UCA Universidad de Cádiz

Facultad de Ciencias

Grado en Matemáticas - Departamento de Matemáticas

Actividad Formativa del Programa de Doctorado en Matemáticas

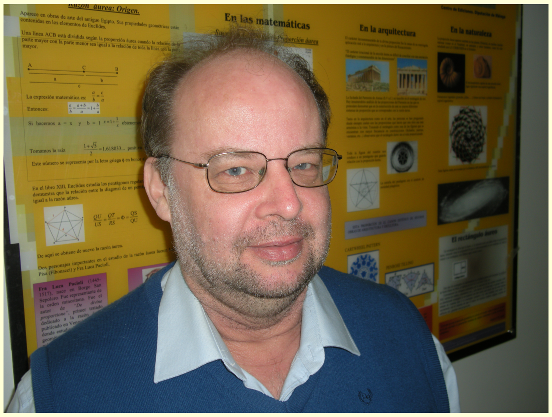
ANUNCIO DE CONFERENCIA

AUTOMATIC TOOLS FOR SECURITY PROTOCOL ANALYSIS

a cargo de

Jozef Jirasek

Faculty of Science, Institute of Computer Science,
Pavol Jozef Šafarik University in Košice (Eslovaquia)



Security protocols are communication protocols that use cryptography to achieve goals such as authentication and key distribution. Even when security protocols have been developed carefully, often some flaws may be found in them later. Analyzing security protocols consists of two complementary activities. The first is to find flaws in those protocols that are not correct, and the second is to establish the correctness of those that are. Several analyses based on logics of knowledge and belief (BAN, GNY) and model checking are known, some of them were automated or semi-automated. In the talk, we discuss the possibilities of use these analysis to develop automatic tools for verification of protocols security.

Día y hora: Viernes, 12 de abril de 2013, a las 11h30'.
Lugar: Sala de Grados de la Facultad de Ciencias, Puerto Real.

Financiación: III Plan Andaluz de Investigación, Grupo de Investigación *Análisis Teórico y Numérico de Modelos de las Ciencias Experimentales*, FQM-315. Máster de Matemáticas.