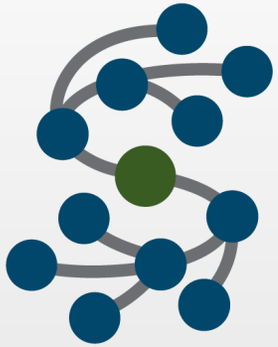


SEARCCH

Sharing Expertise and Artifacts for Reuse through Cybersecurity Community Hub

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

Presented to 2020 Virtual NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure

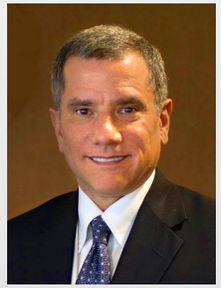
David Balenson, SRI International
September 24, 2020

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

CEF Study and Community Engagement

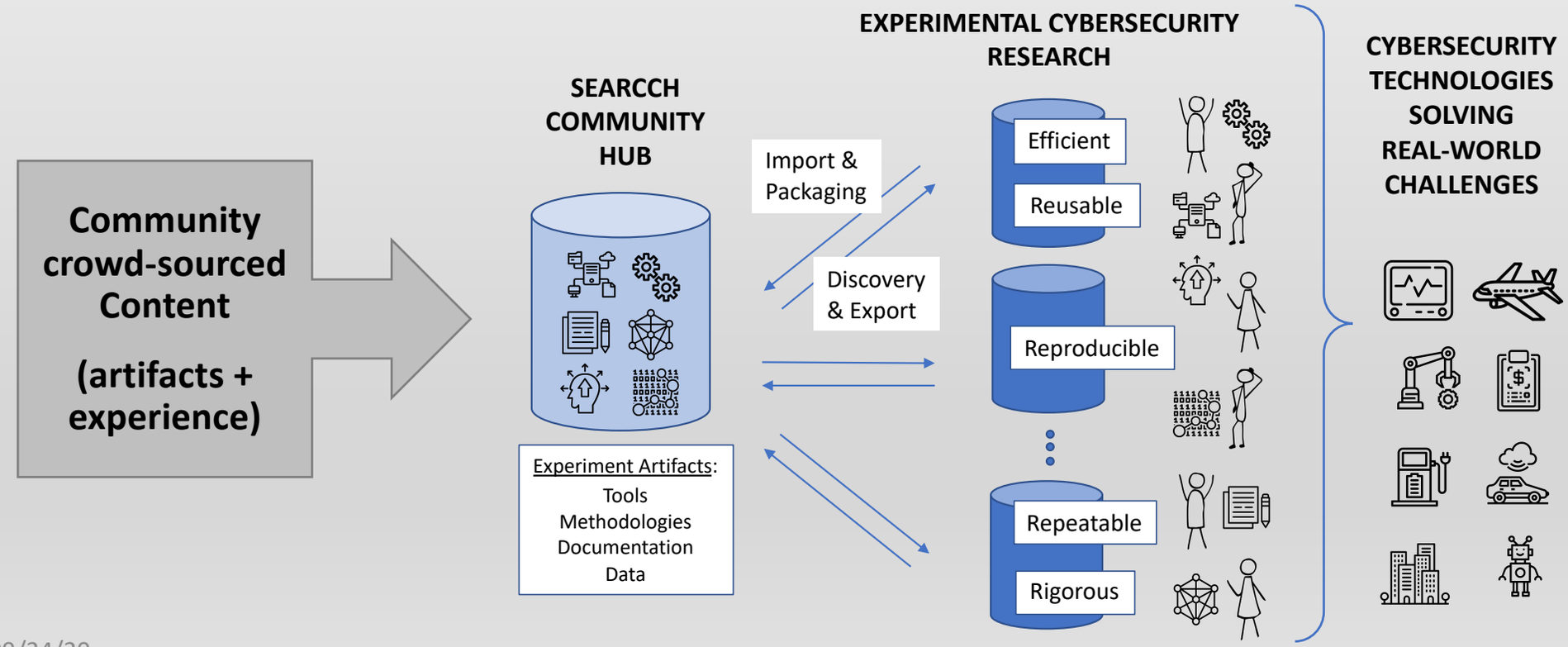
- SEARCCH is motivated by the conclusions of the NSF-funded Cybersecurity Experimentation of the Future (CEF)
- Community-based study groups and subsequent community engagement workshops
- Feedback indicating strong interest in community infrastructure that facilitates sharing and reuse of experimental designs, methodologies, tools, and artifacts

