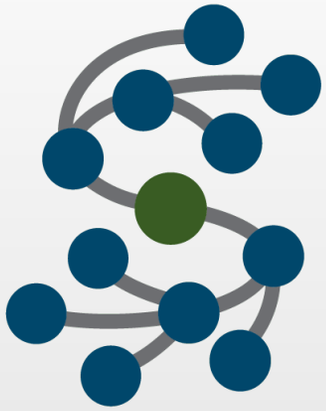


SEARCCH

Sharing Expertise and Artifacts for Reuse through Cybersecurity Community Hub

Research Results: Better, Faster, Sooner through Artifacts Sharing

Laura Tinnel & David Balenson, SRI International

Teesh Shahi, UIUC and David Johnson, University of Utah

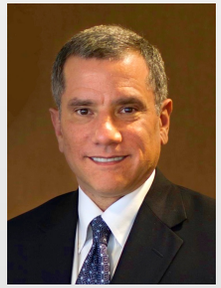
December 11, 2020

This material 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.

SEARCCH Collaborative Team PIs


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

USC Viterbi
Information Sciences Institute

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

SRI International®

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

THE UNIVERSITY OF UTAH

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

ILLINOIS

Our Community's Challenges & Needs

- Sharing of repeatable, reproducible, and reusable artifacts in cybersecurity experimentation
  - Can greatly enhance one's ability to build upon the work of others
  - Helps in comparing solutions.

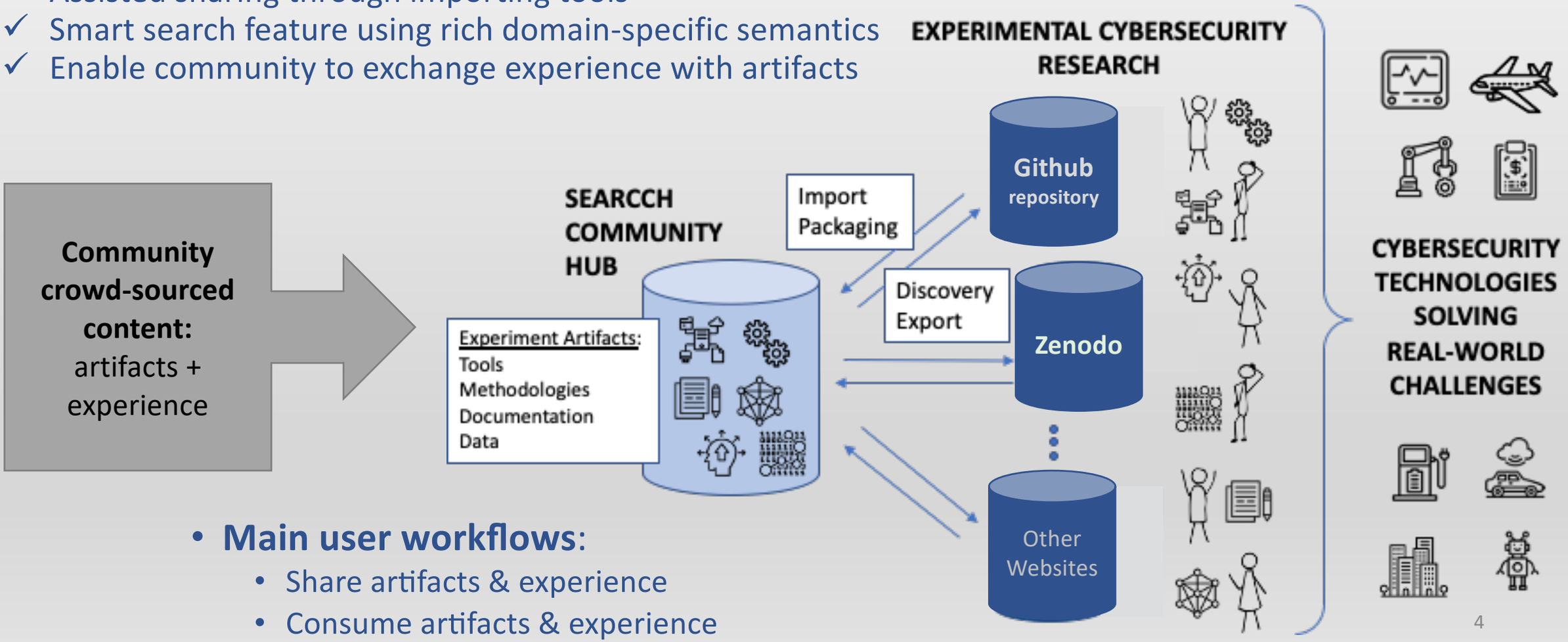
- Sharing artifacts can be difficult and time-consuming
- Finding relevant experiments and artifacts can be challenging and time-consuming
- We need:
  - ✓ Broad sharing of experiment artifacts
  - ✓ Solution that facilitates rapid and open community sharing and reuse

