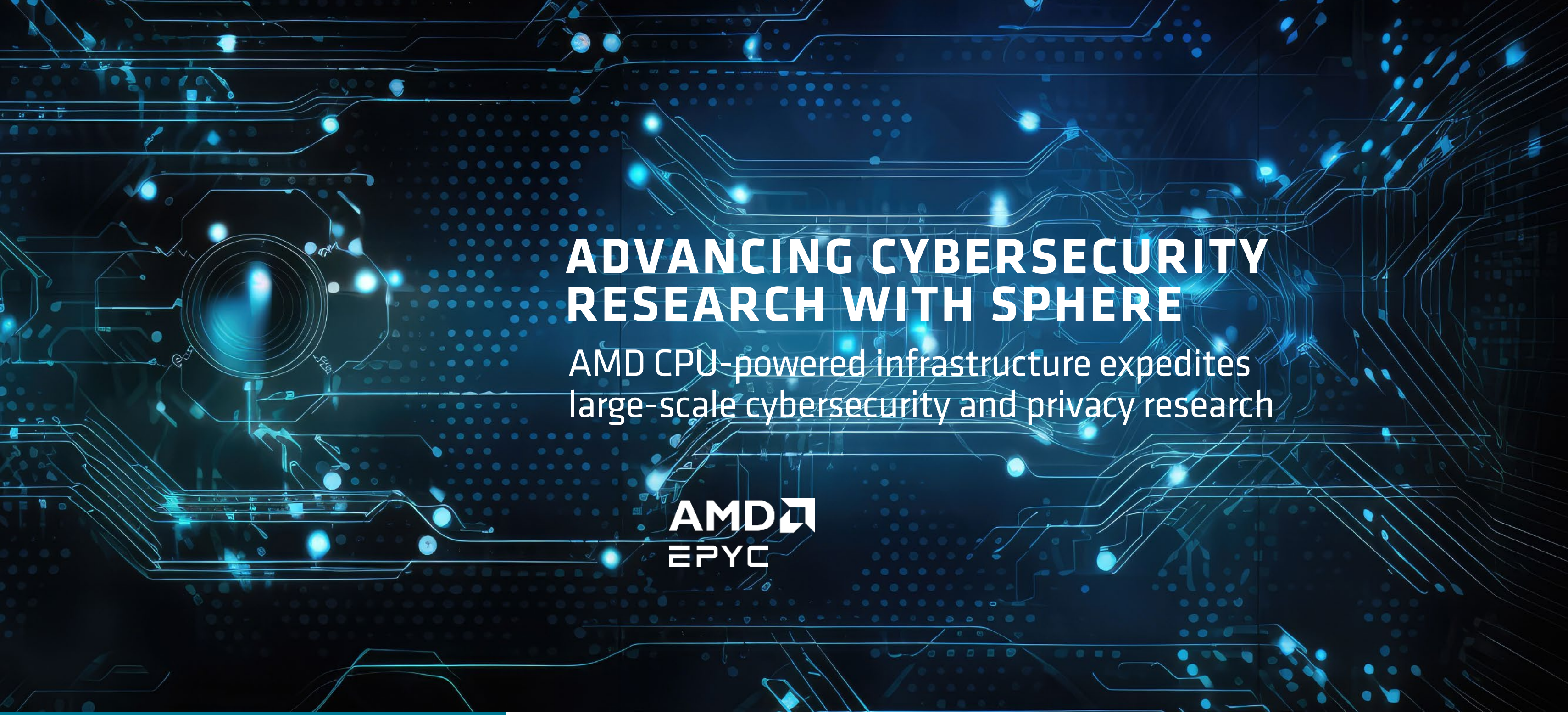

ADVANCING CYBERSECURITY RESEARCH WITH SPHERE

AMD CPU-powered infrastructure expedites large-scale cybersecurity and privacy research

AMD EPYC

CUSTOMER

USC INFORMATION SCIENCES INSTITUTE

INDUSTRY

Cybersecurity

CHALLENGES

Providing real-time access to resources, data, and companion services for researchers to study realistic threat scenarios at scale

SOLUTION

Developing an advanced research infrastructure for reproducible and deployable research products powered by AMD EPYC™ Processors

RESULTS

Delivering trusted execution environment (TEE) capabilities with robust processing power in an efficient design to emulate real-world digital environments

AMD TECHNOLOGY AT A GLANCE

AMD EPYC™ Processors

TECHNOLOGY PARTNER

Colfax International

COLFAX
Customized Solutions

In the age of digital connectivity, cybersecurity technology and research are more critical than ever.

