UNIVERSIDAD COMPLUTENSE MADRID

Facultad de Informática

ANUNCIO DE CONFERENCIA

Term Rewriting applied to Cryptographic Protocol Analysis: the Maude-NPA tool

Prof. Santiago Escobar. DSIC, Universitat Politècnica de València

Facultad de Informática
Sala de Grados • 14 de marzo de 2016 • 15:00
Entrada libre hasta completar el aforo

Resumen:

Maude-NRL Protocol Analyzer (Maude-NPA) is a tool for the symbolic analysis of cryptographic protocols. It searches backwards from a pattern defining secrecy, authentication, or indistinguishability properties of a protocol and it is able to find an attack or prove the absence of any attack. Maude-NPA is designed to take account of the algebraic properties of the crypto systems involved (e.g., exclusive-or, Diffie-Hellman, etc.) in order to give a more complete representation of both the protocol and the attackers capabilities. During the development of the tool we have also defined new theoretical and practical frameworks such as variant-based unification, logical model checking, asymmetric unification, or state-space optimizations that will be presented during the course.

Sobre Santiago Escobar:

Santiago Escobar is associate professor at the Universitat Politècnica de València (UPV), Spain. His research interests include formal methods, security, verification, model checking, rewriting, narrowing, and evaluation strategies. His works on narrowing have become essential for narrowing-based applications such as equational unification, model checking, or protocol analysis. In the security area, he has developed the Maude-NPA cryptographic protocol analyzer in collaboration with Catherine Meadows from the Naval Research Laboratory of Washington D.C. and Jose Meseguer from the University of Illinois at Urbana-Champaign. This is the state-of-the-art tool for verification of protocols with advanced cryptographic properties. He has published more than 60 papers on conferences and journals on formal methods, verification, and security. He has been program chair of specialized workshops on unification (UNIF 2015 & 2012), rewriting logic and applications (WRLA 2014), reduction strategies (WRS 2011), functional and (constraint) logic programming (WFLP 2009), automated specification and verification of web systems (WWV'07&08), and security and rewriting (SecReT'08). Dr. Escobar received a M.Sc. in 1998 and a Ph.D. in Computer Science in 2003 at the Universitat Politècnica de Valencia. For further details: http://www.dsic.upv.es/~sescobar