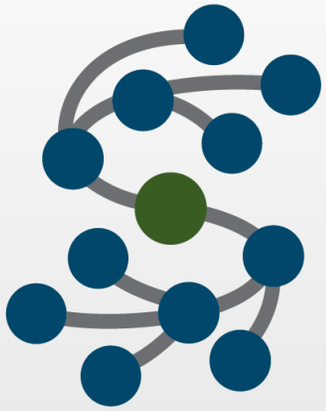


SEARCCH

Sharing Expertise and Artifacts for Reuse through Cybersecurity Community Hub

Research Results: Better, Faster, Sooner through Artifacts Sharing

Laura Tinnel & David Balenson, SRI International

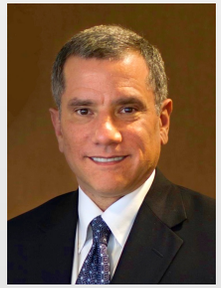
August 12, 2020

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®

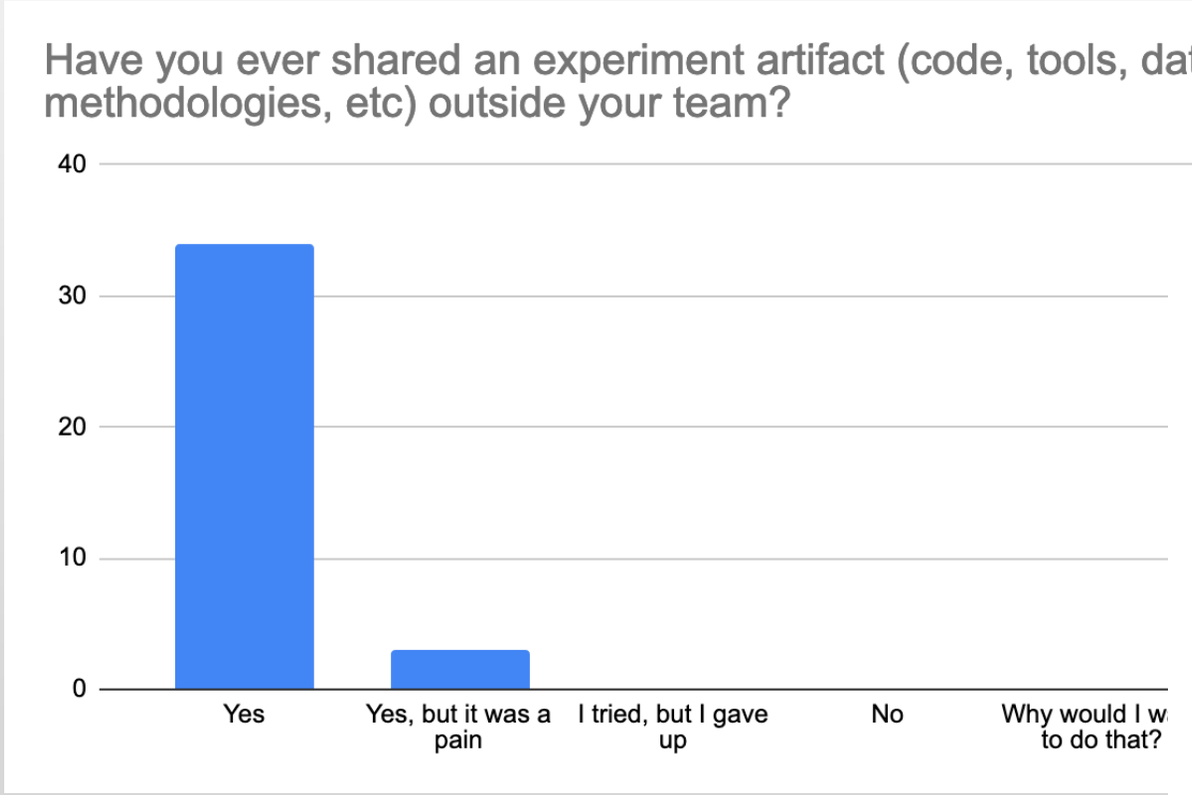
Eric Eide
U. Utah
Salt Lake City, UT
eeide@cs.utah.edu