https://www.cyberexperimentation.org/

SEARCCH Hub Concept of Operations

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

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



The Hub Stores Artifact Metadata

The SEARCCH Hub does not store artifacts, per se

- It stores a rich metadata representation of artifacts
- Enables researchers to assess their nature and usability
- And then locate them 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

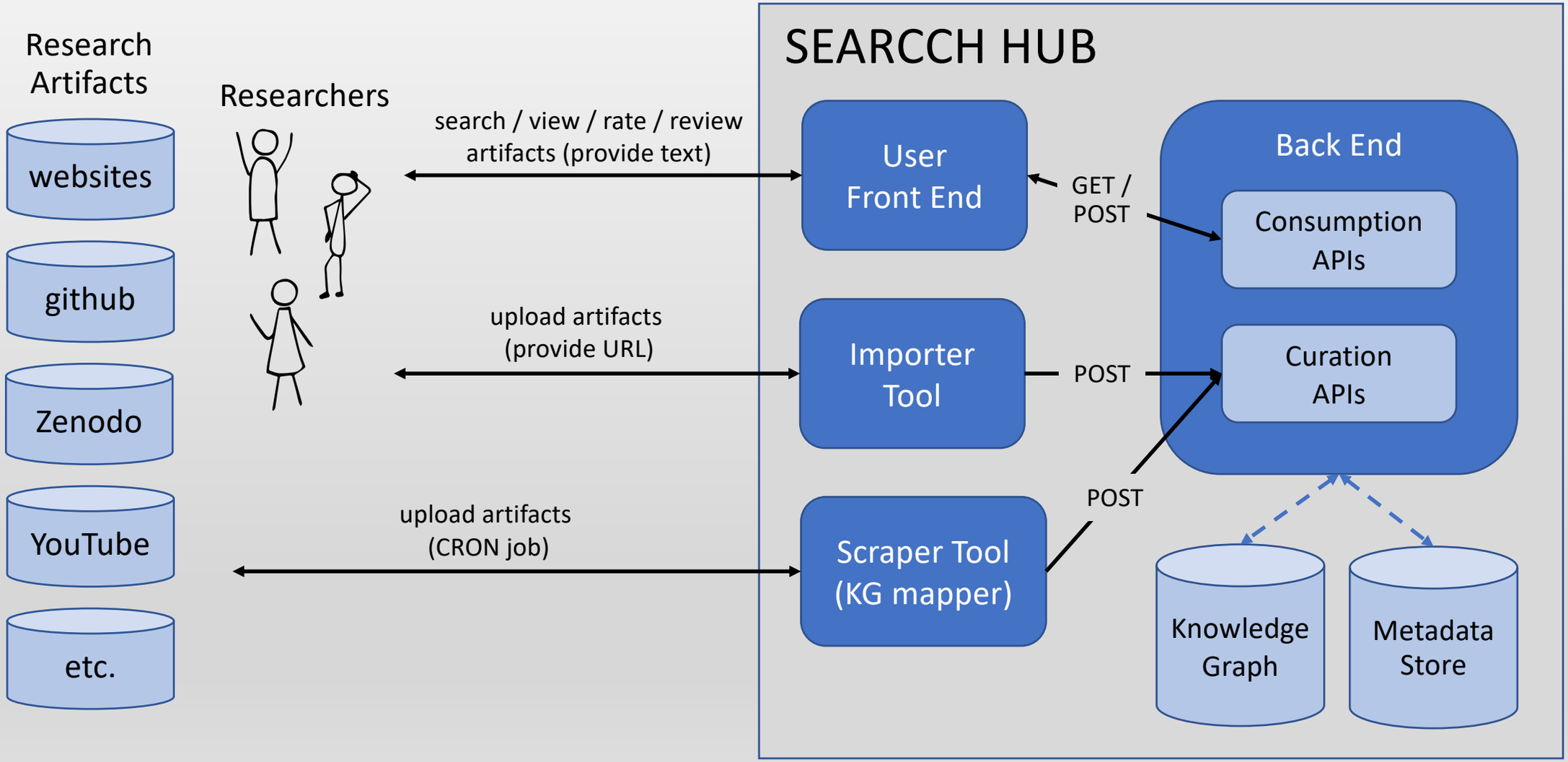
License
- Type
- Restrictions

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

Fundamental Design Questions

- Determine how the hub could best represent cybersecurity experimentation artifacts and the relationships between them, i.e., develop a data model to promote the efficient discovery
- Three related, concurrent areas of activity:
  1) Manual cataloging of cybersecurity artifacts, to better understand the existing space of artifacts
     - Examined existing repositories of cybersecurity research artifacts: ACSAC, FindResearch.org, arXiv, and Zenodo
  2) Automated “mining” of cybersecurity related artifacts from Zenodo
     - Queried Zenodo using 202 terms derived from the NICCS, yielding 64,000 records
       - Developed a TF-IDF-based scoring technique to calculate relevance, with a suitable threshold
       - Iterated on the filtering approach using NLP algorithms until we achieved a high filtering accuracy
       - After filtering, 1,981 articles and 78 artifacts remained
     - Increased the size and variety of our initial artifact corpus
     - Provided insight into refinements of the hub's data model for individual artifacts
     - Development of a "knowledge graph" for encoding relationships between artifacts
  3) Implementation of a general "importer tool" for the hub
     - Partially automates the task of adding a catalog entry to the hub
- Once up and running, we expect that most of the hub's catalog will come from user contributions, not automated mining

Hub High-Level Architecture



