

Security and Privacy Heterogeneous Environment for Reproducible Experimentation (SPHERE)

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

<https://sphere-project.net>



Societal and Research Needs

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

- Our nation depends on correct and reliable functioning of network and computing systems

Frequency and impact of cybersecurity and privacy attacks are constantly increasing

Scientific Impact

Provide the cybersecurity and privacy (CS&P) research community with a common, rich, representative research infrastructure that meets the needs across all members of the community and facilitates reproducible science

Common, rich infrastructure:

- Security and privacy issues affect different technologies differently (e.g., CPU architectures)
- Some emerging technology can create new vulnerabilities (e.g., IoT)
- New technologies can be used for defense (e.g., trusted hardware, SDN)
- Infrastructure must have diverse hardware to meet wide research needs

Meet needs across all members of the community:

- Experienced and novice users, researchers, educators and students

Facilitate reproducible science:

- Help researchers create, share, and reuse research artifacts

SPHERE Research Infrastructure

Diverse hardware to support diverse research needs (nearly 90% of today's publications):

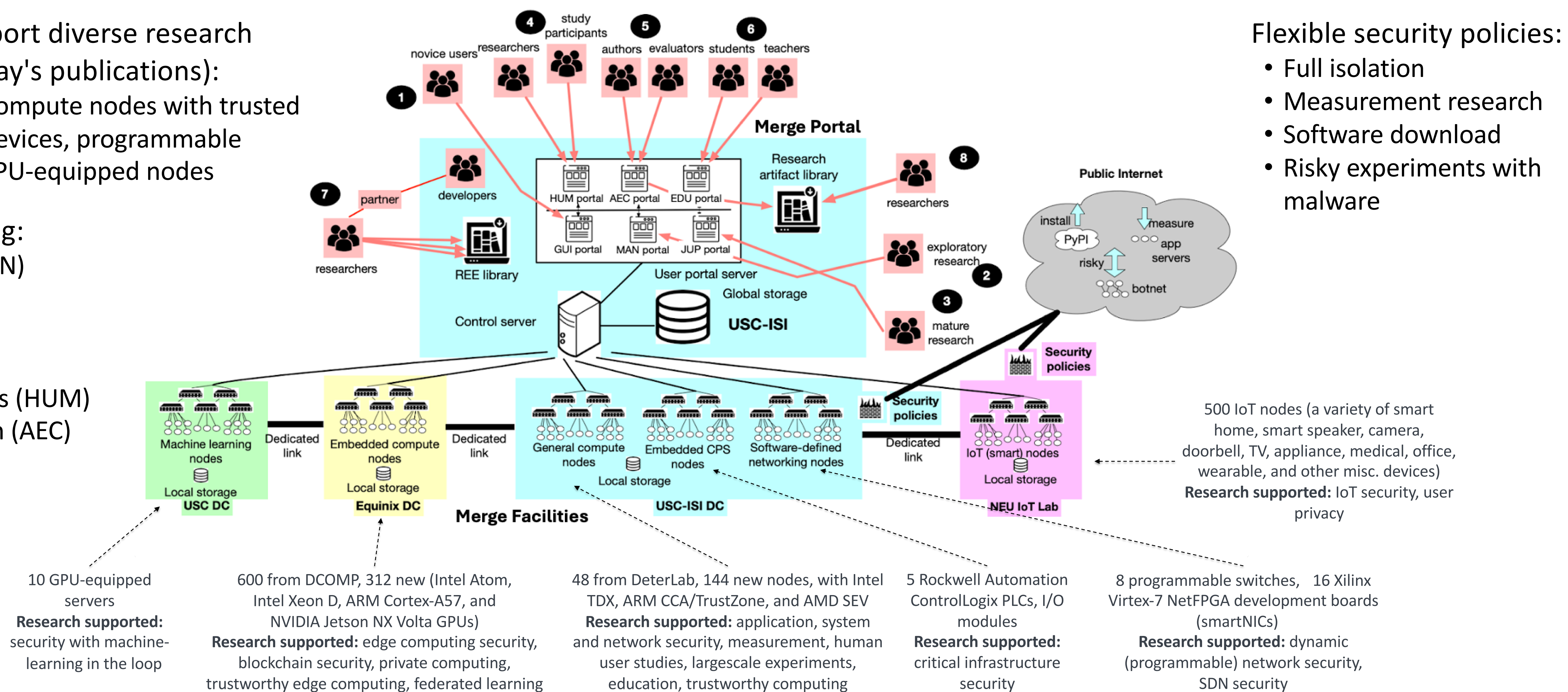
- General and embedded compute nodes with trusted hardware, PLCs and IoT devices, programmable switches and NICs, and GPU-equipped nodes

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

- REEs and other artifacts
- Easy reuse on SPHERE



Flexible security policies:

- Full isolation
- Measurement research
- Software download
- Risky experiments with malware

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

Broader Impact – Research Community

Need-discovery workshops and surveys

- Presentations and BoFs at major conferences
- Engage researchers via surveys and interviews
- Adjust SPHERE development to meet needs

Help develop standards for artifacts

- Engage wide research community in discussion about artifacts
- Help produce specifications around proper and complete artifact documentation

Representative experimentation environments (REEs)

- Used by multiple researchers for a given experimentation task, become a standard for evaluation in a sub-field of CS&P
- Contributed by community - researchers receive supplemental funding to deploy their high-quality artifacts

Streamlining artifact evaluation

- Work with artifact evaluation committees (AECs) to have artifacts evaluated on SPHERE
- Artifact authors can submit their artifacts on SPHERE
- AECs evaluate artifacts on SPHERE
- Artifacts remain hosted on SPHERE

Broader Impact – Education

Broadening participation in computing

- Host students, involve them in SPHERE development
- Provide research infrastructure to under-resourced institutions
- Improve cybersecurity education via EDU portal, hosting of education materials

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.

