

# NATIONAL UNIVERSITY OF SINGAPORE

School of Computing

## C S S E M I N A R

**Title:**        **Semantics-Driven Decompilation of Recursive Datatypes**

Speaker:     Professor Andy King  
              School of Computing  
              University of Kent

Date/Time:   1 November 2016, Tuesday, 02:00 PM to 03:30 PM

Venue:        Video Conference Room, COM1-02-13

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

### Abstract:

Reconstructing the meaning of a program from its binary executable is known as reverse engineering; it has a wide range of applications in software security, exposing piracy, legacy systems, etc. Since reversing is ultimately a search for meaning, there is much interest in inferring a type (a meaning) for the elements of a binary in a consistent way. Unfortunately existing approaches do not guarantee any semantic relevance for their reconstructed types.

This talk presents a new and semantically-founded approach that provides strong guarantees for the reconstructed types. Key to our approach is the derivation of a witness program in a high-level language alongside the reconstructed types. This witness has the same semantics as the binary, is type correct by construction, and it induces a (justifiable) type assignment on the binary. Moreover, the approach effectively yields a type-directed decompiler.

We formalise and implement the approach for reversing MinX, an abstraction of x86, to MinC, a type-safe dialect of C with recursive datatypes. Our evaluation compiles a range of textbook C algorithms to MinX and then recovers the original structures.

This is joint work between Ed Robbins and Tom Schrijvers; the talk will summarise work published in POPL earlier this year.

### Biodata:

Andy King is a professor of computer science at the University of Kent, with a PhD in computer science from the University of Southampton in 1992 on the abstract interpretation of logic programs. He has recently been working on providing rigorous foundations for the program analyses problems that arise in reverse engineering.

