Poster: Sharing Expertise and Artifacts for Reuse through Cybersecurity Community Hub (SEARCCH)

Terry Benzel, Jelena Mirkovic
USC-ISI
Marina Del Rey, CA
{benzel|mirkovic@isi.edu}

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

Eric Eide
U. Utah
Salt Lake City, UT
eeide@cs.utah.edu

Tim Yardley
U. Illinois Urbana-Champaign
Urbana, IL
yardley@illinois.edu

***Abstract*— The Sharing Expertise and Artifacts for Reuse through Cybersecurity Community Hub (SEARCCH) project aims to help improve the overall scientific quality of cybersecurity research by developing, deploying, and supporting new, innovative community infrastructure that facilitates the rapid transfer and reuse of cybersecurity experimentation expertise and artifacts. This infrastructure will provide an open, online "knowledge hub" to support experimentation, testing, and education. The team is developing an initial artifact metadata description, pre-populating the hub with artifacts, developing artifact import tools, and engaging the community to import a diverse set of content.**

Keywords—cybersecurity research, experimentation, testing, education, artifacts, testbeds, methodologies, tools, data.

I. Introduction

The NSF-funded Sharing Expertise and Artifacts for Reuse through Cybersecurity Community Hub (SEARCCH) project [1] is motivated by the R&D community's need to share cybersecurity experimentation artifacts in a way that lowers the barrier to sharing. The evaluation of the cybersecurity properties of computer, networking, and cyber-physical research is frequently performed in ad hoc ways, which severely retards scientific progress. Most researchers use a combination of methods and infrastructure to conduct experiments using one-off, painstaking, and error-prone processes that are rarely shared for reuse and validation. The lack of repeatable, reproducible, and reusable processes and other artifacts limits one's ability to build on the work of others or to compare solutions. Enabling the rapid sharing and reuse of experiment artifacts is crucial to improving our rate of progress and will help transform our scientific community.

SEARCCH aims to help improve the overall scientific quality of cybersecurity research by developing, deploying, and supporting new, innovative community infrastructure that facilitates the expeditious transfer and reuse of cybersecurity experimentation expertise and artifacts, including testbeds, methodologies, tools, data, and best practices (see Fig. 1). This infrastructure will provide an open, online "knowledge hub" to support experimentation, testing, and education. The team developed an initial artifact metadata description, pre-populated the hub with artifacts, developed initial artifact import tools, and is now engaging the community to import a diverse set of content. SEARCCH will enable and support the transfer and sharing of cybersecurity experimentation expertise and artifacts for a wide range of experiments conducted by the research community.

This material is based upon work supported by the National Science Foundation under Grant Nos. CNS-1925773, CNS-1925616, CNS-1925588, and CNS-1925564. 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.

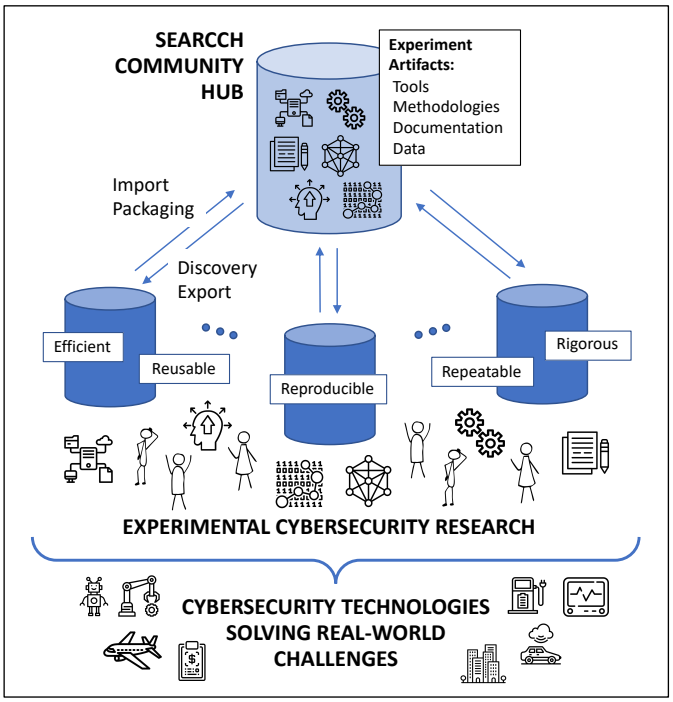


Fig. 1. SEARCCH hub supports experimental research to produce cybersecurity technologies that solve real-world problems

II. Main Thrusts and Tasks

SEARCCH will facilitate sharing through three main areas of work: technology, data collection, and community-building.