THE UNIVERSITY OF UTAH

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

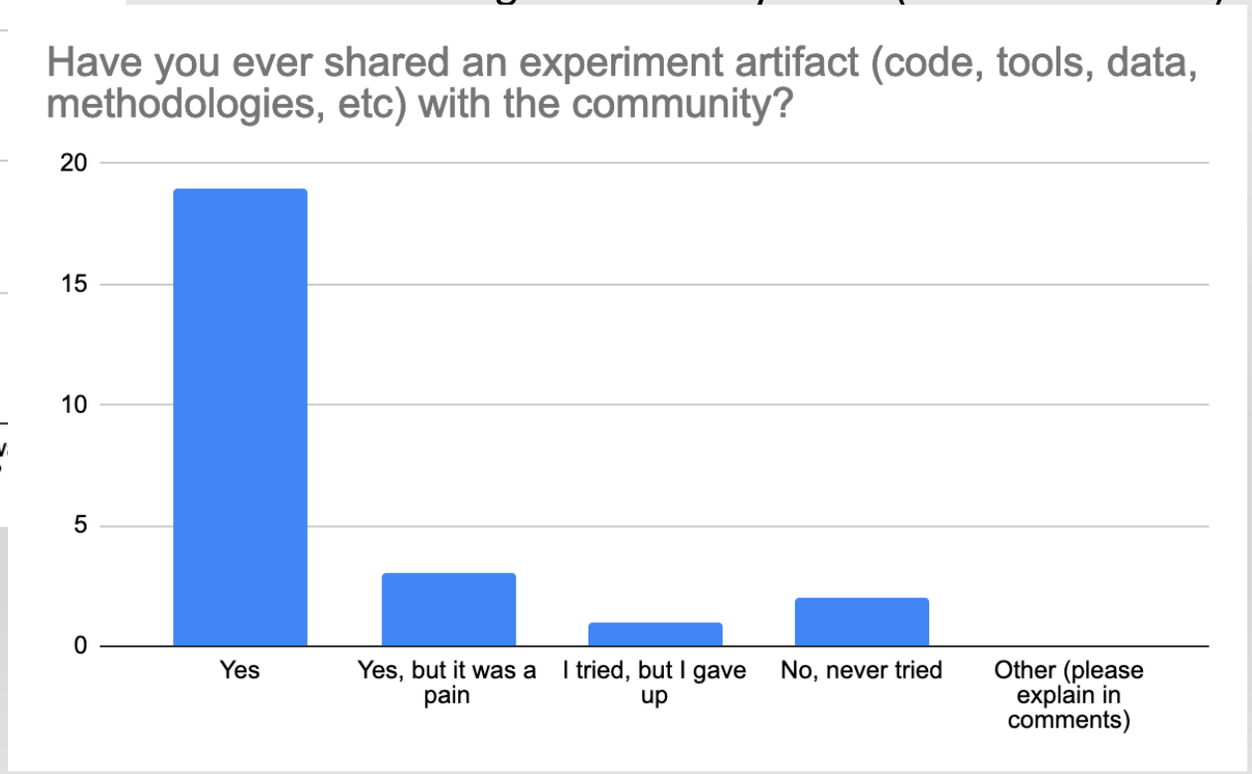
ILLINOIS

(Unscientific) Poll Questions and Results

