Facultad de Informática
Universidad Complutense de Madrid

ANUNCIO DE CONFERENCIA

Formal certification of code-based cryptographic proofs.

Dr. Gilles Barthe

IMDEA Software, Madrid.

Sala de Grados • 17 de marzo de 2009 • 16: 00

entrada libre hasta completar el aforo

resumen:

As cryptographic proofs have become essentially unverifiable, cryptographers have argued in favor of systematically structuring proofs as sequences of games. Code-based techniques form an instance of this approach that takes a code-centric view of games, and that relies on programming language theory to justify steps in the proof---transitions between games. While these techniques contribute to increase confidence in the security of cryptographic systems, code-based proofs involve such a large palette of concepts from different fields that machine-verified proofs seem necessary to achieve the highest degree of confidence. In an inspiring paper, Halevi convincingly argued that a tool assisting in the construction and verification of proofs is necessary to solve the crisis with cryptographic proofs.

CertiCrypt is a framework to construct machine-checked code-based proofs in the Coq proof assistant. CertiCrypt achieves many goals of Halevi's ideal tool. At the same time, it brings a formal semanticist perspective on the design of the tool, and in particular ensures the highest guarantees with the smallest trusted base. The main characteristics of CertiCrypt are:

* Direct and faithful encoding of code-based techniques.
* Support for code-based proofs.
* Complete and independently verifiable proofs.

The talk shall describe the design of CertiCrypt and its applications to machine-checked proofs of encryption and signature schemes.

sobre Gilles Barthe:

Gilles Barthe received a Ph.D. degree in Mathematics from the University of Manchester, UK, and an Habilitation a diriger les recherches in Computer Science from the University of Nice, France. He is currently a research professor at IMDEA Software.

His main research interests are formal methods, programming languages, software security, cryptography, and foundations of mathematics and computer science. He has published over 80 refereed papers in these areas.

He has been coordinator of many national and international projects, and is currently scientific coordinator of the FP6 FET integrated project "MOBIUS: Mobility, Ubiquity and Security" for enabling proof-carrying code for Java on mobile devices.

He also served on the programme committee of a large number of conferences, and is an editor of the Journal of Automated Reasoning.