17

Experimentation with the PRESERVE VSS and the Score@F System

Security and privacy enhancing technologies are an essential feature for ITS deployment. As the security system generally introduces an overhead, the test and evaluation of a defined security solution is as important as its design. In this context, the PRESERVE project aims to design, implement and test a secure and scalable security system for ITS. In this chapter, we focus on the PRESERVE security tests and precisely on the joint trial tests with the French Score@F FOT. We present the test cases of PRESERVE VSS integrated with Score@F FOT system and evaluate performance indicators. This is the first chapter to describe PRESERVE test cases and Score@F platforms integrating security solution.

17.1. Introduction

Intelligent Transportation Systems (ITS) will enable new cooperative applications, e.g. Road Hazardous Signaling, to improve road safety, traffic efficiency and increase passengers comfort. To achieve this, specialized equipment, the so-called ITS-Stations (ITS-S), will be integrated in vehicles, roadside infrastructure units and central servers. Vehicle to vehicle (V2V) or vehicle to infrastructure (V2I) communications will allow the exchange of Cooperative Awareness Messages (CAM) and Decentralized Environmental Notification Messages (DENM). Based on the exchanged messages, the ITS-enabled applications will provide relevant information to the driver. ITS communications are based on ITS-S reference communication architecture described in ETSI standard EN 302 665 [ETS 10]. The ETSI communication architecture, which is shown in Figure 17.1, consists of four horizontal layers: access, networking/transport, facilities and

Chapter written by Rim Moalla, Brigitte Lonc, Gerard Segarra, Marcello Laguna, Panagiotis Papadimitratos, Jonathan Petit and Houda Labiod.

Traffic Safety, First Edition. Edited by George Yannis and Simon Cohen.

applications layers, and two cross entities one for security and the other for management.

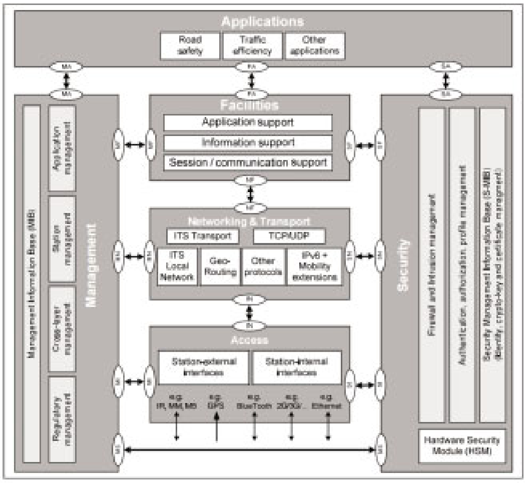

Figure 17.1. *Communication architecture of an ETSI ITS station [ETS 10]*

Without an appropriate design, a compromise of the ITS could have dire consequences: cyber-attacks could make transportation inefficient or put cars and drivers in danger; and ITS could easily give away the whereabouts of cars and thus drivers. That is why security and privacy enhancing technologies are an essential feature for the ITS deployment. This has recently been well understood.

As a result, many European projects dealt with security and privacy of vehicular communications, notably SeVeCom, DRIVE C2X, PRECIOSA and EVITA. Currently, PRESERVE is providing support for on-going Field Operational Tests (FOT) on cooperative ITS. PRESERVE contributes to the security and privacy of vehicular communications and ITS in general. PRESERVE specifies and develops a Vehicular Security Subsystem (VSS) that will be integrated in experimental projects, including, notably, Score@F in France. The Score@F project participates in the preparation of ITS deployment by evaluating standardized application messages (CAM, DENM and I2V messages) in different road environments through selected V2X cooperative driving use cases. Moreover, Score@F implements GeoNetworking protocol and Basic Transport Protocol (BTP) defined by ETSI for vehicular communication based on ITS G5, which is the European profile of IEEE 802.11p. For security and privacy issues, the Score@F system integrates the PRESERVE VSS.