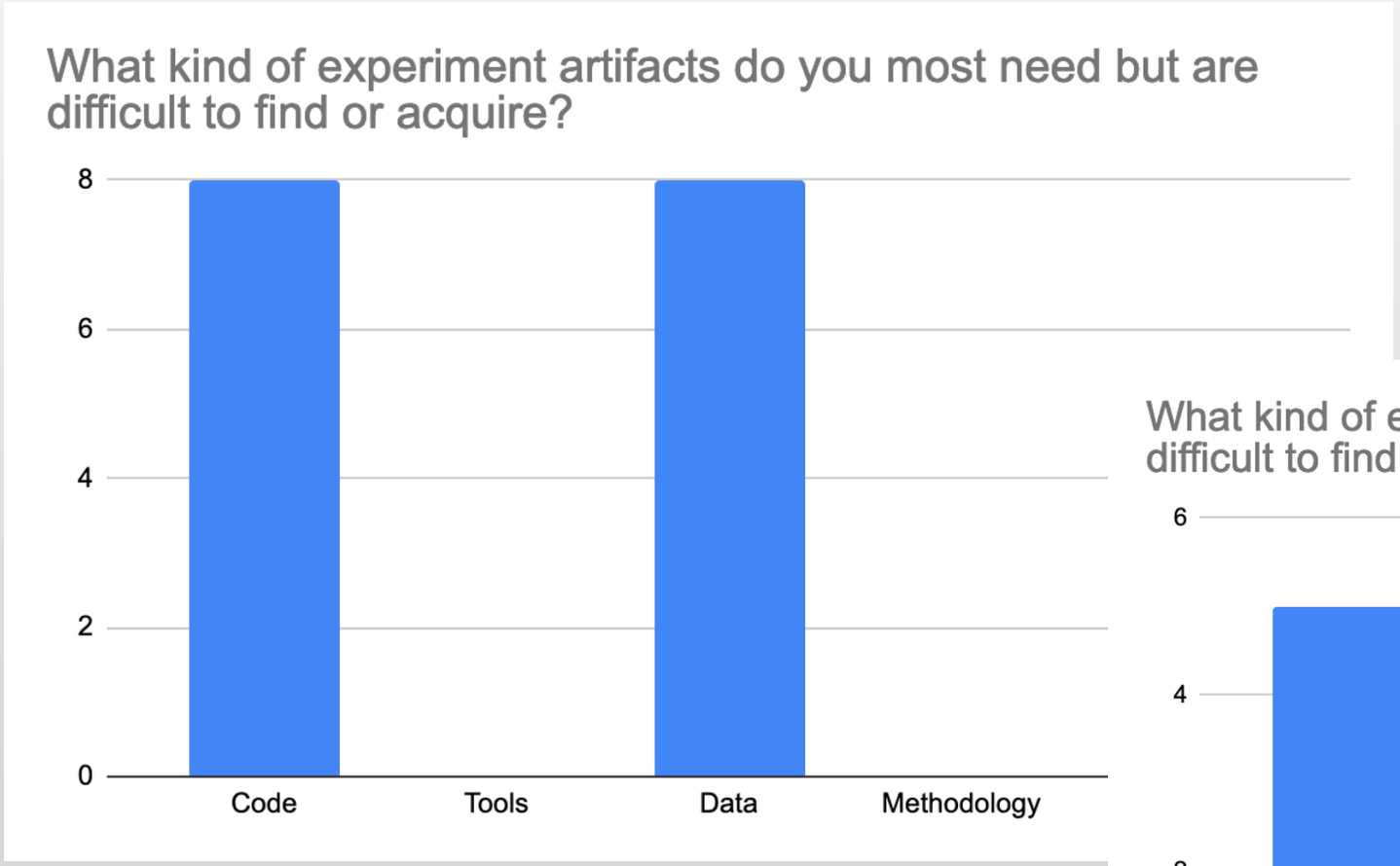


#sec20 NON-anonymous (809 subscribers)

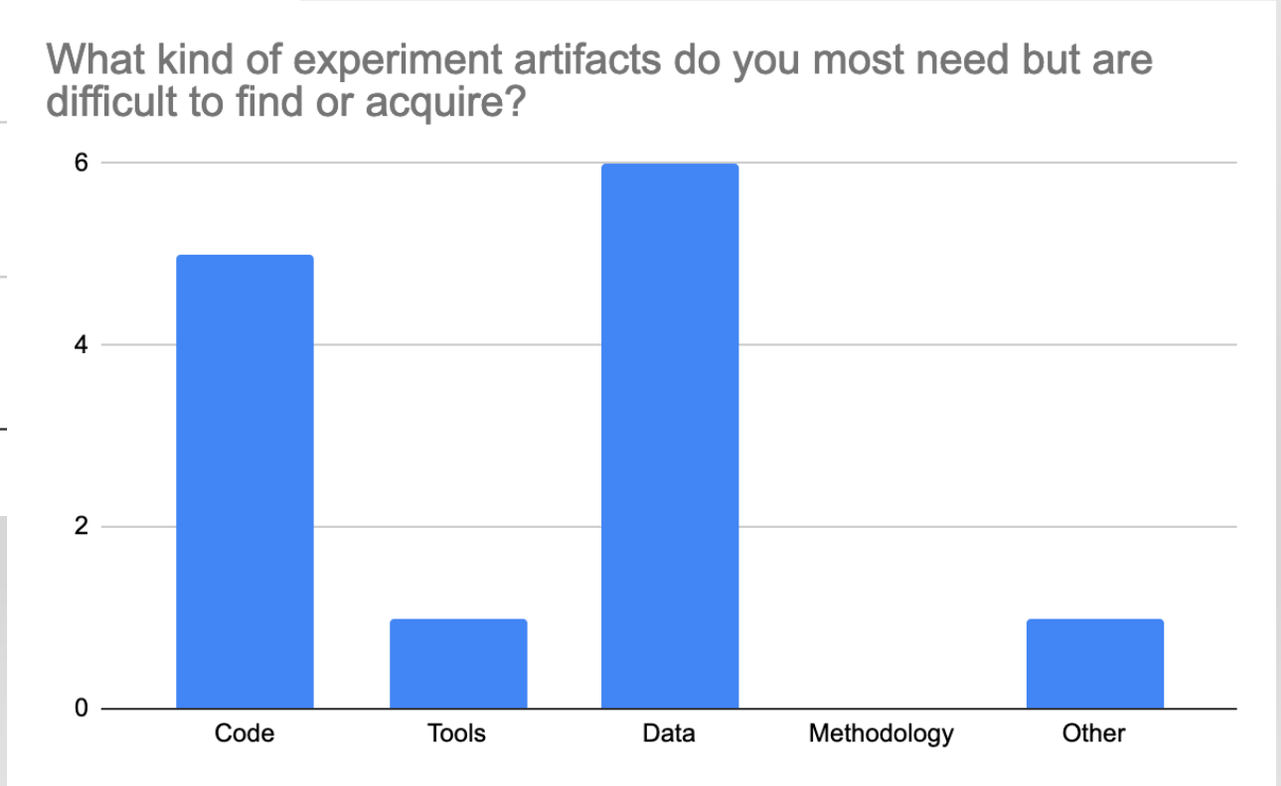
#-general anonymous (811 subscribers)