Cyberattacks are becoming more sophisticated, driven by the availability of powerful hacking tools, the rise of well-funded nation-state hacker groups, and the proliferation of cybercrime forums as places for attackers to share information. As a result, attackers seem to be evolving faster than defenders. To compound the problem, attack vectors are becoming more widespread. A key example is seen in the emergence of supply chain attacks, where attackers introduce backdoors or other malicious components into otherwise innocuous products and services from reputable vendors.

> "Cybersecurity research is often done in isolation, and documenting every network, device, connection, wire and script used to allow other researchers to repeat the same experiment is difficult. My hope is that we will see faster progress and be able to free up more of researchers' time."
>
> Jelena Mirkovic, Principal Investigator, ISI

Digital transformation has impacted the attack surface of modern infrastructure. The impacts can be seen across industries – including a ransomware attack on a major pipeline company that limited access to gasoline, numerous ransomware attacks on hospital networks that threaten patient privacy, and Stuxnet-like attacks that target industrial control systems.

Emergent trends in cybersecurity are helping organizations combat these growing risks:

Cybersecurity research often utilizes digital twins to recreate aspects of real-world infrastructures. Virtualization technology allows deployment of high-fidelity network models in a cost-effective manner, which enables evaluation of new security technologies in realistic environments.

Artificial intelligence (AI) builds a foundation for sophisticated and autonomous security features that detect and respond to attacks in real-time. AI-based capabilities are a core focus of many security products and forward-looking research projects.

Programmable networks provide the ability to deploy increasingly complex security logic into network infrastructure. For example, technologies such as deep packet inspection offer better visibility into network operations and thus can enable quicker and more accurate attack detection. Programmable networks have lowered the performance cost associated with these technologies, increasing their uptake.

The latest compute processors now include TEE capabilities, which allow security critical code to execute in secure, isolated enclaves with encrypted memory. These capabilities offer protections from many attack vectors, and can limit lateral movement from components that are compromised.

Researchers seeking to explore these catalysts need access to novel hardware devices, datasets and tools to create attack scenarios, and scalable compute environments that can emulate real world digital environments.

Advancing cybersecurity research

The Information Sciences Institute (ISI) is part of the Viterbi School of Engineering at the University of Southern California (USC). Its mission to advance society through pioneering research and technological innovation. ISI research and development ranges from AI, networking and security, and computational systems and technology to space engineering. Bridging multiple technology disciplines through both academic and industry expertise, ISI continues to shape the technologies of tomorrow.

In collaboration with Northeastern University, ISI received funding from the National Science Foundation Mid-Scale Research Infrastructure Program to build an environment for conducting cybersecurity and privacy research. The environment was named Security and Privacy Heterogeneous Environment for Reproducible Experimentation, or SPHERE.

> "No one has ever done this before. The research conducted in the new testbed can help increase consumer awareness of the security risks of using smart devices at home."
>
> David Choffnes, Co-Principal Investigator, Cybersecurity and Privacy Institute

SPHERE will be a research infrastructure for at-scale, realistic, and reproducible experimentation across diverse hardware. The four-year construction effort began in October 2023. It is currently operating in a "beta" mode, inviting early-stage users and innovators to explore its state-of-the-art technology and incorporate it into their research.

SPHERE
RESEARCH INFRASTRUCTURE
sphere-project.net

Building a robust research infrastructure

The road to completion has considerable obstacles before SPHERE can operate at full capacity. ISI must meet the data and technology requirements of their researchers to deliver a high-performing infrastructure:

- Operating large-scale resources while maintaining a modest physical footprint
- Emulating high data rate networks
- Providing diverse hardware relevant for today's attacks and countermeasures

The ultimate goal for the SPHERE project is to provide resources, datasets, and companion services that allow researchers to easily study realistic threat scenarios at the correct scale. ISI has partnered with Colfax International and AMD to identify hardware and software solutions to meet each of these challenges. Their approach is to work with Colfax to determine SPHERE's architectural needs and constraints, then collaborate with AMD to recommend the most effective AMD technologies for the job. AMD is an obvious partner of choice for this project as a leading provider of CPU technology as well as innovative security features. The latest AMD EPYC processors offer a range of solutions that are designed to solve the problems facing the modern data center, optimizing infrastructure for the most complex virtualization tasks. 5th generation processors offer AMD Secure Encrypted Virtualization (SEV) which provides built-in security at the silicon level. AMD SEV uses one key per virtual machine to isolate guests and the hypervisor from one another. Trusted computing capabilities like this are crucial for SPHERE users performing research in confidential computing and other privacy-preserving technologies.

