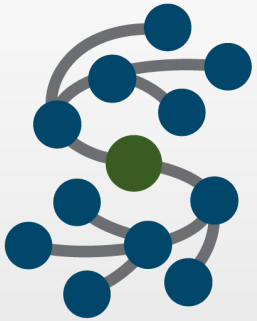


SEARCCH

Sharing Expertise and Artifacts for Reuse through Cybersecurity Community Hub

Research Results: Better, Faster, Sooner through Artifacts Sharing

Laura Tinnel & David Balenson, SRI International

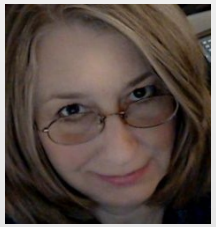
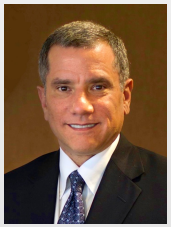
August 10, 2020

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


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

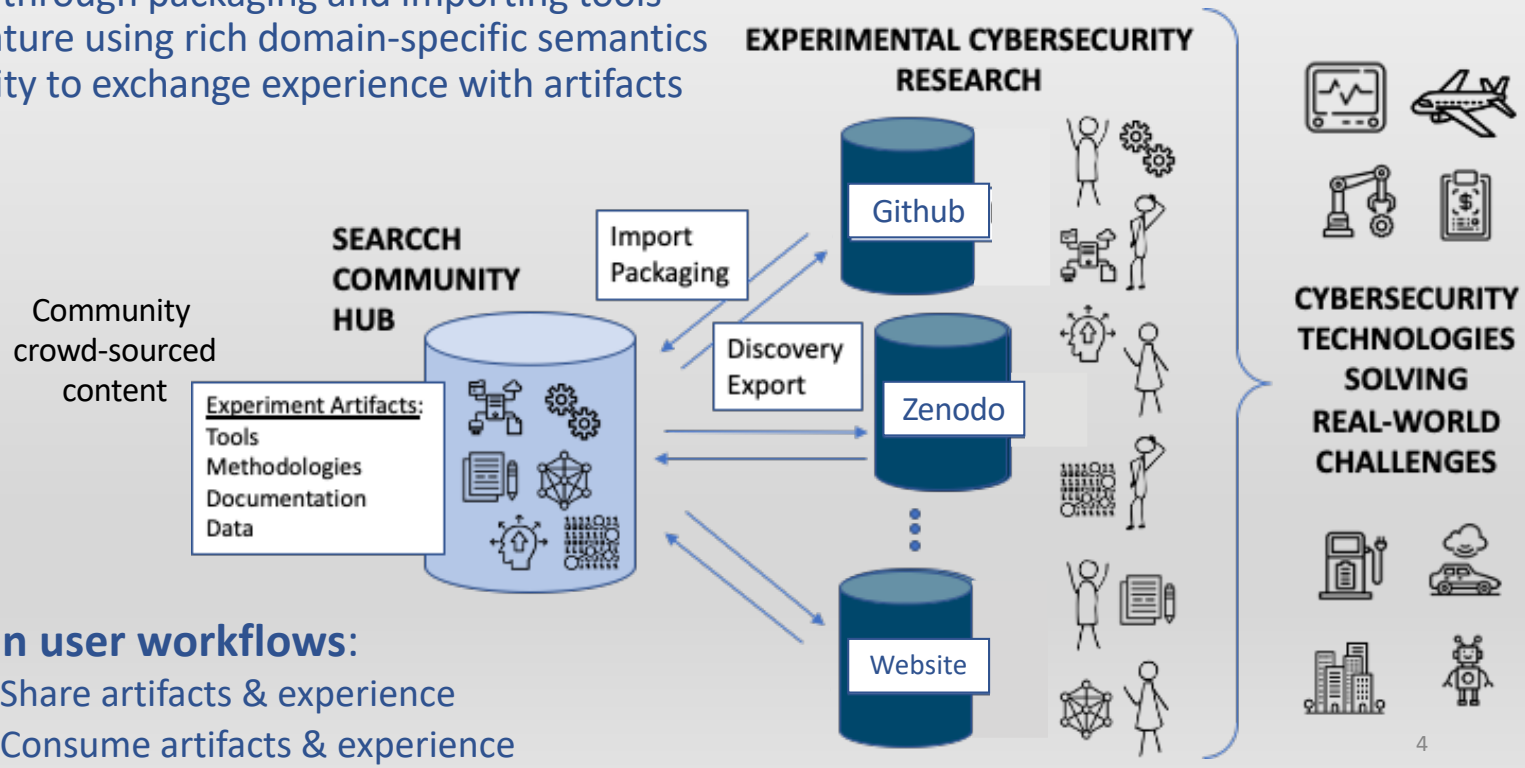
https://www.business2community.com/leadership/8-keys-innovation-mindset-0882548

