UNIVERSIDAD COMPLUTENSE
MADRID

AVISO DE CONFERENCIA

Inference of Fractional, Counting and Chalice Access Permissions via Abstract Interpretation

Prof. Pietro Ferrara. ETH Zurich

Facultad de Informática
Sala de Grados • 13 de junio de 2012 • 15: 00
entrada libre hasta completar el aforo

resumen:

Frame information is a key component in the specification of object-oriented programs. In particular, each method has to specify which heap locations it accesses, and which access permissions it gives back at the end of the execution. These access permissions are widely used in several program verification approaches (e.g., separation logic and implicit dynamic frames) to simplify framing and to provide a basis for reasoning about concurrent code. Various systems (e.g., fractional permissions) have been proposed during the last decade. However, the process of annotating the code with access permissions could be quite difficult and time-consuming. In this talk, we propose a new system to automatically infer access permissions via abstract interpretation. Starting from a program that contains no annotation, we infer a symbolic over approximation of the permissions owned for each heap location at each program point. A system of linear constraints is then inferred following the standard semantics of access permissions. Finally, linear programming is applied to solve the system, obtaining permissions that are (i) strong enough to perform the heap accesses contained in the program, and (ii) as weak as possible. Our approach is parametric in the permission system and supports fractional, counting, and Chalice permissions. Experimental results demonstrate that our system is fast and is able to infer almost all access permissions for our case studies.

sobre Pietro Ferrara:

Pietro Ferrara received a PhD in 2009 from the Polytechnique/Ecole Normale Superiore (Paris) and Universita' Ca' Foscari (Venice), under the supervision of Prof. Radhia Cousot and Prof. Agostino Cortesi. After completing his PhD he was a postdoc at the Chair of Programming Methodology at ETH Zurich with Prof. Peter Müller, and since February 2012 he holds a lecturer position at ETH. Pietro's main research interests are focused on the static analysis of multithreaded and object-oriented programs via abstract interpretation. His research included development of several static analysis tools such as: Sample, Static Analyzer of Multiple Programming Languages; and Checkmate: Static Analyzer for Java Multithreaded Programs.