



# 10<sup>th</sup> IEEE Workshop on Network Measurements

In conjunction with IEEE LCN 2016

## Dubai, UAE | Nov 7-10, 2016

**Submission:** May 23, 2016  
**Notification:** July 25, 2016  
**Camera-ready:** August 15, 2016  
**Workshop Webpage:** <http://wnm2016.csis.mtroyal.ca/>  
**Direct EDAS Submission Link:** <https://edas.info/N22480>

The 10th Anniversary Edition of IEEE Workshop on Network Measurements is soliciting papers in the areas of **computer network measurement, monitoring, security and privacy**. We invite mature and early works using traditional and new methodologies, and especially works that challenge conventional wisdom in relationship between traffic monitoring, security and privacy. We seek submissions that treat all aspects of measurement, security and privacy across the networking stack, distributed applications and services and especially encourage works that involve new and emerging systems, applications, and environments.

The importance of data increases from one year to the next, and we have witnessed significant changes in technologies related to generation, collection, transmission, analysis and storage of data, including virtualization and cloud technologies, big data processing and storage systems. The sheer volume of data poses challenges to traditional measurement and monitoring techniques, as well as transmission into analysis systems, where so much data is generated that it cannot be copied, transmitted or stored before processing that includes downsizing.

As data becomes more important, more precise and detailed extraction from network traffic and applications is necessary. Often times, considerations for security and privacy preservation are lacking or come later as a secondary concern. A question arises how to build powerful measurement and monitoring systems that generate valuable data without compromising security and privacy of consumers, and increasingly IoT devices, that generate it. In fact, many measurement and monitoring systems do not have built-in privacy and security protection mechanisms and data is sanitized off-line or during post-processing. On the other hand, some systems are built with only security or privacy in mind so that effective measurement and monitoring of those systems is impossible.

We invite the measurement, monitoring, security and privacy community to contribute original submissions that cover a broad range of topics across wired and wireless networks, with and without security and privacy aspects:

- \*Measurement tools, techniques, design, and evaluation
- \*Measurement of new protocols such as HTTP/2, QUIC and similar alternatives
- \*Measurement of emerging modes of communication such as NFC and spontaneous interaction of devices
- \*Measurement for wearables and Internet of Things
- \*Measurement in Network Function Virtualization and Software-Defined Networking
- \*Building Quality of Experience (QoE) metrics from network measurements
- \*Measurement related to performance, security and privacy
- \*Preserving security and/or privacy in measurement and monitoring systems
- \*Preventing network intrusions and attacks on monitoring and measurement systems
- \*Detecting vulnerabilities in network systems
- \*Anonymization and privacy preservation
- \*Building secure and privacy-preserving monitoring systems and infrastructures
- \*Privacy enhancing technologies
- \*Privacy and anonymity in the Web, cloud systems, online social networks, mobile networks, P2P networks
- \*Privacy in identity management systems
- \*Design, performance, and measurements of privacy-preserving systems
- \*Design, performance, and measurements of secure networks
- \*Measurement methodologies for privacy and anonymity
- \*User profiling mechanisms
- \*Mechanisms for processing of private data
- \*Quantification of privacy threats and anonymity loss
- \*Privacy challenges in smart systems
- \*Current and emerging regulatory frameworks for privacy

The workshop seeks novel, previously unpublished papers, which are not currently under review by another conference, workshop, or journal. All submissions should be in PDF for-mat, written in English with a maximum paper length of eight printed pages (IEEE Transactions style double-column format, 10pt font size), including figures. The paper should include a brief abstract of up to 150 words. The submission will be handled via EDAS. The accepted papers will be published in the conference proceedings and will be available via the IEEE Xplore website. Please refer to workshop website for details.

### Workshop Chairs

**Aniket Mahanti**

**University of Auckland, New Zealand**

**Emir Halepovic**

**AT&T Labs—Research, USA**

### Web Chair

**Mingwei Gong**

**Mount Royal University, Canada**