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

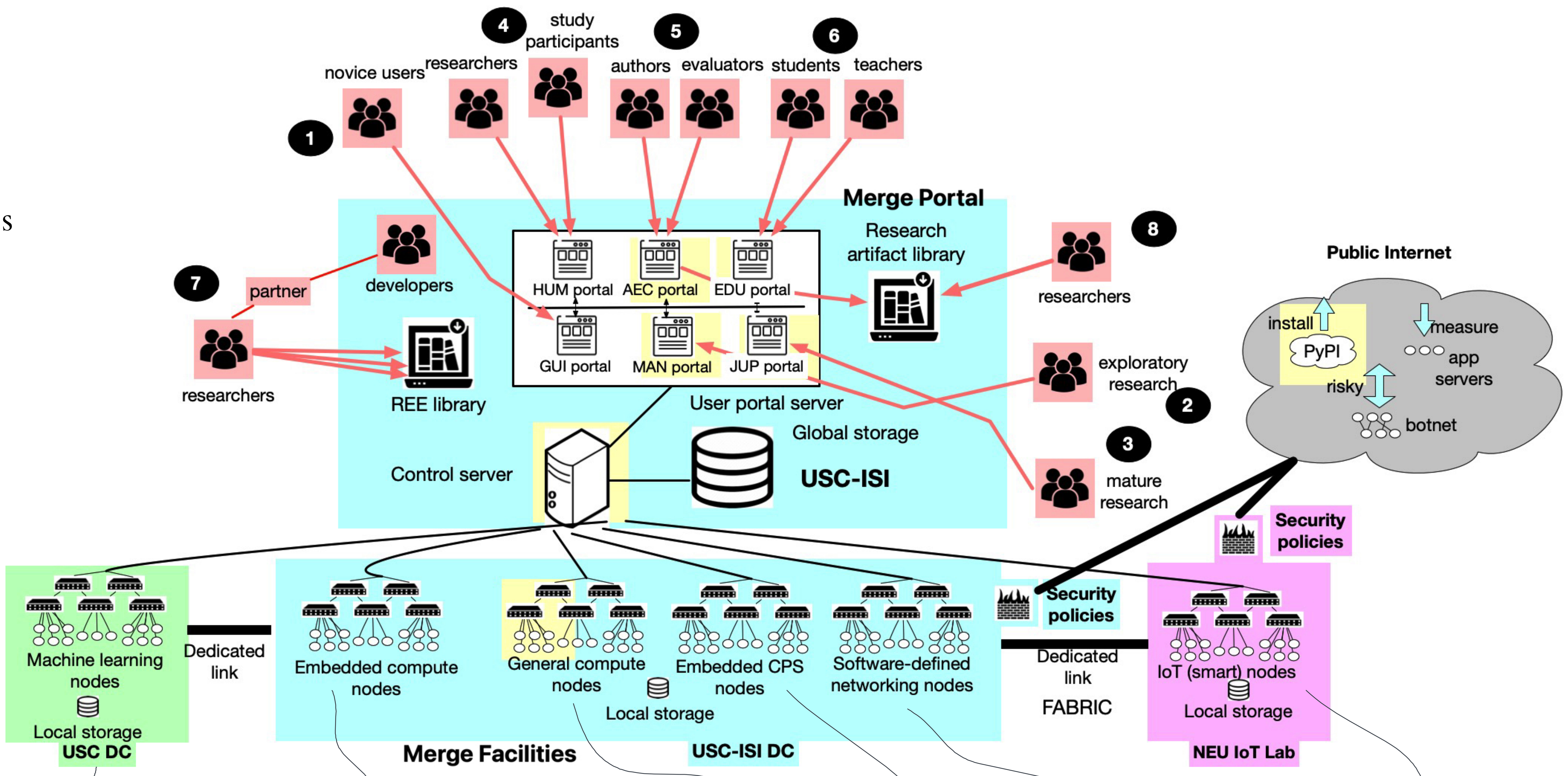
- **Advancing research in cybersecurity and privacy** is of critical global importance for safeguarding people, infrastructure, and data worldwide.
- As societies grow increasingly interconnected and reliant on digital systems, **robust and reproducible research** is essential to counter evolving threats and strengthen the security, privacy, and resilience of our shared global community.

Research Need

- The global cybersecurity and privacy research community needs a **common, comprehensive, and representative research infrastructure** that meets the needs of all its members and enables reproducible science.
- Such an infrastructure must support **realistic experimentation, foster widespread collaboration,** and accelerate the **development of solutions** that enhance cybersecurity and privacy worldwide.

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)
  - Education (EDU)
  - Human user studies (HUM)
  - 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, large-scale experiments, education, trustworthy computing

32 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** 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

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

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

	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

- Designing CPS, embedded, and programmable enclaves
- Running control infrastructure and MAN, JUP, and EDU portals
- Piloting AEC portal, used for part of NDSS

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.