IWSEC 2021 The 16th International Workshop on Security

September 8 (Wed) – September 10 (Fri), 2021
Online (Virtual Conference)

Web: https://www.iwsec.org/2021/
Mail: iwsec2021-inquiry@iwsec.org

Call for Papers

Original papers on the research and development of various security topics, as well as case studies and implementation experiences, are solicited for submission to IWSEC 2021. Topics of interest for IWSEC 2021 include all theory and practice of cryptography, information security, and network security, as in the previous IWSEC workshops. We classify the topics of interest into two tracks as follows, but not limited to:

A: Cryptography track

- Applied cryptography
- Biometrics security and privacy
- Blockchain and cryptocurrency
- Cryptanalysis
- Cryptographic primitives
- Cryptographic protocols
- Financial cryptography
- Formal methods for security analysis
- Multiparty computation
- Post-quantum cryptography
- Privacy-preserving data mining
- Public-key cryptography
- Real-world cryptographic systems
- Symmetric-key cryptography

B: Cybersecurity and privacy track

- Cyberattacks and defenses
- Cyber physical systems security
- Forensics
- Hardware security
- Internet-of-Things security
- Intrusion detection and prevention
- Law and ethic cybersecurity
- Machine learning security
- Malware analysis
- Measurements for cybersecurity
- Mobile and web security
- Network, system and cloud security
- Privacy-enhancing technologies
- Program analysis
- Usable security and privacy

Important Dates (Tentative)

Submission deadline	March 29, 2021
Notification of decision	May 28, 2021
Camera-ready version due	June 16, 2021

(Please check the IWSEC 2021 web page for details and the latest information)

Best Paper Award

Prizes will be awarded to the authors of the Best Paper(s) and the Best Student Paper(s). Program Committees will select awards sometime after the paper notification and before the conference.

To be eligible for Best Student Paper Award, the main author should be a full-time graduate or undergraduate student as of March 2021. To enter as a candidate, please tick the appropriate box in the online submission form. Candidates must submit a copy of their student ID with facial photo to the Program Chairs (after the paper notification).

Journal Recommendation

It is planned that Program Co-Chairs will recommend the authors of best papers to submit their full versions to either of “IEICE Trans. on Fundamentals, Special Section on Cryptography and Information Security” or “Journal of Information Processing, CSEC Special Issue” after consultation between Program Co-Chairs and the authors.

Proceedings

The conference proceedings will be published by Springer, in the Lecture Notes in Computer Science (LNCS) Series. All of the past IWSEC proceedings have been published in LNCS.

Instructions for authors

All submitted papers must be original, unpublished, and not submitted in parallel to any other peer-reviewed conferences or journals. Submitted papers must be written in English and be fully anonymous with no author names, affiliations, acknowledgements, or obvious references.

Authors should consult Springer's authors' guidelines and use their proceedings templates, either for LaTeX or for Word, for the preparation of their papers. Springer encourages authors to include their ORCIDs in their papers. In addition, the corresponding author of each paper, acting on behalf of all of the authors of that paper, must complete and sign a Consent-to-Publish form. The corresponding author signing the copyright form should match the corresponding author marked on the paper. Once the files have been sent to Springer, changes relating to the authorship of the papers cannot be made.

Submitted papers may contain at most 16 pages excluding appendices and references, and at most 20 pages including appendices and references. The Abstract input to EasyChair should be less than 500 words. Note that according to the latest LNCS guideline, appendices are required to be placed before the references. Figures and tables with color can be included in papers. However, these materials will appear in black and white in the conference proceedings.

Optionally, any amount of clearly marked supplementary materials may be supplied, following after the main body of the submitted paper; however, reviewers are not required to read or review them, and submissions should be intelligible without them. Supplementary materials are mostly intended for additional data such as experimental data or source code. Note that supplementary materials are not allowed to be included in the camera-ready version.

Submissions are to be made via the submission website. Only PDF files will be accepted. Please choose track (A or B) when submitting. Submissions not meeting these guidelines may be rejected without consideration of their merit. Also, for more appropriate reviews, your paper may be reviewed on the other track than the track selected. For each accepted paper, at least one of the authors must register for the workshop before the due date of the camera-ready version and is also required to present the paper at the workshop. The title and the list of authors of the final version cannot be changed from the submitted version unless otherwise approved by the program co-chairs. Note that some papers may be accepted as short papers, merged papers, or conditionally accepted for shepherding.

Committees

General Co-Chairs:
Tetsuya Izu (Fujitsu Laboratories Ltd., Japan)
Yuji Suga (Internet Initiative Japan Inc., Japan)
Program Co-Chairs:
Toru Nakanishi (Hiroshima University, Japan)
Ryo Nojima (National Institute of Information and Communications Technology, Japan)

(Last update: Feb. 16, 2021)