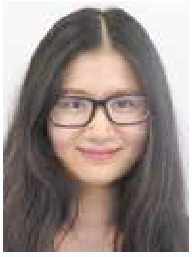
THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

Department of Computing
電子計算學系

Research Seminar

Privacy vs. Utility: A Battle between Data Owners and Data Analysts



Dr Mengyuan Zhang
Research Assistant Professor
Department of Computing
The Hong Kong Polytechnic University
Hong Kong

Date : 18 December 2020 (Friday)
Time : 2:30 p.m. - 3:30 p.m.

► Abstract

As the owners of large-scale network data, today's ISPs and enterprises usually face a dilemma. With the sophistication of security monitoring and analytics, those organizations are motivated to outsource such tasks to third-party analysts, e.g., Managed Security Service Providers (MSSPs). However, they are also reluctant to share their network trace data, and even less willing to publish them, mainly due to privacy concerns. To address this issue, the anonymization of sensitive data while still enabling security auditing, i.e., preserving both privacy and utility, has attracted a lot of attention recently. In the first part of this talk, I will present a demo that showcases how to preserve both privacy and utility by shifting the trade-off from between privacy and utility to between privacy and computational cost. Furthermore, to quantify the level of privacy in a data set, differential privacy (DP) has emerged as a de facto privacy notion for a wide range of applications. Utility metrics in different applications are defined to measure the usefulness of the anonymized data. In the second part of this talk, I will present an approach that automatically optimizes utility metrics for different applications under a common framework. The work related to these two concepts has been published in CCS'18, TOPS, TDSC, and CCS'20.

► About the Speaker

Dr Mengyuan Zhang is a newly appointed Research Assistant Professor in the Department of Computing at PolyU. She worked as an Experienced Researcher at Ericsson Research, Montreal, QC, Canada. She received her Ph.D. in Information and Systems Engineering from Concordia University in Montreal. Her research interests include security metrics, attack surface, cloud computing security, privacy, and applied machine learning in security. She has published book chapters and several research papers in top-tier peer-reviewed international journals and conferences such as TIFS, TDSC, CCS, ESORICS.

ALL are welcome!

Enquiries : Professor George Baciu
Email : csgeorge@polyu.edu.hk
Tel : 2766 7272

We drive innovation through
SMART COMPUTING