Trusted CI Webinar Series

Title: SPHERE - Security and Privacy Heterogeneous Environment for Reproducible Experimentation

Presenters: Dr. Jelena Mirkovic & David Balenson (USC-ISI)

Host: Jeannette Dopheide

Slides: https://tinyurl.com/5n6nev4z

The meeting will begin shortly.

Participants are muted. Click the chat button to ask a question.

This meeting will be recorded.

The Trusted CI Webinar Series is supported by National Science Foundation grant #2241313.

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the NSF.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

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

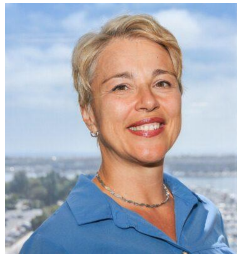
University of Southern California Information Sciences Institute,
Northeastern University, University of Utah

Presented by: Jelena Mirkovic, PI <mirkovic@isi.edu> and

David Balenson, Outreach Director <balenson@isi.edu>

SPHERE is based upon work supported by the National Science Foundation under Grant #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.

SPHERE Project Team



Jelena Mirkovic
USC-ISI
Lead PI

Brian Kocoloski
USC-ISI
Co-PI, Tech Lead

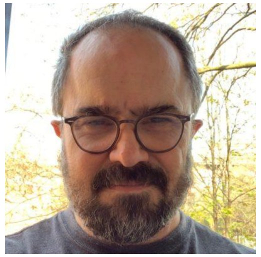
David Choffnes
NEU
Co-PI

Daniel Dubois
NEU
