Call for Papers

Important dates

Paper submission deadline:
June 3, 2024 AoE
Authors' notification:
July 3, 2024 AoE
Camera-ready submission:
July 14, 2024 AoE
Early registration deadline:
July 20, 2024 AoE
Workshop dates:
September 2–4, 2024

Workshop chairs

Neetesh Saxena (UK)
Prosanta Gope (UK)
Sridhar Adepu (UK)

Technical program committee

Chuadhry Mujeeb Ahmed (UK)
Ali Ismail Awad (AE)
John Henry Castellanos (DE)
Z. Berkay Celik (US)
Luis Garcia (US)
Joe Gardiner (UK)
Rajvir Kaur (IN)
Charalambos Konstantinou (SA)
Ajit Kumar (KR)
Pradeep Kumar (UK)
Daisuke Mashima (SG)
Aryan Pasikhani (UK)
Gauthama Raman (SG)
Sangram Ray (IN)
Giedre Sabaliauskaite (UK)
Vishal Sharma (UK)
Mayank Swarnkar (IN)
Nikhil Tripathi (IN)
Sarad Venugopalan (UK)
Rohit Verma (IE)

Publicity chairs

Subhash Lakshminarayana (UK)
Siraj Ahmed Shaikh (UK)

Contact us

saxenan4@cardiff.ac.uk
p.gope@sheffield.ac.uk
sridhar.adepu@bristol.ac.uk

Asset discovery in IT and network systems is carried out with substantial tools to provide more accurate and specific information about digital assets. However, with the emergence of cyber-physical systems (CPSs), traditional techniques are not practically useful in providing answers to the key questions about the cyber and physical assets present in the systems. Examples of such systems are electric vehicles (EVs) infrastructure, autonomous vehicles (AVs)/connected AVs (CAVs), unmanned aerial vehicles (UAVs), smart grids, and smart manufacturing. Asset discovery in operational technology (OT) and understanding the criticality of its assets are not yet explored enough. These assets could be specific devices such as PLCs, HMI, RTUs, etc., or IoT and Industrial IoT devices, including sensors, actuators, and other related components. Security of such critical assets is crucial in strengthening the security of the CPSs. Similarly, such assets are having privacy concerns and issues considering big data collection and processing at different devices (edge/cloud/fog). Most importantly, improving and ensuring the resilience of such assets by understanding the impact of cyber-attacks on physical assets will greatly enhance the systems' cyber resilience. The accelerating adoption of new technologies brings challenges primarily associated with the cyber security and safety of the applications, where confidentiality, integrity, and data availability are crucial. Further, AI techniques can be embraced to improve state-of-the-art understanding of asset criticality and safeguard solutions against cyber attempts on physical and digital assets of CPSs. This workshop aims to explore and develop new research ideas from the wider CPS context focusing on security, privacy and resilience of critical assets.

The workshop is held in conjunction with the IEEE CSR 2024 conference as a **hybrid event**, during September 2–4, 2024. Prospective authors are encouraged to submit previously unpublished contributions from a broad range of topics, which include but are not limited to the following:

- Security, privacy and resilience analysis on IoT/IIoT/IoE assets
- Risk management and governance for critical asset applications
- Security, privacy and resilience of physical assets in cyber-physical systems
- AI-assisted critical infrastructure security for critical assets
- Detection, prevention, response, and recovery against potential threats to critical assets
- Automated threat modelling for critical assets
- Situational awareness and traceability for critical assets
- Applied crypto for securing critical assets
- Blockchain for trustworthy critical asset applications
- Privacy-preserving techniques for critical assets
- Cyber threat intelligence for critical assets
- Device specific asset criticality (e.g., RTUs, PLCs, etc.)
- Cyber-attacks' impact on critical assets

The CSR SPARC workshop will accept high-quality research papers presenting strong theoretical contributions, applied research and innovation results obtained from funded cyber-security and resilience projects, and industrial papers that promote contributions on technology development and contemporary implementations.

Submitted manuscripts should not exceed 6 pages (plus 2 extra pages, being subject to overlength page charges) and should be of sufficient detail to be evaluated by expert reviewers in the field. Accepted papers will be submitted for inclusion into IEEE Xplore subject to meeting IEEE Xplore's scope and quality requirements. Detailed information about paper submission and guidelines for authors can be found at the workshop's website https://www.ieee-csr.org/sparc.

IEEE
IEEE SMC Systems, Man, and Cybernetics Society
SMC Homeland Security Technical Committee
LOGOS RI RESEARCH&INNOVATION