NATIONAL UNIVERSITY OF SINGAPORE

School of Computing

C S S E M I N A R

Title: **Symbolic trace analysis for security protocols**

Speaker: Dr. Alwen Fernanto Tiu
Assistant Professor
School of Computer Science and Engineering
Nanyang Technological University

Date/Time: 6 June 2016, Monday, 02:00 PM to 03:30 PM

Venue: Executive Classroom, COM2-04-02

Chaired by: Dr Jaffar, Joxan, Professor, School of Computing
(joxan@comp.nus.edu.sg)

Abstract:

Many security properties associated with a protocol can be expressed in terms of properties of its traces. For example, secrecy and authentication can be specified as a reachability problem, i.e. whether there exists a trace of actions/communications from an initial state of the protocol to a state where certain secrets can be inferred or certain privileged actions can be performed by the attacker. Less obvious are privacy-type properties such as anonymity or unlinkability, which require comparisons between different traces, or even different sets of traces of a protocol. Since in the analysis of security protocol the attacker is often assumed to control the commnucation network and hence controls the input to protocol participants, the potential traces of a protocol is infinite. There is thus a need to represent these traces symbolically; leaving the attacker's actions and the attacker's synthesized messages uninstantiated until they are actually needed in the analysis. In this talk, I will discuss two basic trace analysis problems that often appear in symbolic analysis of security protocols. One is a single-trace analysis which converts a symbolic trace into a deducibility constraint system, whose solvability implies the symbolic trace can be turned into an actual trace of attack. The other deals with the equivalence problem between symbolic traces. I will show that the latter can be solved using the former as building block.

Biodata:

I am an assistant professor at the School of Computer Science and Engineering, Nanyang Technological University. My main research interests span theoretical as well as practical aspects of computer science; these include formal methods, computational logic, automated theorem proving and computer security. More specifically, I am interested in modelling

aspects of computational systems (such as parts of operating systems, communication protocols, simple authentication devices, etc) as mathematical theories, and developing tools and techniques to prove their correctness or to find potential flaws.