Tech Lead

David Balenson
USC-ISI
Outreach Director

Alba Regalado
USC-ISI
Project Manager

Terry Benzel
USC-ISI



Geoff Lawler
USC-ISI

Joseph Barnes
USC-ISI

Christopher Tran
USC-ISI

Srivatsan Ravi
USC-ISI

Ganesh Sankaran
USC-ISI

Erika Bobbitt
USC

Luis Garcia
Utah

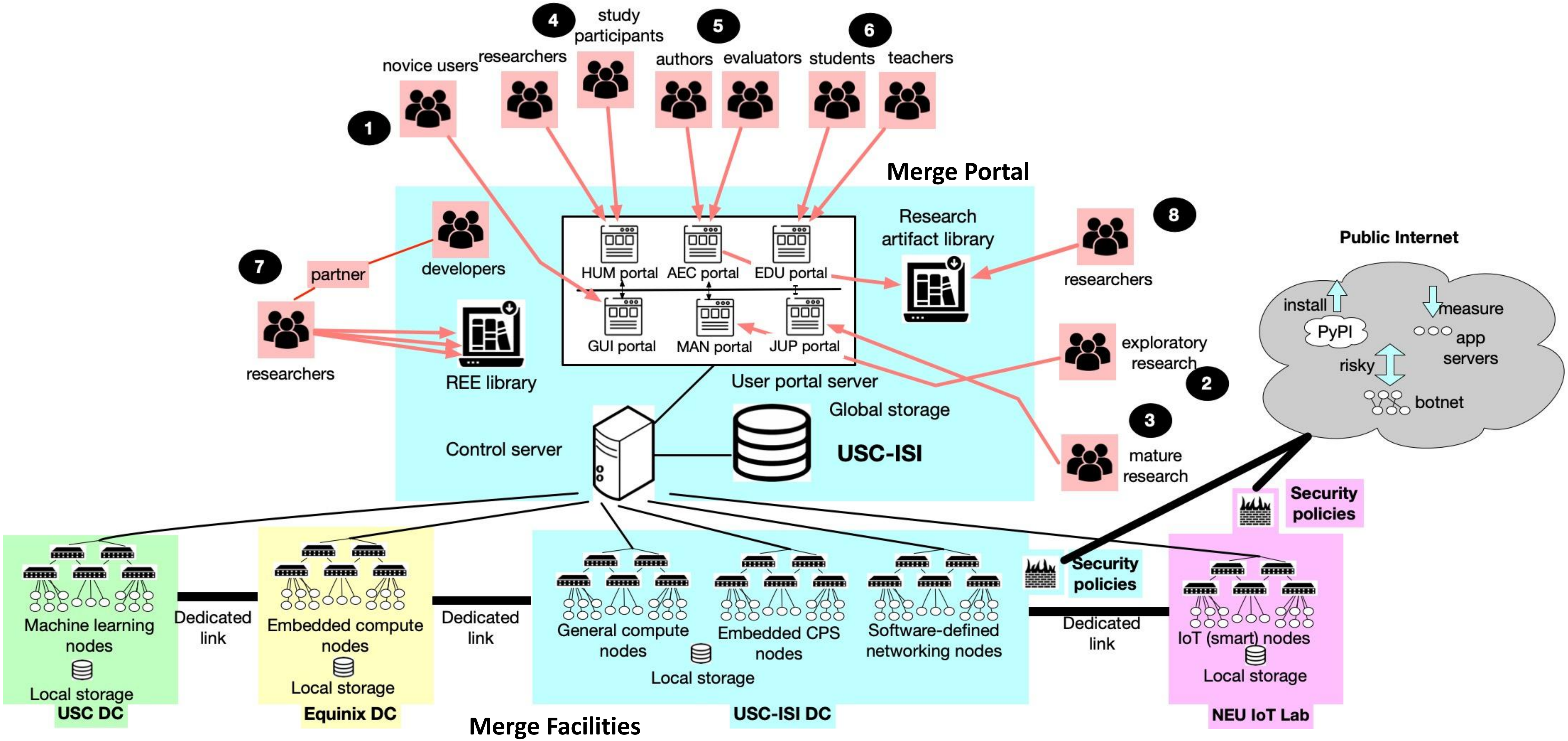
Motivation and Need

- **Motivation:** Cyber threats affect every aspect of our daily lives, critical infrastructure, science, and government. Research solutions are simplistic, piecemeal, and opportunistic, and slow to reach the market
- **Community need:** Common, rich, representative research infrastructure, which meets the needs across all members of the community and facilitates reproducible science

vertical progress, integrated research
more sophisticated solutions

- **Proposed:** SPHERE research infrastructure
  - Heterogeneous resources to meet 90% of research needs in the community
  - Multiple user portals to meet the unique needs of different classes of users
  - Processes/incentives for the community to create representative experimentation environments (REEs) on SPHERE
  - Integrated reproducibility support and processes/incentives for stakeholders to share/reuse research artifacts

