3rd IEEE International Conference on Artificial Intelligence,
Modelling and Simulation, Kota Kinabalu, Malaysia, 2-4 December 2015

Keynote

Modelling and Simulation in Experimental Cybersecurity Research

Yong Meng TEO
Department of Computer Science
National University of Singapore
Email: teoym@comp.nus.edu.sg
url: www.comp.nus.edu.sg/~teoym

Cybersecurity challenges today are very real and wide-ranging with significant implications across multiple domains and communities. For cybersecurity research to be impactful, an experimentation infrastructure with shared and validated models, tools and testbeds will enable researchers to design meaningful experiments and test environments. Among the pillars of science, modelling and simulation is a mean of scientific discovery that employs computing to simulate a physical system according to laws derived from theory and experiment. This keynote discusses a national shared infrastructure, currently being developed, to provide computing resources, repeatable and controllable experimental environments, among others, for the cybersecurity R&D community in Singapore.

This keynote, divided into *three* main parts, aims to share our experience in setting up a national infrastructure for modelling and simulation experimentation in cybersecurity. First, we review experimental cybersecurity infrastructures with different capabilities, namely, small stand-alone, localized, and large distributed. Next, we discuss the hardware infrastructure and software tools to support both user physical and/or virtual cybersecurity testbeds. The hardware is designed to support dynamic provisioning of computing nodes as bare metal or virtual machines, and network and storage allocation as dedicated physical hardware. To support the modelling and simulation experiment life cycle, software tools are required to model and construct experiments, emulate human and system activity and orchestrate network experiments among others. Cybersecurity experimentation must capture real world scale and human activity because it often involves analysis of large, complex, decentralized systems. To illustrate the use of the national infrastructure, we discuss the design of a simulation application for studying the effect of human behavior on cybersecurity and emergent behavior on new security vulnerabilities.

Biography

TEO Yong Meng is an Associate Professor of Computer Science at the National University of Singapore (NUS) and an Affiliate Professor at the NUS Business Analytics Centre. He was a Visiting Professor at various institutes in the Chinese Academy of Science, China from 2010-2014. He received his PhD in Computer Science from the University of Manchester. His research interest is on parallel and distributed systems and applications. In the last five years, he focused on the performance of parallel systems, cloud computing, and emergent properties in complex systems. The paper on strategy-proof dynamic pricing of cloud computing resources won the **Best Paper Award** at the 10th International Conference on Algorithms and Architectures for Parallel Processing in 2010. Another paper, co-authored with his PhD student, on time-based semantic validation won the **ACM SIGSIM Best PhD Student Paper Award** in 2009. He leads the Computer Systems Research Group. He also served as Advisor (Director's Office) on Large-Scale Computing Systems, Asia-Pacific Science and Technology Centre, Sun Microsystems Inc. from 2007-2008, and External Grant Evaluator, European Research Council (Ideas Specific Program) from 2008-2013. He has received numerous external research grants including European Commission, Fujitsu Computers (Singapore) Pte Ltd, Fujitsu Laboratories Ltd (Japan), Sun Microsystems/Oracle (USA), Nvidia, and PSA Corporation (Singapore) among other institutions.