SRI International

PANEL: Cybersecurity Experimentation of the Future (CEF): Catalyzing a New Generation of Experimental Cybersecurity Research

December 10, 2015

David Balenson
Computer Science Laboratory
SRI International

Panel Topics and Questions

The role of experimental science and its corresponding future needs for advances in methodologies and techniques, new approaches to community collaboration, and advanced infrastructure for applied cybersecurity research.

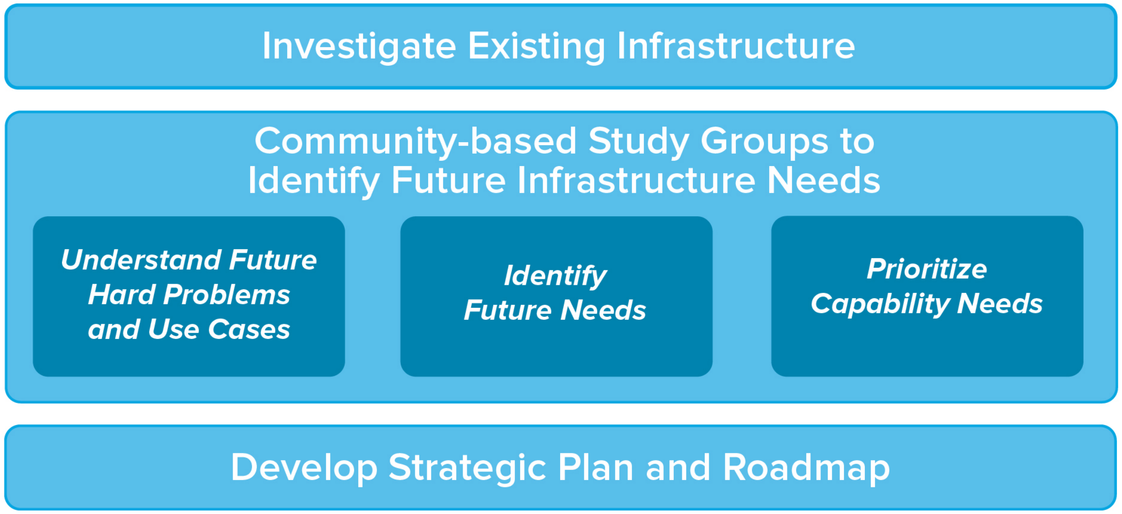
- Briefly describe your research and work in the area of cybersecurity and cybersecurity experimentation.
- What is your perspective on the role of experimental science and research infrastructure in the cybersecurity space?
- What experimental infrastructure have you developed and/or do you leverage as part of your cybersecurity research?
- What are the key experimentation tools and methodologies needed to support future research?
- How can the research community best collaborate to generate and share experimental infrastructure, tools, and/or results?
- What do you see as your role as an early supporter, adopter, or contributor to advanced, accessible experimentation infrastructure?

CEF Study

- Community-based effort to study current and expected cybersecurity experimentation infrastructure, and to produce a strategic plan and roadmap for developing infrastructure that supports tomorrow’s research

SRI and USC-ISI Collaborative Team

Advisory Group



Investigate Existing Infrastructure

Community-based Study Groups to Identify Future Infrastructure Needs

Understand Future Hard Problems and Use Cases

Identify Future Needs

Prioritize Capability Needs

Develop Strategic Plan and Roadmap

Funded by NSF CISE/ACI under awards ACI-1346277 and ACI-1346285

CEF Report

The CEF Report presents a strategic plan and enabling roadmap intended to catalyze generational advances in experimental cybersecurity research

- Executive Summary
- Introduction
- Study Description
- Survey of Existing Infrastructure
- Roadmap
- Conclusions and Recommendations
- Acknowledgements
- References
- Appendices
  - Survey of existing infrastructure
  - Study Group agendas and participants
  - Advisory Group

Cybersecurity Experimentation of the Future (CEF): Catalyzing a New Generation of Experimental Cybersecurity Research

Community Plan and Roadmap to Develop Future Experimentation Infrastructure in Support of Cybersecurity Research

FINAL REPORT
July 31, 2015

The Need for Transformational Progress

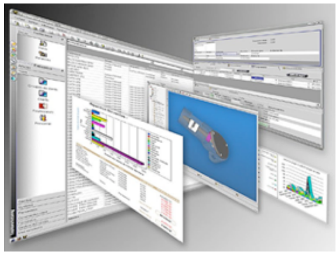
- Transformational progress in three distinct, yet synergistic areas is required to achieve the desired objectives:

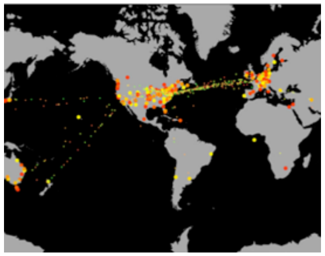
1) Fundamental and broad intellectual advance in the field of experimental methodologies and techniques
    - With particular focus on complex systems and human-technical interactions
2) New approaches to rapid and effective sharing of data and knowledge and information synthesis
    - That accelerate multi-discipline and cross-organizational knowledge generation and community building
3) Advanced experimental infrastructure capabilities and accessibility

A Science of Cybersecurity Experimentation!

A Definition of “Cybersecurity Experimentation Infrastructure”

- General purpose ranges and testbeds (physical and/or virtual)
- Specialized ranges and testbeds (physical and/or virtual)
- Software tools that supports one or more parts of the experiment life cycle, including, but not limited to:
  - Experiment design
  - Testbed provisioning software
  - Experiment control software
  - Testbed validation
  - Human and system activity emulators
  - Instrumentation – systems and humans
  - Data analysis
  - Testbed health and situational awareness
  - Experiment situational awareness
  - Other similarly relevant tools
- Specialized hardware tools – simulators, physical apparatus, etc.

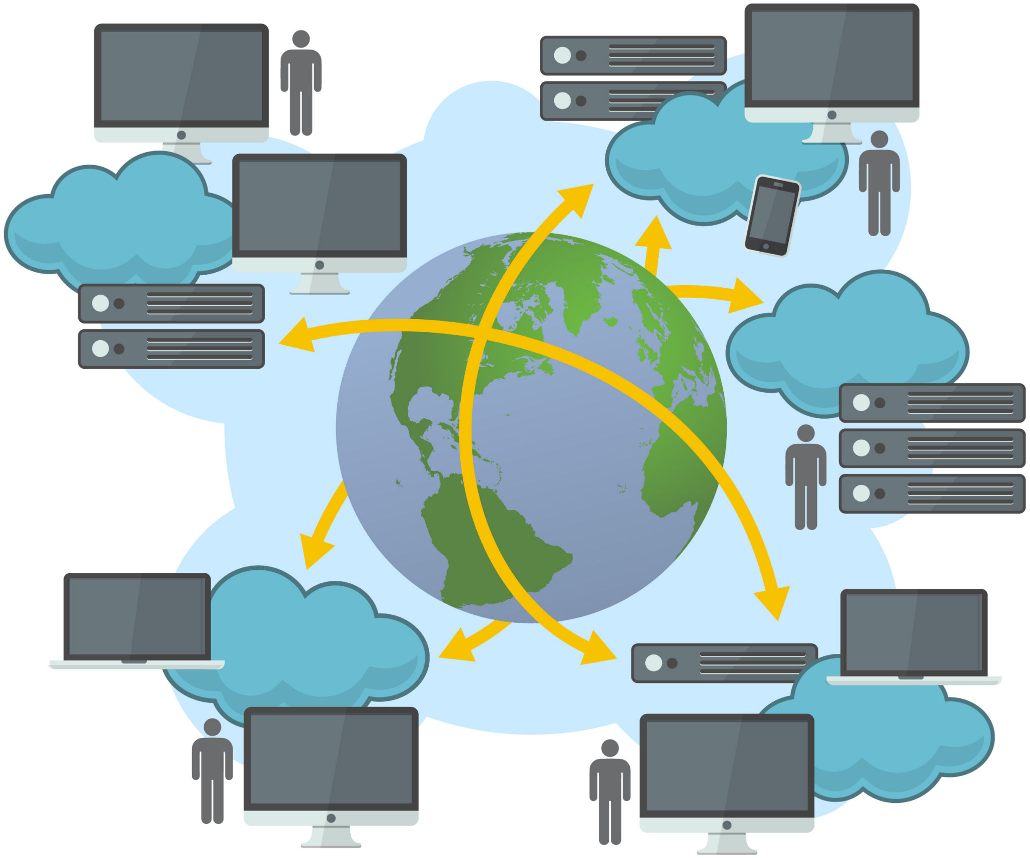




Ecosystem of Different Experimental Capabilities Spanning Multiple Domains

- The goal is not to create a single instance of a cyber experimentation testbed or facility
- Over time the roadmap may be realized through an ecosystem of many different instantiations
  - Small, stand-alone
  - Localized
  - Large distributed

