Facultad de Informática
Universidad Complutense de Madrid

ANUNCIO DE CONFERENCIA

Compilación de Programas y Transformación de Certificados.

César Kunz

IMDEA software. Madrid.

Sala de Grados • 18 de marzo de 2009 • 16: 00
entrada libre hasta completar el aforo

resumen:

El paradigma de código móvil supone la distribución de aplicaciones o componentes de software desde sus desarrolladores hasta sus consumidores.
Al final de los años noventa, el Código con Certificado (Proof Carrying Code) surgió como un método para proveer garantías sobre la corrección del código recibido. Esta técnica consiste en suministrar, además del código ejecutable, un certificado que una vez verificado, a través de un proceso eficiente, implica que el código recibido satisface los requisitos de corrección especificados.
El principal inconveniente para la implantación de plataformas para Código con Certificado es la generación de certificados, que ha estado hasta hoy limitada a un proceso automático, como parte del compilador, y por lo tanto restringido a la verificación de propiedades básicas (debido a que deben ser decidibles).
En esta charla, se presentará una técnica cuyo fin es extender el conjunto de propiedades que pueden ser certificadas para un código móvil. Tal técnica consiste en trasladar el resultado de verificación de código fuente, a la certificación de código ejecutable, y así poder extender arbitrariamente el conjunto de propiedades a considerar, con el posible costo adicional que implica la verificación interactiva.
Se analizará cómo las diferentes etapas de compilación pueden obstaculizar la transferencia de certificados desde el código fuente hasta el código compilado, y se propondrán técnicas para transformar certificados de código fuente en certificados para el código ejecutable, en presencia de optimizaciones estándar.

sobre César Kunz:

My research area focus on the interaction between compilation and verification condition generators (VC generators), which are used in many interactive verification environments to guarantee the correctness of source programs, and by several proof carrying code (PCC) architectures to check the correctness of compiled programs. The main objective of my research is to transfer the evidence of source code correctness to its compiled counterpart.