Security of C–ITS Messages: a Practical Solution
The ISE Project Demonstrator

Pierpaolo Cincilla[1], Arnaud Kaiser[1], Brigitte Lonc[2], Houda Labiod[3],
Rémi Blancher[4], Christophe Jouvray[5], Richard Denis[6], and Antoine Boulanger[7]

[1]IRT SystemX, 8 avenue de la Vauve, 91120 Palaiseau, e-mail: FirstName.LastName@irt-systemx.fr
[2]Renault, 1 avenue du Golf, 78288 Guyancourt, e-mail: brigitte.lonc@renault.com
[3]Telecom Paristech, 46 rue Barrault, 75634 Paris, e-mail: houda.labiod@telecom-paristech.fr
[4]OpenTrust, 175 rue Jean–Jacques Rousseau, 92130 Issy-les-Moulineaux, e-mail: remi.blancher@opentrust.com
[5]Trialog, 25 rue du Général Foy, 75008 Paris, e-mail: christophe.jouvray@trialog.com
[6]Valeo, 43 Rue Bayen, 75017 Paris, e-mail: richard.denis@valeo.com
[7]PSA Peugeot Citroën, Route de Gisy, 78943 Vélizy-Villacoublay, e-mail: antoine.boulanger@mpsa.com

***Abstract*—Cooperative Intelligent Transport Systems (C–ITS) offer innovative ways of wireless communication between Intelligent Transport Systems (ITS) stations and ITS road–side stations. They favour the development of ITS applications to improve traffic management, road safety, mobility and other comfort services. C–ITS systems have to guarantee communication security, especially in heterogeneous network environments. Safety critical applications require authentication to avoid attackers to send spoofed or reforged information, nevertheless, cars and drivers privacy must be maintained.**

We present a demonstration of the C–ITS security management infrastructure of the ITS-Security (ISE) project [1]. Throught our demonstrator we show how ISE provides message authentication without violating cars and drivers privacy. Our demonstrator allows the public to run an attack scenario with and without the ISE security system, making evident importance of securing ITS communications.

***Keywords*—C–ITS, Safety, Security, Privacy, authentication, PKI.**

I. Introduction

C–ITS are new wireless networks that raise critical challenges involving driver safety and security. Security issues are related to geographic routing management and car heterogeneous connections to the infrastructure (e.g. roads) via Road–Side Units (RSUs) or cellular networks. Vehicle–to–Vehicle (V2V) communication has strong time constraints and reliability requirements in autonomous and connected vehicles environment where vehicles communication have to be ensured due to the sensitivity of exchanged information such as road accident, traffic jams or electronic emergency notifications.

As vehicles are connected to external networks, they become the prey of hackers and malicious users. That is, new communication interfaces and embedded electronics bring many threats and create new attack surfaces. Communication interfaces not only suffer from classical IT attacks such as Denial of Services (DoS) but are also vulnerable to new C–ITS specific attacks which concern the exchanged contents e.g. an illusion attack where the attacker takes the role/rigths of a more priviledge vehicle. In addition, connected cars communicate permanently between them by periodically broadcasting Cooperative Awareness Messages (CAMs) (also known as *beacon* messages) that contain relevant informations such as car position and speed. This makes possible for an attacker to track vehicles by eavesdropping on the communication channel [2], [3]. Vehicle tracking poses serious privacy issues because vehicle paths can reveal sensitive informations about the driver as its identity, residence, workplace, habits, etc [4]. For this reason, CAM messages are anonymized and signed using frequently changing certificates (called *pseudonym certificates*) [2].

Entities involved in message exchanges must be autenticated without violating their privacy. In our demonstator, we show how the Public Key Infrastructure (PKI) developed in the ISE project autenticates messages ensuring privacy (non–traceability) by using short–term pseudonym certificates. We tackle the PKI scalability challenge in order to be able to distribute thousands of new digital identities each second and manage billions of those digital identities. Moreover, compliance with European Telecommunications Standards Institute (ETSI) and Committee for European Normalisation (CEN)/International Organization for Standardization (ISO) security standards is considered to ensure the interoperability of our PKI.

II. IRT-SystemX ISE Project

The ISE project[1] is positioned to provide operational solutions to respond to new technological and economic challenges of automotive environment including cooperative V2V/Vehicle–to–Infrastructure (V2I)/Infrastructure–to–Vehicle (I2V) communications. We focus on design a management security system to support innovative use cases and services.

The ISE project aims at addressing the following challenges:

- Build affordable ITS systems and provide the guidelines for their deployment by implementing a security management infrastructure (PKI).
- Design system architecture such that it provides a good balance between security, safety, costs and scalability.
- Develop methods and tools for the design and validation of systems that promote trust between systems and cooperative applications (trust in the information

[1]ISE partners are: SystemX, Institut Mines–Télécom, OPENTRUST, PSA Peugeot Citroën, Renault, Trialog, Valeo and Oppida. Renault is the project coordinator.

received from other vehicles and infrastructure is crucial for integration into advanced driver assistance and automatic driving systems).
- Develop solutions (system architectures, platforms, applications, etc.) that are interoperable and allows vehicle roaming on the European road network.
- Assess the scalability of the proposed solutions.
- Support the emergence of autonomous vehicles.

