DOCTORATS INDUSTRIALS

EL PLA DE DOCTORATS INDUSTRIALS

PROJECTE DE DOCTORAT INDUSTRIAL EXPEDIENT 2016 DI 056

DADES DE L'EMPRESA I DE L'ENTORN ACADÈMIC

Títol del projecte
Analysis of communication and manipulation protection in an automotive environment Car2X

Empresa
SEAT, S.A.

Responsable de l'empresa
Guillermo Marti

Universitat
Universitat Rovira i Virgili

Director/a de tesi
Jordi Castellà Roca

Treballador/a de l'empresa i doctorand/a
Ana Cristina Hernandez Gomez

BREU DESCRIPCIÓ DEL PROJECTE DE RECERCA

In the IoT (Internet of Things) era, the integration of wireless communications in the automotive environment is growing due to its significant advantages. For example, users (mobile phones), cars, components, etc. can establish a fast and easy connection in order to perform a certain task without requiring a physical connection.

Wireless environments offer big opportunities but they also bring important threats. More specifically, attackers can perform their operations with no direct contact with devices or components that were inaccessible previously. As a result, an insufficient level of security in one of these devices may be enough to compromise a whole system and an attack (manipulation) can lead into a malfunction and/or a lack of safety for the users. Therefore, it is mandatory to design a wireless connected vehicle considering all the threats that may come from external entities (other vehicles, infrastructures, mobile phones, etc...) and may compromise the safety of the vehicle.

As a first step in this path, we will study the current status of possible attacks on connected vehicles and on their communications. In this stage, we will identify and classify all the security threats and we will prepare a complete state of the art of the current solutions designed to deal with them. The completion of this task allows the preparation of new and better solutions and strategies that will increase the privacy of

the customers and the security of swarm intelligence. Due to the fact that any proposed method will be executed in a vehicular platform, we will also perform a study of hardware based cryptographic modules for modern connected cars and hardware security modules used in automotive software projects.

The designed/proposed security solutions will depend, among others, on the computing power of the existing hardware (chips), so that it can be obsolete during the life cycle (of about 7 years) of the product (i.e. car). A trusted software and secure over the air update strategy will be therefore be necessary to be also studied and planned, framed under hardware security modules in automotive software projects and automotive security engineering standards, avoiding or detecting intrusion and responding to it. As OEM is automotive cyber security testing and validation also of importance.

Finally, it is worth mentioning that, a key point to be considered during the research process is tackling the authentication and authorization user-car, i.e. what are the credentials of (each) system users or components necessary to carry out a secure and robust authentication and based on it.