SRI International

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

January 14, 2016

Laura S. Tinnel
Computer Science Laboratory – Infrastructure Security Group
SRI International

What is CEF?

- Joint effort between SRI/ USC-ISI
- Community-based study
- Identify cybersecurity experimentation infrastructure needs for future research
- Determine gaps between needs and what currently exists
- Goal: create strategic plan, enabling roadmap intended to catalyze generational advances in experimental cybersecurity 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

Study completed 2015

Source: https://www.nsa.gov/research/tnw/tnw192/article4.shtml

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

“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.

CEF Results

The CEF Report published July 2015

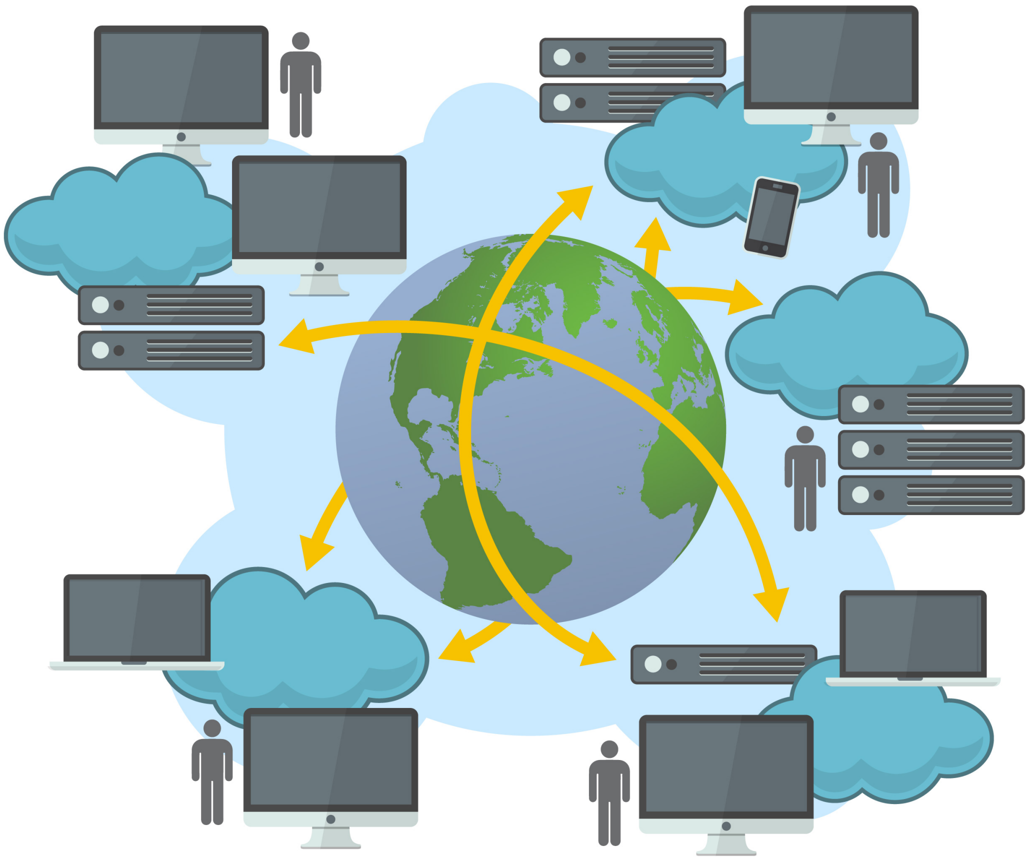
- Vision for future cybersecurity experimentation
- Capabilities needed
- High level gap analysis
- Top Five Recommendations
- Overarching findings

www.CyberExperimentation.org

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

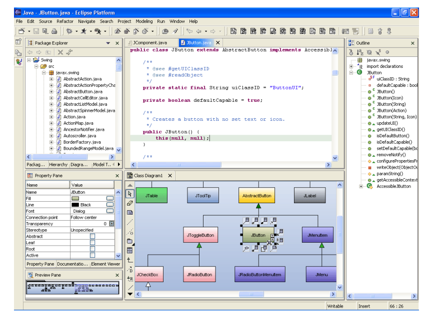
all spanning multiple domains

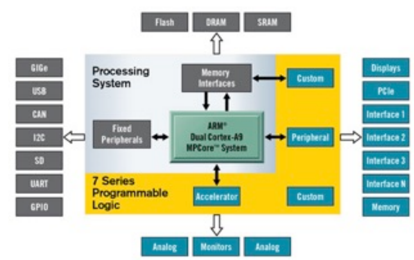


Hybrid Architectures Based on Different Building Blocks

- Cloud technology
- Software defined networking (SDN)
- Knowledge sharing and community environments
- Integrated Development Environments
  - E.g., Eclipse
- Emulated and simulated environments
  - E.g., RTDS, wireless
- Specialized hardware
  - E.g., FPGA, GPU, Intel Xeon Phi

- No single hardware/software substrate





Roadmap: 30 Key Capabilities in 8 Core Areas

Section and Area	Capabilities
4.1 Domains of applicability	Support for cross domain experimentation (critical infrastructure sectors)
	Multidisciplinary experimentation that includes computer science, engineering, mathematics, modeling, human behavior, sociology, economics, and education
	Portability of experiments, packaged for sharing and use in cross-discipline experiments
4.2 Modeling the real world for scientifically sound experiments	Models of real world environments
	Experiments that scale
	Experimentation with systems-of-systems
	Human activity
4.3 Frameworks and building blocks for extensibility	Workflow & management (comprehensive, human)
	Open/standard interfaces (API for extensibility, plugins write to API)
	Building Blocks (libraries)
	Tool integration framework (to glue pieces together)
4.4 Experiment design and instantiation	Design tools, specifications, ontologies, compiler
	Reusable designs for science-based hypothesis testing
	Automated discovery of local and distributed resources
	Dynamic instantiation of domain-specific test apparatus
	Validation of instantiated test environments and apparatus

