



SEMINARIO

Departamento de Sistemas Informáticos y Computación

Facultad de Informática
Universidad Complutense de Madrid

2-2-2010

Grupo de Análisis Estático y
Certificación de Propiedades

14:00
Sala de Grados
Facultad de
Informática

Ricardo Peña
Director del Grupo

Después de la presentación
habrá un pequeño refrigerio
en la Sala de reuniones.

Aunque en su origen pretendían generar un código más eficiente, los análisis estáticos se están utilizando también en los últimos años para comprobar propiedades de corrección de los programas tales como la terminación, el consumo acotado de recursos y otras.

El código con certificado (Proof Carrying Code, o PCC) es una línea emergente de investigación cuyo objetivo es crear una infraestructura en la que los programas vayan provistos de una demostración matemática (certificado) que garantiza que satisfacen ciertas propiedades útiles. Estos certificados son comprobados automáticamente por el receptor del código utilizando herramientas apropiadas.

Los análisis estáticos y el PCC encajan bien porque el compilador puede emitir certificados sobre las propiedades inferidas durante el análisis. Nuestro proyecto SELF, continuado parcialmente en STAMP, ha desarrollado Safe, un lenguaje previsto para aplicaciones móviles ejecutadas en plataformas con pocos recursos. Su objetivo es dotar a los programas de certificados que garanticen la ausencia de punteros descolgados y un consumo acotado de memoria. Como lenguaje y herramienta de certificación utilizamos el asistente Isabelle/HOL. La presentación ilustrará todos estos aspectos con una demostración en la que accederemos a nuestro compilador en línea.