IWAPS 2023
3rd International Workshop on Advances on Privacy Preserving Technologies and Solutions (IWAPS 2023)

to be held in conjunction with the 18th International Conference on Availability, Reliability and Security
(3rd IWAPS 2023 - https://www.ares-conference.eu/workshops/iwaps-2023/**)**
(ARES 2023 – http://www.ares-conference.eu)
August 29 – September 01, 2023

The availability of massive amounts of data, coupled with high-performance cloud computing platforms, has driven significant progress in artificial intelligence and, in particular, machine learning and optimization. It has transformed into a fertile surface for cyber-attacks skyrocketing the cyber risk of involved industries and impacting several areas, including computer vision, natural language processing, transportation, trust computing, identity management and psychological manipulation.

This workshop aims to strengthen security and privacy through research and relevant activities in the models and design of secure, privacy-preserving and trust architectures, investments in cyber-defense, data analyses, fusion platforms, protocols, algorithms, services, and applications for next generation systems and solutions. We especially encourage security and privacy solutions that employ innovative machine learning techniques to tackle the issues of inspecting large data volumes, cyberattacks, and variety problems that are systemic in IoT platforms, theoretical and practical challenges related to the design of privacy-preserving AI systems and algorithms and will have strong multidisciplinary components, including soliciting contributions about policy, legal issues, and societal impact of privacy and affect the cyber risk of the participating entities.

The 2023 IWAPS will bring together researchers, engineers, and practitioners to present and discuss latest advances and innovations in theories, infrastructure, schemes, and applications for secure computation, privacy technologies, security economics, human computer interaction, as well as to identify emerging research topics and define the future trends.

The workshop is co-organized from the following European Commission (Horizon 2020 Programme) and Greek state (EPAnEK) projects:

SECONDO
INCOGNITO
ERATOSTHENES
PHYSICS
EVOLVED-5G
aerOS
ENTRUST
TRUSTEE
CHRISS
OASEES

FAME
COBALT
RESCALE

We invite authors to submit unpublished work describing research or experience in all areas of usable privacy and security. We accept a variety of research methods, including both qualitative and quantitative approaches. Papers will be judged on their scientific quality, and contribution to the field.

Topics include, but are not limited to

- Architectures and protocols for scalable, secure, robust and privacy enhancing technologies
- Security and privacy frameworks
- Cryptographic approaches for security and privacy
- Trust frameworks and management models for IoT
- Threat and attack models in IoT
- Intrusion and malware detection for IoT
- End-to-end system security models for IoT
- Machine Learning for security and privacy in privacy preserving technologies
- Protection solutions against adversarial machine learning attacks
- Deep Learning and privacy preserving
- Machine learning technique for deep packet inspection
- Machine learning to analyze cryptographic protocols
- Privacy-preserving and machine-learning-based data analytics
- Analysis of mitigations and automating
- Machine Learning technique to predict psychological manipulation
- Machine Learning in predicting the weakest link in an architecture
- Game Theoretic approach to predict attacking paths
- Privacy enhancing and anonymization techniques
- Privacy preserving security/privacy policies
- Privacy preserving in IoT
- Applications of privacy-preserving AI systems
- Attacks on data privacy
- Differential privacy: theory and applications
- Distributed privacy-preserving algorithms
- Human rights and privacy
- Privacy issues related to the Covid-19 outbreak
- Privacy policies and legal issues
- Privacy preserving optimization and machine learning
- Privacy preserving test cases and benchmarks
- Surveillance and societal issues
- Security economics
- Investments in cyber-defense

- COVID-19 impact in psychological manipulation
- Human firewall
- Weakest link in Cybersecurity
- Ethical, psychological, sociological, or anthropological aspects of usable security and privacy
- Machine Learning in automated software testing
- Cybersecurity risk management
- Security controls and budget allocation

Submission Deadline	May 31, 2023
Author Notification	June 14, 2023
Proceedings Version	June 28, 2023
Conference	August 29 – September 01, 2023

WORKSHOP CHAIRS

Christos Xenakis
University of Piraeus, Greece
xenakis@unipi.gr

Apostolis Zarras
University of Piraeus, Greece
zarras@ssl-unipi.gr

Konstantinos Loupos
Inlecom Innovation, Greece
konstantinos.loupos@inlecomsystems.com

Ilias Politis Industrial Systems Institute of ATHENA Research and Innovation
Center, Greece
ilpolitis@isi.gr

Raisia Gorbunov
InQBit Innovation SRL, Romania
raisia.gorbunov@inqbit.io