Technology tasks include development and integration of:

(1) The hub, a community collaboration portal which will (i) host an extensible catalog of experimental artifacts and (ii) employ elements of social media to create an environment that encourages sharing, reuse, and community; and

(2) Artifacts import tools that include a) a rich ontology (common set of semantics) designed specifically for cybersecurity experimental artifacts that will be used to

create searchable metadata that help other researchers quickly find and reuse artifacts in the hub, and b) testbed-specific packaging tools that lower researcher cognitive load by helping identify useful pieces of experimental artifacts and package them for sharing via the hub;

(3) Artifacts storage mechanisms for linking to large artifacts and storing their metadata;

(4) Artifacts discovery and export mechanisms that help researchers rapidly find and extract artifacts for use in their own environment; and

(5) Experiment design support tools that make use of the ontology and hub content to help researchers more rapidly design high-quality experiments.

Data collection tasks include mining, classifying, organizing and cataloging existing experimental artifacts and populating the SEARCCH hub. We developed automated artifacts collection tools to support this activity and used these tools to pre-populate the hub with content published on Zenodo and GitHub.

Community-building tasks include outreach to and engagement with cybersecurity researchers and experimenters. SEARCCH will recruit from the broader research community, including from the NDSS community, to create a body of active participants and to encourage and reward the sharing and reuse of experimental artifacts and infrastructure. Through community engagement, we are actively involving the community in the design, development, testing, and eventual ongoing use of the hub.

III. Related Work

SEARCCH is motivated by the conclusions of the NSF-funded Cybersecurity Experimentation of the Future (CEF) community-based study of expected needs for experimentation infrastructure [2] and subsequent community engagement workshops and feedback indicating strong interest in community infrastructure that facilitates sharing and reuse of experimental designs, methodologies, tools, and artifacts [3].

The SEARCCH hub is building on and leveraging general-purpose, open-access repositories such a GitHub, Zenodo, and HAL-Inria and facilitating the use of these resources for cybersecurity research.

SEARCCH complements and supports the growing trend towards artifact evaluation and sharing in cybersecurity conference publications, such as the Annual Computer Security Applications Conference (ACSAC) artifacts initiative [4], which is based on ACM's Artifact Review and Badging process [5].

IV. Impacts

Community impacts will be realized as SEARCCH supports the broader community and enables new cybersecurity research through the ready and increased availability of expertise and artifacts on top of existing lab resources. The SEARCCH team developed an initial artifact metadata description to elicit feedback from the community as well as populate the SEARCCH hub with metadata for an initial set of experiment artifacts. The initial description currently includes the artifact metadata types listed in Table I. The team developed a preliminary version of the artifact import tool using these artifact metadata types. Note that the SEARCCH hub does not store artifacts directly; rather it stores a rich metadata representation of artifacts. This enables researchers to quickly vet artifact relevance to their work and then access actual artifacts in their native location.

Table I. Initial Artifact Metadata Types

Artifact Title, Description, and Author(s)
Subject Descriptor / Research Domain
Datasets
Source Code – any script, research product, traffic generator, simulation, etc.
Publications
Executables – specific binaries used in experiment
Organizations – metadata at the collection level
Licenses

By facilitating sharing and reuse of experiment artifacts, SEARCCH will enable vertical development (i.e., enable researchers to think in more complex, systematic, strategic, and interdependent ways), which will improve quality, maximize efficiency, and reduce the time and effort that researchers must invest in evaluation of their research prototypes. In turn, this will enable researchers to focus more on innovation and development tasks and produce higher quality solutions.

The SEARCCH infrastructure will ultimately advance the knowledge, understanding, rigor, and practice of experimental cybersecurity research by making experimentation faster, simpler, and more robust. It will enable researchers to more easily build upon the work of others and to compare solutions by facilitating and encouraging sharing and reuse. The resulting infrastructure will directly support the broader research community in validating the security properties of diverse research solutions and in rapidly creating effective cybersecurity solutions to meet today's complex challenges. Ultimately, these advances will transform the way that experimental knowledge is accessed, shared, and validated and move the community from one of craftsmanship to a scientific discipline of rigorous experimentation. We invite the NDSS community to actively participate in planned SEARCCH community engagement activities and to contribute to and make use of experiment expertise and artifacts in the SEARCCH hub.

