# Secure Communication in Vehicular Networks

## PRESERVE VSS Kit 1 Demo

M. Lagana[1], M. Feiri[2], M. Sall[3], M. Lange[4], A. Tomatis[5], P. Papadimitratos[1]
[1] KTH - Kungliga Tekniska högskolan, Stockholm, Sweden, Email: {lagana,papadim}@kth.se
[2] University of Twente, Enschede, The Netherlands, Email: m.feiri@utwente.nl
[3] Trialog, Paris, France, Email: michel.sall@trialog.com
[4] Escrypt, Munich, Germany, Email: mirko.lange@escrypt.com
[5] Hitachi Europe, Sophia Antipolis, France, Email: andrea.tomatis@hitachi-eu.com

***Abstract*— Security and privacy are fundamental prerequisites for the deployment of vehicular communications. The near-deployment status of Safety Applications for Intelligent Transport Systems (ITS) calls for strong evidence on the applicability of proposed research solutions, notably close-to-reality situations and field-operational trials. The contribution of our work is in this direction: We present a demonstration of the integration and the interoperability among components and security mechanisms coming from different Research and Development projects, as per the PRESERVE project. In fact, we show that the components of the SeVeCom and EVITA projects within the PRESERVE architecture lead to strong and practical security and privacy solutions for Vehicular Ad-hoc Networks (VANETs).**

***Keywords; Security, privacy, ITS, interoperability, PRESERVE, EVITA***

## I. INTRODUCTION

For Intelligent Transport Systems (ITS), vehicles and road-side infrastructure are equipped with on-board sensor devices, computers, and wireless communication modules. ITS rely on Vehicular Communications (VC), i.e. Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication, to enable transportation safety and efficiency and other applications [1].

Strong but also practical security enhancing mechanisms need to be integrated in the VC [2]. Privacy requirements need also to be addressed [3], especially with the frequent broadcasting of positioning information. This led to the Secure Vehicle Communication (SeVeCom) [4] and the Privacy Enabled Capability in Co-operative Systems and Safety Applications (PRECIOSA) [5] projects, as well standardization efforts by European Telecommunications Standards Institute (ETSI) [6], IEEE 1609 WG [7] and the institution of the Car2Car Communication Consortium (C2C-CC).

Nevertheless not only the VC have to be secured, but the vehicle internal communication buses should also be protected against tampering attacks [8]. The objective of the E-safety Vehicle Intrusion protected Applications (EVITA) project was to develop a secure automotive on-board network [9].

Based on the conclusions of past and on-going Field Operational Tests (FOTs), such as Système COopératif Routier Expérimental Français (SCORE@F), safety applications have reached a near-deployment maturity state. The Preparing Secure Vehicle-to-X Communication Systems (PRESERVE) research project [10] plays a crucial role in this direction, bringing in strong and practical security and privacy protection, notably in field testing. With all the above efforts, an integrated, comprehensive solution, and a practical evaluation, i.e. FOTs, towards deployment of an overall secure architecture for automotive networks.

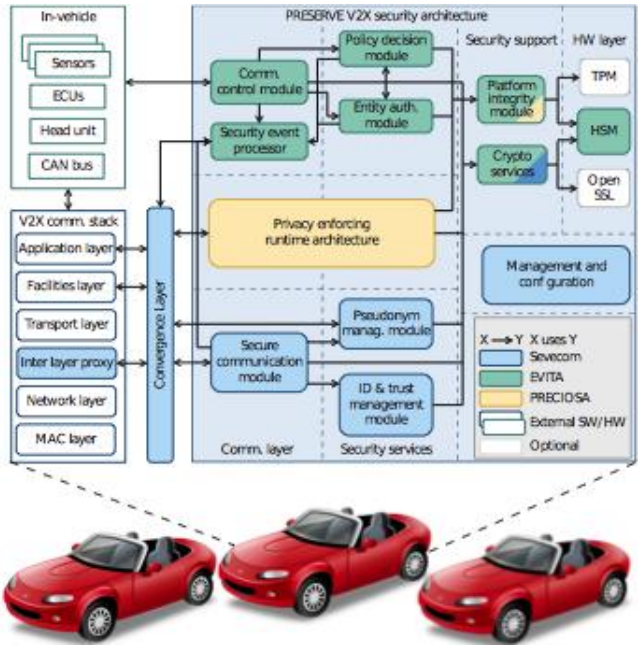


Figure 1. Illustration of the various components involved in the demonstration

In this paper we briefly describe the overall integration of components in Sec. II, notably to achieve interoperability between EVITA on-board system and the PRESERVE architecture. In Sec. III we describe the demonstration setup.

## II. SYSTEM DESCRIPTION

The system architecture for this demonstration is derived from the PRESERVE project. We have components from the vehicle on-board network plus secure communication capabilities. Figure 1 shows the relationships among components from the involved project [10].

### A. *On-Board Network*

Modern cars are equipped with several embedded Electronic Control Units (ECUs), which are interconnected via various vehicular buses. The exchanged information can be critical for the safety of the car itself or nearby vehicles. The EVITA project defines an architecture for automotive on-board networks, where security-relevant components are protected against tampering, and sensitive data are protected against compromise. To achieve this degree of security, a trusted Hardware Security Module (HSM) that provides generation and verification of Message Authentication Codes (MACs), is attached to each ECU.