https://www.business2community.com/leadership/8-keys-innovation-mindset-0882548

Artifacts-sharing Hub Concept of Operations

Collaborative, community-driven platform that lowers barrier to sharing and reuse

- ✓ Assisted sharing through importing tools
- ✓ Smart search feature using rich domain-specific semantics
- ✓ Enable community to exchange experience with artifacts



- **Main user workflows**:
  - Share artifacts & experience
  - Consume artifacts & experience

The Hub Stores Artifact Metadata

The SEARCCH Hub does not store artifacts directly; rather it

- stores a rich metadata representation of artifacts,
- enables researchers to quickly vet artifact relevance to their work and then access actual artifacts in their native location

Artifact Title, Description, and Author(s)
Subject Descriptor / Research Domain
Research Questions and Hypothesis
Methodology
Metrics
Dataset
- Type (several options plus freestyle entry)
- Time of collection
- How/where it was collected

Source Code - any script, research product, traffic generator, simulation, etc.
- Description
- Role in the experiment (e.g., research code, simulator, orchestration code, etc.)
- Language
- Dependencies
- How long it runs
- Any special memory, CPU, hardware, OS requirements

Publication
- Type (e.g., journal article, conference, whitepaper, blog post, technical report, thesis (MS/PhD), book, instructions (installation, use), citation)
- Where published
- Year of publication
- References

Executable - specific binaries used in experiment
- Type
- Purpose
- Supporting Information
- Visuals
- Supplements
- Tutorial

Organization - metadata at the collection level
- Type (e.g., company, academia, government)
- Name
- Group

System Environment
- Testbed
- Resources

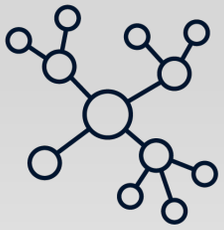
License
- Type
- Restrictions

Domain (aka., Research Applications)
- Current
- Potential

Note: source code details, if captured in the source's README file will show up in the hub as part of the text description.

Fundamental Research Design Question

- Determine how to best represent cybersecurity experiment artifacts and the relationships between them and develop an optimized data model that facilitates the efficient artifact discovery
  1) Manually cataloged cybersecurity artifacts to better understand existing artifact features and the breadth of artifacts
  2) Performed automated “mining” of cybersecurity related artifacts from Zenodo as test subjects
  3) Implemented a general artifact "importer tool"
- Once fully operational, we expect most of the hub's catalog to come from user contributions, not automated mining



Current Hub Features & Capabilities

- Search hub repository for artifacts
- For found artifacts
  - View
  - Favorite
  - Rate
  - Review
  - See other reviews
- Import new artifacts

SEARCCH Hub Demo

Questions for the Community

- What did you like about the hub features you saw?
- What features should be changed and how?
- What additional functionality should we consider?

SEARCCH Beta Program

- Opening for Beta use in mid-January
- Training session
  - Probably 2nd week of January
  - Get set up with account
  - Bring an artifact to import
- Open beta program to more users
  - Probably end of January

- For more information
  - Talk to us
  - Follow us on Twitter: @SEARCCH_Hub
  - Visit us on the web: https://searcch.cyberexperimentation.org
  - Send us email: beta-test@searcch.cyberexperimentation.org