IEEE International Conference on Computer,
Communication and Signal Processing, Chennai, India, Jan 10-11, 2017

Keynote

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

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. At NUS, he is the technical leader for Systems Research and he leads the Computer Systems Research Group. He was a Visiting Professor at the Chinese Academy of Science in China from 2010-2014. He received his PhD and MSc in Computer Science from the University of Manchester. His research interests include parallel computing, systems modeling and simulation and performance analysis. His recent work focuses on modeling the performance of heterogeneous parallel systems and emergent properties in complex systems among others. He has over 150 journal and conference publications and a number of best paper awards including the *Best Applied Paper Award* at the annual Wintersim Conference in 2015 and 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 won the *ACM SIGSIM Best PhD Student Paper Award* in 2009. He has received various research grants including European Commission, Fujitsu Computers (Singapore) Pte Ltd, Fujitsu Laboratories Ltd (Japan), Sun Microsystems/Oracle (USA), NVIDIA and PSA Corporation.

Social Interactions and System Vulnerabilities

More than 40% of computer and organizational security professionals believe that their greatest security threat is insider threats where employees jeopardized security through data leaks or similar errors [1]. Though insider threats are of growing interest and importance in system security, it is not well understood and investigated. This talk discusses the role of social interactions in an organization and the insider threats it presents on system vulnerabilities.

In this keynote, we discuss a three-step approach to investigate the effects of social interactions and the risks it present on system vulnerabilities. Firstly, we show how user's roles, security policies and their interactions are modeled as facts and interaction rules. Secondly, a reasoning engine consumed these facts and interaction rules and together with a model of the hardware system configuration, to produce an attack graph. An attack graph represents the cumulative effect of attack steps, showing how series of individual steps or network paths can potentially enable an intruder to gain privileges in the system. Lastly, the attack graph is analyzed to obtain an objective measure of risks and to prioritize security hardening measures among others. For examples "how likely is it that an intruder could gain privilege X?", "which user group and system component are most vulnerable?" Preliminary results on the impact of security leakage due to user interactions on system vulnerabilities are discussed.

Reference

1. *Unintentional Insider Threats: Social Engineering*, Technical Report, Software Engineering Institute, Carnegie Mellon University, Jan 2014.