cyber Experimentation Testbeds</td>
<td>Rob Ricci, U. Utah</td>
</tr>
<tr>
<td>12:00</td>
<td>Lunch</td>
<td></td>
</tr>
<tr>
<td>1:00</td>
<td>Scaling techniques for cyber emulation</td>
<td>John Floren, Sandia</td>
</tr>
<tr>
<td>1:30</td>
<td>Building dedicated Emulytics nodes with coreboot, u-root, and minimega</td>
<td>Ron Minnich, Google</td>
</tr>
<tr>
<td>2:00</td>
<td>Staghorn: An Automated Large-Scale Distributed System Analysis Platform</td>
<td>Steven Elliott, Sandia</td>
</tr>
<tr>
<td>2:30</td>
<td>Break</td>
<td></td>
</tr>
<tr>
<td>2:45</td>
<td>Virtually the Same? The Empirical Differences Between Physical and Virtual Networks</td>
<td>Jon Crussell, Sandia</td>
</tr>
<tr>
<td>3:15</td>
<td>TBD</td>
<td></td>
</tr>
<tr>
<td>3:45</td>
<td>Discussion/next steps/wrap up</td>
<td>Casey Deccio, All</td>
</tr>
<tr>
<td>4:45</td>
<td>Adjourn</td>
<td></td>
</tr>
</tbody>
</table>
Questions for wrap-up discussion

- What are the user needs?
- How can the user select the right tool for the experimental question?
- What are the research gaps?
  - Technical gaps in experimental infrastructure
  - Gaps between tool research and where the user applies the tools
- How can we address the gaps?
Thank You

- Casey Deccio, David Fritz
- Jeff Boote, Zach Benz, David White
- Lynde Farhat-Corbett, Stephani Pease, Megan Sabo, Jenni Hidalgo
- Garré Vineyard and Winery
- Presenters
- Attendees