

Avances en Proof-Carrying Code

Francisco Bavera* Martín Nordio* Ricardo Medel[†] Jorge Aguirre*
Gabriel Baum[‡]

Resumen

Uno de los principales desafíos en el diseño e implementación de sistemas que involucran código móvil es garantizar la seguridad del receptor frente a la ejecución del código foráneo. La técnica de *Proof-Carrying Code* (PCC) establece una infraestructura que permite garantizar que los programas se ejecutarán de manera segura. En esta alternativa, el productor de código adjunta al código móvil una demostración, mediante la cual el consumidor del código puede verificar su seguridad antes de la ejecución del programa. Esto elimina la necesidad de validaciones en tiempo de ejecución y de identificación del emisor. Los esfuerzos de distintos grupos de investigación han logrado grandes avances en el tema y existen varias líneas de investigación tendientes a desarrollar una infraestructura flexible, escalable y confiable, quedando aún muchos problemas por resolver. Partiendo del análisis de los resultados obtenidos y de los enfoques actuales se pretende diseñar e implementar una arquitectura PCC que permita su uso en el “mundo real”.

Palabras Clave: Lenguajes de programación, Teoría de Tipos, Compilador Certificante, Código Móvil.

Enviado a: CACIC'03 Congreso General

*Universidad Nacional de Río Cuarto, {pancho,nordio,jaguirre}@dc.exa.unrc.edu.ar

[†]Stevens Institute of Technology (New Jersey, EE.UU.), rmedel@cs.stevens-tech.edu

[‡]Universidad Nacional de La Plata, gbaum@sol.info.unlp.edu.ar