Key Hub Features & Capabilities

- Import
- Search
- View
- “Like”
- Rate
- Review
- Hub feedback

SEARCCH Hub Demo (Mock-up)

SEARCCH

Sharing Expertise and Artifacts for Reuse through Cybersecurity Community Hub

Welcome to the SEARCCH Hub

The SEARCCH hub is a collaborative, community-driven platform that lowers the barrier to sharing by aiding researchers in packaging, importing, locating, understanding, and reusing experiment artifacts. The artifacts organized by the hub, including tools, methodologies, documentation, and data, can be deployed to community testbeds for performing new experiments.

For more information on SEARCCH, check out the project homepage.

To get started click continue...

SEARCCH is supported by the National Science Foundation under Grant Numbers 1925773, 1925616, 1925588, 1925564

CONTINUE

SEARCCH

Sharing Expertise and Artifacts for Reuse through Cybersecurity Community Hub

DDoS

4.009 publication

Proactive Detection of Ddos Attacks Utilizing k-Nn Classifier in an Anti-Ddos Framework

21 reviews

★ ☆ ☆ ☆ ☆

Distributed denial-of-service (DDoS) attacks pose a serious threat to network security. There have been a lot of methodologies and tools devised to detect DDoS attacks and reduce the damage they cause. Still, most of the methods cannot simultaneously achieve (1) efficient detection with a small number of false alarms and (2) real-time transfer of packets. Here, we introduce a method for proactive detection of DDoS attacks, by classifying the network status, to be utilized in the detection stage of the proposed anti-DDoS framework. Initially, we analyse the DDoS architecture and obtain details of its phases. Then, we investigate the procedures of DDoS attacks and select variables based on these features. Finally, we apply the k-nearest neighbour (k-NN) method to classify the network status into each phase of DDoS attack. The simulation result showed that each phase of the attack scenario is classified well and we could detect DDoS attack in the early stage.