all spanning multiple domains



Panel

- Moderator:
  - David Balenson, Computer Science Laboratory, SRI International
- Panelists:
  - Terry Benzel, Deputy Division Director, Internet and Networked Systems, USC Information Sciences Institute
  - Trent Jaeger, Professor of Computer Science and Engineering and Co-Director of the SIIS Lab, Pennsylvania State University
  - Jinpeng Wei, Assistant Professor, School of Computing and Information Science, Florida International University
  - Lee Rossey, CTO, SimSpace

David Balenson, SRI International

- David Balenson is a Senior Computer Scientist in the Computer Science Laboratory at non-profit research institute SRI International.
- He provides technical and project management support for the U.S. Department of Homeland Security Science and Technology Directorate (DHS S&T) Cyber Security R&D Program, including the DETER Project.
- Balenson is a Co-PI for the NSF-funded Cybersecurity Experimentation of the Future (CEF) project, a community-based effort to study current and expected cybersecurity experimentation infrastructure, and to produce a strategic plan and roadmap for developing infrastructure that supports tomorrow's research.

Terry V. Benzel, USC-ISI

- Terry V. Benzel is Deputy Director for the Computer Networks Division at the Information Sciences Institute (ISI) of the University of Southern California (USC). She participates in business development, technology transfer and special projects with industrial and academic partners.
- She is the technical project lead for the Cyber Defense Technology Experimental Research (DETER) testbed projects funded by DHS, NSF and DARPA. The projects are developing an experimental infrastructure network and scientifically rigorous testing frameworks and methodologies to support the development and demonstration of next-generation information security technologies for cyber defense.
- Terry is the USC-ISI PI for the CEF study.

Trent Jaegar, Penn State

- Trent Jaeger is a Professor in the Computer Science and Engineering Department at The Pennsylvania State University (PSU) and the Co-Director of the Systems and Internet Infrastructure Security (SIIS) Lab.
- His research area is computer security, specifically systems security, program analysis for security, virtualization, trusted computing, and access control.
- Trent is also a member of the Army Research Laboratory (ARL) Cyber-Security Collaborative Research Alliance (CRA) led by PSU.

Jinpeng Wei, Florida International

- Jinpeng Wei is an assistant professor at the School of Computing and Information Sciences, and the director of the Systems Security Lab at Florida International University.
- His research interests include secure computer systems, including stealthy malware detection and defense, botnet C&C covert channels, high assurance of systems software, information flow security in distributed systems (e.g., web service composition), security in cloud computing, and software vulnerability modeling, detection, risk-assessment, and prevention.
- Jinpeng presented the paper, MOSE: Live Migration Based On-the-Fly Software Emulation, this morning at the conference.

Lee Rossey, SimSpace

- **Lee Rossey** is the Chief Technology Officer and Co-founder of SimSpace, an early stage cyber security software company offering state-of-the art network emulation and modeling tools for realistic cyber training, assessment, and hardening.
- Lee was previously a Group Leader for the Cyber System Assessments Group at MIT Lincoln Laboratory (MIT-LL) where he and the team developed tools and processes for conducting independent assessments of cyber systems and capabilities for the U.S. Government.

Panel Topics and Questions

The role of experimental science and its corresponding future needs for advances in methodologies and techniques, new approaches to community collaboration, and advanced infrastructure for applied cybersecurity research.

- Briefly describe your research and work in the area of cybersecurity and cybersecurity experimentation.
- What is your perspective on the role of experimental science and research infrastructure in the cybersecurity space?
- What experimental infrastructure have you developed and/or do you leverage as part of your cybersecurity research?
- What are the key experimentation tools and methodologies needed to support future research?
- How can the research community best collaborate to generate and share experimental infrastructure, tools, and/or results?
- What do you see as your role as an early supporter, adopter, or contributor to advanced, accessible experimentation infrastructure?

SRI International

Thank You

David Balenson

703-247-8551

David.balenson@sri.com

Headquarters
333 Ravenswood Avenue
Menlo Park, CA 94025
+1.650.859.2000

Princeton, NJ
201 Washington Road
Princeton, NJ 08540
+1.609.734.2553

Additional U.S. and
international locations

www.sri.com