Poster: Cybersecurity Experimentation of the Future:

Catalyzing a New Generation of Experimental Cybersecurity Research

David Balenson, Laura Tinnel
SRI International
Arlington, VA
{david.balenson|laura.tinnel}@sri.com

Terry Benzel
USC Information Sciences Institute
Marina del Rey, CA
tbenzel@isi.edu

***Abstract*—The ever-increasing cyber threat landscape demands new forms of advanced research and development coupled with new revolutionary approaches to cyber experimentation. SRI International and USC Information Sciences Institute produced a strategic plan and roadmap intended to catalyze generational advances in the field of experimental cybersecurity research [1]. These results represent the conclusions of our Cybersecurity Experimentation of the Future (CEF) study, conducted with broad participation by the cybersecurity research, research sponsor, and customer communities. Our overarching finding is that transformational progress in three distinct, yet synergistic, areas is required: (1) fundamental advances in the field of experimental methodologies and techniques; (2) new approaches to accelerate multi-discipline and cross-organizational knowledge generation and community building; and (3) advanced experimentation infrastructure capabilities and accessibility. The central result of our study is a roadmap that presents requirements, objectives and goals in eight core capability areas, over three, five and ten year phases. Our conclusion is that strong, coupled, and synergistic advances across each of the capabilities areas will move the field beyond today's state of the art.**

Keywords—cybersecurity; experimental research; research infrastructure; experimental methodologies and techniques; knowledge sharing; experimentation infrastructure

I. INTRODUCTION

Cybersecurity is a relatively young field. By nature, it focuses on worst-case adversary-driven system behaviors and rare events. This means that cybersecurity researchers must address a number of intrinsically hard challenges. Reliable research infrastructure is crucial to the cybersecurity experimentation process. It enables new research hypotheses to be tested, stressed, observed, reformulated, and ultimately proven before making their way into production environments.

The ever increasing cyber threat landscape demands new forms of advanced research and development and in parallel new revolutionary approaches to experimentation. While the current state of the art in cybersecurity experimentation has recently had increased focus and investment, there is clearly a need for future research infrastructure that can play a transformative role for cybersecurity research well into the next decade.

This material is based upon work supported by the National Science Foundation under Grant No. ACI-1346277 and ACI-1346285. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

Members of SRI International's Computer Science Laboratory (SRI) and the University of Southern California's Information Sciences Institute (USC-ISI) conducted the CEF study as a collaborative effort, with broad participation by members of the cybersecurity research, research sponsors, and customer communities. An Advisory Group, comprised of seven senior leaders from government, industry, and academia, helped inform and guide our work. The study included three main thrusts: (1) investigate and assess existing experimentation infrastructure and user community experience; (2) identify future cybersecurity experimentation infrastructure needs; and (3) organize the requirements and needed capabilities into a strategic plan and roadmap for future cybersecurity infrastructure development. The future needs were identified through a series of community-based study groups to understand hard cybersecurity problems and use cases that can benefit from experiment-driven research, identify the experimentation infrastructure needed to facilitate research, identify gaps between needed and current capabilities, and prioritize capabilities based on domain needs.

II. FIELD OF EXPERIMENTAL CYBERSECURITY R&D

It became clear at the outset of the study that research infrastructure encompasses far more than just test apparatuses. Thus, our overarching finding is that transformational progress in three distinct, yet synergistic, areas is required to achieve the desired objectives: (1) broad intellectual advances 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; and (3) advanced experimentation infrastructure capabilities and accessibility [1].