READ MORE

Back

Knowledge Graph Artifact 10.5281/zenodo.1072908

Proactive Detection of DDoS Attacks Utilizing k-NN Classifier in an Anti-DDos Framework

★★½☆☆ 2.5 (88)

Description

Distributed denial-of-service (DDoS) attacks pose a serious threat to network security. There have been a lot of methodologies and tools devised to detect DDoS attacks and reduce the damage they cause. Still, most of the methods cannot simultaneously achieve (1) efficient detection with a small number of false alarms and (2) real-time transfer of packets. Here, we introduce a method for proactive detection of DDoS attacks, by classifying the network status, to be utilized in the detection stage of the proposed anti-DDoS framework. Initially, we analyse the DDoS architecture and obtain details of its phases. Then, we investigate the procedures of DDoS attacks and select variables based on these features. Finally, we apply the k-nearest neighbour (k-NN) method to classify the network status into each phase of DDoS attack. The simulation result showed that each phase of the attack scenario is classified well and we could detect DDoS attack in the early stage.

Artifact Type

Journal article

Creators

Hoai-Vu Nguyen Yongsun Choi

Keywords

distributed denial-of-service (DDoS) k-nearestneighbor classifier (k-NN) anti-DDoS framework DDoS detection.

Files

9510.pdf (size: 510621 bytes)

zenodo

Search | Upload | Communities | Log in | Sign up

March 24, 2010

Journal article | Open Access

Proactive Detection of DDoS Attacks Utilizing k-NN Classifier in an Anti-DDos Framework

Hoai-Vu Nguyen; Yongsun Choi

Distributed denial-of-service (DDoS) attacks pose a serious threat to network security. There have been a lot of methodologies and tools devised to detect DDoS attacks and reduce the damage they cause. Still, most of the methods cannot simultaneously achieve (1) efficient detection with a small number of false alarms and (2) real-time transfer of packets. Here, we introduce a method for proactive detection of DDoS attacks, by classifying the network status, to be utilized in the detection stage of the proposed anti-DDoS framework. Initially, we analyse the DDoS architecture and obtain details of its phases. Then, we investigate the procedures of DDoS attacks and select variables based on these features. Finally, we apply the k-nearest neighbour (k-NN) method to classify the network status into each phase of DDoS attack. The simulation result showed that each phase of the attack scenario is classified well and we could detect DDoS attack in the early stage.

Preview

Page: 1 of 6 | Automatic Zoom

Proactive Detection of DDoS Attacks Utilizing k-NN Classifier in an Anti-DDos Framework

Hoai-Vu Nguyen and Yongsun Choi

***Abstract*—**Distributed denial-of-service (DDoS) attacks pose a serious threat to network security. There have been a lot of methodologies and tools devised to detect DDoS attacks and reduce

computing and communication resources. Although the technique of DDoS attacks is relatively simple, it can attack both the Internet and system resources.

Since the extent of damage by DDoS attacks has increased,

42 views | 31 downloads

See more details...

Indexed in OpenAIRE

Publication date:
March 24, 2010

DOI:
DOI 10.5281/zenodo.1072908

Keyword(s):
distributed denial-of-service (DDoS) | k-nearestneighbor classifier (k-NN) | anti-DDoS framework | DDoS detection.

Communities:
World Academy of Science, Engineering and Technology

SEARCCH

Sharing Expertise and Artifacts for Reuse through Cybersecurity Community Hub

Type keyword...

4.009 publication

Proactive Detection of Ddos Attacks Utilizing k-Nn Classifier in an Anti-Ddos Framework

123 reviews

★ ★ ★ ★ ☆

Distributed denial-of-service (DDoS) attacks pose a serious threat to network security. There have been a lot of methodologies and tools devised to detect DDoS attacks and reduce the damage they cause. Still, most of the methods cannot simultaneously achieve (1) efficient detection with a small number of false alarms and (2) real-time transfer of packets. Here, we introduce a method for proactive detection of DDoS attacks, by classifying the network status, to be utilized in the detection stage of the proposed anti-DDoS framework. Initially, we analyse the DDoS architecture and obtain details of its phases. Then, we investigate the procedures of DDoS attacks and select variables based on these features. Finally, we apply the k-nearest neighbour (k-NN) method to classify the network status into each phase of DDoS attack. The simulation result showed that each phase of the attack scenario is classified well and we could detect DDoS attack in the early stage.

