Technology Transfer in Computing Systems

D3.17: Individual TTP17 abstract

Project no.:	609491
Funding scheme:	Collaborative project
Start date of the project:	1st September 2013
Duration:	36 months
Work programme topic:	FP7-ICT-2013-10
Deliverable type:	Report
Deliverable reference number:	ICT-609491 / D3.17
WP and tasks contributing:	WP 3 / all
Due date:	30/04/2015
Actual submission date:	15/06/2015
Responsible Organization:	UNIPI
Dissemination Level:	Public
Revision:	1.0

TETRACOM D3.17: Analysis of security risks & threats and design of a hardware secure module to perform cipher algorithms for automotive applications

*Luca Fanucci, Berardino Carnevale, Francesco Falaschi, Luca Crocetti (*University of Pisa, Italy*),*
Harman Hunjan, Samson Bisase (Renesas Electronics Europe Ltd, United Kingdom)

In the last years, the progress of automotive electronics has led to cars that are no longer mere mechanical devices but complex systems with a large number of interconnected elements. Furthermore, communication among cars and between cars and the external environment seem to be the next step in the Internet of Things evolution. The increased connectivity requires an improved level of security due to the high number of access points offered to a potential attacker.

The aim of this TTP is to merge the background of University of Pisa in the field of IP macrocell design and the experience of Renesas Electronics Europe Ltd in the automotive security environment to provide a secure IP for in-car network micro controllers. In particular, the target has been an Ethernet controller with cryptographic capabilities. Indeed, car industry is moving towards Ethernet backbones for in-car communication due to the high bandwidth, flexibility and reduced cost.

University of Pisa implemented an Ethernet Media Access Control (MAC) Layer compliant with the IEEE 802.1AE MAC Layer Security Standard (MACSec). The design trade-offs have been carefully evaluated taking into account the requirements and limitations of the automotive context: low area occupation, reduced software capabilities and high speed. The solution integrates a low area and low latency AES-GCM encryption core and a complete interface with the Logical Link Control (LLC) and Physical (PHY) Layers of the OSI model. Finally, several optimizations, from RTL to gate level, have been realized to meet the requirements in terms of area and timing.

The final implementation when compared with some state-of-art MACSec implementations and industrial products shows an optimization of at least 20% in terms of area occupation. Therefore, it represents an appealing trade-off for the resource-limited automotive environment. The product was finally delivered to Renesas Electronics Europe Ltd and the technology transfer phase has been started with the purpose of integrating the final result into Ethernet interfaces of the new generation of Renesas micro-controllers.

This TTP paved the way for future collaborations between University of Pisa and Renesas Electronics Europe Ltd. It will involve new MACSec products including the IEEE 802.1AEbn and IEEE 802.1AEbw standards. Future partnership will also embrace the development of secure IPs for additional automotive communication protocols (CAN, LIN, FlexRay…).