Hacking program analysis: a systematic approach to code protection

(Invited Talk)

Roberto Giacobazzi
Università di Verona, Italy
roberto.giacobazzi@univr.it

The talk concerns the design of code protecting transformations for anti reverse engineering applications. This is a gentle introduction for non-specialists to some of the results and studies I made in the last years on the limits and possibilities of making analyses imprecise by systematic code transformation. These technologies are widely used in code protection (e.g., IP protection or key protection), malware design, anti tampering, code watermarking and birth-marking of code. The battle scenario involves attackers intended to extract information by reverse engineering the code, and protecting code transformations modeled as distorted compilers devoted to inhibit these attacks. Attacks are inhibited by maximizing imprecision in all attempts made by the attacker to exploit control and data-flow of the obscured code. After a brief survey on the state of the art in the field, we introduce a model for code obfuscation which is general enough to include generic automated static and dynamic attacks. Protecting transformations are then systematically and formally derived as distorted compilers, obtained by specializing a suitably distorted interpreter for the given programming language with respect to the source code to protect. The limits of these methods are shown in the context of computational theory. Interestingly this distortion corresponds precisely to defeat the potency of the expected attacker, which is itself an interpreter and whose potency consists in its ability to extract a complete and precise view of program's execution.

Short Bio: Roberto Giacobazzi received the Laurea degree in Computer Science in 1988 from the University of Pisa, and in 1993 he received the Ph.D. in Computer Science from the same university, with a Ph.D. thesis on Semantic aspects of logic program analysis, under the supervision of Prof. Giorgio Levi. From 1993 to 1995 he had a Post Doctoral Research position at Laboratoire d'Informatique (LIX), Ecole Polytechnique (Paris) in the equipe Cousot. From 1995 to 1998 he was (tenured) Assistant Professor in Computer Science at the University of Pisa. From May 2000 until now he is Full Professor in Computer Science at the University of Verona. The research interests of Roberto Giacobazzi include abstract interpretation, static program analysis, semantics of programming languages, program verification, abstract model-checking, program transformation and optimization, digital asset protection, code obfuscation, malware detection, software watermarking and lattice theory. He has been Program Chair of SAS, VMCAI, of workshops in programming languages and language based security, and General Chair of ACM POPL2013. He was in the Steering committee of SAS and ACM POPL.

Submitted to:
VPT 2019