READ MORE

Back

Proactive Detection of Ddos Attacks Utilizing k-Nn Classifier in an Anti-Ddos Framework

496 reviews

★ ★ ★ ☆ ☆

Distributed denial-of-service (DDoS) attacks pose a serious threat to network security. There have been a lot of methodologies and tools devised to detect DDoS attacks and reduce the damage they cause. Still, most of the methods cannot simultaneously achieve (1) efficient detection with a small number of false alarms and (2) real-time transfer of packets. Here, we introduce a method for proactive detection of DDoS attacks, by classifying the network status, to be utilized in the detection stage of the proposed anti-DDoS framework. Initially, we analyse the DDoS architecture and obtain details of its phases. Then, we investigate the procedures of DDoS attacks and select variables based on these features. Finally, we apply the k-nearest neighbour (k-NN) method to classify the network status into each phase of DDoS attack. The simulation result showed that each phase of the attack scenario is classified well and we could detect DDoS attack in the early stage.

John Doe -- Comment 1

★ ★ ★ ½ ☆

Lorem ipsum dolor sit amet consectetur adipisicing elit. Sunt consequuntur eos eligendi illum minima adipisci deleniti, dicta mollitia enim explicabo fugiat quidem ducimus praesentium voluptates porro molestias non sequi animi!