As security generally introduces an overhead (communication and processing and complexity), we have to thoroughly test and evaluate our security system. In particular, we must be certain that the secured ITS remain practical and effective. For this, we have defined a set of performance indicators to evaluate and a test methodology and process to follow that we present in this paper. In fact, we start by internal tests of the PRESERVE VSS, in order to validate the security system *per se*. Then, we integrate the PRESERVE VSS with Score@F use cases, in order to evaluate the effect of security and privacy protection on the communication and networking. Finally, in parallel, we evaluate the effect of security on the performance of the cooperative applications. These tests will be done in two steps: first, in a static environment, and then in a real environment with mobile vehicles. The results of these tests will be the inputs for simulation in order to evaluate the scalability of PRESERVE solution.

The rest of this chapter is organized as follows. Section 17.2 provides an overview of our test methodology. Then, in the following section, we present our defined performance indicators which will be evaluated during joint trial tests with Score@F. In section 17.4 we detail security environments: we present Score@F use cases and platform, we give an overview of PRESERVE security system and we describe test sites. Section 17.5 concludes this chapter.

17.2. Test methodology

In order to determine the overhead introduced by our security system on processing and communication, three different security evaluation/analysis levels are specified. The first analysis level is cryptographic overhead analysis: these tests will evaluate the performance of the crypto-system, e.g. cryptographic delays for signature generation and verification operations. The second level of security evaluation consists of testing and evaluation of delays and overhead relating to the VSS internal processing. For example, for the signature verification process, we test and evaluate three different security policies: verify the signature only, verify the signature and the certificate of the sender and verify the signature and certification chain. Each security evaluation level will be done in two steps: first, in a static environment, and then in a real environment with mobile vehicles.

The third level of security evaluation is evaluation of end to end security overhead such as the time latency introduced by security system from the sender application to the received one. These tests will be done on a real environment with the presence or simulation of attackers. The results of these tests will be the inputs for simulation in order to evaluate the scalability of PRESERVE solution.

17.3. Performance indicators

We defined a set of performance indicators to evaluate our security system.

– Signature Generation Delay *SGD* (ms): the delay for generating one packet signature. This includes calculating a hash (HD) plus performing the actual digital signature generation operation. SGD = HD + SD.

– Signature Verification Delay *SVD (ms)*: the delay for verifying one packet signature. This includes verification of certificate chain plus calculating a hash (HD) plus performing the actual digital signature verification operation.

– Packet Signature Generations per Second *SGPS (1/s)*: for every packet sent, one needs to generate a suitable signature, i.e. SGPS = OPSS. We assume that every packet needs to be signed, which is true at least for CAMs and DENMs, if we do not apply omission schemes.

– Packet Signature Verifications per Seconds *SVPS (1/s)*: for every signed packet received, one needs to verify the signature plus the certificate.

– Pseudonym Change Delay *PCD* (ms): the additional delay introduced when the ITS station switches from one pseudonym certificate to another. It is measured as additional time added to signature generation for a packet.

For performance indicators evaluation we fix points and sensors within the PRESERVE V2X Security System where measurements need to be taken. We also introduce measurement points on the communication stack especially on the Networking and transport layer where VSS is integrated.

17.4. Test environment

17.4.1. *Score@F applications and platform*

Score@F is the French FOT for Cooperative intelligent transportation systems (see [SCO 11, GER 13, JAC 11]). Cooperative ITS systems are based on local wireless communication systems that enable direct two-way communication between vehicles and road infrastructure units (V2I) and between vehicles (V2V). This project aims to develop and validate the standardized ITS communication architecture [ETS 10] and to conduct Field Operational Tests on motorway and CG78 road environments.

SCORE@F project has been assessing applications belonging to three service domains such as represented in Figure 17.2 below. Road safety applications are mainly the signalization of immediate hazards to drivers. Several use cases have been assessed such as road works, stationary vehicles, human presence on motorway, traffic jam ahead and bad weather conditions. A few collision risk warning use cases (electronic emergency brake light, signal violation and wrong way driving) have also been tested in SATORY controlled environment.

Traffic management applications have also been assessed on the request of road operator partners. This includes the collect of traffic data from standard safety messages (CAM & DENM), the provision of the processed data to traffic management center using DATEX II and the immediate feedback of traffic management center through contextual speed and In-Vehicle Signage information to act immediately on the vehicle flows.

Some mobility services have been assessed such as Electronic Hitchhiking enabling a pedestrian to broadcast with his or her smartphone a car-pooling request or the broadcasting of Point of Interest notification facilitating the mobility or achieving the promotion of local businesses. These two categories of applications included some multimedia dissemination (audio, photo and video clip).

