# Poster: SPHERE: A National Testbed for Reproducible Cybersecurity and Privacy Research

Jelena Mirkovic*, David Balenson*, Erik Kline*, David Choffnes†, Daniel Dubois†,
Geoff Lawler*, Joseph Barnes*, Yuri Pradkin*, Christopher Tran*, Srivatsan Ravi*,
Terry Benzel*, Alba Regalado*, Luis Garcia‡, and Ganesh Chennimalai Sankaran§
* USC Information Sciences Institute, Email: mirkovic, balenson, kline,
glawler, jdbarnes, yuri, ctran, sravi, benzel, alba@isi.edu
† Northeastern University, Email: choffnes@ccs.neu.edu, d.dubois@northeastern.edu
‡ University of Utah, Email: la.garcia@utah.edu
§ RENCI, Email: sankarang@renci.org

***Abstract*—Researchers need a common, rich, representative research infrastructure that meets the needs across all members of the research community, and facilitates reproducible science. USC Information Sciences Institute, Northeastern University, and University of Utah have been funded by the NSF mid-scale research infrastructure program to build Security and Privacy Heterogeneous Environment for Reproducible Experimentation (SPHERE). SPHERE research infrastructure will offer access to an unprecedented variety of user-configurable hardware, software, and network resources. It will offer six user portals geared toward different populations of users. It will support reproducible research via a combination of infrastructure services and community engagement activities.**

**SPHERE is currently completing the second year out of four funded years. We have started development of general-purpose, machine-learning, and IoT enclaves. Some general-purpose nodes are already available to beta users, and we have successfully transitioned past DeterLab's research and education users to SPHERE.**

## I. Introduction

Cybersecurity and privacy threats increasingly impact our daily lives, our national infrastructures, and our industry. Recent newsworthy attacks targeted nationally important infrastructure, our government, our nuclear facilities, our researchers, and research facilities. The landscape of what needs to be protected and from what threats is continuously evolving: new technologies are released and the threat actors improve their own capabilities through experience and close collaboration. Meanwhile, defenders often work in isolation, using private data and facilities, and producing defenses that are quickly outpaced by new threats. To transform cybersecurity and privacy research into a highly integrated, community-wide effort, researchers need a common, rich, representative research infrastructure that meets the needs across all members of the research community, and facilitates reproducible science.

To meet researcher needs, USC Information Sciences Institute, Northeastern University, and University of Utah have been funded by the NSF mid-scale research infrastructure program to build Security and Privacy Heterogeneous Environment for Reproducible Experimentation (SPHERE). This research infrastructure will offer access to an unprecedented variety of hardware, software, and other resources, all relevant to cybersecurity and privacy research, connected by user-configurable network substrate, and protected by a set of security policies uniquely aligned with cybersecurity and privacy research needs. SPHERE will offer six user portals, closely aligned with needs of different user groups, facilitating widespread adoption. It will provide built-in support for reproducibility, via easy experiment packaging, sharing, and reuse. SPHERE will build a process, a standard, and incentives for community-wide efforts to develop representative experimentation environments for cybersecurity and privacy research, and to continuously contribute high-quality research artifacts. You can learn more about SPHERE by visiting https://sphere-project.net.

## II. Community Need

In recent years, essential aspects of daily life—including work, education, finance, infrastructure, and governance—have become increasingly dependent on digital systems. This shift has heightened our reliance on the correct and secure functioning of networked and computing technologies, leading to a rise in the frequency and impact of cybersecurity and privacy (CS&P) attacks. **Advancing CS&P research is critically important** to protect people, infrastructure, and data from growing threats. To better understand research needs in this space, USC Information Sciences Institute convened two community workshops in 2022: the *Cybersecurity Artifacts Workshop* [1] and the *Cybersecurity Experimentation of the Future 2022 Workshop* [3]. These workshops highlighted a shared recognition among CS&P researchers of the need for **shared, rich, and representative research infrastructure** that supports the full community and enables reproducible science—allowing a shift from *piecemeal, opportunistic efforts* to *integrated, rigorous, and community-driven research*.

## III. SPHERE Research Infrastructure

We are building innovative, transformative research infrastructure (RI) for CS&P experimentation: SPHERE – Security and Privacy Heterogeneous Environment for Reproducible

Experimentation. In this section we describe the architecture, services, and community-building activities we plan to undertake to transform CS&P research from piecemeal and opportunistic to highly integrated, community-wide effort that is sophisticated and reproducible.