Jane Doe -- Another Comment

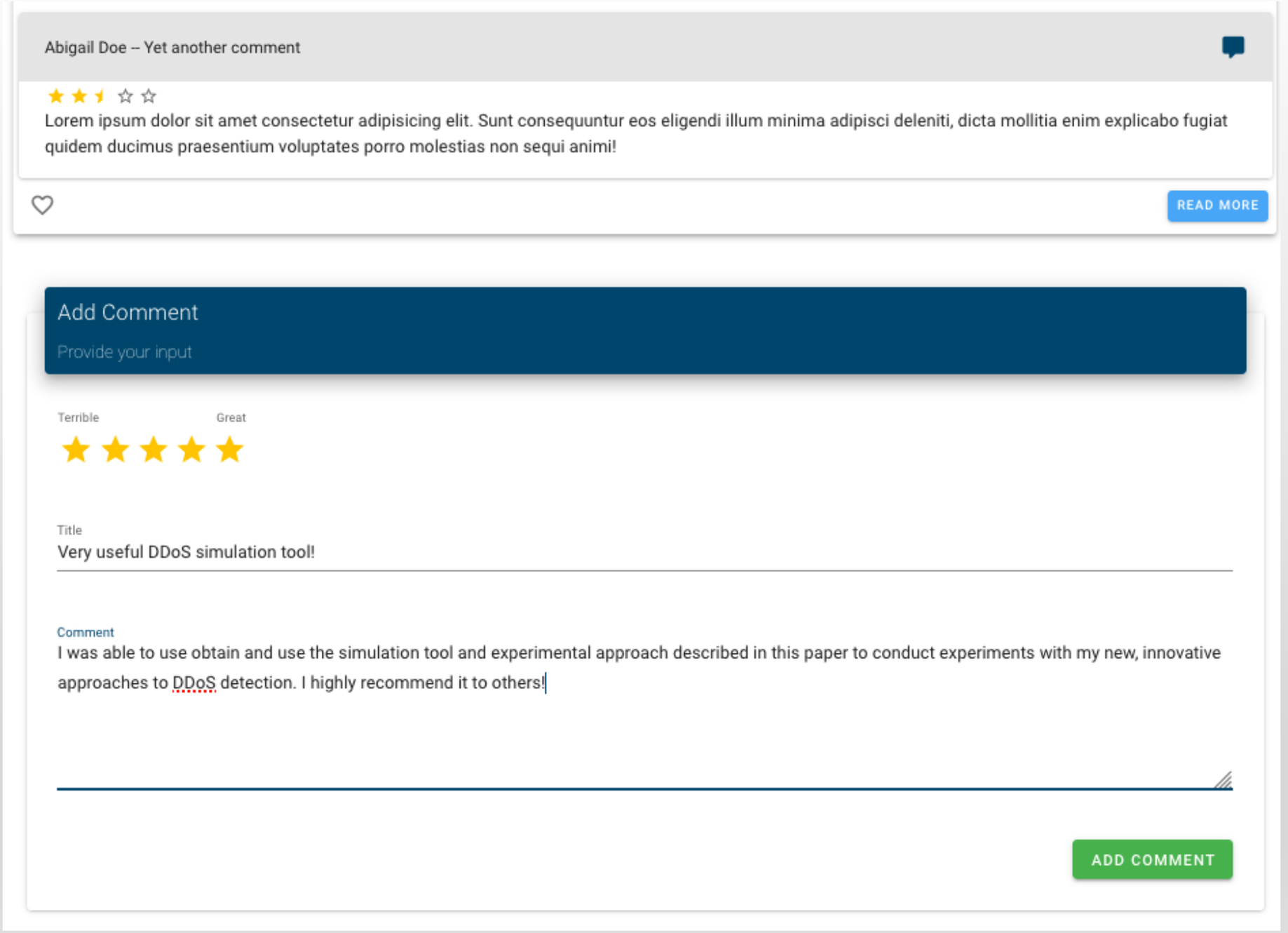
★ ★ ★ ☆ ☆

Lorem ipsum dolor sit amet consectetur adipisicing elit. Sunt consequuntur eos eligendi illum minima adipisci deleniti, dicta mollitia enim explicabo fugiat quidem ducimus praesentium voluptates porro molestias non sequi animi!

Charlie Doe -- More Comments

★ ★ ★ ★ ½

Lorem ipsum dolor sit amet consectetur adipisicing elit. Sunt consequuntur eos eligendi illum minima adipisci deleniti, dicta mollitia enim explicabo fugiat quidem ducimus praesentium voluptates porro molestias non sequi animi!