SPHERE High-Level Architecture

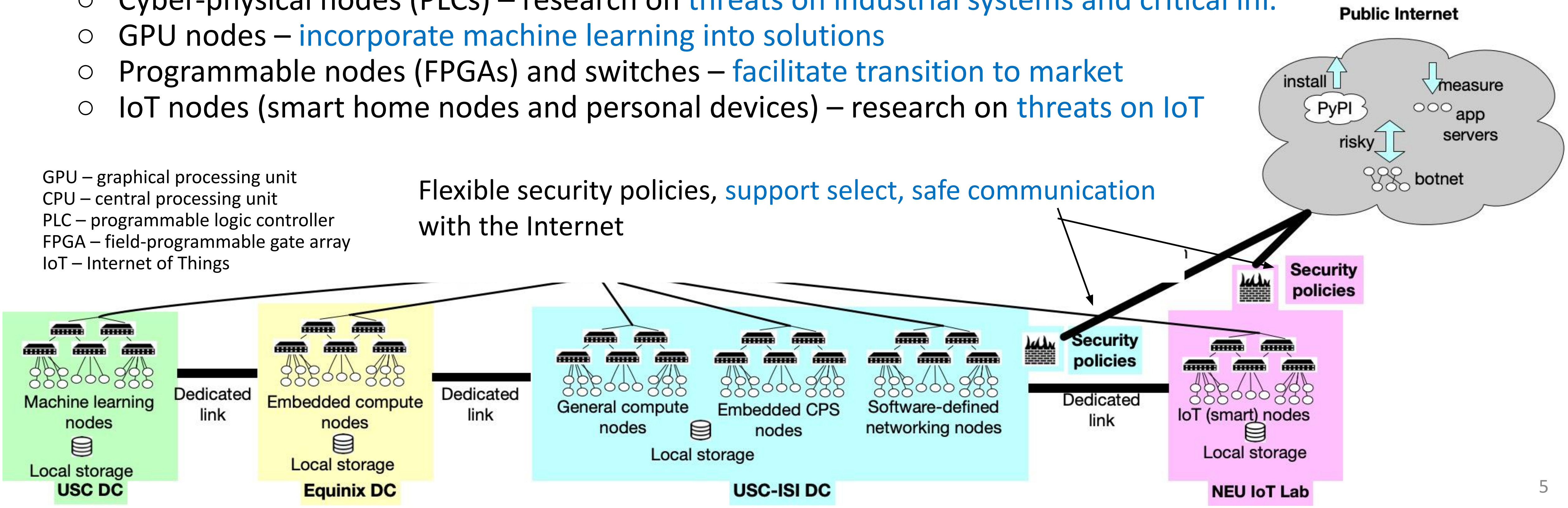


SPHERE Multiple Types of Resources

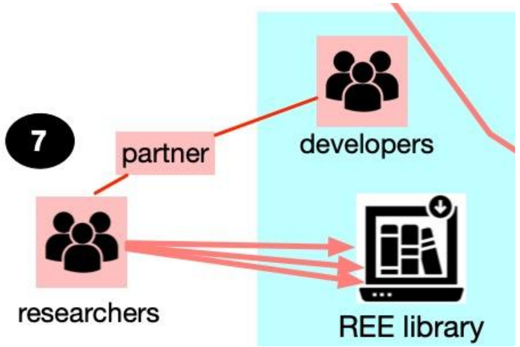
- **Multiple** types of resources, needed for **emerging cybersecurity and privacy research**:
  - General compute nodes with trusted computing technology – research on network, cloud computing and system threats
  - Embedded compute nodes (e.g., in phones, tablets, etc.) – research on distributed threats, threats on distributed computing, attacks on specific CPU architectures
  - Cyber-physical nodes (PLCs) – research on threats on industrial systems and critical inf.
  - GPU nodes – incorporate machine learning into solutions
  - Programmable nodes (FPGAs) and switches – facilitate transition to market
  - IoT nodes (smart home nodes and personal devices) – research on threats on IoT

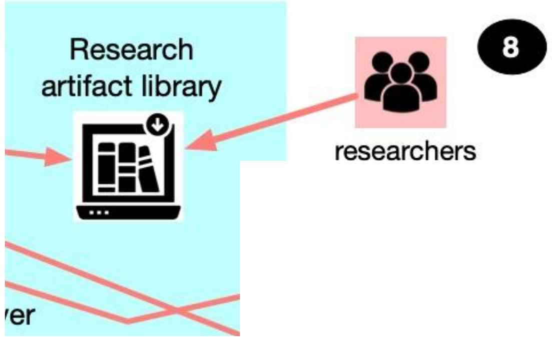
GPU – graphical processing unit
CPU – central processing unit
PLC – programmable logic controller
FPGA – field-programmable gate array
IoT – Internet of Things

Flexible security policies, support select, safe communication with the Internet



SPHERE REEs and Research Artifacts





Representative Experimentation Environments (REEs)

