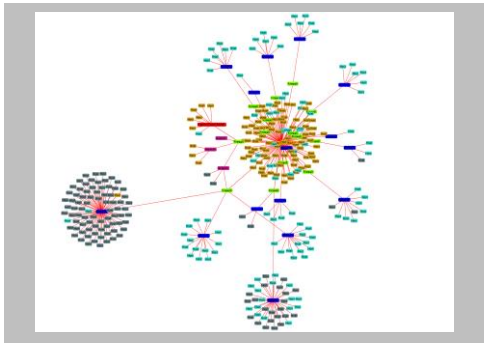
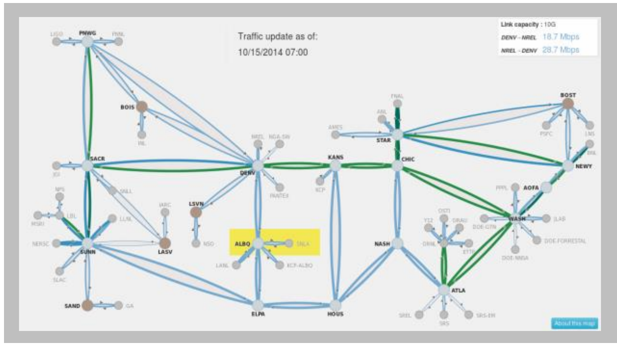
Exceptional service in the national interest

Sandia National Laboratories

Operator
Cyber Attacks
HMI
Security App
Hosted Services (DNS)
RTU Device
Network
PLC Device
Network
RTU Device
Refinery
Physical Attacks
Power System





Research Directions in Cyber Experimentation

Thomas D. Tarman

tdtarma@sandia.gov

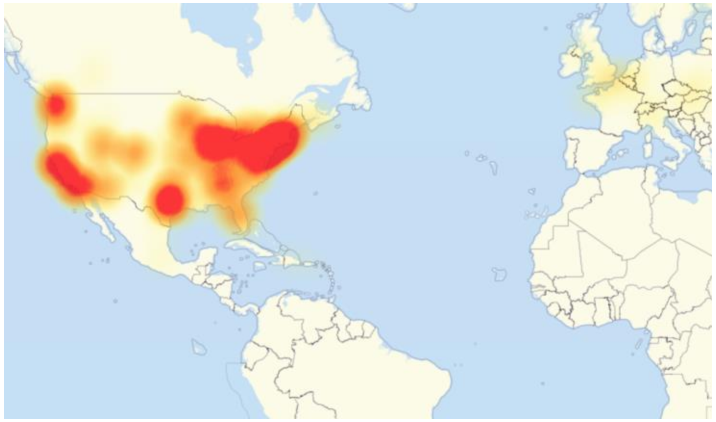
U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-8537 C.

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



Source: DownDetector

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

[1] "Cybersecurity Experimentation of the Future", available at http://www.cyberexperimentation.org/report/

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?

Agenda

Time	Topic	Presenter
8:30	Breakfast	
9:00	Introduction, workshop purpose/format	Tom Tarman, Sandia
9:15	Cybersecurity Experimentation of the Future (CEF)	David Balenson, SRI
10:15	Building Beyond DETER: Toward the Future of Cyber Experimentation with Advanced DETERLab Technologies	Terry Benzel, USC ISI
11:00	Break	
11:15	Infrastructure for building Cyber Experimentation Testbeds	Rob Ricci, U. Utah
12:00	Lunch	
1:00	Scaling techniques for cyber emulation	John Floren, Sandia
1:30	Building dedicated Emulytics nodes with coreboot, u-root, and minimega	Ron Minnich, Google
2:00	Staghorn: An Automated Large-Scale Distributed System Analysis Platform	Steven Elliott, Sandia
2:30	Break	
2:45	Virtually the Same? The Empirical Differences Between Physical and Virtual Networks	Jon Crussell, Sandia
3:15	TBD	
3:45	Discussion/next steps/wrap up	Casey Deccio, All
4:45	Adjourn	

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