Roadmap: 30 Key Capabilities in 8 Core Areas

Section and Area	Capabilities
4.5 Interconnected research infrastructure	Automated, transparent federation to interconnect resources
	Dynamic and on demand, with sharing models
	Support integrated experiments that include real, emulated (virtual), and simulations
4.6 Experiment execution and management	Experiment orchestration
	Visualization and interaction with experiment process
	Experiment debugging with checkpoint and rollback
	Experiment execution validation
4.7 Instrumentation and experiment analysis	Instrumentation and data collectors
	Transport and protection mechanisms
	Data repositories
	Data analysis
4.8 Meta properties	Usability (experiments, owner/operator)
	Confidentiality, availability and integrity of experiment ecosystem
	Social and cultural changes

Survey of Existing Infrastructure - High Level Gap Analysis

- Surveyed mostly US-based infrastructure
- Existing, openly available cybesecurity experimentation research infrastructure (i.e., testbeds, tools, and methodologies) mapped to needed capabilities

Top 5 Recommendations

- **Domains of Applicability**
  - **Multidisciplinary Experimentation:** Focus on multidisciplinary experimentation that includes computer science, engineering, mathematics, modeling, human behavior, sociology, economics, and education
- **Modeling the Real World for Scientifically Sound Experiments**
  - **Human Activity:** Accurately represent fully reactionary complex human and group activity in experiments, including live and synthetic humans
- **Frameworks and Building Blocks for Extensibility**
  - **Open Interfaces:** Develop common models of infrastructure and experiment components to open interfaces and standards
- **Experiment Design and Instantiation**
  - **Reusable Designs for Science-based Hypothesis Testing:** Create open standards and interfaces, for both experimental infrastructure facilities and for experiments themselves
- **Meta-properties**
  - **Usability and Cultural Changes:** Cybersecurity research infrastructure must be usable by a wide range of researchers and experts across many different domains of research, and researchers must make a concerted effort to take advantage of community based resources

Core requirements needed to enable others

Overarching Findings: The Need for Transformational Progress

Transformational progress in three distinct, yet synergistic areas is required:

1) Fundamental and broad intellectual advance in the field of experimental methodologies and techniques
   - Particular focus on complex systems and human-technical interactions

2) New approaches to rapid and effective sharing of data and knowledge and information synthesis
   - Accelerate multi-discipline and cross-organizational knowledge generation and community building

3) Advanced experimental infrastructure capabilities and accessibility

Need: A Science of Cybersecurity Experimentation

What's Next?

- Catalyze Collaboration and Sharing
  - Set up infrastructure to enable sharing and discussion
  - Community-wide identification of existing components to share – from prior research efforts
- Moving Forward
  - Structure research efforts to include as outputs newly developed sharable infrastructure
  - Identify and encourage investment in core capabilities by research funding organizations

Thank You

Laura Tinnel
703-247-8533
Laura.Tinnel@sri.com

Source: https://www.nsa.gov/research/tnw/tnw192/article4.shtml

www.CyberExperimentation.org

SRI International

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

BACKUP

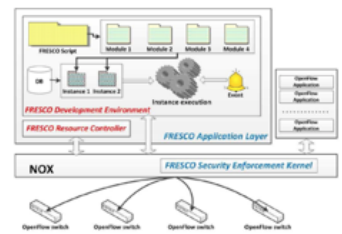
Science of Cybersecurity Experimentation

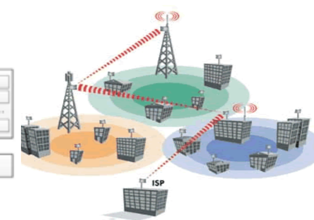
- New direction for the field of experimental cybersecurity R&D
- R&D must be grounded in scientific methods and tools to fully realize the impact of experimentation
- Different than and complementary with the science of cybersecurity

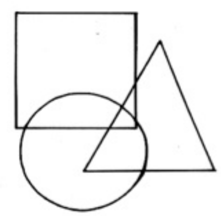
- New approaches to sharing all aspects of the experimental science – data, designs, experiments, and research infrastructure
- Cultural and social shifts in the way researchers approach experimentation and experimental facilities
- New, advanced experimentation platforms that can evolve and are sustainable as the science and the community mature

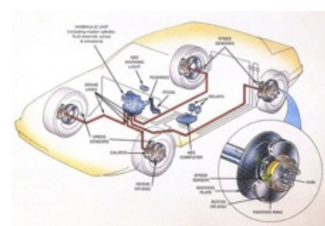
Motivation: Why are We Doing This?

- Society's cyber dependencies are rapidly evolving
- In nearly every aspect of our lives, we are moving toward pervasive embedded computing with a fundamental shift in network properties
- These changes bring a very real and wide-ranging set of challenging cyber threats
- Addressing these challenges will require cybersecurity research based on sound scientific principles
- The scale and complexity of the challenges will require that researchers apply new experimentation methods that enable discovery, validation, and ongoing analysis









Research Infrastructure for **Cybersecurity Research**

- Cybersecurity R&D is still a relatively young field
- It involves intrinsically hard challenges
  - Inherent focus on worst case behaviors and rare events
  - In the context of multi-party and adversarial/ competitive scenarios
- Research infrastructure is crucial
  - Allow new hypotheses to be tested, stressed, observed, reformulated, and ultimately proven before making their way into operational systems
- Ever increasing cyber threat landscape demands new forms of R&D and new revolutionary approaches to experimentation and test
- Clearly a need for future research infrastructure that can play a transformative role for future cybersecurity research