Poster Abstract: SPHERE CPS Enclave: A Reconfigurable Testbed for Industrial Control System Security Experimentation

Luis Garcia (University of Utah), Jelena Mirkovic (USC-ISI), David Balenson (USC-ISI), Erik Kline (USC-ISI), Yuri Pradkin (USC-ISI), David Choffnes (Northeastern University), Daniel Dubois (Northeastern University), Terry Benzel (USC-ISI), Srivatsan Ravi (USC-ISI), Joseph Barnes (USC-ISI), Geoff Lawler (USC-ISI), Chris Tran (USC-ISI), Alba Regalado (USC-ISI)
la.garcia@utah.edu,{mirkovic,balenson,line,yuri}@isi.edu,choffnes@ccs.neu.edu,d.dubois@northeastern.edu
{tbenzel,sravi,sankara,jdbarnes,glawler,ctran,alba}@isi.edu

Abstract

Cyber-physical systems (CPS) increasingly face security threats that can disrupt critical infrastructure operations. The SPHERE CPS enclave is a modular, remotely accessible industrial control system (ICS) testbed designed to support security experimentation on programmable logic controllers (PLCs), industrial networks, and digital twin simulations. It enables researchers to investigate cyber-physical attacks, anomaly detection, and intrusion resilience strategies. Unlike general cybersecurity testbeds, SPHERE's CPS enclave provides a configurable, realistic environment for studying adversarial scenarios that bridge cyber and physical domains. The infrastructure offers controlled, reproducible experiments with customizable network topologies and hardware-in-the-loop validation. This poster presents the design philosophy, community-driven experimental goals, and deployment considerations of the SPHERE CPS enclave, demonstrating its potential for advancing CPS security research.

CCS Concepts

• **Computer systems organization → Sensors and actuators**; **Embedded and cyber-physical systems**; • **Security and privacy** → *Domain-specific security and privacy architectures*; • **General and reference → Experimentation**; *Evaluation*;

Keywords

Cybersecurity & privacy, research, reproducible, experimentation

ACM Reference Format:
Luis Garcia (University of Utah), Jelena Mirkovic (USC-ISI), David Balenson (USC-ISI), Erik Kline (USC-ISI), Yuri Pradkin (USC-ISI), David Choffnes (Northeastern University), Daniel Dubois (Northeastern University), Terry Benzel (USC-ISI), Srivatsan Ravi (USC-ISI), Joseph Barnes (USC-ISI), Geoff Lawler (USC-ISI), Chris Tran (USC-ISI), Alba Regalado (USC-ISI). 2025. Poster Abstract: SPHERE CPS Enclave: A Reconfigurable Testbed for Industrial Control System Security Experimentation. In *ACM/IEEE 16th International Conference on Cyber-Physical Systems (with CPS-IoT Week 2025) (ICCPS '25), May 6–9, 2025, Irvine, CA, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3716550.3725158

ICCPS '25, Irvine, CA, USA
© 2025 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-1498-6/2025/05
https://doi.org/10.1145/3716550.3725158

1 Introduction

Cybersecurity and privacy threats increasingly impact our daily lives, our national infrastructures, and our industry. Recent newsworthy attacks targeted nationally important infrastructure, our government, our nuclear facilities, our researchers, and research facilities. The landscape of what needs to be protected and from what threats is continuously evolving: new technologies are released and the threat actors improve their own capabilities through experience and close collaboration. Meanwhile, defenders often work in isolation, using private data and facilities, and producing defenses that are quickly outpaced by new threats. To transform cybersecurity and privacy research into a highly integrated, community-wide effort, researchers need a common, rich, representative research infrastructure that meets the needs across all members of the research community, and facilitates reproducible science.

To meet researcher needs, USC Information Sciences Institute and Northeastern University have been funded by the NSF midscale research infrastructure program to build Security and Privacy Heterogeneous Environment for Reproducible Experimentation (SPHERE). This research infrastructure will offer access to an unprecedented variety of hardware, software, and other resources, all relevant to cybersecurity and privacy research, connected by user-configurable network substrate, and protected by a set of security policies uniquely aligned with cybersecurity and privacy research needs. SPHERE will offer six user portals, closely aligned with needs of different user groups, facilitating widespread adoption. It will provide built-in support for reproducibility, via easy experiment packaging, sharing, and reuse. SPHERE will build a process, a standard, and incentives for community-wide efforts to develop representative experimentation environments for cybersecurity and privacy research, and to continuously contribute high-quality research artifacts. You can learn more about SPHERE by visiting https://sphere-project.net.

Community Need. The increasing interdependence of cyber and physical systems heightens the risks posed by cyber threats. The Covid-19 pandemic accelerated digital transformations across sectors, further increasing reliance on secure computing and networking infrastructures. High-profile cyberattacks, such as the SolarWinds supply-chain breach [4] and the Colonial Pipeline ransomware attack [7], underscore the urgent need for resilient security solutions. Reports indicate ransomware attacks have tripled [5], DDoS incidents have doubled [2], and data breaches have surged by 70% [6], demonstrating the evolving threat landscape. Recognizing these challenges, USC Information Sciences Institute hosted two workshops in 2022—*Cybersecurity Artifacts Workshop* [1] and *CEF 2022 Workshop* [3]—to assess community needs. Researchers consistently emphasize the necessity of a shared, representative research infrastructure to support reproducible experimentation and interdisciplinary collaboration. SPHERE directly addresses this gap by providing a scalable testbed with diverse computing, networking, and ICS resources. The USC Information Sciences Institute has ran two workshops in 2022 to learn about community need around cyber security and privacy research: the *Cybersecurity Artifacts Workshop* [1] and the *CEF 2022 workshop* [3]. Researchers need **common, rich, representative research infrastructure, which meets the needs across all members of the community, and facilitates reproducible science** to move from *piecemeal, opportunistic research* to *pursuing integrated, sophisticated, community-encompassing research*. We also need a well-educated workforce that is knowledgeable about cyber threats, and that has mastery over practical skills to prevent, detect and recover from cyber attacks.

