Research Infrastructure: Mid-scale RI-1 (M1:IP): SPHERE - Security and Privacy Heterogeneous Environment for Reproducible Experimentation

Jelena Mirkovic and Erik Kline, USC-ISI; David Choffnes, NEU; Luis Garcia, U. Utah

Award #CNS-2330066, 2023, https://sphere-project.net/, https://sphere-testbed.net/

Key Problems and their Significance

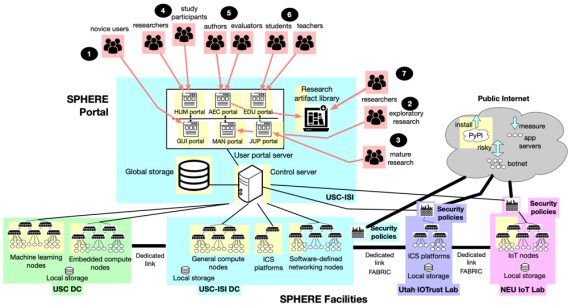
- Cybersecurity and privacy experiments increasingly depend on complex, rapidly evolving combinations of hardware, software, networks, devices, and data.
- Researchers often lack persistent access to representative environments. Even when artifacts are released, incomplete dependencies, configurations, and workflows can make results difficult or impossible to reproduce and extend.
- One-off local environments increase setup costs, impede meaningful comparison across studies, and create barriers for researchers and institutions without extensive infrastructure.
- Risky experiments involving malware, adversarial behavior, Internet measurement, or vulnerable devices require specialized isolation and security policies.
- The community needs shared, flexible infrastructure that supports realistic experimentation while preserving complete experimental environments as reusable research artifacts.

Scientific Impact and Impact on SaTC Research

- SPHERE makes experimental environments first-class research outputs by capture and sharing of code, data, configurations, hardware mappings, and workflows.
- Common infrastructure and experiment artifacts provide reusable baselines for validation, comparison, replication, and follow-on research.
- Reproducibility services (including user-action logging, artifact packaging and verification, and support for stable, portable execution) reduce uncertainty and setup effort.
- Heterogeneous resources enable results to be examined across architectures, scales, and levels of fidelity, supporting cumulative research across application, system, network, AI/ML, IoT, ICS, embedded, programmable-networking, and privacy research.
- SPHERE provides a platform through which other SaTC projects can preserve and share their experimental contributions for validation, education, and extension.

Technical Approach

- Diverse hardware to support diverse research needs (nearly 90% of today's publications)
- User portals supporting exploratory research, novice users, mature users, as well as education use, human user studies, and artifact evaluation.
- Flexible security and execution policies, including full isolation for risky experiments.
- Reproducibility support, including user action logging, artifact packaging and verification.
- Libraries of artifacts that can be easily reused.



SPHERE Resource Categories and Enabled Research

Resource Category	Enabled Research
General-Purpose Compute	Application, system, and network security experimentation; measurement studies; large-scale experiments; human user studies; trustworthy computing research
Machine Learning and GPU Resources	Security with machine learning in the loop; evaluation of ML-based defenses and attacks; reproducibility of machine learning security experiments
Internet of Things Devices	IoT security and privacy studies; behavior analysis of consumer and enterprise devices; experimentation with heterogeneous, real-world IoT ecosystems
Cyber-Physical and Industrial Control Systems	Critical infrastructure security; industrial control system experimentation; realistic CPS threat modeling and defense evaluation
Embedded and Edge-Computing Platforms	Edge and embedded system security; private and trustworthy edge computing; blockchain and federated learning in resource-constrained environments
Programmable Networking and SmartNICs	Programmable network security; software-defined networking (SDN) security; in-network measurement, detection, and mitigation mechanisms

Broader Impact (Society)

- Researchers can conduct realistic experiments and build on prior work rather than building evaluation environments from scratch.
- Industry, critical-infrastructure stakeholders, and government can evaluate, compare, and mature security and privacy solutions before deployment.
- Authors and artifact evaluation committees can package and assess artifacts in a consistent, shared environment.
- Society benefits from faster, more rigorous development of technologies that protect people, data, services, and infrastructure.

Broader Impact (Education/Outreach)

- The EDU portal supports hands-on labs, assignments, demonstrations, and defense/offense exercises without requiring comparable local infrastructure.
- Undergraduate and graduate students learn using modern systems and research practices.
- On-site and virtual internships engage students in testbed development, research, and artifact porting.
- Workshops, conference activities, surveys, and collaborations with artifact evaluation committees help align SPHERE with community needs and improve artifact-sharing practices.

Broader Impact (Participation)

- SPHERE's resources address experimental needs represented in nearly 90% of cybersecurity and privacy publications.
- Approximately 150 research beta users and 1,000 education beta users have used SPHERE.
- 23 interns in 2026 participated through on-site and virtual programs.
- Shared national infrastructure expands access for institutions unable to acquire and operate comparable resources.
- Researchers and educators can use SPHERE, contribute/evaluate artifacts, develop course materials, or federate complementary infrastructure.

Progress To Date

- Established the multi-site SPHERE architecture and integrated initial general-purpose, GPU, IoT, ICS, and embedded resources.
- Deployed the MAN, JUP, and EDU portals and made general-purpose, GPU, and initial IoT resources available to beta users.
- Supported research and education through experiments, courses, demonstrations, and artifact-evaluation pilots.
- Developed the artifact library and populated it with community-contributed artifacts.
- Conducted extensive community outreach through posters, presentations, workshops, surveys, and interviews, and engaged dozens of on-site and virtual interns.

Next Steps

- Complete deployment of the remaining IoT, ICS, embedded-compute, and programmable-networking resources.
- Mature the GUI, HUM, and AEC portals and broaden access beyond the beta community.
- Expand artifact library and improve workflow capture, verification, portability, and reproducibility support.
- Strengthen onboarding, education, and artifact-evaluation support while establishing a sustainable path for continued operation.

Publications

Jelena Mirkovic, David Balenson, Brian Kocoloski. Enabling Reproducibility through the SPHERE Research Infrastructure. USENIX ;login: Online, USENIX Association. December 16, 2024. https://www.usenix.org/publications/loginonline/enabling-reproducibility-through-sphere-research-infrastructure