IEEE TRUSTCOM 2019
The 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom 19)

5 – 8 August 2019
Novotel Lakeside Rotorua
NEW ZEALAND
crow.org.nz/trustcom2019

TrustCom 2019 Call For Papers

In a fast-growing cyber security threat landscape, game-changing techniques in information security, trust, privacy and forensics are required for a sustainable future. CROW and STRATUS are proud to host the 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-19) which will be held at Rotorua, New Zealand on 5-8 August 2019.

As a leading international conference in the area of trust, information security and privacy, and forensics, the IEEE TrustCom 2019 conference aims to bring together international researchers and practitioners working on trusted computing and communications, with regard to trust, security, privacy, reliability, dependability, survivability, availability, and fault tolerance aspects of computer systems and networks – providing a forum to present and discuss emerging ideas and trends in this highly challenging research field.

Topics of interest include, but not limited to:

Trust Track
Trust semantics, metrics and models, Trusted computing platform, Trusted network computing, Trusted operating systems, Trusted software and applications, Trust in social networks, Trust in e-commerce and e-government, Trust in mobile and wireless communications, Trust in automotive environments, Trust visualization, Risk and reputation management, Survivable computer systems/networks, Trust of 5G, Hardware for chains and roots of trust, Software trustworthiness and quality, Provenance for trust, Novel techniques in provenance

Security Track
Network security, Computer security, Database security, Hardware security, Side-Channel attacks, Fault attacks, Obfuscation and reverse engineering, Web applications security, Machine learning applied to security applications, Security policy, model and architecture, Security in social networks, Security in parallel and distributed systems, Security in mobile and wireless communications, Security of 5G, Security in grid/cloud/pervasive/fog/edge computing, Authentication, authorization and accounting, Emerging topics in information security and applied cryptography, Miscellaneous security issues, Provenance for security, Emerging topics in security attribution, Consumer/User-centric security

Privacy Track
Privacy in Web-based applications and services, Privacy in database systems, Privacy in parallel and distributed systems, Privacy in grid/cloud/pervasive computing, Privacy in mobile and wireless communications, Privacy in e-commerce and e-government, Privacy in network deployment and management, Privacy and policy conformance (GDPR, HIPPA, etc.), Privacy and trust, Privacy and security, Privacy and anonymity, Privacy preservation in 5G, Privacy in surveillance systems, Miscellaneous privacy issues, Consumer/User-centric privacy

Forensics and Analytics Track
Anti-forensics, Biometrics, Cryptanalysis, Big data forensics, CCTV forensics, Cloud forensics, Computational forensics, Cyber-physical system forensics, Data Mining for forensics, Facial recognition, Fingerprint forensics, Image forensics, Malware forensics, Mobile app forensics (e.g. Skype, WeChat and Facebook), Mobile device forensics, Multimedia forensics, Network forensics, Steganography and steganalysis, System reverse engineering, Watermarking, Automotive Forensics, Behavioural biometrics

Emerging Technologies
Blockchain security and privacy, Blockchain consensus, Blockchain implementation, Blockchain based IoT security solutions, Blockchain in cyber physical systems, Blockchain in social networking, Directed Acyclic Graph (DAG) distributed ledger, Smart contract, Cryptocurrencies security and privacy, IoT security and privacy, Attacks in blockchain/cryptocurrency , IoT implementations for security and privacy, Industry Control systems, Post-quantum cryptography , Security models for the post-quantum era, Implementations of post-quantum cryptosystems, Cyber insurance technologies, Emerging and disruptive technologies for security, privacy, trust and forensics.

Submission Guidelines
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 clearly presented in English, must not exceed 8 pages, including tables, figures, references and appendixes, in IEEE Computer Society proceedings format with Portable Document Format (.pdf). Please submit your paper via https://easychair.org/conferences/?conf=ieeetrustcom2019

Papers will be selected based on their originality, timeliness, significance, relevance, and clarity of presentation. Submission of a paper should be regarded as a commitment that, should the paper be accepted, at least one of the authors will register and attend the conference to present the work. Accepted and presented papers will be included in the IEEE CPS Proceedings. Distinguished papers presented at the conference, after further revision, will be recommended to high quality international journals.

Important Dates
Submission Deadline: March 14, 2019
Authors Notification: April 27, 2019
Camera-Ready Manuscript Due: May 27, 2019

General Chairs
Ryan Ko, University of Queensland, Australia
Liqun Chen, University of Surrey, United Kingdom
Liming Zhu, Data61, CSIRO, Australia

Website : https://crow.org.nz/TrustCom2019