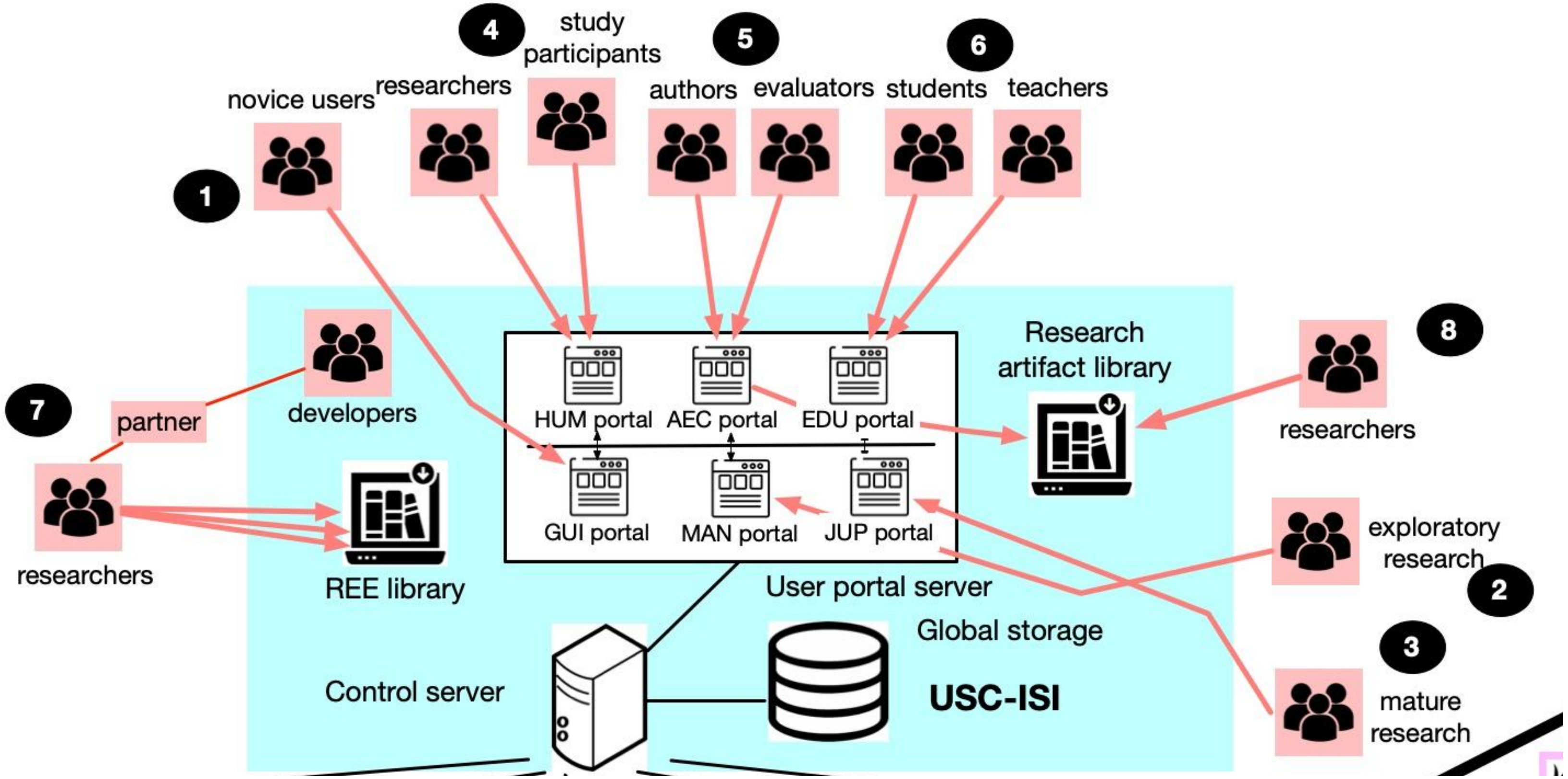
- Make research more relevant, vertical and sophisticated
- “Standard” for experimentation in each CS&P area
- Integrated by their authors into SPHERE (funded)

Research Artifacts

- Make research more vertical and reproducible
- Acquired via partnership with artifact evaluation committees (AECs)
- Integrated by their authors into SPHERE as part of artifact evaluation for a conference

CS&P – cybersecurity and privacy
AEC – artifact evaluation committee

SPHERE Portals



- Multiple user portals, supporting different types of users and use modalities
  - Manual, scripted, and GUI-only use support exploratory, mature, and novice research
  - Dedicated support for AECs, education, Internet measurement, and human user studies