*Includes data

Artifacts-sharing Hub Concept of Operations

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

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



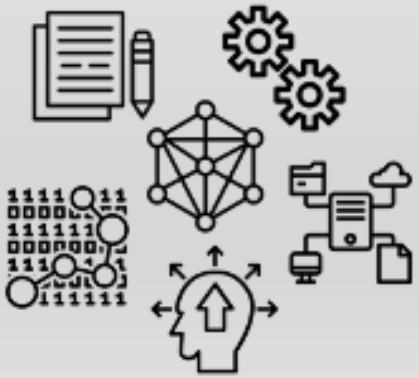
- **Main user workflows**:
  - Share artifacts & experience
  - Consume artifacts & experience

SEARCCH Thrust/Task Year 1 Status

Thrust	Task	Status
Technology	Hub	Hub framework stood up at University of Illinois
	Artifacts import	Framework for import and cybersecurity domain specific data model Automated tools that import structured metadata for Zenodo artifacts Automated tools that create structured metadata for github artifacts (to be imported)
	Artifacts metadata storage	Database for artifact metadata persistence
	Artifacts discovery and export	Simple search capability complete Search relevance scores
	Experiment design support	Provide hub-integrated tools to help researchers design sound experiments using hub artifacts
Artifacts collection	Curate content	Harvested initial set of artifacts from Zenodo Initial analysis of ACSAC artifacts
Community building	Outreach	Website stood up, social media presence established, several posters (ongoing)
	Engagement	IEEE S&P BoF, CSET panel, USENIX Security BoF, other efforts planned (ongoing)

SEARCCH Next Steps

- Content
  - Import github and ACSAC artifacts
  - Identify new sources for artifacts
- Technology
  - Evolve the data model as needed to improve artifact discoverability, importability, exportability, reusability
  - User ability to import artifacts
  - Refine and extend UI with added usability features
    - Enhanced search function
    - User accounts
    - Ability to save found artifacts
    - Ability to comment on artifacts
- Community building
  - Recruit beta users



We Need Your Involvement!

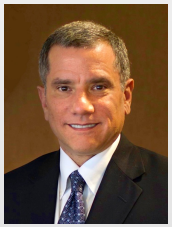
- Join our USENIX Security BoF on Wednesday at 1:15pm PT
  - See a demo of the pre-beta SEARCCH hub
  - Share your workflows/use cases
  - Requirements/needs
  - Other thoughts and comments
- Got artifacts to share? Please talk to us!

- Follow us on Twitter: @SEARCCH_Hub
- Visit us on the web: https://searcch.cyberexperimentation.org
- Sign up for our mailing list for announcements
  - Send email address or post in chat

Contact Us


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

Joint Questions For Discussion

- Artifacts and data types
  - What kinds of data have you used (e.g., network traffic or flows, system logs, etc.)?
  - What kinds of data do you think you'll need in the future?
- Data sources
  - Do you use or can you use model-based, synthetically generated data or data from emulated environments (e.g., DETERLab, CloudLab)?
  - Do you need real/operational data for your research? Are you able to get the operational data if you need it? If so, how?
- Artifact and data sharing
  - Do you share your artifacts and data? What are the barriers for sharing or the conditions under which you would be willing to share? (e.g., must be sanitized to some level)
  - What are the barriers for you to use other people's data? What would you need to know about the data to use it? E.g.,
    - Does the data collection method matter (e.g., following certain protocols, ethics, etc)?
    - Do you require ground truth?
    - Quality (and if so, who is responsible for determining quality?)
- Sometimes code cannot be separated from data. Are there issues sharing and re-using data + code?
- Long-term sustainability - how to cover costs associated with maintaining online sharing platforms
  - What sustainment models would be acceptable? Ideal? (e.g., subscriptions, part of university services, donor sponsorship, paid advertising, Condo model, other?)
  - Any issues with these? (e.g., paid advertising may not work - small audience)