(Unscientific) Poll Questions and Results

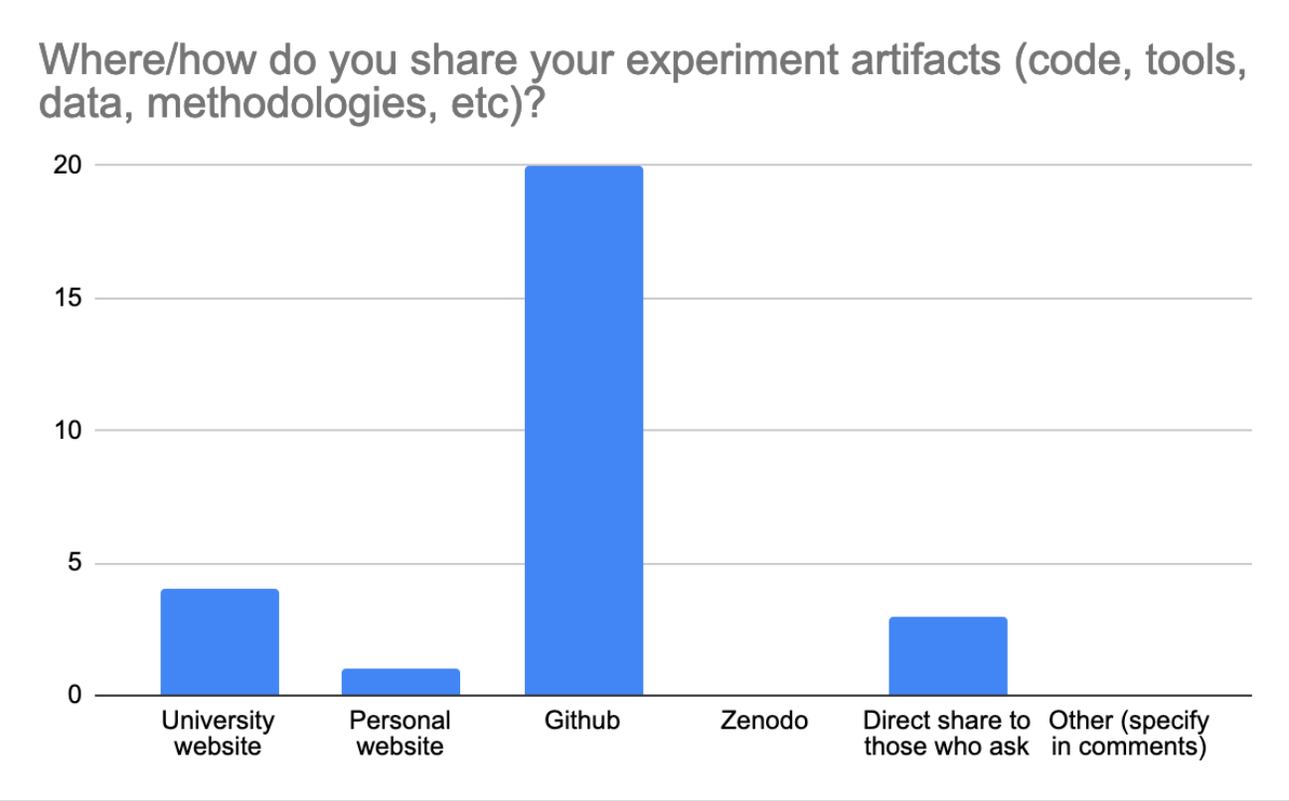


#sec20 anonymous

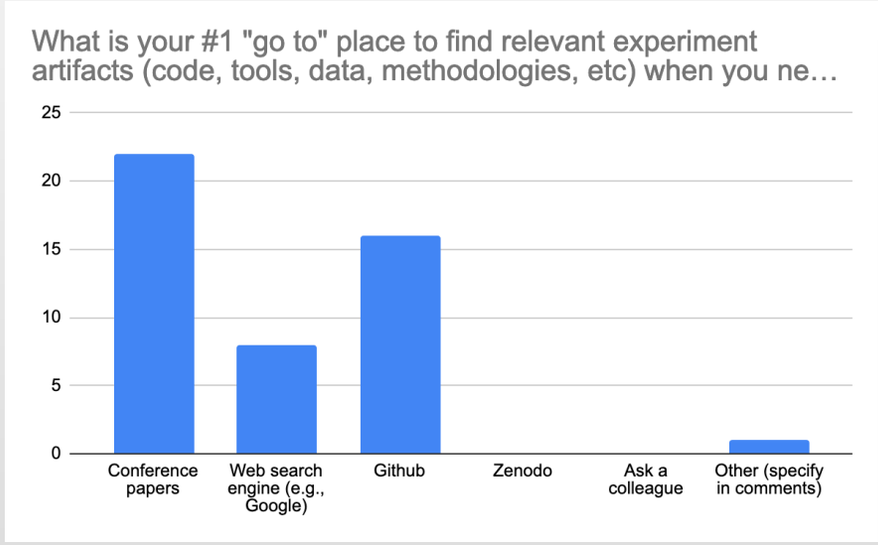


#-general anonymous

