WORKSHOP

1st international workshop on Safeguarding CybersEcurity iN hEalthcare (SCENE 2023)

Call for papers

The healthcare sector is facing an increasing number of cyber threats, as the digitization of healthcare and the use of connected medical devices continue to grow. These threats can come from a variety of sources, including malicious hackers, nation-state actors, and even insiders. Cybersecurity incidents in healthcare can have serious consequences, including the loss or theft of sensitive patient data, disruption of vital services, and damage to an organization's reputation. Safeguarding CybersEcurity iN hEalthcare aims to bring together viewpoints from diverse areas to explore the commonalities of cybersecurity issues and solutions in the healthcare sector. The workshop is supported by the EU-funded projects AI4HealthSec (https://www.ai4healthsec.eu/), HEIR (https://heir2020.eu/), ASCAPE https://www.ascape-project.eu/, and SMART-BEAR (https://www.smart-bear.eu/). We welcome submissions on a wide range of topics, including but not limited to:

- Best practices for data protection in healthcare: GDPR compliance, HIPAA compliance, encryption, and access controls
- The role of artificial intelligence and machine learning in healthcare cybersecurity
- Legal and ethical considerations in healthcare cybersecurity: patient privacy, consent, and data governance
- Emerging threats and trends in healthcare cybersecurity: IoT, 5G, and cloud computing
- Strategies for promoting a culture of cybersecurity in healthcare organizations
- Best practices for training and educating healthcare professionals on cybersecurity
- Responding to and recovering from cyber incidents: developing a cybersecurity incident response plan for healthcare organisations
- Designing and proposing treatment strategies and measures as a result of risk assessment activities

SUBMISSION GUIDELINES

Submissions of original unpublished papers are solicited. Papers will be reviewed on novelty, significance and contribution to the body of knowledge, correctness, and clarity. We expect all papers to provide adequate detail to enable reproducibility of their experimental results. They should be in pdf IEEE 2-column conference style, limited to five (5) pages. The DRCN 2023 conference is technically Co-Sponsored by the IEEE Communications Society. All accepted and presented papers will be included in the DRCN 2023 proceedings and will be subsequently submitted to IEEE Xplore for publication. At least one author is required to register, at the full rate, to present accepted papers at the conference and for the paper to appear in the conference proceedings and in IEEE Xplore. Authors must submit their papers electronically through EDAS using the link: https://edas.info/newPaper.php?c=30643

IMPORTANT DATES

- Papers submission deadline: March 6, 2023
- Acceptance/rejection notification: March 13, 2023

- Final papers due: March 20, 2023

WORKSHOP ORGANIZERS:

- Mario Ciampi (Institute for High Performance Computing and Networking National Research Council of Italy (ICAR-CNR), mario.ciampi@icar.cnr.it)
- Herve Debar (Télécom SudParis, herve.debar@telecom-sudparis.eu)
- Michail Smyrlis (SPHYNX Technology Solutions AG, smyrlis@sphynx.ch)