

# NATIONAL UNIVERSITY OF SINGAPORE

School of Computing

## C S S E M I N A R

**Title:** LJGS: Gradual Security Types for Object-Oriented Languages

**Speaker:** Professor Peter Thiemann  
Department of Computer Science  
University of Freiburg

**Date/Time:** 28 November 2016, Monday, 03:00 PM to 04:30 PM

**Venue:** Executive Classroom, COM2-04-02

**Chaired by:** Dr Sulzmann, Martin, Visiting Professor, School of Computing  
(sulzmann@comp.nus.edu.sg)

### Abstract:

LJGS is a lightweight Java core calculus with a gradual security type system. The calculus guarantees secure information flow for sequential, class-based, object-oriented programming with mutable objects and virtual method calls. An LJGS program is composed of fragments that are checked either statically or dynamically.

Statically checked fragments adhere to a security type system so that they incur no run-time penalty whereas dynamically checked fragments rely on run-time security labels. The programmer marks the boundaries between static and dynamic checking with casts so that it is always clear whether a program fragment requires run-time checks. LJGS requires security annotations on fields and methods. A field annotation either specifies a fixed static security level or it prescribes dynamic checking. A method annotation specifies a constrained polymorphic security signature. The types of local variables in method bodies are analyzed flow-sensitively and require no annotation. The dynamic checking of fields relies on a static points-to analysis to approximate implicit flows. We prove type soundness and non-interference for LJGS.

### Biodata:

Peter Thiemann obtained his diploma in computer science in 1987 at the Technical University of Aachen, Germany. He graduated in 1991 at the University of Tübingen, Germany, where he worked as a research and teaching assistant until 1997. In 1998, he was a lecturer in Computer Science at the University of Nottingham, England. Since 1999 he teaches at the University of Freiburg, Germany. He is a full professor at the computer science department and leads the programming languages group.

His research interests comprise theory and practice of modern programming languages, in particular typing, program analysis, and program transformation.

He has authored and co-authored more than 150 papers on these and related topics. The focus of his recent research is on static and dynamic program analysis for JavaScript, Java, and Go as well as gradual typing in a security context.