HOME | Call for Papers | Committees | Participation | Venue | Program | Post Conference | Contact

The Third International Conference on Cyber-Technologies and Cyber-Systems
CYBER 2018
November 18, 2018 to November 22, 2018 - Athens, Greece

Submit a Contribution

Registration

Camera Ready

Deadlines

Submission	Aug 01, 2018
Notification	Sep 04, 2018
Registration	Sep 17, 2018
Camera ready	Sep 25, 2018

Past Events

Publication

Published by IARIA XPS Press

Archived in the free access ThinkMind Digital Library

Prints available at Curran Associates, Inc.

Authors of selected papers will be invited to submit extended versions to a IARIA Journal

Indexing Procedure

Affiliated Journals

CYBER 2018

ISSN: 2519-8599
ISBN: 978-1-61208-683-5

- Registered: with the Library of Congress of the United States of America (ISSN)
- Hosted: by Technische Informationsbibliothek (TIB) - German National Library of Science and Technology (Open Access)
- Free Access: in ThinkMind Digital Library

CYBER 2018 is colocated with the following events as part of NexTech 2018 Congress:

- UBICOMM 2018, The Twelfth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies
- ADVCOMP 2018, The Twelfth International Conference on Advanced Engineering Computing and Applications in Sciences
- SEMAPRO 2018, The Twelfth International Conference on Advances in Semantic Processing
- AMBIENT 2018, The Eighth International Conference on Ambient Computing, Applications, Services and Technologies
- EMERGING 2018, The Tenth International Conference on Emerging Networks and Systems Intelligence
- DATA ANALYTICS 2018, The Seventh International Conference on Data Analytics
- GLOBAL HEALTH 2018, The Seventh International Conference on Global Health Challenges
- CYBER 2018, The Third International Conference on Cyber-Technologies and Cyber-Systems

Special tracks:

ES4IOT: Embedded Systems for the Internet of Things
Chair and Organizer: Dr. Xing Liu, Kwantlen Polytechnic University, Surrey, B.C., Canada xing.liu@kpu.ca

BC4IOT: BlockChain for the Internet of Things
Chair and Organizer Dr. Xing Liu, Kwantlen Polytechnic University, Surrey, B.C., Canada xing.liu@kpu.ca

BDCF: Big Data and Cloud Forensics
Chair and Organizer: Dr Petra Leimich, The Cyber Academy, Edinburgh Napier University, Edinburgh, UK P.Leimich@napier.ac.uk

CAS-IAADR + CCAML: Cyber Attack Surfaces and the Interoperability of Architectural Application Domain Resiliency (CAS-IAADR) via Cyber Characterization, Analytics, and Machine Learning (CCAML)
Chair and Organizer: Dr. Steve Chan, Decision Engineering Analysis Laboratory, USA stevechan@alum.mit.edu
Co-Chair and Organizer: Dr. Tom Klemas, Decision Engineering Analysis Laboratory, USA tklemas@alum.mit.edu

CSSE: Cybersecurity within Smart Space Ecosystems
Chair and Organizer: Dr Abdullahi Arabo, Cyber Security Research Unit, University of the West of England, Bristol, UK Abdullahi.arabo@uwe.ac.uk

CTC-Gov-CRS: Critical Test Capabilities for Informed ICT Governance of Cyber-Resilient Systems
Chair and Organizer: Dr Keith Joiner, Australian Cyber Security Centre (ACSC), University of New South Wales (UNSW), Canberra, Australia k.joiner@adfa.edu.au

CYBER 2018 conference tracks:

Cyber Resilience

Cyber security assessment; Data analytics for Cyber resilience; Organizational security (government, commercial); Resilient smart cities; Resilient Internet of Things (RIOT); Cyber-cities and Cyber-environments; Critical infrastructure security; Back up and recovery for systems of systems; Disaster planning and management from Cyber perspective; Integrated and smarter sensors

Cyber Security

Security management [overall information security management in the sense of 27000 series applied to cyber systems]; Compliance management [verify/check compliance with defined policies, provide corresponding management reports]; Security administration of cyber systems [technical security management of security services]; Security and privacy regulations and laws; Securely interconnected cyber systems [firewalls, cross-domain security solutions]; Self-securing and self-defending cyber systems; Trust management, trust-based information processing [using possibly untrustworthy data sources in a controlled way]; Security technologies for protecting cyber systems and devices; Identity and access management in cyber systems; Anti-counterfeiting; Secure production and supply chain; Cloud computing security; Big-data security; Advanced persistent threats; Network traffic analysis and trace-back; Cyberspace operations; Incident response, investigation, and evidence handling; Intrusion detection and prevention; Cyberspace protection and anti-malware; Cooperation and sharing for Cyber-defense

Cyber Infrastructure

Cyber-Cities and Cyber-environments; Information technology infrastructure; Telecommunications and networks; Cyber-space and data centers; Cyber-enabled control systems; Cyber-enabled critical infrastructure systems; Cyber-physical systems and Internet of Things; Special application domains (smart grid, traffic management systems, autonomous driving, etc.); Embedded processors and controllers; Mobility in Cyber-space; Virtualization in Cyber-space

Cyber Forensics

Computer and networks forensics; Social networking forensics; Digital forensics tools and applications; Applications of information hiding; Identification, authentication, and collection of digital evidence; Anti-forensic techniques and methods; Watermarking and intellectual property theft; Privacy issues in network forensics; Tools, applications, case studies, best practices

Cyber Crime

Cyber-crimes: Challenges in detection/prevention; Anomalies detection; Advanced Persistent Threats and Cyber-resilience; BotNets and MobiNets; Cyber crime-related investigations; Challenges and detection of Cyber-crimes; Network traffic analysis, traceback; Security information and event management (SIEM); Stealthiness improving techniques: information hiding, steganography/steganalysis, etc.

Nature-inspired and Bio-inspired Cyber-defense

Bio-inspired anomaly & intrusion detection; Autonomic and Adaptive Cyber-Defense; Adaptive and Evolvable Systems; Cooperative defense systems; Network artificial immune systems; Adaptation algorithms for cyber security; Biometrics related to cyber defense; Bio-inspired security and networking algorithms and technologies; Biomimetics related to cyber security; Bio-inspired cyber threat intelligence methods and systems; Bio-inspired algorithms for dependable networks; Correlations in moving-target techniques; Neural networks, evolutionary algorithms, and genetic algorithms for cyber security Prediction techniques for cyber defense; Information hiding solutions (steganography, watermarking) and detection

Social-inspired opportunistic mobile Cyber-systems

Design of cyber-physical applications for opportunistic mobile systems based on behavioral models; Social metrics for networks and systems operations; Application of mixed physical and online social network sensing; Social-aware modeling, design and development of routing algorithms in cyber-physical; Incentive mechanisms, reputation systems and key management algorithms in cyber-physical opportunistic mobile systems; Participatory mobile sensing for mining integration in cyber-physical opportunistic mobile systems; Experiments with cyber-physical opportunistic mobile systems

---

Deadlines:

Submission	Aug 01, 2018
Notification	Sep 04, 2018
Registration	Sep 17, 2018
Camera ready	Sep 25, 2018