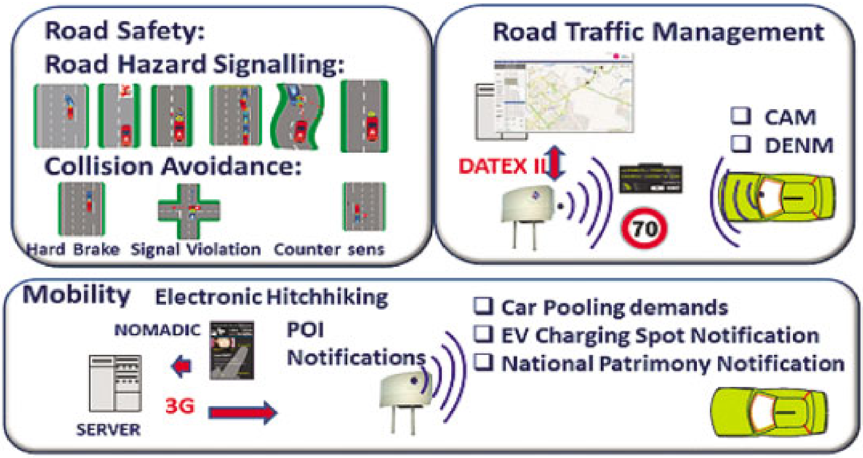

Figure 17.2. *Score@F use cases*

However, the system was tested on two different platforms presented in Figure 17.3. The first platform is formed by two units: an application unit regrouping applications and facilities layers. This application unit is a Nexcom VTC6201. The application unit communicates via Ethernet to the IEEE 802.11p modem, which is a DENSO or COHDA modem. An implementation of the Geo-networking and BTP protocols is integrated on the modem. The application unit retrieves the vehicle data via CAN adapter and vehicle position on the road via camera. The second platform is formed by only Nexcom VTC unit, which integrates an ITRI card as a G5 modem. In both the platforms, an Android tablet is used as a HMI for user field tests.

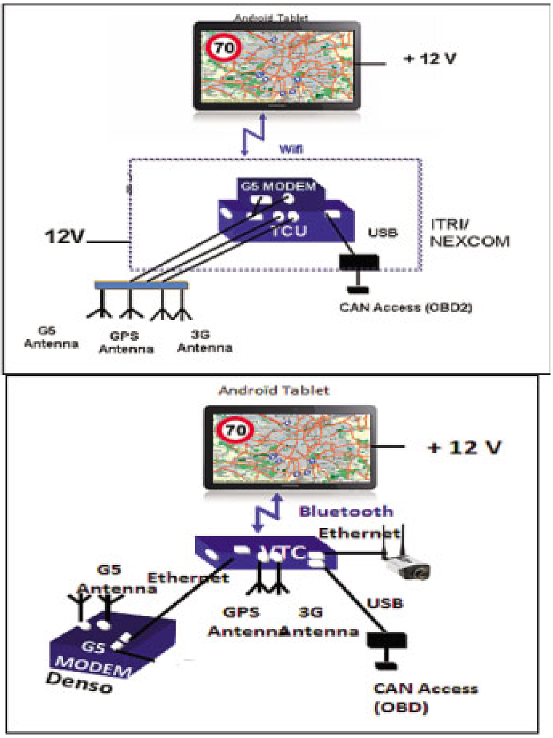

Figure 17.3. *Score@F platforms*

17.4.2. *PRESERVE system*

PRESERVE develops a complete security and privacy solution for V2X communication including an onboard V2X security subsystem (VSS) that will be integrated on ITS-S and an offboard PKI composed of three certificate authorities: RCA, LTCA and PCA. The VSS will integrate results from the SeVeCom, PRECIOSA and EVITA. PRESERVE develops three versions for the VSS: (1) only software security solution, (2) software and FPGA security system and (3) a security ASIC. For the moment, the VSS includes just four modules: secure communication module, pseudonym management module, identity and trust management module and management and configuration. Further modules dealing with privacy enforcing and in-vehicle security will be integrated later. During PRESERVE and Score@F test sessions, we test the VSS software kit and the FPGA-based HSM kit. Regarding PRESERVE PKI, we evaluate PKI performance and test it following test cases detailed in the next section.

