Facultad de Informática
Universidad Complutense de Madrid

ANUNCIO DE CONFERENCIA

Certificación de no-interferencia y borrado usando la lógica de reescritura

Prof. Santiago Escobar Román
Universitat Politècnica de València

Aula 7 • 6 de junio de 2011 • 15: 00
entrada libre hasta completar el aforo

resumen:

La no-interferencia es una propiedad semántica que asigna niveles de confidencialidad a datos y variables y previene el flujo ilícito de información desde niveles de alta seguridad a niveles de baja seguridad. El borrado es una forma de fortalecer la confidencialidad imponiendo niveles más altos de seguridad, hasta el extremo de requerir la eliminación de toda información de alta seguridad del sistema. En esta charla, proponemos una técnica de certificación de la confidencialidad para clases Java que soporta políticas de no-interferencia y borrado. Esta técnica está basada en la lógica de reescritura y la abstracción.

sobre Santiago Escobar:

Santiago Escobar Román es Titular de Universidad en la Universidad Politécnica de Valencia, miembro del grupo de investigación Extensiones de la Programación Lógica de la Universidad Politécnica de Valencia, liderado por María Alpuente, y colaborador habitual del grupo de investigación Formal Methods and Declarative Languages Laboratory de la University of Illinois at Urbana-Champaign, EE.UU., liderado por José Meseguer.

Santiago es doctor en Informática desde 2003 y ha desarrollado su investigación principalmente en el estrechamiento como mecanismo de programación lógico-funcional y sus diversas aplicaciones. Ha desarrollado estrategias de evaluación perezosas para reescritura y estrechamiento, y anotaciones de evaluación perezosa para la familia de lenguajes OBJ/Maude. Ha definido técnicas para la unificación ecuacional basada en el estrechamiento, obteniendo decidibilidad de la unificación bajo determinadas circunstancias gracias a la definición de técnicas para probar la terminación del estrechamiento o gracias a la definición de estrategias especializadas de estrechamiento.

Entre las aplicaciones, participa en el desarrollo de la herramienta de verificación de protocolos criptográficos denominada Maude-NPA, participa en la definición e implementación del estrechamiento para el lenguaje Maude, y participa en el desarrollo de un marco de código con demostración asociada para programas Java usando el lenguaje Maude. Además, ha definido un marco de model checking simbólico (con variables lógicas y propiedades de lógicas temporales) en Maude.