GUI – graphical user interface
AEC – artifact evaluation committee

SPHERE History

- **Over the past 20 years:** USC-ISI designed, built and operated DETERLab
  - 389 research project teams from 278 institutions, and involving 1,042 researchers from 205 locations and 46 countries
  - 230 classes from 147 institutions and helped educate more than 20,000 students
- **2019:** Merge software for testbed control and management
  - Built w/ modern open-source tools for large-scale, high-fidelity, robust experimentation
  - Merge has run several of our testbeds for the past four years – DCOMP, Searchlight, RedStar and modernized DeterLab
- **Modernized software and hardware:** via NSF CCRI grant 2019-2022 and ARO DURIP grant 2019-2021
  - 48 new nodes, 6 new switches, Merge software, user transition
- Modernized DETERLab will become the first seed to grow SPHERE as part of its general compute enclave

SPHERE Unique Research Capabilities

SPHERE RESEARCH INFRASTRUCTURE

- **Relevance:** Experiments with emerging technology and specialized hardware, not currently available to many researchers, support 90%
- **Realism:** Experiments that combine different hardware devices to create realistic scenarios
  - e.g., IoT nodes with GPU nodes and programmable switches to filter attacks
- **Reproducibility:** Experiments on common RI, with extensive support for artifact sharing and reuse, facilitate vertical development
- **BPC:** Different experimentation portals cater to users with different abilities and interests, lowering barrier to entry
- **Impact:** Faster pace of innovation in CS&P and faster technology transition to practice, enabling U.S. to become the global leader in this area

IoT – Internet of Things
GPU – graphical processing unit
CS&P – cybersecurity and privacy

SPHERE Team Background

SPHERE RESEARCH INFRASTRUCTURE

- **DeterLab:** the only public cybersecurity testbed for **18 years**

389 research groups
1K researchers
237 classes
20K students

- Additional testbeds for formal eval. of DARPA programs
- **Merge:** mature testbed management software, running all three testbeds

ported to 4 partner institutions

- **Mon(IoT)r:** largest private IoT testbed and datasets

560 downloads

- Prior NSF funding: **SEARCCH** (reprod.), **DEW** (reprod., usab.), **DeterLab modernization** (RI)
- Many publications on experimentation, reproducibility, IoT privacy
- Founded **CSET workshop**, led NSF-funded **CEF study**, organized **CEF 2022** and **Cybersecurity Artifacts 2022** workshops, pioneered use of testbeds in education

IoT - Internet of Things
CSET – Cyber Security Experimentation and Test, running for 16 years
CEF – Cybersecurity Experimentation of the Future

SPHERE Research Value

- Transform CS&P research from piecemeal, opportunistic to integrated; and from reactive to proactive
- Enable reproducible experimentation that is easily and remotely accessible to all U.S. researchers
  - Especially benefits underserved researcher populations (evidence from DeterLab)
- Students from MSIs and HBCUs recruited for paid internships
- Work with AECs to transform the research process and host artifacts
- REEs and artifacts will lead to increase in publications and data products

CS&P – cybersecurity and privacy
MSI – minority serving institution

HBCU – historically black colleges and universities
REEs – representative experimentation environments
AEC – artifact evaluation committee

SPHERE Societal Benefits

SPHERE
RESEARCH INFRASTRUCTURE

- Faster pace of innovation in CS&P and more mature solutions on the market
- Protect scientific infrastructure and society from various threats: ransomware, data theft, data corruption, supply chain attacks, denial of service, etc.
- Produce larger, more diverse, better educated and prepared CS&P workforce
- Help integrate CS&P solutions into new and emerging technologies before they get widely deployed

CS&P – cybersecurity and privacy

SPHERE Community Outreach

- Presentations, posters, and other activities at major conferences
  - Major cybersecurity conferences: NDSS, S&P, USENIX Security, CCS, ACSAC
  - NSF events: RIW, SaTC PI meeting, Cybersecurity Summit
  - Other conferences: IoT, CPS, HPC, etc.
  - Underrepresented communities: Tapia, Grace Hopper, SACNAS NDiSTEM
- Engage researchers via surveys and interviews
  - Google form at https://bit.ly/SPHERE-Needs-Survey
  - No more than five minutes, six open-ended questions
  - Anonymous and can skip questions
- Adjust SPHERE development to meet community needs

