Terry Benzel
USC – ISI
December 10, 2015

Cybersecurity Experimentation of the Future (CEF)

Three of the Panel Questions

- 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?

The DETER Project

- A research program:
  - To advance capabilities for experimental cybersecurity research
- A testbed facility:
  - To serve as a publicly available national resource…
- A community building activity:
  - To foster and support collaborative science

The DETER Facility

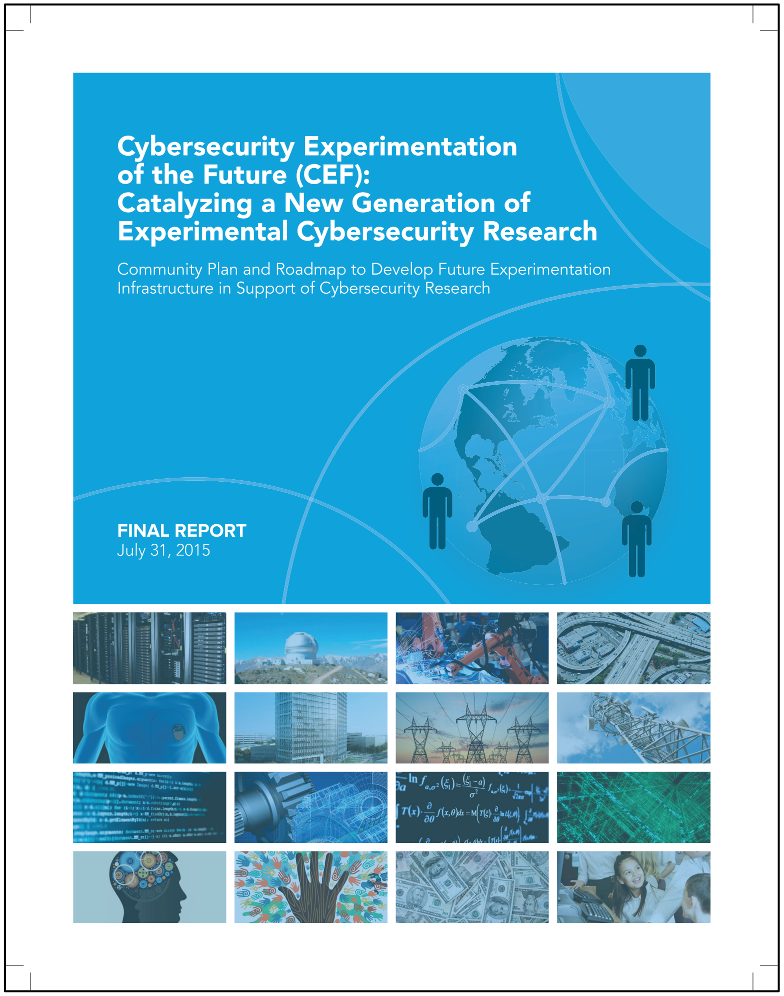
A general purpose, *Accessible Remote* flexible platform for modeling, emulation, and controlled study of large, complex networked systems

- Elements located at USC/ISI (Los Angeles), UC Berkeley, and USC/ISI (Arlington, VA)
- Funded by NSF and DHS, started in 2003
- Based on Emulab software, with focus on security experimentation
- Shared resource – multiple simultaneous experiments subject to resource constraints
- Open to academic, industrial, govt researchers essentially worldwide – very lightweight approval process

Key Technologies and Capabilities

- Multi-resolution virtualization
- Scalable experimental control
- Traffic generation facilities
- Human behavior modeling tools
- Data collection, visualization and situational awareness support

Cybersecurity Experimentation of the Future (CEF)



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

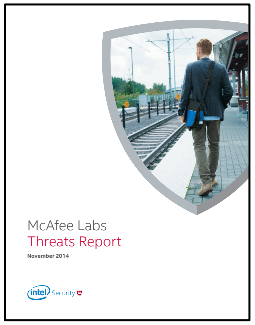
Community Plan and Roadmap to Develop Future Experimentation Infrastructure in Support of Cybersecurity Research

FINAL REPORT
July 31, 2015

- SRI and USC Study
- Created roadmap:
- Available for download:
- http://www.cyberexperimentation.org/report/

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



McAfee Labs
Threats Report
November 2014

intel Security

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

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

Dependable Experiment
Repeatability
Reproducibility
Validity

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

- 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

Where is Experimentation Applicable?

