



Special Issue on Systems Security Engineering

Call for Papers

Systems Security Engineering focuses on designing, implementing, and maintaining secure systems that protect against cyber threats. It involves integrating security principles into the engineering lifecycle, from initial design to ongoing operations. This discipline emphasizes risk management, secure coding practices, and robust security architecture to ensure data confidentiality, integrity, and availability. Systems Security Engineering professionals collaborate to identify vulnerabilities, mitigate risks, and enhance overall system resilience against evolving cyber attacks.

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:

- Network security
- Secure software development
- Access control and authentication
- Cryptography and encryption
- Intrusion detection and prevention
- Secure system architecture
- Risk management and assessment
- Cloud security
- Cyber-physical systems 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	July 30th, 2024
Publication Date	September 2024

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



Scientific Research
Open Access

Journal of Information Security

ISSN Online: 2153-1242

JIS Editorial Office

jis@scirp.org