IEEE International Workshop on Cyber Forensics in Software Engineering (CFSE 2020)

In conjunction with the 20th IEEE International Conference on Software Quality, Reliability, and Security
Macau, China, Decmeber 11-14,2020
https://qrs20.techconf.org

Description

Cyber forensics has been an emerging research area for IT-related professionals, practitioners, and researchers for the last decade. As we continue the research on how to collect and analyze digital evidence in an existing software/hardware environment, we are also interested in and challenged by the questions of the "built-in" issues in how to design and create software/hardware applications with forensic awareness so that a cooperative environment for the purpose of cyber forensics is provided.

The theme of the workshop is to advance research on data-driven and legal-proceedings-enforced cyber physical systems in an innovative way. We believe that to build forensics components into software/hardware applications will help us more efficiently in collecting/identifying evidence of illegal and unethical activities, more effectively in preventing/detecting cyber attacks on critical infrastructures, more confidently in preserving anonymity and protecting privacy. In addition to the research on the "after the fact" issues in collection, examination, and analysis of digital evidence, it is also critical to involve cyper forensic readiness in the early stage of software/hardware application development, especially for a data-rich and cyber-physical system with pervasive IoT devices. As the principles of the software engineering suggest, the effort to build forensics "by design" will make digital ecosystems more supportive and cost-effective in a later forensic search and investigation. It is believed that the effort made by this workshop will help driving intelligent transformation of the cyber world.

Topics

The list of topics includes, but is not limited to:

Augmented and Virtual Reality Forensics
Blockchain Technology in Cyber Forensics and Cybersecurity
Cloud Forensics / Fog Forensics
Cyber Defense/Offense/Operation
Cyber Physical Systems (CPS) Forensics
Cyber Security and Digital Forensics
Curriculum Development in Digital Forensics and Cyber Security
Data-Driven Cybersecurity and Incident Response
Data-Driven Digital Forensics and Investigation
Digital/Computer Forensics in Digital Ecosystems
Electronic Discovery and Fraud Detection/Investigation
Forensic Readiness in Software Engineering / Forensics by Design

Forensic Testing / Cyber Crime Simulation
Game / Virtual World Forensics
Image Forensics / Information Hiding Technology
IoT (Internet of Things) Forensics and Security
Legal, Ethical, and Privacy Issues in Computing
Malware and Intrusion Detection and Penetration Testing
Quantum Computing Forensics/Next Generation Forensics
Risk Analysis in Security, Safety, Privacy, and Forensics Applications
SCADA / Critical Infrastructures Forensics
Social Networking Forensics and Security
Software Application Forensics (Medical, Financial, and Governmental)
Software Forensics and Profiling
System Software Forensics and Security
Ubiquitous/Mobile/iPhone Forensic Computing and Cyber Security
Visualization of Computer/Digital Forensics

Paper submission:
Authors are invited to submit original unpublished research papers as well as industrial practice papers. Simultaneous submissions to other conferences are not permitted. Detailed instructions for electronic paper submission, panel proposals, and review process can be found at https://qrs20.techconf.org/submission.

The length of a camera ready paper will be limited to eight pages, including the title of the paper, the name and affiliation of each author, a 150-word abstract, and up to 6 keywords. Shorter version papers (up to four pages) are also allowed.

Authors must follow the IEEE Computer Society Press Proceedings Author Guidelines to prepare their papers. At least one of the authors of each accepted paper is required to pay full registration fee and present the paper at the workshop. Arrangements are being made to publish selected accepted papers in reputable journals. Submissions must be in PDF format and uploaded to the conference submission site.

Program Chairs

Ryoichi Sasaki
Tokyo Denki University, Tokyo, Japan
r.sasaki@mail.dendai.ac.jp

Tetsutaro Uehara
Ritsumeikan University, Kyoto, Japan
uehara@cs.ritsumei.ac.jp

Jigang Liu
Metropolitan State University, St. Paul, MN, USA
jigang.liu@metrostate.edu

Program Committee:

Yuki Ashino, NEC, Japan
Francis Avorgbedor, Metropolitan State University, USA
Vinod Bhattathiripad, G J Software Forensics, India
Farris Hassan, Minnesota IT Services, USA
Satoshi Kai, Hitachi Ltd., Japan
Anyi Liu, Oakland University, USA
Dan Lo, Kennesaw State University, USA
Masakatsu Nishigaki, Shizuoka University, Japan
Mathew Nyamagwa, Metropolitan State University, USA
Songpon Teerakanok, Ritsumeikan University, Japan
Sean Thorpe, University of Technology, Jamaica
Michael Tu, Purdue University Calumet, USA
Ben Turnbull, Defense Science and Technology, Australia
Shiuh-Jeng Wang, Central Police University, Taiwan
S. M. Yiu, the University of Hong Kong, China
Hiroshi Yoshiura, The University of Electro-Comm., Japan
Yanjun Zuo, University of North Dakota, USA