5th International Paper/Poster Competition in Cybersecurity Sponsored by SICSA

Edinburgh, UK, June 22, 2022
Event website: https://attend.ieee.org/dsc-2022/sicsa-event/

Outline

In parallel with IEEE DSC 2022, we are running the 5th International Paper/Poster Competition in Cybersecurity sponsored by SICSA. In a recent report by International Information System Security Certification Consortium (ISC)² in October 2021, the world's largest non-profit association of certified cybersecurity professionals, it is estimated that there will be a global shortage of 2.72 million cybersecurity professionals, so cybersecurity career opportunities are certainly available. On the other hand, females are hugely under-represented at all levels within cybersecurity, both in industry and academia. The lack of women in cybersecurity is something that the UK government, industries, and universities are keen to address. Therefore, this event aims to inspire more people, particularly more women, into cybersecurity roles by bringing together cyber researchers from across the UK and worldwide in the form of a paper/poster competition. Having this competition held in parallel with IEEE DSC 2022, not only connects males and females in cybersecurity to leading experts but also provides for greater collaboration. Please note that any gender from any university can enter the competitions for best papers and best posters, competing for first place, second place, and third place. However, only females are allowed to enter the Outstanding Woman in Cyber (paper & poster) categories.

The event is for competitors from any university in the UK and worldwide. All entrants must use the submission link provided. Additionally, 10 free places are reserved for competitors from Scottish Universities, this includes the cost of registration, attendance, and publication. If you are eligible for one of these free places (i.e., you are a competitor from a Scottish University) you must also apply for this opportunity by contacting (n.moradpoor@napier.ac.uk).

The event will select a total of x8 winners (x4 winners for the best papers and x4 winners for the best posters) as follows:

Prizes for x4 winners (total: £230), best posters:

- First place: X1 £100 Amazon voucher; X1 Certificate from the event
- Second place: X1 £50 Amazon voucher; X1 Certificate from the event
- Third place: X1 £30 Amazon voucher; X1 Certificate from the event
- Outstanding woman in cyber (poster category): X1 £50 Amazon voucher; X1 Certificate from the event

Prizes for x4 winners (total: £230), best papers:

- First place: X1 £100 Amazon voucher; X1 Certificate from the event
- Second place: X1 £50 Amazon voucher; X1 Certificate from the event
- Third place: X1 £30 Amazon voucher; X1 Certificate from the event
- Outstanding woman in cyber (paper category): X1 £50 Amazon voucher; X1 Certificate from the event

Call for papers/posters

Topics of interest include, but are not limited to:

- Advanced Persistent Threat (APT)
- Big Data Analysis- Botnet and Intrusion Detection
- Cryptographic Methods and Toolkits
- Cyberattacks

- Data/Information Reliability
- Database Security and Privacy
- Embedded Systems and IoT Devices
- Experimentation, Measurement, and Assessment
- Mobile and Cloud Computing
- Software vulnerabilities
- Malware analysis- SDN and NFV
- Security and Privacy for AI
- Hardware security and reliability
- CAD Algorithms and Tools
- Electronic Circuits and Systems
- Fault-Tolerant Architectures and Designs
- Industrial Design Experiences
- Noise-Aware Designs
- Power-Aware Designs
- Soft-Error Analysis and Models
- Stochastic Circuits and Systems
- Temperature-Aware Designs
- Variable-Latency Designs
- Security Circuits, Designs, and Detection
- Attacks on Information Systems and/or Digital Information Storage
- CSIRTs, Incident Analysis, and Response
- Honeypots/Honeynets- Malware Analysis and Reversing
- Mobile Communications Security and Vulnerabilities
- Newly discovered vulnerabilities in software and hardware
- Offensive (and Counter-Offensive) Information Technology
- Reverse Engineering, Forensics, and Anti-Forensics
- Spyware, Phishing and Distributed Attacks
- VLSI/CAD Design Knowhow
- Data Security and Privacy

Important dates

Please consult the event website (https://attend.ieee.org/dsc-2022/sicsa-event/) for the most up-to-date info on the following:

- Paper Submission by: **27 March 2022**
- Author Notification: **26 April 2022**
- Camera Ready Submission: **6 May 2022**
- Event date: **22 June 2022**

Submission Instructions

The following two types of papers are welcome:

- Paper – scientific research papers, surveying works and industrial experiences describing significant advances. Papers should be no longer than 6 pages, inclusive of figures, tables, references and appendix using IEEE Conference Proceedings Manuscripts style (two-columns, single-spaced, 10 fonts).

- Poster – early results or work in progress with initial findings. Papers should be maximum 4 pages long, inclusive of figures, tables, references and appendix using IEEE Conference Proceedings Manuscripts style (two-columns, single-spaced, 10 fonts).

Papers must be written in English and should not exceed 6 pages for paper category and 4 pages for poster category, inclusive of figures, tables, references and appendix using IEEE Conference Proceedings Manuscripts style (two-columns, single-spaced, 10 fonts). The materials presented in the papers should not be published or under submission/review elsewhere. All submitted papers will be peer-reviewed. Accepted papers will appear in the IEEE DSC 2022 conference proceedings and will be eligible for submission to the IEEE Xplore Digital Library. At least one of the authors of any accepted paper is requested to register the paper at the conference.

Paper templates can be downloaded from IEEE website.

Electronic submission site: **https://easychair.org/conferences/submission_new?a=27933494**

Organisers

- Dr. Naghmeh Moradpoor; Edinburgh Napier University (Lead)
- Dr. Pooneh Bagheri Zadeh; Leeds Beckett University
- Dr. Kia Dashtipour; Edinburgh Napier University