The 2022 IEEE Conference on Dependable and Secure Computing (IEEE DSC 2022)

Edinburgh, UK | 22 – 24 June 2022

https://attend.ieee.org/dsc-2022/

The IEEE Conference on Dependable and Secure Computing solicits papers, posters, practices, and experiences for presenting innovative research results, problem solutions, and new challenges in the field of dependable and secure computing. The whole spectrum of IT systems and application areas, including hardware design and software systems, with stringent relevant to dependability and security concerns are of interest to DSC. Authors are invited to submit original works on research and practice of creating, validating, deploying, and maintaining dependable and secure systems.

The scope of DSC includes, but is not limited to, the following topics.

Main Track: Computer Systems, Networks, and Software/Hardware

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

Experience and Practice Track

The DSC conference will also include a submission category for experience and practice papers on new findings in the aforementioned topics. The PC will evaluate a submission to the experience and practice track with the understanding that it predominantly contributes to design knowhow or the extension of the community's knowledge about how the security protection of known techniques fares in real-world operations. Authors have to submit a 2-page paper along with a supplemental 3-min video to demonstrate the implementation and/or the practicability of the work. Topics of interest include, but are not limited to:

- 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

Submission Instructions

Papers should be no more than 8 pages for regular papers and 2 pages for experience and practice papers. Papers must be written in English conforming to the IEEE standard conference format (US letter, two-column). All submitted papers will be peer-reviewed. Accepted papers will appear in the conference proceedings and will be eligible for submission to the IEEE Xplore Digital Library. Paper templates can be downloaded from IEEE website, i.e. https://www.ieee.org/conferences/publishing/templates.html.

Electronic submission site: https://easychair.org/conferences/?conf=ieeedsc2022

Important Dates

- Paper submission: 31 December 2021
- Author notification: 31 March 2022
- Camera ready: 30 April 2022
- Conference Date: 22 – 24 June 2022

Sponsors

IEEE
IEEE Reliability Society
bcs The Chartered Institute for IT
sicsa The Scottish Informatics & Computer Science Alliance
University of Exeter