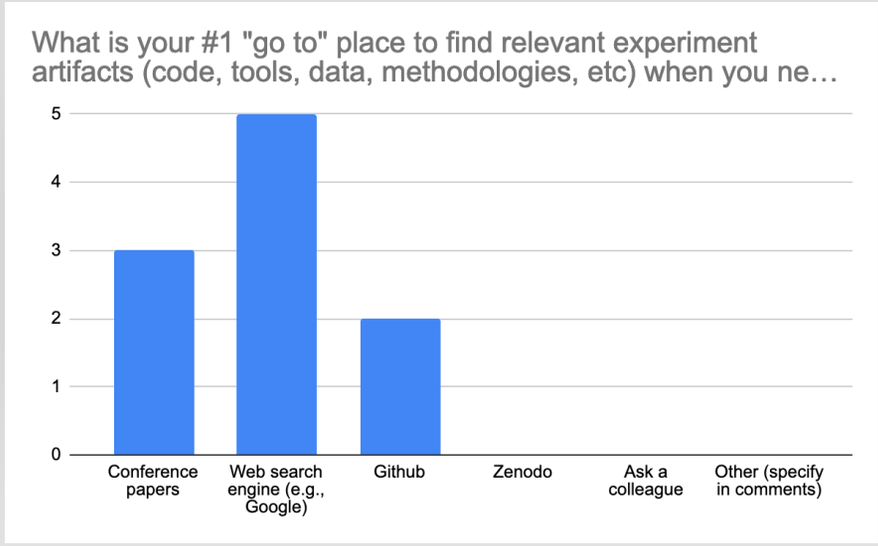
(Unscientific) Poll Questions and Results



#sec20 anonymous



#-general anonymous



#search-bof anonymous

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.

