Roadmap to safer cyberspace

December 17 2015

Cybersecurity experimentation spans multiple domains and multiple disciplines. Credit: Information Sciences Institute, USC Viterbi School of Engineering

How do cybersecurity experts discover how to properly defend a system or build a network that's secure?

As in other domains of science, this process involves hypothesis, experimentation, and analysis—or at least it should. In reality, cybersecurity research can happen in an ad hoc fashion, often in crisis mode in the wake of an attack.

However, a set of researchers has imagined a different approach, one in which experts can test their theories and peers can review their work in realistic but contained environments—not unlike the laboratories found

in other fields of science.

"Our adversaries have an incredible environment for testing out attacks: the Internet, on which all our production systems operate," said Terry Benzel, deputy director for the Internet and Networked Systems Division at the Information Sciences Institute (ISI) of the University of Southern California. "They can sit and analyze our vulnerabilities for as long as they want, probe and poke and run experiments until they find the right way in. Our researchers and leading technology developers don't have anything like that."

This "asymmetry," as researchers call it, is part of the reason so many cyberattacks and breaches occur. It also served as motivation for the the National Science Foundation (NSF) moving in 2013 to fund a multi-year effort to determine how to best advance the field of experimental cybersecurity.

Led by cybersecurity researchers from SRI International and ISI with decades of years of experience designing, building, and operating large cybersecurity testbeds, the effort involved more than 150 experts, representing 75 organizations. They participated in three workshops in 2014.

The researchers released a report resulting from this activity, titled "Cybersecurity Experimentation of the Future (CEF): Catalyzing a New Generation of Experimental Cybersecurity Research," in July 2015.

The Science of Cybersecurity Experimentation

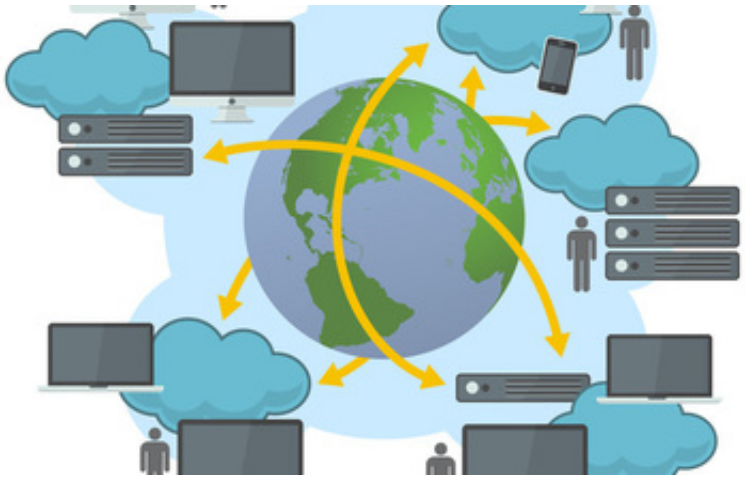
Though one might expect the report to focus on the types of hardware, software and networking required for conducting cybersecurity experiments, the main takeaway is even more fundamental: the research community needs to develop a "science of cybersecurity

experimentation."

The report stressed that key elements of that discipline should include methods, approaches and techniques that researchers can use to create reproducible studies that the community can test, reuse and build upon.

"Experimentation is an inherent part of the scientific method and you can't do research without doing experimentation," said Douglas Maughan, Director of the Cyber Security Division at the Department of Homeland Security, Science and Technology Directorate. "This report is a critical first step to re-think what is needed in cyber experimentation before we build the infrastructure."

Using the scientific method also requires peer review and repeatability. The report emphasized the need for infrastructure that supports and enables repeatable experiments by creating easy ways for researchers to test each others' results.



The study authors recommended developing flexible and automated capabilities for connecting research infrastructure. Credit: USC's Information Sciences Institute and SRI International

Moreover, instead of uncoordinated, domain-specific studies—some related to denial of service attacks or password cracking, others related to critical infrastructure or automotive testing—researcher need common standards and ways to work across disciplines and domains.

"The adversary isn't looking narrowly," Benzel said, "and researchers can't afford to either."

Finally, the community needs to develop new approaches for sharing and synthesizing data in order to accelerate knowledge and community building across disciplines and organizations.

"We need a way that makes it easy for researchers, not only from different aspects of cybersecurity, but across different domains, to share their problems and draw from a library of experimental cyber components to put together a big problem," Benzel said.

Recommendations for Securing our Cyber-Future

Based on input from scholars, the authors synthesized five key observations that they believe, if followed, will yield transformational results.

First, research must be multidisciplinary. Whereas today, experts typically specialize in one area, in the future, individuals and teams must incorporate a wider range of knowledge and skills.

"We need to bring in different disciplines, from computer science, engineering, math and modeling to human behavior, sociology, economics and education," said David Balenson, another of the lead authors and a senior computer scientist at SRI International.

Second, experiments must accurately model and incorporate human

activity.

"Everything we do needs to be grounded in the real world and include the human element—users, operators, maintainers, developers and even the adversary," Balenson said.

DeterLab, an advanced testbed facility where leading researchers and academics conduct critical cybersecurity experimentation and educational exercises. Credit: DETER Project, USC Information Sciences Institute

NSF Program Director Anita Nikolich said performing cybersecurity research "in an isolated, contained environment that doesn't mimic reality is not conducive to discovering the nuances inherent in this sort of research. New approaches to testing are needed in order to produce useful, actionable results."

Third, different experimental environments must be able to work together in a plug-and-play fashion by following common models of infrastructure and experiment components using open interfaces and standards.

"Without shared experimental infrastructure, researchers have to spend lots of money developing their own experimental infrastructure which takes away from their core research," said Laura Tinnel, a senior research engineer at SRI International and one of the study's authors. "People are reinventing the wheel."

Fourth, experimental frameworks must allow reusable designs to better enable science-based hypothesis testing.

"In most other sciences, someone can come and repeat your experiment, but that's not typically the case in cyber," Benzel said. Hardwiring such capabilities into the structure of the experimental framework would allow researchers to do broader experiments, and also lower the barrier to entry and improve education and training.

Finally, any infrastructure that is built must be useable and intuitive, so researchers and students spend less time learning to use the infrastructure and more time doing critical scientific inquiry. Moreover, the community must adopt a more rigorous scientific model for research and supporting infrastructure.

"People have been doing things the same way for some time now, and trying to get them to work in a more community-oriented way is going to take some shifts in their thinking as well as cultural changes," Balenson said.

However, the study's authors believe that if the scientific community follows the recommendations, such a shift would not only change the balance of power between hackers and cybersecurity experts, but result in systems that are secure by design—something that long-discussed in the cybersecurity world but not yet successfully implemented.

"We can shift this asymmetric cyberspace context to one of greater

planning, preparedness, anticipation and higher assurance solutions," Benzel said.

Provided by National Science Foundation

Citation: Roadmap to safer cyberspace (2015, December 17) retrieved 26 April 2024 from https://phys.org/news/2015-12-roadmap-safer-cyberspace.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.