The SPHERE research infrastructure will offer rich, abundant, and diverse hardware resources, which would meet the experimental needs of nearly 90% of researchers today [2]. The devices we plan to purchase and integrate with SPHERE as *experimental nodes*, and the research that benefits from these are as follows: (1) **General compute nodes:** 48 from DeterLab, 144 new nodes, with Intel TDX, ARM CCA/TrustZone, and AMD SEV; **Research supported:** application, system and network security, measurement, human user studies, large-scale experiments, education, trustworthy computing; (2) **Machine learning nodes:** 10 GPU-equipped servers; **Research supported:** security with machine-learning in the loop; (3) **Cyber-physical nodes:** 15 Rockwell Automation ControlLogix PLCs, I/O modules; **Research supported:** critical infrastructure security; (4) **Embedded compute nodes:** 600 from DCOMP, 312 new (Intel Atom, Intel Xeon D, ARM Cortex-A57, and NVIDIA Jetson NX Volta GPUs); **Research supported:** edge computing security, blockchain security, private computing, trustworthy edge computing, federated learning; (5) **IoT nodes:** 500 IoT nodes (a variety of smart home, smart speaker, camera, doorbell, TV, appliance, medical, office, wearable, and miscellaneous devices); **Research supported:** IoT security, user privacy; and (6) **Programmable nodes:** 32 NetFPGA development boards (smartNICs); **Research supported:** dynamic (programmable) network security, SDN security. SPHERE will support most popular and relevant devices for CS&P research today. If CS&P research trends change in the future, new devices can be easily added by adding new installation and control scripts.

Many CS&P researchers study phenomena that interact closely with network topology, protocols and actors – SPHERE will meet the field's unique needs by offering a dedicated, user-configurable network substrate. CS&P experiments may include generation of harmful traffic, taking live measurements from the real Internet, running human user studies, and even interacting with malicious Internet actors. To support these different research needs, and protect the Internet, SPHERE will provide safe network security policies.

All SPHERE nodes will be accessible via a single user interface. To meet the needs of various classes of users, SPHERE will provide six user portals : MAN (manual) - for exploratory research, JUP (Jupyter) – for mature research, GUI – for novice users, EDU – for use in education, AEC – for artifact evaluation committees, and HUM – for human user studies. Users will be able to access all portals from the user interface, and obtain a consistent view of their experiments, while being able to switch between portals as their needs evolve.

SPHERE will promote integrated research in cybersecurity and privacy and facilitate reproducible science by building a streamlined process, standards, and incentives for the community to develop, share and reuse high-quality research artifacts. The SPHERE team has been engaging with research and education communities in CS&P to learn about their experimentation needs and about needs around artifact sharing and reuse. To aid artifact packaging, SPHERE is building infrastructure services that include extensive logging of user actions and support for various approaches to capture experiment topology, setup and workflow. In addition to these technological advances, the SPHERE team is engaging with artifact evaluation committees at conferences and journals to support artifact evaluation on SPHERE. Additionally, SPHERE has issued an open call for mature research artifacts to be deployed on SPHERE as representative experimentation environments.

**Current Status.** SPHERE is currently completing the second year out of four funded years. We have started development of general-purpose, machine-learning, and IoT enclaves. Some general-purpose nodes are already available to beta users. We have also started design for the CPS, embedded compute, and programmable enclaves. Our control infrastructure is up and running, and so are the MAN, JUP and EDU portals. We have a pilot implementation of the AEC portal, and it was used for a part of NDSS 2024 artifact evaluation . We have also started work on designing artifact libraries. We have done extensive outreach to researchers and educators, clocking in almost 30 trips, and hundreds of direct emails. Finally, we have successfully transitioned past DeterLab's research and education users to SPHERE. We currently serve around 150 research beta users and, during school year, around 1,000 class beta users.

## IV. Conclusion

This poster describes SPHERE[1], a new research infrastructure for cybersecurity and privacy that will be built by USC-ISI, Northeastern University, and University of Utah. It is our hope that SPHERE will transform and propel CS&P research to new advances, by providing a common experimentation platform for the research community.

## References


[1] D. Balenson, J. Mirkovic, E. Eide, L. Tinnel, T. Benzel, D. Emmerich, and D. Johnson, "Cybersecurity artifacts workshop – report," https://bit.ly/CyberArtifactsWkshp2022, 2022.

[2] J. Mirkovic, "Survey of Experimentation Approaches in Cybersecurity and Privacy Papers," https://bit.ly/CyberPapersSurvey2022, 2022.

[3] J. Mirkovic, D. Balenson, S. Ravi, L. Garcia, and T. Benzel, "Cybersecurity Experimentation Workshop – 2022 – Report," https://bit.ly/CyberExperWkshp2022, 2022.



[1]SPHERE is based upon work supported by the National Science Foundation under award number 2330066. 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.