17.4.3. *Test site description*

We conducted four joint test sessions; the first two sessions were conducted on a controlled test area which is the Satory track presented in Figure 17.4. This site, owned by the Defense Ministry and managed by Nexter, provides a set of three different tracks from 2 to 4 km, which reproduce a large variety of road situations. The site is equipped with two RSUs covering the whole area and we equipped the two vehicles with the VSS FPGA based version. These tests are conducted only for PRESERVE system validation which is why we tested only signature generation and signature verification functionalities.

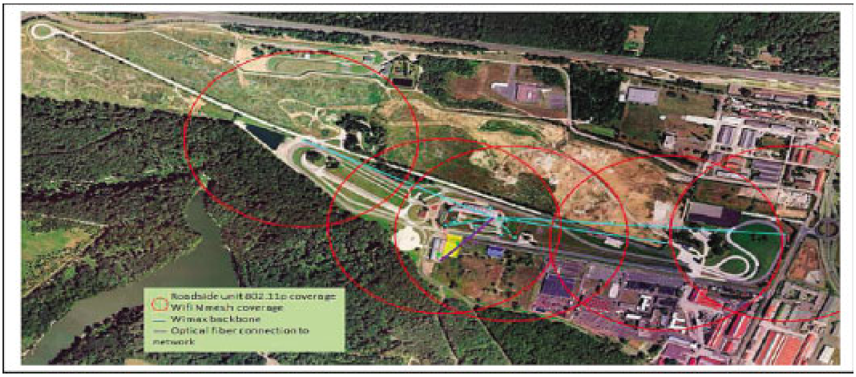
Roadside unit 802.11p coverage
Wifi N mesh coverage
Wimax backbone
Optical fiber connection to network

Figure 17.4. *Satory test site. For a color version of the figure, see www.iste.co.uk/jacob/safety.zip*

The last two test sessions, held in May and September 2013, were conducted on the Yvelines – Versailles open road site including a section of RD91 of 3.5 KM with five RSU and two vehicles. RSU are set-up from the RD91/RN12 exchanger at Versailles up to the Georges Besse place in Guyancourt, entrance of the Renault Technology Center. This portion, located in a peri-urban/rural area has several interesting configurations. The tested vehicles were equipped with a software-based version of PRESERVE VSS and RSUs were not equipped with PRESERVE. The main objectives of these tests are demonstrating the correct behavior of the whole system in a realistic FOT environment including stations equipped with PRESERVE VSS and others that are unequipped. We integrated the PRESERVE VSS software based on the GeoNetworking stack on both Score@F platforms, one Score@F platform per test session. During these tests, we conducted functional test cases and attack scenarios that we describe in the next section.

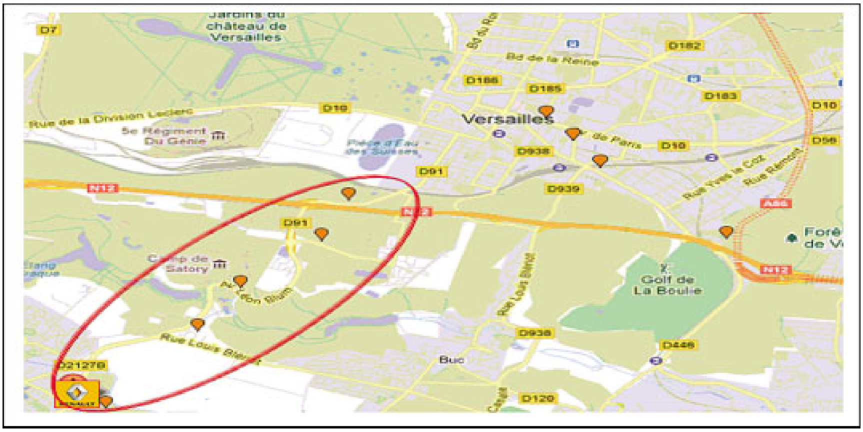

Figure 17.5. *Yvelines – Versailles test site*

17.5. Test case description

We present the use cases tested on PRESERVE and Score@F joint tests. Use cases are split into functional use cases that check the correct functionality and attack use cases that are evaluating behavior of the VSS under certain attacks.

