Guest Editorial
Special Issue on Behavior Data Analytics for Cybersecurity

Chi-Hung Chi[1], Raymond Wong[2], Kwok-Yan Lam[3]

[1] Data61, CSIRO, Australia
[2] University of New South Wales
[3] Nanyang Technological University, Singapore

With rapid development of smart cities and digital economy, cybersecurity has already become the cornerstone to ensure the resilience of the entire ecosystem. On top of traditional systems/data/network security research, cybersecurity is facing new challenges. This is mainly due to the increasing scale of complex collaboration among stakeholders on a loosely regulated network of insecure devices. Advances in hacking and malware techniques, including APTs (advanced persistent threats), fileless malware, zero-days exploits, …, etc. already make active in-time defense difficult to achieve. Even worse, insider threats and human factors have already moved to the top in the main security threat list. Conventional security measures often find to be ineffective when dealing with them; and all these are just magnifying the negative impacts of cyber-attacks.

Facing this challenge, it is believed that behavior analytics, in particular using knowledge modeling and semantics to couple with data mining and pattern discovery, is very effective in understanding not only the transactional behavior patterns of entities in the cyberspace, but also the causations behind these patterns as well as the quantification of their cognitive experience. When these two areas are put together, it creates a promising direction to address new cybersecurity challenges. It also opens up new fundamental research questions in both fields, data analytics, and cybersecurity.

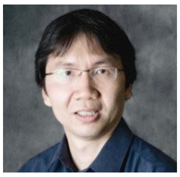
This special issue offers an update of research field in line with behavior data analytics and cybersecurity. It was generated from the 18th International Conference on Information and Communications Security 2016 and papers submitted for this special issue. It includes four papers. The first paper, “A Machine Learning Framework for Adaptive FinTech Security Provisioning” by La and Kim presents a software architectural framework for behavior model-driven security analytics. It details not only the architectural aspects but also covers details about the analytics algorithms involved. With such framework, behavior-driven analytics and threat intelligence initiatives can be built and supported. The second paper, “Towards a Flexible Experience of Data Provenance Summarization”, by Pei and Ye investigates the bridges between transactional raw data and aggregated knowledge. It also looks into the potentials and effects of interactive human machine collaboration, which is a critical step in behavior-driven analytics. The third paper, “Real Time Attacker Behavior Pattern Discovery and Profiling Using Fuzzy Rules”, by Mallikarjunan and Shalinie et al. goes deep into the algorithm aspects of behavior analytics for cyber attack detection. Finally, the last paper, “Smart TV Face Monitoring for Children Privacy”, by Hung et al. investigates the issue of privacy for behavior analytics. This is particularly important to insider threats in cybersecurity. On one hand, analytics for cybersecurity demands multi- data sources to re-construct the persona of human for risk analysis and active defense. On the other hand, such approach will definitely touch the sensitive issue of privacy in behavior analytics.

We thank the Journal of Internet Technology for supporting this special issue. We also thank all contributors and referees for their kind co-operation in helping this special issue.

Guest Editors

Chi-Hung Chi is currently a senior principal research scientist in Data61, CSIRO, Australia. He obtained his Ph.D. degree from Purdue University, West Lafayette, USA. Before joining CSIRO in 2012, he has worked in industry (Philips Research and IBM) and universities (Chinese University of Hong Kong, National University of Singapore, and Tsinghua University) for more than 20 years. His current research areas include behavior modelling and knowledge base, cybersecurity, big data and analytics, service engineering, cloud computing, and social networking. He has published about 300 papers in international conferences and journals and holds 6 U.S patents.

*Corresponding Author: Chi-Hung Chi; E-mail: chihungchi@gmail.com



Raymond Wong is currently an Associate Professor at the School of Computer Science & Engineering, University of New South Wales, Sydney, Australia. From 2005-2011, he founded and led the Database Research Program at NICTA (the largest ICT organization in Australia). His research expertise lies in database systems and data mining. He has published more than 180 research publications and 2 US patents in these areas. He has also supervised 18 Ph.D. students to completion. He received his BSc from Australian National University, and MPhil and Ph.D. from Hong Kong University of Science & Technology; and did his Postdoc at UCLA and Stanford University.

Lam Kwok Yan is currently a Professor with Nanyang Technological University. He is a renowned Cyber Security researcher and practitioner. Professor Lam has collaborated extensively with law-enforcement agencies, government regulators, telecommunication operators and financial institutions in various aspects of Infocomm and Cyber Security in the Asia-Pacific region. He is the Lead P.I. of the SPIRIT Programme, an S$11,000,000 programme on smart nation research funded by NRF. Prior to joining NTU, he has been a Professor of the Tsinghua University, PR China (2002-2010) and a faculty member of the National University of Singapore and the University of London since 1990. He was a visiting scientist at the Isaac Newton Institute of the Cambridge University and a visiting professor at the European Institute for Systems Security. In 1997, he founded PrivyLink International Ltd, a spin-off company of the National University of Singapore, specializing in e-security technologies for homeland security and financial systems. In 2012, he co-founded Soda Pte Ltd with a HK-based medical clinics operator. Soda (or Safe of Data App), the Winner of the Most Innovative Start Up Award at the RSA 2015 Conference, is a technology start-up which specialises in data security protection of mobile cloud users.