References

[1] Sharing Expertise and Artifacts for Reuse through a Cybersecurity Community Hub (SEARCCH) (website). (https://searcch.cyberexperimentation.org/)

[2] D. Balenson, L. Tinnel, and T. Benzel, Cybersecurity Experimentation of the Future (CEF): Catalyzing a New Generation of Experimental Cybersecurity Research, July 31, 2015. (https://www.cyberexperimentation.org/cef-study/report/)

[3] Cybersecurity Experimentation of the Future (CEF) (website). (https://www.cyberexperimentation.org)

[4] Annual Computer Security Applications Conference (ACSAC 2020), Paper Artifacts (website). (https://www.acsac.org/2020/submissions/papers/artifacts/)

[5] Association for Computing Machinery, Artifact Review and Badging (website). (https://www.acm.org/publications/policies/artifact-review-badging)

SEARCCH

Sharing Expertise and Artifacts for Reuse through Cybersecurity Community Hub

Terry Benzel, Jelena Mirkovic
USC-ISI
Marina Del Rey, CA
{benzel|mirkovic@isi.edu}

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

Eric Eide
U. Utah
Salt Lake City, UT
eeide@cs.utah.edu

Tim Yardley
U. Illinois Urbana-Champaign
Urbana, IL
yardley@illinois.edu

CHALLENGE

- **Ad hoc** cybersecurity experimentation severely retards scientific progress
- **Use of one-off**, painstaking, and error-prone processes; **not shared** for reuse and validation
- **Lack** of repeatable, reproducible, and reusable processes and other artifacts

APPROACH

Technology

- **Hub** - Community collaboration portal for collecting and sharing experimental artifacts
- **Artifacts import** - Provide structure for shared artifacts & tools that facilitate content packaging for sharing
- **Artifacts storage** - Provide or link to persistence mechanisms for content and/or metadata
- **Artifacts discovery and export** - Provide tools that facilitate rapid content identification and extraction
- **Experiment design support** - Provide hub-integrated tools to help researchers design sound experiments using hub artifacts

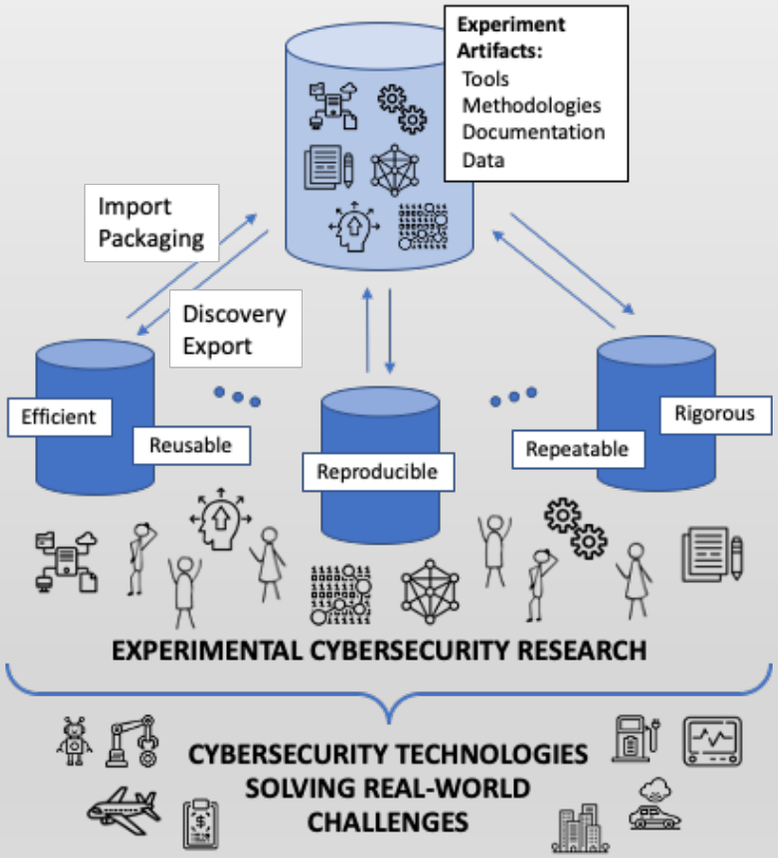
Data Collection

- **Curate content** - Build and use tools to harvest external artifacts to populate hub

Community Building

- **Outreach** - Recruit new collaborators from the community and keep participants informed
- **Engagement** - Actively involve community in requirements, design, and testing of hub

SEARCCH COMMUNITY HUB



SCIENTIFIC IMPACT

- **Enable** the community to build upon the work of others or to compare solutions
- **Transform** the way cybersecurity experimental research is conducted
- **Advance** the knowledge, understanding, rigor, and practice of experimental cybersecurity research

BROADER IMPACT

- **Enable** new cybersecurity research and innovation
- **Lower** the barrier to underrepresented communities
- Increasing **metrics** over three years – contribution, adoption, publication, results, etc.

INVITATION TO NDSS COMMUNITY

- **Actively participate** in planned SEARCCH community engagement activities
- **Contribute to** and **make use of** experiment expertise and artifacts in the SEARCCH hub

FOR MORE INFORMATION

- **https://searcch.cyberexperimentation.org/**

SEARCCH is based upon work supported by the National Science Foundation under Grant Numbers 1925773, 1925616, 1925588, 1925564. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.