



Special Issue on Systems Security Engineering

Call for Papers

Systems Security Engineering is an interdisciplinary field focused on designing, developing, and maintaining secure and resilient systems throughout their lifecycle. It encompasses security architecture, threat and risk assessment, secure system design, vulnerability management, access control, privacy protection, resilience and security assurance. Research explores methods for integrating security requirements into complex systems, identifying and mitigating emerging threats, and improving the reliability, safety and trustworthiness of software, hardware, networks and critical infrastructure.

In this special issue, we intend to invite front-line researchers and authors to submit original research and review articles on **Systems Security Engineering**. Potential topics include, but are not limited to:

- Security Architecture and Secure System Design
- Threat Modeling and Risk Assessment
- Security Requirements Engineering
- Cryptographic Protocol Design and Analysis
- Cryptography and Data Protection
- Information Assurance and Protection
- Software and Application Security
- Network and Infrastructure Security
- Identity, Authentication and Access Control
- Incident Response and Digital Forensics
- Intrusion detection and prevention
- Formal Methods and Verification
- Cloud & Edge Security
- Systems Security Assurance and Verification
- Privacy and Data Security Engineering
- Resilient and Dependable Systems Security
- Hardware Security & Trusted Computing
- Embedded and Cyber-Physical System Security

Authors should read over the journal's [For Authors](#) carefully before submission. Prospective authors should submit an electronic copy of their complete manuscript through the journal's [Paper Submission System](#).



Please kindly notice that the “**Special Issue**” under your manuscript title is supposed to be specified and the research field “**Special Issue – Systems Security Engineering**” should be chosen during your submission.

According to the following timetable:

Submission Deadline	November 20th, 2026
Publication Date	January 2027

For publishing inquiries, please feel free to contact the Editorial Assistant at submission.entrance1@scirp.org

JIS Editorial Office