These three objectives point to a new direction for the field of experimental cybersecurity research and development. The importance of research into *the science of cybersecurity experimentation* is an overarching need. Any set of requirements or capabilities for cybersecurity experimentation must be backed by transformational progress in the science of experimentation. It is only by grounding our research in scientific methods and tools that we can realize the impact that experimentation can have. It should be noted that this call for research into the science of cybersecurity experimentation is different from the current fundamental research into the science of cybersecurity, though they are certainly complementary in their eventual goals. Along with establishing a field of research into the science of cybersecurity

experimentation, substantial new approaches to sharing are needed in order to enable scalable, cross-discipline experiments. Needed new approaches to sharing include all aspects of the experimental science, from data, to designs, to experiments to the research infrastructure itself. In addition, cultural and social shifts in the way in which researchers approach experimentation and experimental facilities are needed. Our final recommendation is that experimental facilities need new, advanced experimentation platforms that can evolve and are sustainable as the science and the community mature.

III. Roadmap of Key Capabilities

The central result of our study is a roadmap that presents requirements, objectives and goals of 30 key capabilities in eight core areas, over three, five and ten year phases [1]. The capability areas are organized in a layered structure from the outside "application" layer to the base system and a corresponding set of meta-properties. Thus they move from domains of applicability, to models, to frameworks, to design, to interconnection, to execution, and finally to instrumentation and analysis. Each of these capability groups and their corresponding capabilities are briefly described below:

Domains of applicability

- Support for cross domain experimentation (critical infrastructure sectors)
- Multidisciplinary experimentation that includes computer science, engineering, math/modeling, human behavior, sociology, and economics
- Portability of experiments, packaged for sharing and use in cross-discipline experiments

Modeling the real world for scientifically sound experiments

- Models of real world environments
- Experiments that scale
- Experimentation with systems-of-systems
- Human activity

Frameworks and building blocks for extensibility

- Workflow and management (comprehensive, human)
- Open/standard interfaces (API for extensibility, plugins written to API)
- Building blocks (libraries)
- Tool integration framework (to glue the pieces together)

Experiment design and instantiation

- Design tools, specifications, ontologies, and compilers
- 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

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

Experiment execution and management

- Experiment orchestration
- Visualization and interaction with experiment process
- Experiment debugging (checkpoint and rollback)
- Experiment execution validation

Instrumentation and experiment analysis

- Instrumentation and data collectors
- Transport and protection mechanisms
- Data repositories
- Data analysis

Meta-properties

- Usability (researchers, owners/operators)
- Confidentiality, availability and integrity of experiment ecosystem
- Social and cultural changes

Taken together, these areas paint a vision for a new generation of experimental cybersecurity research – one that offers powerful assistance in helping researchers shift the asymmetric cyberspace context to one of greater planning, preparedness, and higher assurance fielded solutions.

IV. Conclusion

The capabilities identified in the roadmap take into account the current state of the art in experimental cybersecurity research and its supporting infrastructure. We found that a large amount of the research infrastructure and capabilities needed either do not exist or are not generally available for use. A set of shared, vetted community research capabilities will provide a solid basis upon which to build future cyber experimentation environments. Its use will increase sharing amongst researchers and reduce the time and money spent building one-off test environments in support of new research efforts. Building upon previously vetted capability components and utilizing test environment validation tools will improve overall experimental result quality. Uncaught errors in a test environment can not only invalidate a specific experiment but could also amplify as other research efforts are built upon invalid results and then make their way into products.

An emphasis on infrastructure alone will fall far short of achieving the transformational shift in research, community, and the supporting experimentation required to address cybersecurity in the rapidly changing cyber environment. In addition to leveraging current and expected capabilities in cybersecurity and adjacent areas, we assume there will be advances in key computer science disciplines such as ontologies, meta-data, libraries, and corresponding resource discovery. Our fundamental conclusion is that strong, coupled, and synergistic advances across each of the areas outlined above – fundamental methodological development, fostering and leveraging communities of researchers, and in the capabilities of the infrastructure supporting that research – will move the field beyond today's state of the art.

References

[1] D. Balenson, L. Tinnel, and T. Benzel, Cybersecurity Experimentation of the Future (CEF): Catalyzing a New Generation of Experimental Cybersecurity Research (DRAFT), February 27, 2015 (http://www.cyberexperimentation.org/cef-draft-report/)