### B. *On-Board Unit*

The vehicles are also equipped with an On-Board Unit (OBU) that runs the ITS applications, the communication facilities (i.e. radio, communication stack), and it is connected to the on- board network. The OBU is responsible for transmitting packets according to the ETSI GeoNetworking (GN) protocol, and it also integrates the IEEE 1609 standard. The OBU includes also the V2X Security Subsystem (VSS) that provides security services to protect on-board communication and external VC.

### C. *Hardware Security Modules*

The embedded ECUs and the VSS use a Hardware Security Module (HSM) to accelerate cryptographic primitives and securely store cryptographic credentials. Different HSMs attached to each ECU are defined in the EVITA project. The HSM dedicated to the VSS has been developed within the PRESERVE project in a form of Field-Programmable Gate Array (FPGA) that composes the VSS Kit 1.

## III. DEMONSTRATION SETUP

The proposed demonstration includes different devices, standing for two ITS vehicles acting as a transmitter and a receiver, respectively. We demonstrate the overall security and notably the secure V2V communication.

One vehicle is represented by: (i) a Laptop, running the on board network, (ii) a 802.11p modem with the GN communication stack and the PRESERVE module, to which (iii) the PRESERVE FPGA is connected, to enable the hardware accelerated cryptographic functions and secure storage. Laptops run a generic GNU/Linux operating system, and they host all the EVITA components, and interconnected internally. Each Laptop also hosts a Graphic User Interface (GUI) that displays the data and the related MAC, generated from the sensor and verified by the ECU, always using the EVITA HSM in software version. It also displays the vehicle's signature generation and verification. Figure 2 shows a screenshot of the GUI window.

Each Laptop is connected to a 802.11p modem via Ethernet cable. Those modems are usually x86, ARM, or PPC based devices, running a modified version of the GNU/Linux operating system. We included in the modems the GN protocol stack for VC, implemented by Hitachi Europe in the context of

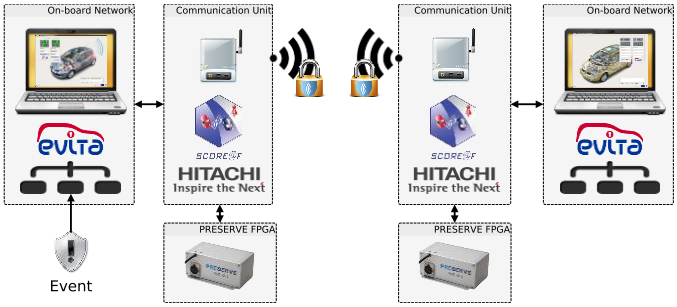


Figure 2. The whole demo setup and GUI that shows the triggered events and their transmission.

SCORE@F. The ECU will transmit the internally verified message to the GN stack, where it will be signed under the vehicle's current pseudonym and broadcasted over the 5.9 GHz wireless band. The ECU and the modem together constitute the OBU.

The message is then received by the second vehicle's modem and it is verified by the other FPGA, while going upstream in the GN stack. If the verification is successful, the message is forwarded to the ECU where a new MAC is attached, and it finally reaches the actuator that verifies the integrity. The overall setup is illustrated in Figure 2.

In conclusion, we provide a milestone towards the integration between multiple projects, to achieve a single consistent implementation of a secure and privacy-aware ITS architecture.

## REFERENCES


[1] P. Papadimitratos et al. 'Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation'. In: *IEEE Communications Magazine* 47.11 (Nov. 2009), pp. 84–95.

[2] P. Papadimitratos et al. 'Secure Vehicular Communication Systems: Design and Architecture'. In: *IEEE Communcations Magazine* 46.11 (Nov. 2008), pp. 100–109.

[3] F. Schaub, Z. Ma, and F. Kargl. 'Privacy Requirements in Vehicular Communication Systems'. In: *13th IEEE International Conference on Computational Science and Engineering* 3 (2009).

[4] R. Kroh, A. Kung, and F. Kargl. *SEVECOM - D1.1 - VANETs Security Requirements Final Version*. July 2006. URL: http://www.sevecom.org.

[5] PRECIOSA. *PRivacy Enabled Capability In Cooperative Systems and Safety Applications - D1*. Nov. 2009. URL: http://www.preciosa-project.org/.

[6] ETSI TR 102 638. *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions*. June 2009.

[7] IEEE 1609. *Family of Standards for Wireless Access in Vehicular Environments (WAVE)*. Sept. 2009.

[8] F. Stumpf et al. 'A Security Architecture for Multipurpose ECUs in Vehicles'. In: *25th Joint VDI/VW Automotive Security Conference*. Ingolstadt, Germany, Oct. 2009.

[9] B. Weyl et al. 'Securing vehicular on-board IT systems: The EVITA Project'. In: *25th Joint VDI/VW Automotive Security Conference*. Ingolstadt, Germany, Oct. 2009. URL: http://www.evita-project.org/.

[10] PRESERVE Project. *Security Requirements of Vehicle Security Architecture*. June 2011. URL: http://preserve-project.eu/.