17.5.1. *Functional tests*

In this section, we present functional test cases that we conduct on the last PRESERVE and Score@F joint test session. We give a detailed description of each test case and we indicate which performance indicators are evaluated on each test.

Generation of signed message: on the different test sessions, all messages generated by Score@F use cases and sent over G5 are signed. The purpose of this test case is to evaluate at first the signature generation delay as crypto delay evaluation and next to evaluate packet signature generations per second. In fact the generation of a signed message may require a pseudonym change processing before the signature generation. The packet signature generations per second depends on the VSS processing delay and on the communication (GeoNetworking) stack policy.

Verification of signed message: when the GeoNetworking stack receives a signed packet, it sends it to the VSS for signature verification. The signature verification operation normally includes certificate chain verification. The VSS implements several verification policies. Indeed we can just verify the signature of the received message, we can verify the signature and the certificate of the sender and we can verify the signature and all the certificate chain. We first select the verification policy on the VSS configuration file and then evaluate the signature verification delay for each policy.

Pseudonym certificate change: for privacy requirements, the ITS-Vehicle has to change the pseudonym certificate. The PRESERVE VSS and precisely the pseudonym management module triggers the pseudonym change depending on its pseudonym change policy. Two pseudonym change policies are implemented on PRESERVE VSS; the first one consists of changing pseudonym after a period of time predefined by the administrator. The second policy is based on the number of times a pseudonym is used. We select first the pseudonym change policy on the configuration file of PRESERVE VSS. As prerequisites for this test case: the VSS has a non-revoked/expired long term certificate and has at least two valid pseudonym certificates. When the VSS triggers a pseudonym change all layers of the communication stack have to block message generation. The VSS has to change the pseudonym certificate and the new certificate is preloaded on the VSS. The pseudonym change must be synchronized with the change of identifiers on all communication layers (MAC address, GN ID and station ID). As a result of the pseudonym change test, the VSS has a new pseudonym certificate that is used to sign outgoing messages and the communication stack has a new identifier on each layer. The purpose of this test case is to evaluate the pseudonym change delay, which includes processing delay of communication layers for changing their ID.

Pseudonym certificate refill over 3G: when the number of pseudonym certificates stocked on the VSS reaches a predefined threshold, the VSS has to download a new set of pseudonym certificates. In this stage, we test only the pseudonym certificate refill over 3G but we plan to test the pseudonym certificate refill over G5 in the next test sessions. This test case allows us to evaluate the PRESERVE PKI performance and to validate some VSS functionalities. An adequate PKI implementing three certificates authorities is mandatory for this test case. Moreover, the certificate of each certificate authority has to be stored in the vehicle VSS memory and be valid (not revoked, not expired). The vehicle must have a non-revoked or expired long term certificate and must be equipped with a 3G connector. For pseudonym certificates refill, the VSS generates one or several new ECC key pairs. The generated public keys are included in the signed and encrypted pseudonym certificate request generated by the VSS. This request is then sent over IP/3G to the PCA which validates it in collaboration with the LTCA. If the request is verified, the PCA generates a set of pseudonym certificates and sends it back to the vehicle. The new pseudonym certificates must be securely stored on the VSS. The main objectives of this test are to evaluate the delay for a pseudonym request generation on the vehicle and the processing delay for pseudonym request verification and pseudonym certificates generation by the PKI.

17.5.2. *Attack tests*

Securing the cooperative ITS should not have negative effect on the normal system operation and, therefore, the security functions introduced by PRESERVE should be transparent to the running applications and facilities. The functional tests described in the previous section aims to evaluate the correctness and the performances of those functions under normal conditions, while in this section we describe the test case that includes the presence of an adversary.

An extra payload that carries the security header is added to the messages, and a processing delay is expected for the generation and verification of such a payload. We consider the case where the attacker tries to exploit this delay and attempts to temporarily or indefinitely interrupt or suspend services of an ITS-enabled host. To be able to achieve this goal, the attacker usually saturates the target machine with messages that require computation on the receiver side, so much so that it cannot process the legitimate traffic. Such an attack leads to host "overload", and therefore we address this adversary as the "Overload Attacker".

