https://cans2020.at/

CANS 2020 – Call for Papers

The 19th International Conference on Cryptology and Network Security

December 14 – 16, 2020, Vienna, Austria

CANS 2020
19TH INTERNATIONAL CONFERENCE ON CRYPTOLOGY
AND NETWORK SECURITY
December 14-16, 2020, Vienna, Austria

The annual International Conference on Cryptology and Network Security (CANS) focuses on current advances in all aspects of cryptology, data protection, and network and computer security. The proceedings will be published in the Lecture Notes in Computer Science series by Springer.

CANS 2020 is held in cooperation with the International Association of Cryptologic Research (IACR).

Submission guidelines

High quality papers on unpublished research and implementation experiences are solicited for submission. All papers must be original and not substantially duplicate work that has been published at or is simultaneously submitted to a journal or another conference/workshop with proceedings. All submissions must be written in English, at most 20 pages in Springer's Lecture Notes in Computer Science (LNCS) format, including title, abstract, and bibliography. The introduction should summarise the contributions of the paper at the level understandable for a non-expert reader. The introduction should also explain the relation to related work. At most 4 pages of supplemental material may be provided as well-marked appendices, however, the paper should be intelligible without this material. Submissions must be anonymous (no author names, affiliations, acknowledgments, or obvious references).

The conference will also consider short papers, that is, submissions of up to 8 pages (in the LNCS format), for results that are not yet fully fleshed out or that simply require few pages to describe but still make a significant contribution. All submissions must be processed with LaTeX2e according to the instructions given by Springer. Submitted manuscripts must be typeset in plain Springer LNCS format, in particular without changing the font size, margins or line spacing. Submissions not meeting these guidelines may be rejected without consideration of their merits.

Papers must be submitted electronically in PDF format via Easychair using the following link:

https://easychair.org/conferences/?conf=cans2020

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

Presentation and publication

At least one author of every accepted paper must register to the conference by the early registration deadline indicated by the organizers. Papers without a registered author will be removed from the proceedings. Authors have to present their own paper(s). Proceedings including all accepted papers will be published in LNCS and will be available at the conference.

Dates

Paper submission: June 21, 2020
Author notification: August 30, 2020
Camera-ready version: September 19, 2020
Conference: December 14-16, 2020

Conference Chairs

Program Chairs	Haya Shulman (Fraunhofer SIT, Germany) Serge Vaudenay (EPFL, Switzerland)
General Chair	Stephan Krenn (AIT Austrian Institute of Technology, Austria)
Publicity Chairs	Michael Mürling (AIT Austrian Institute of Technology, Austria) Krzysztof Pietrzak (IST Austria, Austria)

Topics of interest include, but are not limited to:

Access Control
Anonymity & Pseudonymity
Applied Cryptography
Attacks & Malicious Code
Authentication, Identification
Biometrics
Block & Stream Ciphers
Blockchain Security and Privacy
Cryptographic Algorithms and Primitives
Cryptographic Protocols
Cyberphysical Security
Data and Application Security
Data and Computation Integrity
Data Protection
Denial of Service Protection
Embedded System Security
Formal Methods for Security
Hash Functions
Identity Management
Key Management
Language-Based Security
Malware Analysis and Detection
Network Security
Security and Privacy for Big Data
Security and Privacy in the Cloud
Security in Content Delivery
Security in Crowdsourcing
Security in zGrid Computing
Security in the Internet of Things
Security in Location Services
Security in Pervasive Systems
Security in Social Networks
Sensor Network Security
Trust Management
Usable Security
Virtual Private Networks
Wireless and Mobile Security
Peer-to-Peer Security & Privacy
Privacy-Enhancing Technologies
Public Key Cryptography
Secure Distributed Computing
Security Architectures
Security Metrics
Security Models
Security Policies

For any questions, please contact cans2020@ait.ac.at.