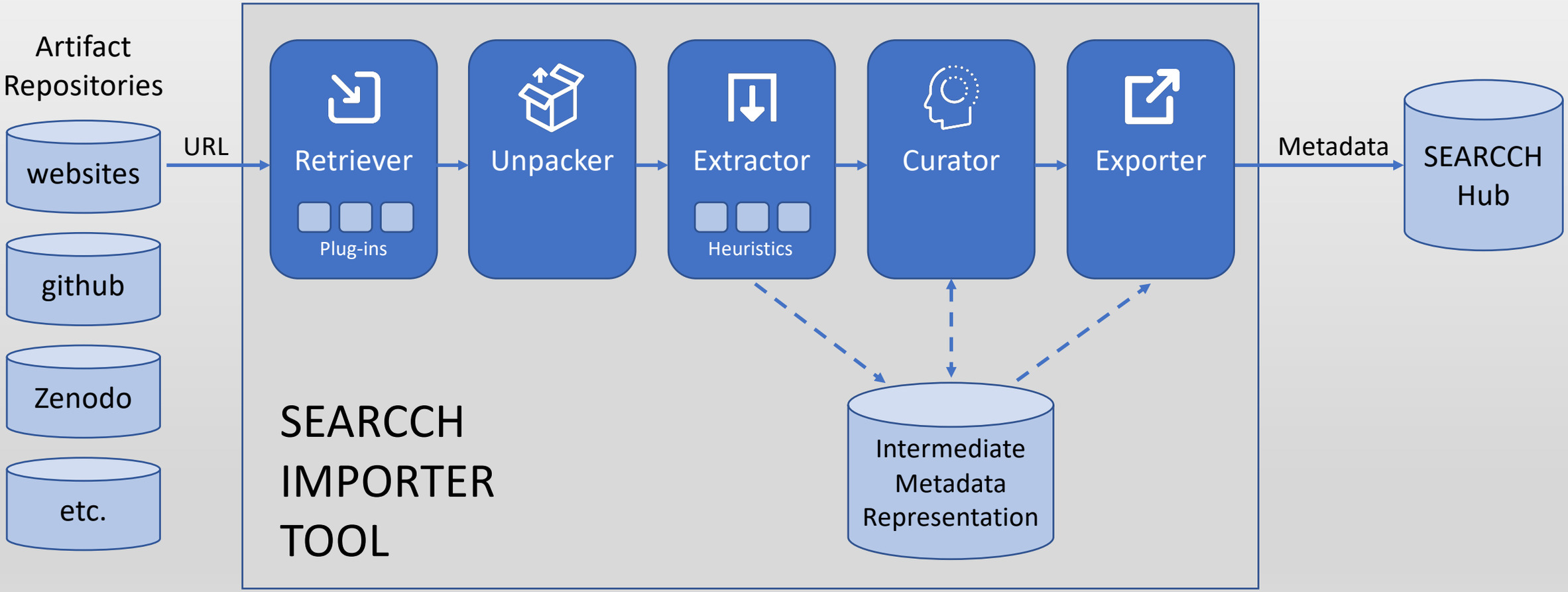

Abigail Doe -- Yet another comment
Lorem ipsum dolor sit amet consectetur adipisicing elit. Sunt consequuntur eos eligendi illum minima adipisci deleniti, dicta mollitia enim explicabo fugiat quidem ducimus praesentium voluptates porro molestias non sequi animi!
READ MORE
Add Comment
Provide your input
Terrible
Great
Title
Very useful DDoS simulation tool!
Comment
I was able to use obtain and use the simulation tool and experimental approach described in this paper to conduct experiments with my new, innovative approaches to DDoS detection. I highly recommend it to others!
ADD COMMENT

SEARCCH Importer Tool

SEARCCH Importer Tool

- Python application that partially automates the task of creating the metadata that describes an artifact
  - Input: publicly accessible location of the artifact to be imported, e.g., a URL or DOI
  - Output: metadata to be stored within the SEARCCH Hub
  - Configuration file: default metadata values, user credentials, etc.
- Allows metadata to be manually edited prior to being exported to the hub
- Also partially automates the maintenance of existing metadata within the hub, when an artifact has evolved or changed location
- Can be used either (1) as a standalone command-line tool, or (2) a back-end for a web form or other interface to help hub users import artifacts

Importer High-Level Architecture



Importer Command-line Usage

```
Usage: searcch-importer [-h] [-d] [-c CONFIG_FILE] {artifact.delete, artifact.export,
artifact.import, artifact.list, artifact.publish, artifact.show, db.check, db.upgrade,
metadata.add, metadata.delete, tag.add, tag.delete}

Subcommands
    artifact.delete     Delete an artifact.
    artifact.export     Export an artifact. Must be published.
    artifact.import     Import an artifact from a URL.
    artifact.list       List artifacts matching filter parameters.
    artifact.publish    Publish an artifact.
    artifact.show       Show artifact details.
    db.check
    db.upgrade
    metadata.add        Add a metadata pair to an unpublished artifact (adds a new curation).
    metadata.delete     Deletes a metadata pair from an unpublished artifact (adds a new
curation).
    tag.add             Add a tag to an unpublished artifact (adds a new curation).
    tag.delete  Deletes a tag from an unpublished artifact (adds a new curation).

Optional arguments:
  -h, --help    Show this help message and exit.
  -d, --debug   Enable debugging log level.
  -c CONFIG_FILE, --config-file CONFIG_FILE     Path to config file.
```

Community Building and Next Steps

SEARCCH Project Thrusts and Tasks

Thrust	Task	Description
Technology	Hub	Community collaboration portal for collecting and sharing experimental artifacts
	Artifacts import	Provide structure for shared artifacts as well as tools that facilitate content packaging for sharing
	Artifacts storage	Provide persistence mechanisms for content
	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 Engagement

Actively involve community in requirements, design, and testing of hub

- Poster at NSF SaTC PI Meeting in November 2019
- Talk at FABRIC Virtual Community Workshop in April 2020
- Poster, short talk, and BoF at IEEE S&P in May 2020
- Joint ResearchSOC and SEARCCH Panel on *Sharing Artifacts and Data for Cybersecurity Experimentation* at CSET Workshop in August 2020
- BoF at Usenix Security Symposium in August 2020

SaTC

Planning additional briefings and engagement events

- Joint FABRIC and SEARCCH workshop planned

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?