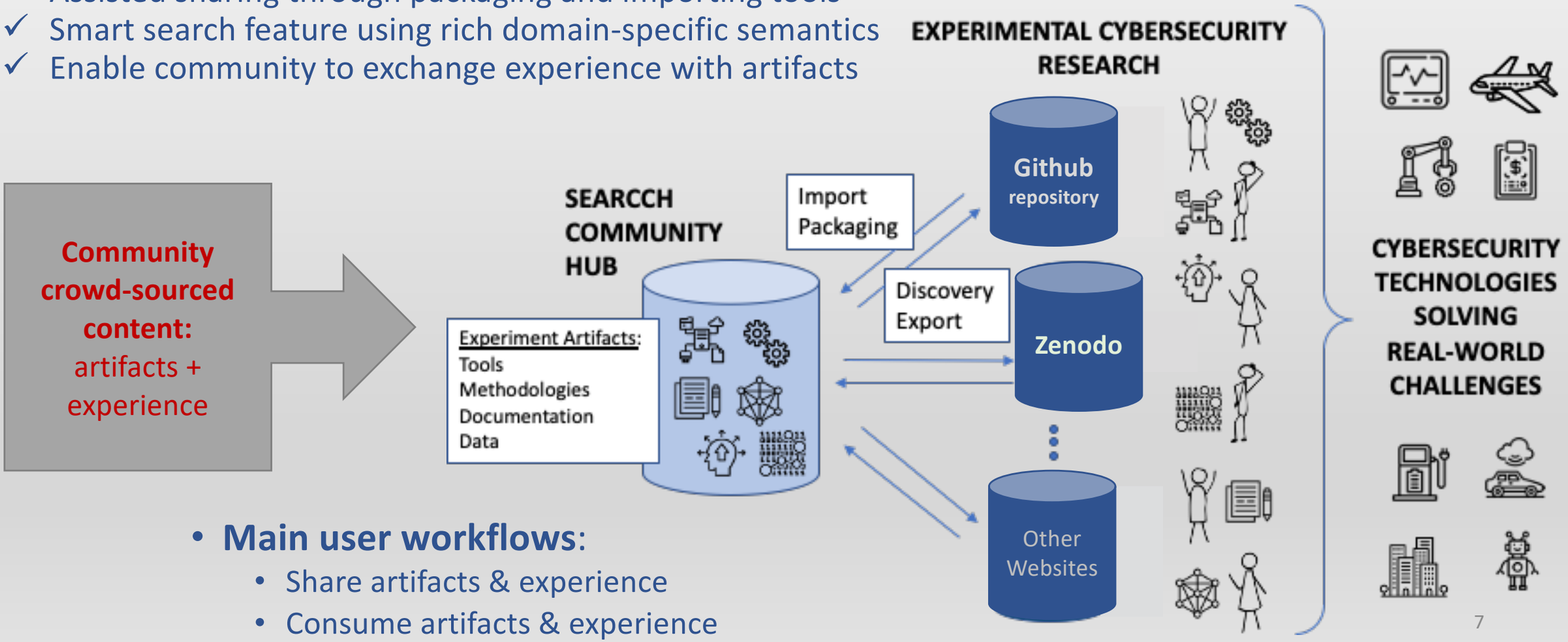
- Sharing artifacts can be difficult and time-consuming
- Finding relevant experiments and artifacts can be challenging and time-consuming
- We need:
  - ✓ Broad sharing of experiment artifacts
  - ✓ Solution that facilitates rapid and open community sharing and reuse

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 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 Demonstration

- Strawman “Find & Vet” Workflow

Questions for the Community

- Hub User Experience
  - What elements of an Amazon-like user model would you like to see?
  - What additional features would be needed? Which existing features are not needed?
  - What features should be changed and how?
  - **What are your top 3 priorities for hub features?**
- Content consumption
  - What kind of artifacts do you most need? What is hard to find?
  - Where do you currently go to find artifacts?
  - **What was hard about adopting artifacts from others? What would make it easier?**
  - **What information would you need to decide to use a specific artifact (methodologies, tools, documentation, data)?**
- Content contribution
  - Have you shared any experiment artifacts with the community?
  - If so, **what was your experience in packaging and uploading? What worked, what was hard?**
  - **What kinds of tools would make sharing artifacts easier and/or faster?**

SEARCCH Ongoing Work & Next Steps

- Using YOUR inputs, actively working on (in parallel)
  - Implement base hub framework (ongoing)
  - Consume artifacts workflows
    - Provide semantically rich, knowledge-based searching
    - Curate artifact collections and seed the hub
  - Share artifacts workflows
    - Provide automated tools to assist with packaging and importing artifacts
      - Metadata extraction and insertion
  - Community consume/share experience workflows
    - Enable ratings and discussions around artifacts

- Planning future engagement events

Continue Your Involvement!

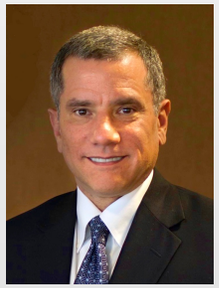
- We need YOUR input
  - Got workflows/use cases?
  - Requirements/needs
  - Other thoughts and comments?
- Got artifacts to share? Please talk to us!
- Join our future engagement events
- Sign up to be a beta user

- 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