ConferenciaTítulo: "Security Analysis of Separation Kernels Specifications and a Framework for the Verification of Concurrent Implementations"

Autor: Dr. David Miguel Sanán Baena, investigador en la Nanyang Technological University en Singapur.

Abstract: Due to the new trend of integrating safe and secure functionalities into one separation kernel, security analysis of ARINC 653 as well as a formal specification with security proofs are thus significant for the development and certification of Separation Kernels (SKs). In this talk we present a specification development and security analysis method for ARINC SKs based on refinement. We present a security model for event-based non-Interference and a stepwise refinement framework that will allow us to check security on sequential SKs specifications. Moreover to be able to reason on SKs implementations running on top of multi-core architectures it is essential to deal with the interference of the environment between SKs instances running on different cores. Concurrent program reasoning techniques such as rely-guarantee can be leveraged to reason on multi-core SKs implementations. However the source code of the programs to be verified often involves language features such as exceptions and procedures which are not supported by the existing mechanizations of those concurrent reasoning techniques. CSimpl, is a rich specification language with concurrency-oriented language features and verification techniques that will allow reasoning on multi-core SKs implementations.