

CALL FOR PAPERS

The 27th World Conference on Information Security Applications

WISA 2026

August 26-28, 2026 / MAISON GLAD, Jeju Island, Korea



Korea Institute of Information
Security & Cryptology



General Chair: Howon Kim (Pusan University)

Program Committee Co-Chairs: Jongsung Kim (Kookmin University), Haehyun Cho (Soongsil University)

Organizing Committee Co-Chairs: Seung-Hyun Seo (Hanyang University), Jungsoo Park (Kangnam University)

OVERVIEW

WISA is the premier security research venue co-hosted by the Korea Institute of Information Security and Cryptology (KIISC) and the Electronics & Telecommunications Research Institute (ETRI) and co-sponsored by the National intelligence service (NIS), the Ministry of Science and ICT (MSIT), the Korea Internet & Security Agency (KISA), and the National Security Research Institute (NSR) by the Korea Institute of Science and Technology Information (KISTI). This year, WISA will be exploring the innovative possibilities of various technologies in enhancing (and threatening) cyber security: artificial intelligence (AI) and blockchain-driven security, hardware cryptography, and all other technical and practical aspects of security applications. We invite participants from a diverse group of researchers and practitioners who are passionate about advancing the state of the art, as well as addressing fundamental security challenges. Join us at WISA 2026 and be part of the conversation that shapes the future of information security.

The areas of interest include, but are not limited to the following:

- Analysis of network and security protocols
- Anonymity and censorship-resistant technologies
- Applications of cryptographic techniques
- Authentication and authorization
- Automated tools for source code/binary analysis
- Automobile security
- AI security
- Botnet defense
- Blockchain security
- Critical infrastructure security
- Denial-of-service attacks and countermeasures
- Digital Forensics
- Embedded systems security
- Exploit techniques and automation
- Hardware and physical security
- HCI security and privacy
- Intrusion detection and prevention
- Malware analysis
- Mobile/wireless/cellular system security
- Network-based attacks
- Network infrastructure security
- Operating system security
- Practical cryptanalysis (hardware, DRM, etc.)
- Security policy
- Side channel attacks and countermeasures
- Storage and file systems security
- Techniques for developing secure systems
- Trustworthy computing
- Trusted execution environments
- Unmanned System Security for Vehicle/Drone/Ship Systems
- Vulnerability research
- Web security

IMPORTANT DATES

- Paper submission deadline: June 13, 2026 (GMT+9)
- Paper acceptance notification: July 18, 2026 (GMT+9)
- Poster submission deadline: July 25, 2026 (GMT+9)
- Poster acceptance notification: August 1, 2026 (GMT+9)
- Pre-proceeding file submission deadline: August 8, 2026 (GMT+9)

INSTRUCTIONS FOR AUTHORS

Authors are invited to submit original papers: they must not substantially duplicate work that any of the authors have published elsewhere or have submitted in parallel to journals or any other conferences that have proceedings. The submission must be anonymous, with no author names, affiliations, acknowledgements, or obvious references. The paper should be limited to at most 12 pages in total and prepared according to the "Authors Instruction for LNCS" ((<https://www.springer.com/gp/computer-science/lncs/conference-proceedings-guidelines>)).

The submission of contributions to WISA 2026 must occur through the following submission system:
<https://easychair.org/conferences/?conf=wisa2026>

Contact

All questions about submissions should be emailed to kiisc@kiisc.or.kr

<https://www.wisa.or.kr>