



CRISIS 2026

21st International Conference on Risks and Security of Internet and Systems

November 25-27, 2026, Rabat, Morocco

Organizing Committee

Honorary Chairs :

Abdelaziz Benjouad
Université Internationale de
Rabat, Morocco

Frederic Cuppens,
Polytechnique Montréal,
Canada

Nora Boulahia-Cuppens,
Polytechnique Montréal,
Canada

General Chairs :

Mohammed Boulmalf,
Université Internationale de
Rabat, Morocco

Hajar Moudoud,
Université du Québec en
Outaouais, Canada

Program Chairs :

Zakaria Abou El Houda,
Institut national de la
recherche scientifique,
Canada

Anass Sebbar,
Université Internationale de
Rabat, Morocco

Publicity Chairs:

Ouassim Karrakchou,
Université Internationale de
Rabat, Morocco

Bouziane Brik,
Sharjah University, UAE

Publication Chairs:

Slim Kallel,
University of Sfax, Tunisia

Call for Papers

The 21st International Conference on Risks and Security of Internet and Systems encourages contributions exploring how artificial intelligence can enhance cybersecurity, as well as how to secure AI-based infrastructures. CRISIS conference aims to bring together researchers, practitioners, and industry experts to discuss emerging challenges and innovative solutions in cybersecurity, risk management, and secure Internet-based systems.

Topics of Interest:

Authors are invited to submit original research contributions including, but not limited to, the following topics:

- AI and machine learning-based security approaches
- Deep learning for intrusion detection and threat analysis
- AI-driven cyber defense and adaptive security systems
- LLMs and generative AI for threat intelligence
- Adversarial machine learning and AI robustness
- Network and communication security
- Software Defined Networking (SDN) security
- Quantum computing
- Network intrusion detection and prevention systems
- Security of new-generation and vehicular networks
- Cyber crisis analysis and response
- Biometrics
- Digital Forensic Analysis
- Cloud computing security
- Security in Edge/Fog computing
- Distributed systems security and safety
- IoT cybersecurity and privacy
- Security of Industrial IoT (IIoT)
- Smart cities, smart grids, and intelligent transportation systems security
- Cryptography, biometrics, and watermarking
- Privacy protection and anonymization
- Security of big data systems
- Blockchain and distributed ledger technologies
- Security metrics and risk evaluation
- Trust management and identity systems
- Systems, Applications & Emerging Threats

Publication: Submitted papers must be original, unpublished, and not under review elsewhere. Manuscripts should be written in English and submitted in PDF format (no anonymization required). Accepted papers will be included in the conference post-proceedings, published by Springer in the Lecture Notes in Computer Science (LNCS) series. Authors of accepted papers must revise their manuscripts according to reviewers' comments before final publication. Papers must follow LNCS formatting guidelines, with a maximum of 16 pages for full papers and 6 pages for short papers. Authors are encouraged to use the Springer LNCS Overleaf template.

Submissions must be made via EasyChair:

<https://easychair.org/conferences/?conf=crisis26>

IMPORTANT DATES

Papers Submission: July 31, 2026

Authors Notifications: September 15, 2026

Final Manuscript: Octobre 01, 2026

