POSTER: Enabling Reproducibility through the SPHERE Research Infrastructure

Jelena Mirkovic, Brian Kocoloski, David Balenson
USC Information Sciences Institute, Marina del Rey, CA USA
{mirkovic, bkocolos, balenson}@isi.edu

Title: Enabling Reproducibility through the SPHERE Research Infrastructure
Authors: Jelena Mirkovic, Brian Kocoloski, David Balenson
Publication: USENIX ;login: Online
URL: https://www.usenix.org/publications/loginonline/enabling-reproducibility-through-sphere-research-infrastructure

Full reference: J. Mirkovic, B. Kocoloski, D. Balenson, "Enabling Reproducibility through the SPHERE Research Infrastructure," USENIX ;login: Online, Dec. 16, 2024. [Online].

Abstract: In October 2023, the U.S. National Science Foundation (NSF) funded the Security and Privacy Heterogeneous Environment for Reproducible Experimentation (SPHERE) project via its mid-scale research infrastructure program. SPHERE is a four-year long construction project to build a modern, versatile, and usable common research infrastructure to support cybersecurity and privacy research and education. Led by USC Information Sciences Institute (PIs Jelena Mirkovic and Brian Kocoloski) and Northeastern University (PI David Choffnes), SPHERE aims to transform cybersecurity and privacy research, enabling representative, sophisticated, and reproducible experimentation that allows researchers to build on the work of their peers, thus supercharging scientific progress. The infrastructure is partially complete and already in operation for beta users.

SPHERE also aims to provide usable infrastructure for various classes of users in cybersecurity and privacy areas: both novice and expert researchers, educators and students, investigators running human user studies, and artifact evaluation committees. SPHERE will further enable unprecedented access to hardware and software that is crucial to emerging cybersecurity and privacy fields, such as confidential computing, cyber-physical system security, IoT security and privacy, secure federated learning, etc.

In this article, we describe motivation and need for SPHERE (Section 1), overall architecture, components and services (Section 2), and current status (Section 3). We also explain how using a common research infrastructure helps researchers and educators (Section 4) and enables faster research progress in the entire community. SPHERE is currently open for beta users at https://sphere-testbed.net. Our project page at https://sphere-project.net provides up-to-date information about the project, describes opportunities for collaboration, and outlines plans for the future developments.

Enabling Reproducibility through the SPHERE Research Infrastructure

Jelena Mirkovic, Brian Kocoloski, David Balenson
USC Information Sciences
{mirkovic, bkocolos, balenson}@isi.edu

Societal Need

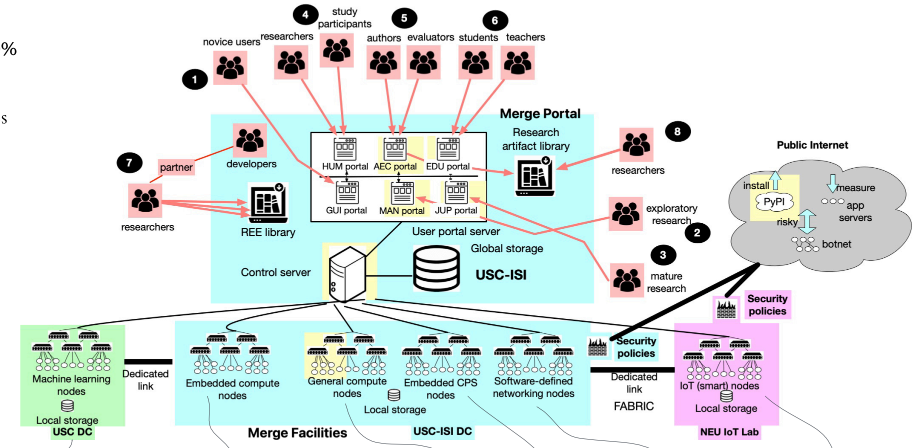
Research progress in cybersecurity and privacy is of critical national importance, to ensure safety of U.S. people, infrastructure and data.

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



10 GPU-equipped servers
Research supported: security with machine-learning in the loop

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

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, largescale experiments, education, trustworthy computing

8 programmable switches, 16 Xilinx Virtex-7 NetFPGA development boards (smartNICs)
Research supported: dynamic (programmable) network security, SDN security

500 IoT nodes (a variety of smart home, smart speaker, camera, doorbell, TV, appliance, medical, office, wearable, and other miscellaneous devices)
Research supported: IoT security, user privacy

15 Rockwell Automation ControlLogix PLCs, I/O modules
Research supported: critical infrastructure security

- **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**
  - Use SPHERE to conduct new innovative research
  - Take our anonymous survey to share your research needs
- **Student Interns**
  - Apply for a summer internship with the SPHERE teams at USC-ISI or NEU
- **Other Research Infrastructure**
  - Merge your resources with the SPHERE infrastructure
- **Teachers**
  - Use SPHERE's educational modules, including homework assignments, for graduate and undergraduate classes, demos for K-12 students, and CTFs
- **Government PMs**
  - Use SPHERE (or other Merge testbeds) to support your research programs
- **Artifact Evaluation Committees**
  - Authors can package and share their artifacts on SPHERE and reviewers can evaluate artifact in a common environment

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

Current Status

- Completed first of four years
- Started development of general-purpose and IoT enclaves
- Some general-purpose nodes available to beta users
- Started design for embedded, CPS, programmable, and GPU enclaves
- Control infrastructure and MAN, JUP, and EDU portals running
- Pilot implementation of AEC portal, used for part of NDSS
- Transitioned DeterLab users

	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

USC Viterbi School of Engineering
USC Information Sciences Institute
Northeastern University Khoury College of Computer Sciences
THE UNIVERSITY OF UTAH

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.