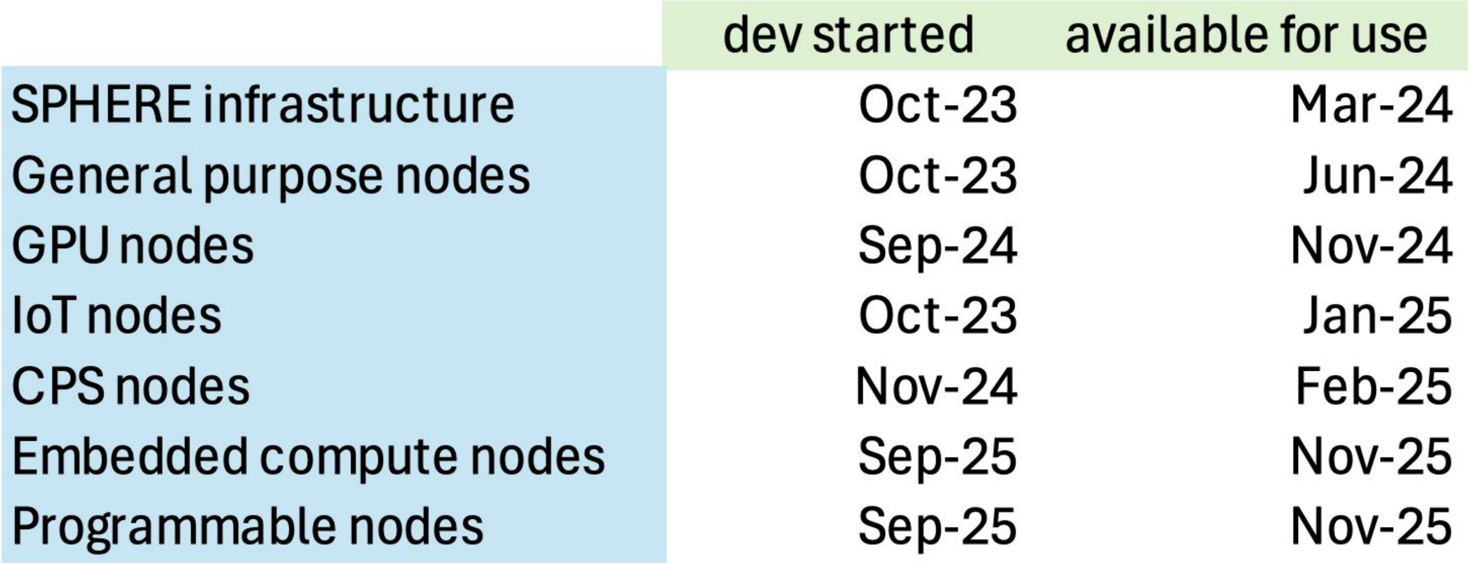
bitly

NDSS – Network and Distributed System Security
S&P – IEEE Symposium on Security & Privacy
CCS – ACM Conference on Computer & Communication Security
ACSAC – Annual Computer Security Applications Conference

RIW – Research Infrastructure Workshop
SaTC – Secure and Trustworthy Cyberspace
SACNAS – Advancing Chicanos/Hispanics & Native Americans in Science
NDiSTEM – National Diversity in STEM

Become a SPHERE Beta User

- Help us grow and improve before we open to larger audience
- Get access to cool new hardware and features
  - Log in remotely via browser, create custom topologies of general purpose VMs (control VM resources, network topology, bandwidth and delay)
  - Access nodes via SSH w/ sudo privileges
  - Experiment directly on nodes or via Jupyter notebooks
  - Able to reach into the Internet, can also support incoming connections
  - Chat-based user support

