



Special Issue on Software Security, Privacy and Trust

Call for Papers

Software Security, Privacy and Trust is an interdisciplinary field focused on protecting software systems, applications, and data from security threats while ensuring privacy, reliability and user trust. It covers secure software development, vulnerability assessment, privacy-preserving technologies, data protection, authentication, access control, software assurance and trustworthy computing. Research explores methods for designing resilient and transparent software that protects sensitive information, mitigates emerging threats, and maintains security and trust throughout the software lifecycle.

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

- Secure Software Engineering and Development
- Security Architecture and Design
- Cryptography and Applied Cryptographic Systems
- Software Vulnerability Analysis and Assessment
- Application and Web Security
- Privacy-Preserving Software and Technologies
- Data Security and Protection
- Authentication, Authorization and Identity Management
- Software Trust and Assurance
- Formal Verification, Program Logic and Certifying Compilation
- Trusted Computing and Secure Platforms
- Security and Privacy in Cloud and Distributed Software
- Malware Analysis and Reverse Engineering
- AI Security, Privacy and Trustworthy Computing

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 – Software Security, Privacy and Trust**” should be chosen during your submission.



According to the following timetable:

Submission Deadline	November 23rd, 2026
Publication Date	January 2027

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

JSEA Editorial Office