Empowering diverse research initiatives

Over the past two decades, ISI's DETER Project built, designed, and operated the Defense Technology Experimental Research Laboratory (DETERLab), a state-of-the-art scientific computing facility for cybersecurity researchers and educators. Researchers engaged in research, development, discovery, experimentation, and testing of innovative cybersecurity technology. Educators used DETERLab to teach security, networking, and operating systems classes. As a shared, public testbed, DETERLab has supported and benefitted research and education in cybersecurity across a vast user population including academia, industry, and government. To date, it has served a broad research community of 389 project teams from 278 institutions with 1,042 researchers from 205 locations and 46 countries. Standout projects include human behavior modeling in cybersecurity scenarios, security features against extremely large-scale distributed denial of service (DDoS) attacks, defenses against worm and botnet attacks, defenses against encrypted traffic classification, and phishing deception.

SPHERE provides a diverse resource offering to researchers through a set of six different enclaves, including:

- **General server nodes** powered by AMD EPYC processors with TEE. These machines enable research into privacy-preserving technologies and attacks as well as defenses for cloud system threats.
- **Embedded computing nodes** with single board computers resembling iPhones and tablets. These machines allow research into distributed systems threats and privacy-preserving technologies, such as federated machine learning.
- **Cyber-physical nodes** with programmable logic controllers (PLCs), which are often present in industrial control systems environments. These machines enable research into threats confronting critical infrastructure in manufacturing, energy, food/agriculture, and other industrial domains.
- **GPU nodes** with GPU accelerators. These machines enable research into the use of AI for novel attack and defense algorithms.
- **Programmable nodes** with programmable devices such as smart NICs and DPUs. These machines enable research into stateful, high-data-rate firewalls and other technologies.
- **IoT nodes** representing a typical "smart home" environment. These machines enable research into measurement and characterization of devices that often contain and transmit sensitive personal information.

Additionally, ISI has developed a testbed software platform (known as MergeTB) that operates the entire SPHERE research infrastructure by providing user, resource, and experiment management, bootstrapping virtual and physical machines, synthesizing virtual overlay networks with custom layer-2 topologies and in-network programmability, and providing flexible traffic containment policies. MergeTB makes use of hardware support for virtualization and network programmability, which ensures the infrastructure can operate efficiently.

Expediting critical cybersecurity efforts

The anticipated SPHERE research infrastructure is designed to transform the rate of progress in cybersecurity and privacy research. ISI projects that SPHERE will facilitate groundbreaking research endeavors. These include reproducible and deployable research products developed and tested in representative environments, integrated and broadly applicable research across multiple disciplines, and research on novel threats and defenses.

As the project continues to evolve, AMD technology will be a cornerstone of its success. ISI believes that AMD EPYC processors and their feature technologies will be beneficial for researchers studying cloud system threats and AI-based cybersecurity technologies and for ISI's team of infrastructure builders and operators. For researchers, AMD EPYC processors offer TEE capabilities, and for operators, AMD processors will support open source libraries and operating systems used by ISI to help greatly reduce the complexity of infrastructure operation and automation for budget-constrained projects.

WANT TO LEARN HOW AMD EPYC™ PROCESSORS MIGHT WORK FOR YOU?

Visit us online at
amd.com/en/products/processors/server/epyc

About ISI

The ISI's mission is to advance society through pioneering research and technological innovation. They cultivate an intellectually vibrant environment where diverse PhD students work side-by-side with research scientists to imagine bold solutions to complex problems and to develop into world-class leaders. Guided by integrity, inclusion, and a commitment to excellence, they create unprecedented capabilities that harness information to transform lives and develop real-world solutions. For more information visit isi.edu and sphere-project.net.

About Colfax International

Colfax helps to accelerate business and research outcomes with expertly engineered solutions. As an Elite AMD Partner, they have established a reputation for solving the most complex problems and securing outstanding results for enterprises, national labs, universities, public agencies, and start-ups. Colfax solutions are built on performance, execution, agility, and knowledge that make up our DNA to power engineers and researchers at the forefront of innovation and discovery. For more information visit colfax-intl.com.

About AMD

For more than 50 years, AMD has driven innovation in high-performance computing, graphics, and visualization technologies. Billions of people, leading Fortune 500 businesses, and cutting-edge scientific research institutions worldwide rely on AMD technology to improve how they live, work, and play. AMD is focused on building leadership high-performance and adaptive products that push the boundaries of what is possible. Learn more about how AMD is enabling today and inspiring tomorrow. For more information visit amd.com.