2 SPHERE Testbed

SPHERE is a transformative research infrastructure designed to advance cybersecurity experimentation through a diverse and reconfigurable set of test environments. The testbed includes the following experimental enclaves: **General Compute Enclaves**: 192 high-performance servers supporting application, system, and network security research; **Machine Learning Enclaves**: 10 GPU-equipped servers for security-focused AI and ML experimentation; **Cyber-Physical Enclaves**: Industrial control systems (ICS), including PLCs and I/O modules, supporting critical infrastructure security research; **Embedded Compute Enclaves**: 912 edge computing platforms for IoT security, federated learning, and trusted execution environments; **IoT Enclaves**: 500+ smart devices, including home automation, medical, and industrial sensors, enabling privacy and security research in interconnected environments; **Programmable Network Enclaves**: Software-defined networking (SDN) components, including Tofino switches and NetFPGA boards, for investigating dynamic network security solutions. SPHERE also incorporates a dedicated, user-configurable network substrate to support complex, real-world cybersecurity experimentation. By integrating cutting-edge hardware, virtualization capabilities, and industrial automation systems, SPHERE offers a unique environment for studying cyber-physical attack vectors, defense mechanisms, and resilience strategies.

2.1 CPS Experimental Capabilities

SPHERE enables controlled, high-fidelity experiments addressing critical cybersecurity and privacy challenges, including: 1) Simulating cyberattacks on industrial automation and critical infrastructure; 2) Evaluating anomaly detection, intrusion prevention, and automated response mechanisms; 3) Investigating security vulnerabilities in control protocols and IoT deployments; 4) Developing secure-by-design methodologies and resilient architectures; and 5) Exploring digital twin integration for predictive security analysis.

SPHERE supports both on-site and remote experimentation, providing researchers with extensive logging, experiment reproducibility tools, and access to collaborative cybersecurity initiatives. Future expansions will incorporate additional industry use cases and emerging cyber-physical threat models.

Experiments further may include generation of harmful traffic, taking live measurements from the real Internet, running human user studies, and even interacting with malicious Internet actors. To support these different research needs, and protect the Internet, SPHERE will provide safe network security policies.

Services and Community Building. All SPHERE enclaves will be accessible via a single user interface. To meet the needs of various classes of users, SPHERE will provide six user portals: MAN (manual) - for exploratory research, JUP (Jupyter) – for mature research, GUI – for novice users, EDU – for use in education, AEC – for artifact evaluation committees, and HUM – for human user studies. Users will be able to access all portals from the user interface, and obtain a consistent view of their experiments, while being able to switch between portals as their needs evolve.

SPHERE hopes to serve not just as environment for experimentation but also for sharing and reuse of high-quality research artifacts, to promote integrated research in cybersecurity and privacy. SPHERE will facilitate reproducible science by building a streamlined process, standards, and incentives for the community to develop representative (realistic) experimentation environments and offering built-in infrastructure supports and community engagement process for artifact sharing and reuse. The SPHERE team will first engage with research and education communities to learn about their experimentation needs and about needs around artifact sharing and reuse. SPHERE will further build infrastructure services that include extensive logging of user actions and support for various approaches to capture experiment topology, setup and workflow. In addition to these technological advances, SPHERE team will engage with artifact evaluation committees at conferences and journals to support artifact evaluation and hosting on SPHERE. Additionally, SPHERE will issue an open call for mature research artifacts to be deployed on SPHERE as representative experimentation environments.

References

[1] David Balenson, Jelena Mirkovic, Eric Eide, Laura Tinnel, Terry Benzel, David Emmerich, and David Johnson. 2022. Cybersecurity Artifacts Workshop – Report. https://bit.ly/CyberArtifactsWkshp2022.

[2] Government Technology. [n. d.]. Hacktivism and DDOS Attacks Rise Dramatically in 2022. https://www.govtech.com/blogs/lohrmann-on-cybersecurity/hacktivism-and-ddos-attacks-rise-dramatically-in-2022.

[3] Jelena Mirkovic, David Balenson, Srivatsan Ravi, Luis Garcia, and Terry Benzel. 2022. Cybersecurity Experimentation Workshop – 2022 – Report. https://bit.ly/CyberExperWkshp2022.

[4] NPR. [n. d.]. A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack. https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

[5] Statista. [n. d.]. Annual number of ransomware attacks worldwide from 2016 to first half 2022. https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/.

[6] Sumeet Wadhwani, Spiceworks. 2022. Data Breaches Soared by 70% In Q3 2022 in an Otherwise Dull Year. https://www.spiceworks.com/it-security/data-security/news/data-breach-report/.

[7] TechTarget.com. [n. d.]. Colonial Pipeline hack explained: Everything you need to know. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know.