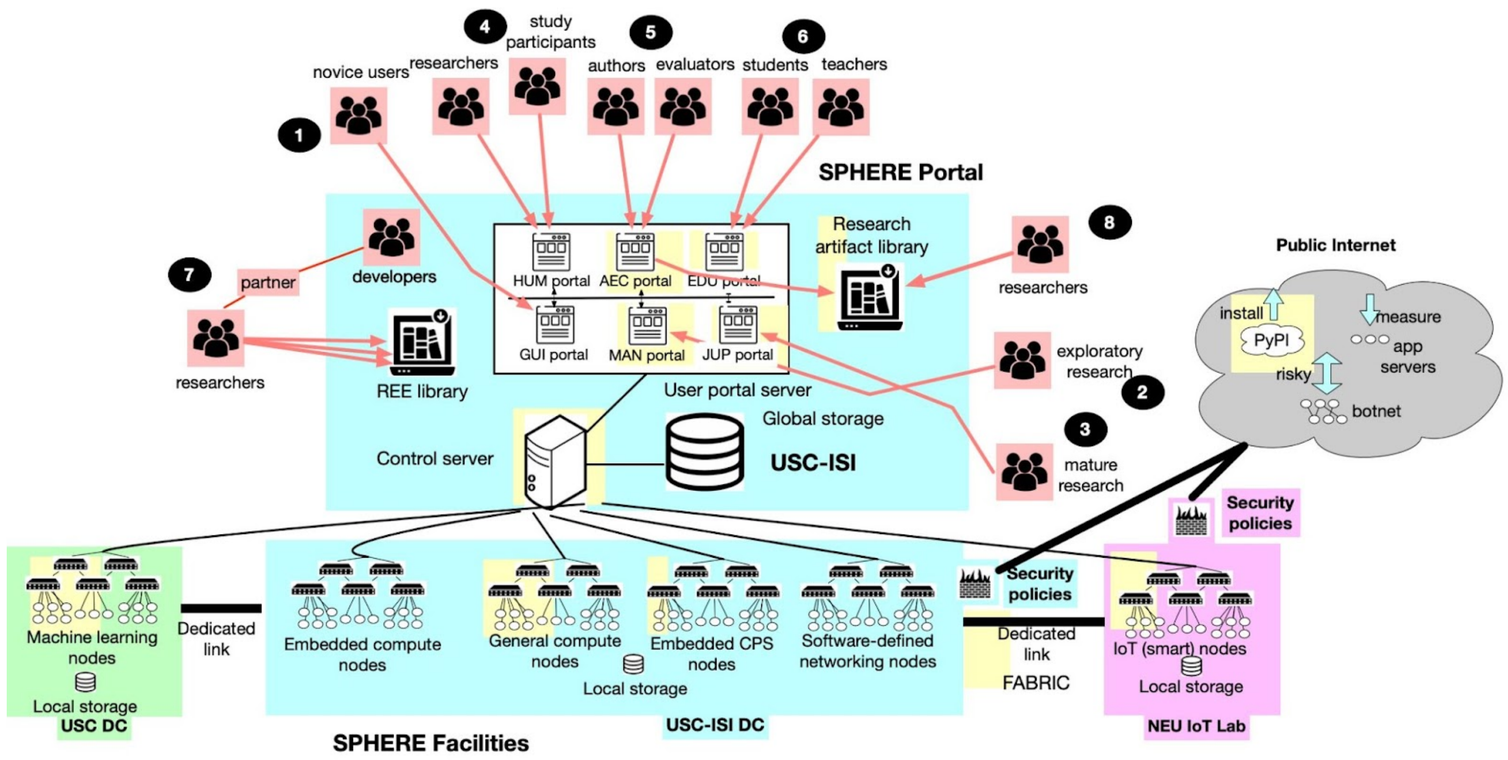
SPHERE: A Community Testbed for Reproducible Cybersecurity and Privacy Research

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

At-a-Glance

SPHERE is a public research testbed funded by the National Science Foundation and built by USC-ISI, Northeastern University, and the University of Utah
- Provides access to diverse, user-configurable hardware, software, and networking resources through six specialized user portals
- Enables integrated, representative, and reproducible cybersecurity and privacy experimentation that allows researchers to build directly on the work of their peers
- Supports a broad range of activities beyond research, including education, workforce training, cybersecurity exercises, and rigorous test and evaluation