# SPHERE: A National Testbed for Reproducible Cybersecurity and Privacy Research

Jelena Mirkovic, David Balenson, and Erik Kline (USC-ISI), David Choffnes and Daniel Dubois (Northeastern University), Geoff Lawler, Joe Barnes, Yuri Pradkin, Christopher Tran, Srivatsan Ravi, Terry Benzel, and Alba Regalado (USC-ISI), Luis Garcia (U. Utah), and Ganesh Chennimalai Sankaran (RENCI)

## Societal Need

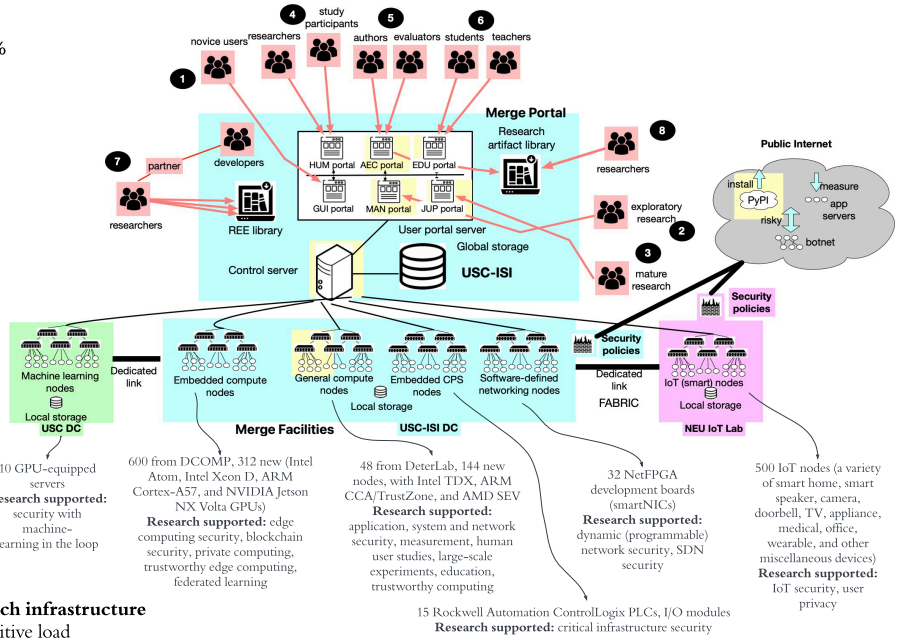
**Research progress in cybersecurity and privacy is of critical national importance, to ensure safety of U.S. people, infrastructure and data.**

## Research Need

**The cybersecurity and privacy research community needs a common, rich, representative research infrastructure, which meets the needs across all members of the community, and facilitates reproducible science.**

## SPHERE Architecture and Capabilities

- **Diverse hardware to support diverse research needs (nearly 90% of today's publications):**
  - General and embedded compute nodes with trusted hardware, PLCs and IoT devices, programmable switches and NICs, and GPU-equipped nodes
- **Six user portals supporting:**
  - Exploratory research (MAN)
  - Novice users (GUI)
  - Mature research (JUP)
  - Use in classes (EDU)
  - Use in human user studies (HUM)
  - Use for artifact evaluation (AEC)
- **Libraries of artifacts**
  - Realistic experimentation environments (REEs) and other artifacts
  - Easy reuse on SPHERE




- **Flexible security policies:**
  - Full isolation
  - Measurement research
  - Software download
  - Risky experiments with malware
- **Sample use cases:**
  - Studying ICS security in a realistic environment
  - Studying IoT behavior and privacy implications
  - Studying AI-enhanced network attack detection and mitigation
  - Evaluation at different levels of fidelity

- **Reproducibility support by research infrastructure**
  - User action logging to alleviate cognitive load
  - Help package artifacts on SPHERE (including workflows)
  - Automatically verify completeness of an artifact and: stability, consistency of results and portability

## Collaborate with Us

- **Graduate Students and Faculty Researchers** can use SPHERE to conduct new innovative research. Take our anonymous survey to share your needs.
- **Student Interns** can apply for a summer internship with the SPHERE teams
- **Other Research Infrastructure** can merge their resources with SPHERE
- **Teachers** can use SPHERE's educational modules, including homework assignments, for graduate and undergraduate classes, demos for K-12 students, and CTFs
- **Government PMs** can use SPHERE (or other Merge testbeds) to support their research programs
- **Artifact Evaluation Committees:** authors can package and share their artifacts and reviewers can evaluate shared artifacts in a common environment

TAKE THE SPHERE SECURITY EXPERIMENTATION SURVEY
**https://bit.ly/SPHERE-Needs-Survey**

## Current Status

- Completing second of four years
- Developing general-purpose, ML, and IoT enclaves
- Approx. 1/3 of general-purpose nodes available to beta users
- Approx. 1/10 of IoT nodes will be available this summer
- Designing CPS, embedded, and programmable enclaves
- Running control infrastructure and MAN, JUP, and EDU portals
- Piloting AEC portal, used for part of NDSS

| | Dev Started | Available for Use | |
|---|---|---|---|
| SPHERE Infrastructure | Oct 2023 | Mar 2024 | |
| General purpose nodes | May 2024 | Oct 2025 | * Old nodes available now |
| GPU nodes | Nov 2024 | Apr 2025 | |
| CPS nodes | Nov 2024 | Aug 2025 | |
| Embedded compute nodes | May 2025 | Jan 2026 | |
| IoT nodes | Oct 2023 | Aug 2025 | |
| Programmable nodes | Sep 2025 | Mar 2026 | * NICs available Fall 2025 |

**Visit us at https://sphere-project.net**

SPHERE is based upon work supported by the National Science Foundation under grant number 2330066. 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.