Feedback from Community

- General comments
  - Motivation and tipping point to get people to participate?
  - Good, rigorous process for admitting artifacts
  - Usability – how best to search for an artifact?
  - Balancing competing demands of being general and also useful for specific subspecialties
  - Needs to be better at indexing than Google
- Specific feedback
  - Artifact testing and validation in docker or Kubernetes
  - More descriptive rating system from different perspectives
  - Submitter attestation for permission to make artifact available publicly
  - Ability to cite and track existing artifact citations; ability to see how an artifact has been used in prior work
  - Ability to bookmark artifacts for later use
  - User attestation about usefulness of artifacts
  - Ability to annotate artifacts
  - Ability to watch an artifact and get notifications about relevant comments or artifact updates
  - Mapping/linking to other relevant artifacts pertaining to a specific dataset

Next Steps

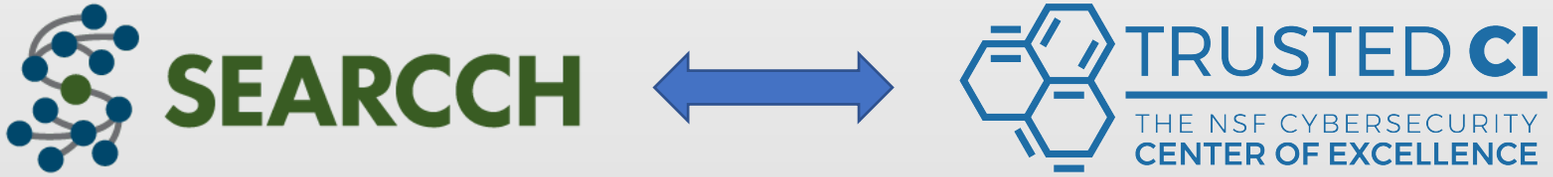
- Launch the base hub in Fall 2020
  - Complete implementation of the hub framework and basic set of features
  - Complete the artifact import tool
  - Finish pre-populating the hub with artifacts

- Expand the base implementation
  - Provide semantically rich, knowledge-based searching
  - Curate artifact collections and further seed the hub
  - Provide automated tools to assist with metadata extraction and insertion
  - Enable ratings and discussions around artifacts

- Continue to conduct community outreach and engagement activities
  - Joint FABRIC and SEARCCH workshop
  - Possible “hack-a-thon” to encourage sharing and reuse of artifacts

SEARCCH and the Trusted CI Community

- SEARCCH aligns with and supports Trusted CI's goals of of advancing cybersecurity research and securing scientific cyber infrastructure



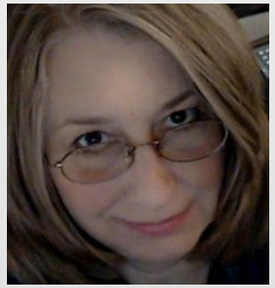
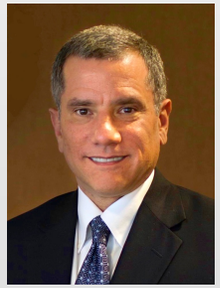
- SEARCCH will enable and support the transfer and sharing of cybersecurity experimentation expertise and artifacts for large-scale experiments running on NSF scientific infrastructure
- We invite members of the Trusted CI community to actively participate in planned SEARCCH community engagement activities and to contribute experiment artifacts and expertise to the SEARCCH hub

Contact Us

Follow us on Twitter: @SEARCCH_Hub
Visit us on the web: https://searcch.cyberexperimentation.org


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