# FPS 2023

16th International Symposium on Foundations & Practice of Security

## CALL FOR PAPERS

The 16th symposium will be hosted by the Bordeaux Institute of Technologies (Bordeaux INP), in **Bordeaux, France, on December 11-13 2023**. We invite papers from researchers and practitioners working in privacy, security, resiliency, trustworthy data systems, and related areas to submit their original papers. **Special care will be given this year to enhancing Cybersecurity and Resiliency with Artificial Intelligence**. Moreover, we are interested in data sharing, data disclosure, individual tracking, and fake news regarding their impacts on security and privacy.

## Important dates:

- Abstract Submission: September 1st, 2023
- Full Paper Submission: September 15th, 2023
- Notification to Authors: October 27th, 2023
- Camera-ready: November 10th, 2023

## Paper Submission:

Accepted papers will be included in post-proceedings published by Springer in the Lecture Notes in Computer Science (LNCS) series. Maximum paper length will be 16 printed pages for full papers and 8 pages for short, position papers or demos in LCNS style. All paper submissions will be handled through the Easy Chair conference management system: https://easychair.org/conferences/?conf=fps2023

## TOPICS OF INTEREST

- Access control
- AI for security, resiliency and privacy
- Blockchain-based systems security and security services
- Code reverse engineering and vulnerability exploitation
- Computer and network security
- Cryptography and cryptanalysis
- Data security
- Digital Currencies
- Ethical and social implications of privacy and security
- Hardware security
- Identity management and protection
- Information-theoretic security
- IoT security and privacy
- Malware, botnet advanced persistent threats
- Privacy and privacy enhancing technologies
- Privacy and security awareness
- Security and privacy in social networks
- Security and privacy management and policies
- Security and Privacy of AI
- Security in sensor networks and RFIDs
- Security of Vehicular networks
- Security of cloud, grid and edge computing
- End-to-end Security
- Security of continuum IoT-Edge-Cloud
- Security of distributed embedded middleware,
- Security of service-oriented architectures
- Security, privacy, and trust of industrial systems
- Side-channel and physical attacks
- Software security
- Systems forensics
- Threat analysis and trust management
- Web Security and Privacy
- Fake news detection
- Mechanisms for Open-source intelligence cybersecurity
- Adversarial attacks in AI/ML and automated cyber defense

# CALL FOR PAPERS

16th edition of the Foundations & Practice of Security (FPS) 2023

December 11-13, 2023, Bordeaux, France.

This 16th edition of the Foundations & Practice of Security (FPS) Symposium will be held on December 11-13, 2023 in Bordeaux, France. The 1st FPS Symposium was held in 2008, following the Canada-France Meeting on Security held at the Simon Fraser University, Vancouver, on December 06-08, 2007. Since then, the FPS Symposium has been held annually, alternating Canadian and French locations. FPS took place in Grenoble, Toronto, Paris, Montréal, La Rochelle, Montréal, Clermont-Ferrand, Québec City, Nancy, Montréal, Toulouse, Montréal, Paris, Ottawa.

Protecting the communication and data infrastructure of an increasingly interconnected world has become vital to the normal functioning of all aspects of our daily life. Many industries and businesses, including healthcare, transportation, and manufacturing, rely on edge computing to process data and deliver real-time services, while enterprise networking is increasingly moving to the cloud to improve scalability and reduce costs. As a result, security and cyber resiliency have emerged as vital scientific disciplines that aim to protect these critical systems against cyber threats and ensure the integrity, availability, and confidentiality of data, applications, and services. The multifaceted complexities of these requirements necessitate collaboration and innovation from communities in mathematics, computer science, and engineering.

The aim of FPS is to discuss and exchange theoretical and practical ideas that address privacy, security and resiliency issues in interconnected systems. It aims to provide scientific presentations as well as to establish links, promote scientific collaborations, joint research programs, and student exchanges between institutions involved in this important and fast-moving research field.

We welcome submissions spanning the full range of theoretical and applied work including user research, methods, tools, simulations, demos, and practical evaluations. We also invite papers from researchers and practitioners working in privacy, security, resiliency, trustworthy data systems, and related areas to submit their original papers. **Special care will be given this year to enhancing Cybersecurity and Resiliency with Artificial Intelligence**. Moreover, we are interested in data sharing, data disclosure, individual tracking, and fake news regarding their impacts on security and privacy.

# Topics of Interest

The topics of interest include but are not limited to (alphabetically ordered):

- Access control
- AI for security, resiliency and privacy
- Blockchain-based systems security and security services
- Code reverse engineering and vulnerability exploitation
- Computer and network security
- Cryptography and cryptanalysis
- Data security
- Digital Currencies
- Ethical and social implications of privacy and security
- Hardware security

- Identity management and protection
- Information-theoretic security
- IoT security and privacy
- Malware, botnet, and advanced persistent threats
- Privacy and privacy enhancing technologies
- Privacy and security awareness
- Security and privacy in social networks
- Security and privacy management and policies
- Security and Privacy of AI
- Security in sensor networks and RFIDs
- Security of Vehicular networks
- Security of cloud, grid and edge computing
- End-to-end Security
- Security of continuum IoT-edge-Cloud
- Security of distributed embedded middleware
- Security of service-oriented architectures
- Security, privacy, and trust of industrial systems
- Side-channel and physical attacks
- Software security
- Systems forensics
- Threat analysis and trust management
- Web Security and Privacy
- Fake news detection
- Mechanisms for Open-source intelligence cybersecurity
- Adversarial attacks in AI/ML and automated cyber defense

# Paper Submission

Submitted papers must not substantially overlap with papers that have been published or that are simultaneously submitted to a journal or a conference with proceedings. Papers must be written in English and must be submitted electronically in PDF format. The papers that will be selected for presentation at the conference will be included in post-proceedings published by Springer in the Lecture Notes in Computer Science (LNCS) series (prior to publication the papers should be revised according to the review comments). Pre-proceedings will appear at the time of the conference.

Maximum paper length (including the references) will be **16 printed pages for full papers and 8 pages for short**, position papers or demos including references in **LNCS style**. Authors of accepted papers must guarantee that their papers will be presented at the conference on-site. All paper submissions will be handled through the Easy Chair conference management system. All Springer books will now be on SpringerLink so you can easily search and find books on the same or related topics.

# Important Dates

- Abstract Deadline Submission: September 1st, 2023 by 23:59, AoE
- Full Paper Submission: September 15th, 2023 by 23:59, AoE (Anywhere on Earth)
- Notification to Authors: October 27th, 2023
- Camera-ready Version: November 10th, 2023
- FPS 2023 Conference: December 11th-13th, 2023