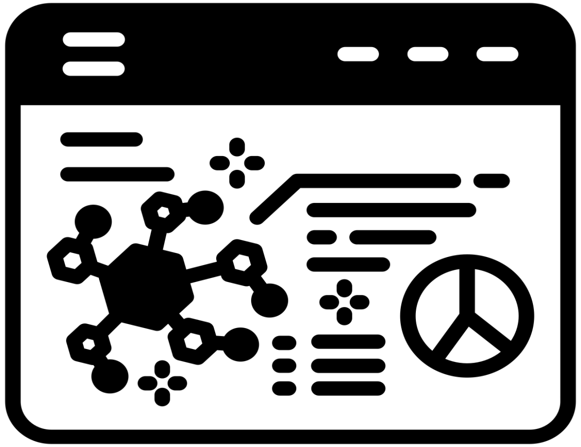


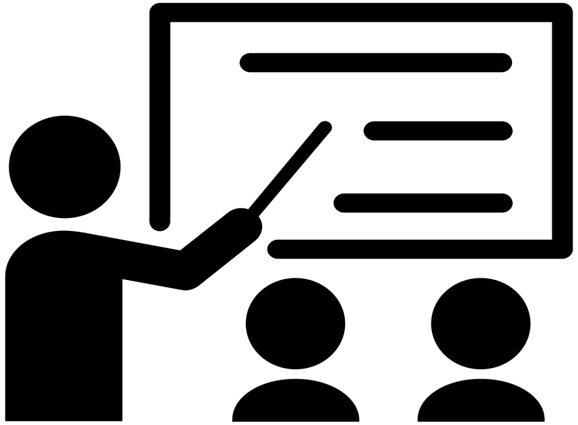
	dev started	available for use	
SPHERE infrastructure	Oct-23	Mar-24	
General purpose nodes	Oct-23	Jun-24	* old nodes available now
GPU nodes	Sep-24	Nov-24	
IoT nodes	Oct-23	Jan-25	
CPS nodes	Nov-24	Feb-25	
Embedded compute nodes	Sep-25	Nov-25	
Programmable nodes	Sep-25	Nov-25	* NICs available Fall 2024

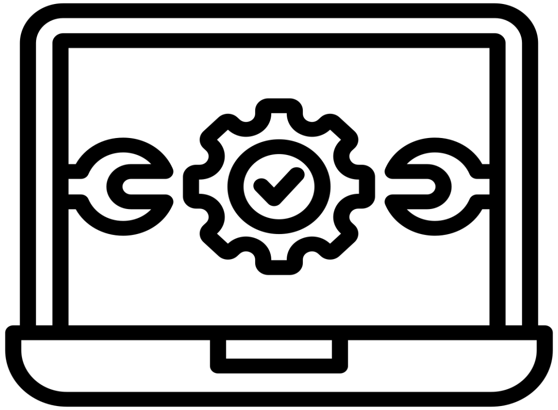
How You Can Help with SPHERE

Promote and leverage SPHERE at your institutions!

- Researchers can use SPHERE to conduct new, innovative research
- Faculty and students can use SPHERE for educational purposes
- IT staff can use SPHERE to test, and evaluate new solutions and technologies







Thank you!

https://sphere-project.net

contact@sphere-project.net

SPHERE

RESEARCH
INFRASTRUCTURE

Questions?

Click on the chat icon to type a question

Community Updates

- Next Webinar: May 20th @ 11am Eastern
  - Topic: NSF Research Infrastructure Guide
  - Speakers: Mike Corn (NSF)
  - **webinars@trustedci.org**
- Trusted CI NSF Cybersecurity Summit (Oct 7-10th) @ Pittsburgh, PA
  - Student Program: Call for applications coming soon!

About the Trusted CI Webinar series

To view presentations, join the announcements mailing list, or submit requests to present, visit: **trustedci.org/webinars** or email **webinars@trustedci.org**

The Trusted CI Webinar Series is supported by National Science Foundation grant #2241313.

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the NSF.

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

TRUSTED CI

THE NSF CYBERSECURITY CENTER OF EXCELLENCE

trustedci.org