Figure 1: Demonstration scenario: a car and a priority vehicle are approaching an intersection.

III. ISE demonstrator

Our proposed demonstrator shows the importance of securing ITS communications through an identity theft attack scenario.

A. Scenario description

Figures 1 and 2 show our demonstrator as it was set up for the Future@SystemX event [5]. The big screen in the background depicts the scenario. Two vehicles are approaching an intersection. Using V2V communications one of the vehicles identifies itself as being a priority vehicle (e.g. an ambulance) and requests priority. The other vehicle has to decide whether or not it lets the priority to the requesting vehicle.

The demonstrator is interactive: two persons play the scenario, one playing the known vehicle driver and the other playing the unknown vehicle driver. The latter chooses between playing an ambulance or a hacker (without telling his choice to the first player). The objective of the first player is to discover the true identity of the second player in order to react accordingly when he requests the priority. The scenario is played twice, first without security, then with the security mechanism activated. On the first run V2V messages are sent without signature so it is difficult for player one to determine whether player two is really an ambulance or not (and consequently if the priority request is legitimate). However on the second run, V2V messages are signed using PKI–based pseudonym certificates. Therefore, the first player can easily determine the true identity of the second player and reacts accordingly.

B. System description

Our demonstrator is composed of three entities: two On–Board Unit (OBU) that represent each one a vehicle and a laptop that shows the current state of the scenario (i.e., the big picture with the intersection). All three entities run Ubuntu 12.04 operating system and are connected to each other via a switch with Ethernet cables as depicted in Figure 2. They also host Firefox web browser as the interactive Graphic User Interface (GUI) is developed in html/javascript.

The OBU implements the PCOM embedded security stack that has been developed within the PRESERVE project [6]. PCOM stack is used to sign and verify outgoing and incoming V2V messages respectively, using ETSI ITS certificates as defined by the ETSI WG 5 in [7]. PCOM is open source and can be found online at [8].

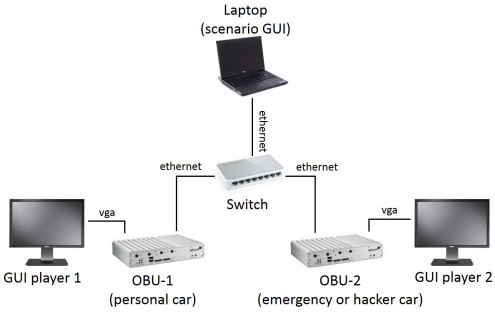

Figure 2: Demonstrator setup.

IV. Speakers biography

Arnaud Kaiser
Arnaud Kaiser obtained his Ph.D. degree in Computer Science from the University of Paris 13 in December 2011. He then joined the Communicating Systems Laboratory at the Atomic Energy Commission as a research engineer where he worked on IPv6 vehicular networks. Since October 2014, he works as a research engineer at the Institute for Technological Research SystemX on security aspects of cooperative intelligent transport systems.

Pierpaolo Cincilla
Pierpaolo Cincilla started his career at INRIA in 2009 as research engineer on Telex, a principled system support for collaborative applications. In October 2011 he started a Ph.D. at INRIA working on distributed systems, data replication, consistency and distributed databases. He obtained the doctoral degree in September 2014. From October 2014 he works as research engineer at the Institute for Technological Research SystemX on the scalability, safety, reliability and adaptability of C–ITS.

References

[1] "ISE Project," http://www.irt-systemx.fr/project/ise/?lang=en, accessed: 2015-03-30.

[2] S. Lefèvre, J. Petit, R. Bajcsy, C. Laugier, and F. Kargl, "Impact of V2X privacy strategies on intersection collision avoidance systems," in *IEEE Vehicular Networking Conference*, Boston, United States, 2013. [Online]. Available: https://hal.inria.fr/hal-00905936

[3] D. Forster, F. Kargl, and H. Lohr, "Puca: A pseudonym scheme with user-controlled anonymity for vehicular ad-hoc networks (vanet)," in *Vehicular Networking Conference (VNC), 2014 IEEE*. IEEE, 2014, pp. 25–32.

[4] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Achieving guaranteed anonymity in gps traces via uncertainty-aware path cloaking," *Mobile Computing, IEEE Transactions on*, vol. 9, no. 8, pp. 1089–1107, Aug 2010.

[5] "Future@SystemX," http://www.irt-systemx.fr/futuresystemx-2015-les-inscriptions-sont-ouvertes/?lang=en, accessed: 2015-03-30.

[6] "Preserve project," in *http://www.preserve-project.eu*.

[7] ETSI, "TS 103 097 v1.1.1 – Intelligent Transport Systems (ITS); Security; Security header and certificate formats," April 2013.

[8] "PCOM software," https://www.preserve-project.eu/vss-download, accessed: 2015-03-30.