HEC MONTRÉAL

Institut multidisciplinaire en cybersécurité et cyberrésilience

FPS 2024

The 17th International Symposium on Foundations and Practice of Security

CALL FOR PAPERS

The first **Foundations & Practice of Security (FPS) Symposium** was held in 2008, following the Canada-France Meeting on Security held at the Simon Fraser University, Vancouver, in 2007. Since then, the FPS Symposium has been held annually, alternating Canadian and French locations. After the previous meetings took place in Grenoble, Toronto, Paris, Montréal, La Rochelle, Clermont-Ferrand, Québec City, Nancy, Toulouse, Ottawa, Bordeaux, the 17th edition will be held on **December 9-11, 2024, in Montréal, Canada**.

Protecting the data and its infrastructure of an increasingly interconnected world has become vital to the normal functioning of all aspects of our daily life. As a result, security and cyber resilience have emerged as scientific research fields focusing on the technologies, processes, and procedures used to protect against cyber threats and to ensure the integrity, availability, and confidentiality of data, applications, and services. Many industries and businesses, including banking, healthcare, transportation, and manufacturing, rely on various technologies both on premise and in the cloud to improve scalability and reduce costs. Alongside technical defenses, behavioral research enhances our ability to protect digital assets by considering the human behavior. All these multifaceted components necessitate research collaborations from various communities such as mathematics, computer science, information systems, management, and criminology.

The aim of the FPS symposium is to discuss and exchange theoretical and practical ideas that address privacy, security and cyber resilience issues in interconnected systems. Moreover, it aims to provide scientific presentations as well as to promote scientific collaborations, joint research programs, and student exchanges between institutions involved in this fast-moving field. **For the 17th edition, special care will be given to innovative behavioral research enhancing privacy and cyber resilience research**. We are particularly interested in topics such as insider threat, user-centric security interfaces, security culture, and user compliance.

Researchers and practitioners are invited to submit their original papers spanning the full range of theoretical and applied work including user research, methods, tools, simulations, demos, and practical evaluations.

Topics of Interest

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

- Access control
- Adversarial attacks to automated cyber defense
- AI for cybersecurity and cybersecurity for AI
- Behavioral cybersecurity 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
- Fake news detection
- Governance and Risk Management for security, privacy and cyber resilience
- Hardware security
- Identity management and protection
- IoT security and privacy
- Malware, botnet, and advanced persistent threats
- Open-source intelligence cybersecurity
- Privacy and privacy enhancing technologies
- Privacy and security awareness
- Security and privacy management and policies
- Security and Privacy of AI
- Security of cloud, grid, and edge computing
- 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 and cybercrime
- Threat analysis and trust management
- Web Security and Privacy

Important Dates

- ❖ September 6, 2024 – Abstract and full paper submission
- ❖ November 1st, 2024 – Acceptance notification
- ❖ November 15, 2024 – Last day for early bird rates
- ❖ November 22, 2024 – Camera-ready version

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 references in LNCS style) will be **16 printed pages for full papers** and **8 pages for short, position papers and demos**. For the **industrial track**, each submission must include at least one author with a non-academic affiliation. Authors are encouraged to contact the industrial track chairs if they need clarification regarding the suitability of their work to this track. 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.

General co-Chairs

- Alina Dulipovici (HEC Montreal, Canada)
- Yvon Kermarrec (IMT Atlantique, France)

Program Committee co-chairs

- Kamel Adi (Université du Québec en Outaouais, Canada)
- Simon Bourdeau (Université du Québec à Montréal, Canada)
- Christel Durand (Deloitte, Canada – *industrial track)*
- Valérie Viet Triem Tong (CentraleSupelec, Inria, Univ. Rennes, CNRS, IRISA Rennes, France)