Architecture and Capabilities



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

- **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, human user studies, and artifact evaluation
- **Flexible security and execution policies**, including full isolation for risky experiments
- **Reproducibility support**, incl. user action logging, artifact packaging and verification
- **Libraries of artifacts** including REEs and others with easy reuse

Citation: 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-researchinfrastructure

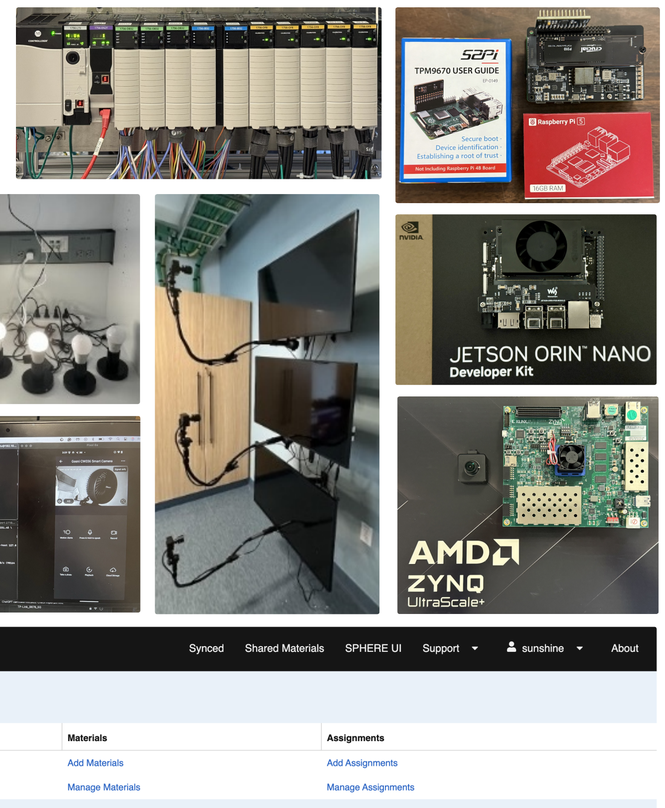
User Communities

RESEARCHERS
- Conduct realistic experiments using diverse, user-configurable hardware and networks
- Safely execute security-sensitive workloads, including malware and adversarial behaviors
- Scale experiments from prototypes to larger deployments
- Package and share complete experimental environments to support validation and follow-on research

TEACHERS AND STUDENTS
- Integrate hands-on cybersecurity experimentation into undergraduate and graduate courses
- Use curated environments and intuitive interfaces without requiring local infrastructure
- Deploy labs, assignments, demonstrations, and capture-the-flag exercises at scale
- Align education with modern research practices and real-world systems

PAPER AUTHORS AND ARTIFACT EVALUATION COMMITTEES
- Package experimental artifacts, incl. code, data, and workflows, in common environment
- Evaluate artifacts using shared, centrally managed infrastructure
- Reduce setup effort and variability across reviewers
- Improve transparency, repeatability, and confidence in experimental results

INDUSTRY AND GOVERNMENT
- Test-drive and evaluate security and privacy solutions prior to deployment
- Demonstrate and stress-test systems in realistic experimental environments
- Compare approaches using shared, reproducible setups
- Collaborate with researchers to validate and mature technologies



REEs

Representative Experimentation Environments hosted as mature, long-lived research artifacts and available as community-accessible infrastructure resources
- Enable reuse, comparison, education, and extension of published work
- Preserve realistic experimental setups beyond the lifetime of individual projects

Current REEs include security paper artifacts, CensorLab, reconstructed datasets, and an automotive CAN bus simulation environment

See the **Call for REEs** and **virtual internship information** on the SPHERE website

Getting Started

Request access to SPHERE resources tailored to meet your goals and expertise
- Explore multiple user portals for research, education, and artifact evaluation
- Deploy existing experiments or REEs without building custom infrastructure
- Use documentation and onboarding materials to quickly experiment

Learn more and get started: 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.