

Call for Papers

Digital Investigation & Information Assurance Techniques (DIIAT)
The 15th International Conference on Wireless Communications and Mobile Computing
IWCMC 2019

IWCMC 2019 Website: <http://iwcmc.org/2019/>

Submission Link: <https://edas.info/newPaper.php?c=24841>

Tangier, Morocco

June 24 — 28, 2019

Technically sponsored by: IEEE and IEEE Morocco Section

Workshop Chair:

Haider Abbas, National University of Sciences and Technology (NUST), Pakistan dr.h.abbas@ieee.org

Workshop Co-Chairs:

Mariagrazia Fugini Politecnico di Milano, Italy

mariagrazia.fugini@polimi.it

Md Zakirul Alam Bhuiyan, Fordham University, NY, USA

mbhuiyan3@fordham.edu

Seong Oun Hwang, Hongik University, Sejong, Korea

bardic@naver.com

Raheel Nawaz, Manchester Metropolitan University, UK

R.Nawaz@mmu.ac.uk

Farrukh Aslam Khan, King Saud University, KSA

fakhan@ksu.edu.sa

Scope

The increasing dependence of modern business organizations on information and communication technologies necessitates management of their information systems security to ensure a resilient and trustworthy digital ecosystem. Being significantly important for establishing trust and assurance baselines and targets, security evaluation is the first step towards an organization's robust security posture. The precision and accuracy of an organization's information security evaluation has direct impact on achievement of organization's information assurance objectives. Digital investigation is another similar concept sharing the same underlying philosophy as information security evaluation. While evaluation focuses on inspection of a system to determine its degree of compliance with a stated security model, security standard, or specification, digital investigation deals with understanding the digital footprints and recognizing threat actors with a view to counter cyber originated attacks. Having the same underlying objective of managing organizations' information security through logical and physical assessments, information security evaluation and digital investigation are conjointly significant for organizations' information assurance.

Topics

Keeping in view the significance of information security evaluation and digital investigation, this Workshop invites the latest and high-quality research findings on theoretical and practical aspects in the following relevant areas.

- Security Evaluation & Measurement
- Information Security Auditing
- Information Assurance Models & Frameworks
- Security Product Evaluation Criteria & Standards
- Use of Data Sets for Security Evaluation
- Evaluation and Investigation Testbed and Experimental Infrastructure
- Risk Management, Governance and Compliance
- Cryptographic hardware design, implementation, and evaluation
- Digital Footprinting Tools & Techniques
- Analysis of real attacks and threat evaluation
- Use of Simulation, Emulation and Virtualization Techniques for Evaluation & Investigation
- Legal & Regulatory Frameworks for Security Evaluation
- Role of Digital Investigations in Crime Mitigation
- Cyber Deterrence Techniques
- Digital Forensics

Important Dates

- Submission: January 10, 2019
- Acceptance notification: March 30, 2019
- Camera-ready paper submissions: April 30, 2019

Submission Guidelines

Prospective authors are invited to submit original technical papers—up to 6 pages of length, using the EDAS link: <https://edas.info/newPaper.php?c=24841> for possible publication in the IWCMC 2019 Conference Proceedings, which will be submitted to the IEEE Xplore. Selected papers will further considered for possible publication in three special issues in the following Journals. For more information, visit: <http://iwcmc.org/2019/>

1. The International Journal of Sensor Networks (IJSNet) <http://www.inderscience.com/browse/index.php?journalCODE=ijsnet>
2. The International Journal of Autonomous and Adaptive Communications Systems (IJAACS) <http://www.inderscience.com/jhome.php?jcode=ijaacs>
3. KSII Transactions on Internet and Information Systems: <http://www.itiis.org/>

4. Peer-to-Peer Networking & Applications:
<http://www.springer.com/engineering/signals/journal/12083>
5. Cyber-Physical Systems journal: www.tandfonline.com/loi/tcyb20

Note: There will be best paper award, best Symposium award and best Workshop award.

TPC Members (TBD)