- Overarching goal is to increase researcher effectiveness and support the generation and preservation of solid empirical evidence
  - Infrastructure to enable research, not constrain
  - New mechanisms to capture and share knowledge (designs, data and results) to enable peer review and allow researchers to build upon each other
- Experimentation is about learning
  - To perform an evaluation (not formal T&E)
  - To explore a hypothesis
  - To characterize complex behavior
  - To complement a theory
  - To understand a threat
  - To probe and understand a technology

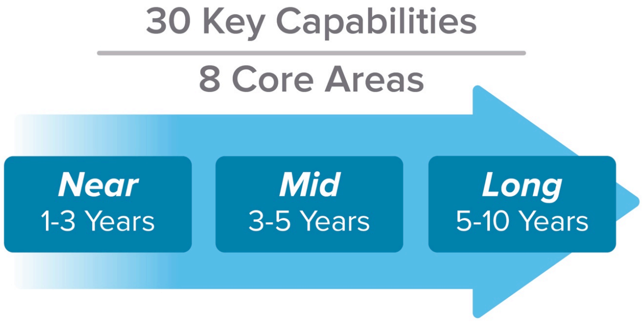
Representative Cybersecurity Hard Problems

- Systems/software
  - Human interactions
  - System of system security metrics
  - Emergent behavior in large scale systems
  - Supply chain and root of trust
  - Societal impacts and regulatory policies
- Networking
  - Anonymity and privacy of data and communication
  - Trust infrastructure
  - Software defined networking (SDN)
  - Political, social, and economic (balance-of-interest) goals in network design
  - Pervasive communications, across organizational and political boundaries

- Cyber-physical systems
  - Embedded devices
  - Autonomous vehicles, smart transportation
  - Electric power, smart grid
  - Medical implants, body sensors, etc.

Roadmap

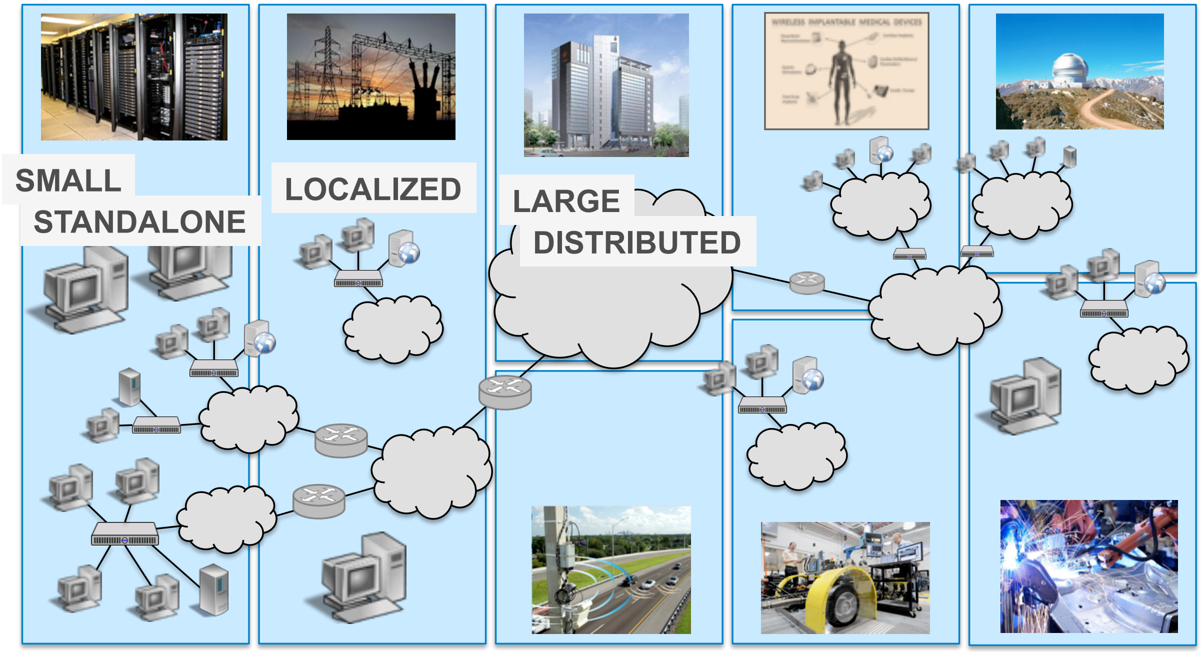
- Requirements, objectives and goals: 30 key capabilities organized into 8 core areas over 3, 5, and 10 year phases



- Key capabilities consider:
  - Current experimental cybersecurity research and its supporting infrastructure
  - Other types of research facilities
  - Existing cyber-domain “T&E” capabilities

