# Becas colaboración curso 2017/2018

*Fecha: 05 Julio 2017*

## Vicerrectorado de Investigación, Innovación y Transferencia

Subcomisión de I+D+i

Propuesta del departamento *SISTEMAS INFORMATICOS Y COMPUTACION*

**Núm Proyecto: *2017/32/00003***


**Responsable**
Escobar Román, Santiago

**E-mail**
sescobar@dsic.upv.es

**Ext.**
73556

**Responsable**
Alpuente Frasnedo, María

**E-mail**
alpuente@dsic.upv.es

**Ext**
79354


**Título proyecto**
Verificación automática de protocolos criptográficos de seguridad

**Valoración proyecto**
4

**Descripción proyecto**
Este proyecto tiene como objetivo verificar diversos protocolos de seguridad existentes utilizando una herramienta avanzada y automática de verificación de protocolos.

**Actividades a realizar por el alumno**
La herramienta Maude-NPA es una herramienta de verificación de propiedades de secreto y autenticación en protocolos de comunicación con propiedades criptográficas que ha sido desarrollada en la UPV en colaboración con la universidad de Illinois en Urbana-Champaign de EE.UU. y la Marina de los EE.UU.
La mayoría de los protocolos a analizar tienen ataques ya conocidos y el objetivo es comprobar si la herramienta Maude-NPA es apropiada para el modelado y verificación de protocolos con distintas propiedades.
Las tareas concretas conllevan modelar la lógica de los protocolos en la herramienta, especificar propiedades y luego verificar si se cumplen las propiedades o hay fallos de seguridad.

**Horario**
El horario es libre y se decidirá con el alumno