The adversary saturates the target machine by forcing the consumption of computational resources, such as bandwidth or processor time. When using the security functionalities, those two resources are directly related: the more messages that are received, the more processing time is required. Therefore, the overload attacker needs to send data faster than the receiver is able to process.

To achieve this without deploying an expensive distributed denial-of-service attack over different machines, a single ITS station is deployed using a modified version of the PRESERVE VSS. Instead of running the CPU-intensive cryptographic operations needed to generate a valid signature, the modified version attaches an invalid, i.e. randomly generated, security header. This operation is orders of magnitude faster that the signature generation, and therefore it allows the adversary to overflow the receiver ITS. As a matter of fact, the receiver must still spend processor time to invalidate such a forged header.

During the normal operations, we enable an outsider ITS station to act as the overload attacker with the modified PRESERVE VSS. This device then starts broadcasting invalid messages to other ITS stations at a rate of 1,000 Hz. We then evaluate the impact of such an attack on the system by comparing the measurements of the packet processing time in the normal operations with the ones obtained during the attack. We consider the test successful if the performance degradation affects the applications and facilities only minimally.

17.6. Test results

During tests on the Satory track, we tested and validated the VSS software version and the FPGA based HSM version. The main result of these tests is that the FPGA is successfully integrated with the VSS software subsystem. Regarding tests on real environment, we collected the data for tests analysis. The data acquisition was done using different logging features, in PRESERVE VSS for the API and several modules of the VSS and also in the communication stack. As we completed our tests on 15 September 2013, we continued to analyze logging files for more detailed and end-to-end results. Table 17.1 describes our primary results.

Performances indicators	Results
Signature generation delay (ms)	2,50
Signature verification delay (ms)	33,40
Packet Signature Generations per Second	400
Packet Signature Verification per Second	30

Table 17.1. *Primary experimentation results of PRESERVE security solution within Score@F system*

In PRESERVE technical report 1 [PRE 13], we estimated target performance requirements for VSS, based on previous simulations studies and on load estimations for a standard scenario and a maximum load scenario in urban and highway traffic provided by SIM-TD. This resulted in the requirement of processing 1,000 verifications per second [PRE 13]. These results prove that a software security solution is insufficient for ITS security requirements. A dedicated hardware module for security solution is needed. That is why PRESERVE defines an ASIC for securing V2X systems. The ASIC was tested in 2015 (see [PRE 15]).

17.7. Conclusion

This chapter focuses on the cooperation between the PRESERVE project and the Score@F project, the result of which is the integration of a security system on a standardized ITS communication architecture. We conducted joint tests between PRESERVE and Score@F in order to evaluate the PRESERVE security system. This evaluation is based on our test methodology presented in this chapter and a set of performance indicators. The complete joint test session between the two projects was held in September 2013. The statically analysis of tests logging data of this recent test session is given in the paper. These are the primary results of the integration of PRESERVE VSS into Score@F FOT, and we expected more results as several test sessions were expected in 2014. We expected to have the complete results by the beginning of 2014.

17.8. Acknowledgments

This work was supported by the PRESERVE (PREparing SEcuRe VEhicle-to-X Communication Systems) FP7 European project under grant agreement no. 269994.

17.9. Bibliography

[EHR 13] EHRLICH J., SCOREF: une étape vers le déploiement des systèmes coopératifs en France, Séminaire 'Voiture connectée: un défi de l'Internet des objets', TélécomParisTech, Available at: http://www.telecom-paristech.fr/formation-continue/les-entretiens-de-telecom-paristech/vehicule-connecte-defi-internet-objets/seminaire.html, 4-5 Décembre, 2013.

[ETS 10] ETSI EN 302 665: Intelligent Transport Systems (ITS); Communication Architecture, v1.1.1, September 2010.

[GÉR 13] GÉRARD SÉGARRA, ALAIN SERVEL, Sue Bai: Fault Tolerant C-ITS for Road safety, ITS WC 2013, Tokyo, 2013.

[PRE 13] PRESERVE Technical Report 1: V2X Security Performance Requirements, v1.1, editor: Frank Kargl, 2013

[PRE 15] PRESERVE Deliverable 3.2: FOT Trial2 Results, editor: Carsten Rolfes, 2015.

[SCO 11] SCORE@F PROJECT WEBSITE, https://project.inria.fr/scoref/, 2011.