Ecosystem of Different Experimental Capabilities Spanning Multiple Domains

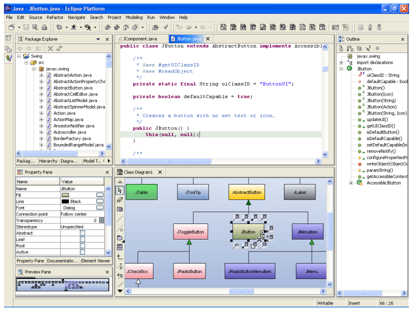
- The goal is not to create a single instance of a cyber experimentation testbed or facility
- Over time the roadmap may be realized through an ecosystem of many different instantiations – from small, stand-alone and localized to large distributed experimental capabilities, all spanning multiple domains



Hybrid Architectures Based on Different Building Blocks

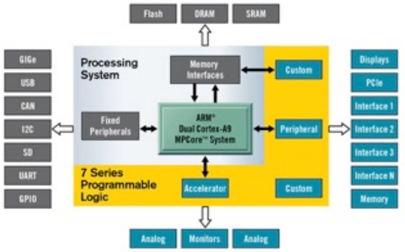
- Cloud technology
- Software defined networking (SDN)
- Knowledge sharing and community environments
- Integrated Development Environments
  - E.g., Eclipse
- Emulated and simulated environments
  - E.g., RTDS, wireless
- Specialized hardware
  - E.g., FPGA, GPU, Intel Xeon Phi

- No single hardware/software substrate



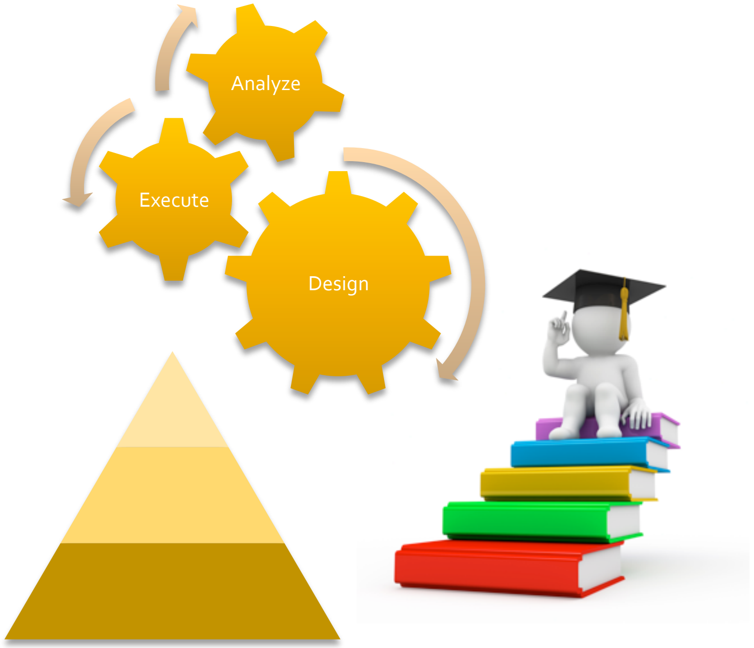
```
public class JButton extends AbstractButton implements Accessibl

    /**
     * @see #getUIClassID
     * @see #readObject
     */
    private static final String uiClassID = "ButtonUI";

    private boolean defaultCapable = true;

    /**
     * Creates a button with no set text or icon.
     */
    public JButton() {
        this(null, null);
    }

    /**
```

Name	Value
Name	JButton
Fill	
Line	Black
Font	Dialog
Connection point	Follow center
Transparency	0
Stereotype	Unspecified
Abstract	□
Leaf	□
Root	□
Active	□



Research Infrastructure is More than Infrastructure

- Research infrastructure >> infrastructure of machines and tools
  - Scientific methodologies, experimental processes, and education are critical to effective use of the machines and tools
- Research infrastructure requires meta-research into:
  - Design specification (multi-layered languages and visualization)
  - Abstraction methodologies and techniques
  - Semantic analysis and understanding of experimenter intent
  - Formal methods and a rich approach to modeling to satisfy science objectives



Top 5 Recommendations

(1) **Domains of Applicability – Multidisciplinary Experimentation:** Focus on multidisciplinary experimentation that includes computer science, engineering, mathematics, modeling, human behavior, sociology, economics, and education

(2) **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

(3) **Frameworks and Building Blocks for Extensibility – Open Interfaces:** Develop common models of infrastructure and experiment components to open interfaces and standards

(4) **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

(5) **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

Summary and Call to Action

- Growing experimentation community increasingly engaged in experimental science of cyber security
- Collaboration is key to mission

Join us

www.cyberexperimentation.org/report/