Towards a Cooperative ITS Vehicle Application Oriented Security Framework

R. Moalla¹, B. Lonc, H. Labiod, and N. Simoni

Abstract— Automotive industry is interested to ITS as it provides attractive services for connected vehicles aiming at creating a new and very promising business market. However, the security remains a major challenge for the ITS deployment as several critical threats have been identified. In this paper, we present our Cooperative ITS Vehicle Application Oriented Security Framework CIVAS for vehicle ITS stations. Our focus is given first to ITS vehicle security requirements and constraints. Then, we provide an overview of the “Defense-in-Depth” model that we adapted for securing ITS vehicle. The proposed security framework follows a modular design and is application oriented. To illustrate the interaction between designed CIVAS layers, we consider a vehicle stationary as example of a road safety use case.

Keywords— Cooperative ITS; security architecture; Defense-in-Depth model; ITS Vehicle Station.

I. INTRODUCTION

Intelligent Transport Systems (ITS) propose several cooperative connected services for the road users. ITS rely on Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I) and Vehicle-to-Device (V2D) communications. According to ETSI communication functional architecture [1], cooperative ITS applications built on exchanged information between ITS Station (ITS-S) enable road safety, traffic efficiency and infotainment applications. An ITS-S can be a vehicle, a roadside unit, a personal device or a server. Automotive industry is interested to ITS as it provides attractive services for connected vehicles aiming at creating a new and very promising business market. However, the security remains a major challenge for the ITS deployment as several critical threats have been identified.

Defining a security solution for ITS includes security system design, security mechanisms, standards selection and security operational processes definition. ITS security system considers two main parts: (1) the first part deals with on board communications security; (2) the second part is related to security infrastructure. The ITS-S security system is composed of software and hardware modules that build the security layer of the ITS-S functional architecture. The ETSI standardized functional communication architecture of ITS-S represents the security as a cross layer. As ITS applications are based on exchanged ITS messages, software applications running on ITS-S have to communicate over secure communication channels. Moreover, these applications need to be executed on top of a secure operating system and to be mapped to a secured hardware processing memory space.

In order to avoid critical ITS-S security attacks, an ITS-S security system has to fulfill several goals: securing ITS-S hardware, securing ITS-S software and securing ITS-S communication. Our proposal, which we term Cooperative ITS Vehicle Application oriented Security framework (CIVAS), seeks to address these challenges. Inspired by “Defense-in-Depth” model applied in information system, we define a security framework covering the whole ITS-S vehicle’s system and not only the communication part as it is usually adopted in other ITS security solutions. The proposed security framework ensures both security services for an ITS-S vehicle and security management services.

Fig. 1 illustrates the ITS-S vehicle architecture where the design follows two levels. Concerning the physical aspect, the system architecture considers an the ITS-S mounted on the vehicle and one physical unit where different applications categories are executed. Concerning the network level, the ITS-S communicates with electronic control units (ECUs) via in-vehicle networks (e.g. CAN). In fact, it is connected to ECUs and sensors that can either be exclusively connected to it (e.g. GPS) or shared with other in-vehicle systems such as speed sensor shared with ADAS calculators. The ITS-S vehicle is equipped with several radio interfaces (e.g. Bluetooth, Wi-Fi, ITS G5, 3G/4G) that allow wireless communication between the in-vehicle network and external devices.

The paper has the following structure. Section II gives an overview of the related works. Section III details the

¹ R. M. and B. L. Authors are with the DEA-SPC service in RENAULT, Guyancourt, FRANCE. (E-mail: [rim.moalla, brigitte.lonc]@renault.com). H. L and N. S authors are with Department of Computer Science and Networks, Institut telecom; Telecom ParisTech. Paris, FRANCE. (E-mail: [labiod, simoni]@telecom-paristech.fr).
security constraints and requirements on the ITS vehicle station. Section IV describes the designed functional security framework and details the interaction between the proposed layers. The last section discusses the conclusion and the future work.

II. RELATED WORK

ITS security is an emergent research topic. The literature study brings to light that, researchers often separate the security architecture works for external communications and the security architecture for embedded systems and internal communications in their studies. Hence, the following sections detail the main previous related works covering both V2V and V2I communications (named V2X communications) and In-vehicle communications.

A. Vehicle-to-X communications

The ETSI TC ITS WG5 and IEEE 1609.2 represent the active standardization groups in Europe and U.S that deal with security of vehicular communications. Several important projects deals with security architecture for V2X communications such as SEVECOM [2] and more recently PRESERVE [3]. There are also various papers covering V2X security architecture. In [4], authors propose a security framework based on a vehicular applications securing process. The presented functional layers are inspired from IEEE 802.1X. A well understanding of the architecture solution is given thanks to an implementation details specifying which layers of the proposed security architecture are parts of vehicle security system. In [5], Papadimitratos et al. present a security architecture for a secure beaconing, a secure neighbor discovery and a secure Geocasting in V2X systems. A dedicated hardware security module (HSM) and certificates are used for securing such type of V2X communications. In fact, the idea of using a dedicated security module has been introduced first in [6] for securing telematics platform in vehicle. SEVECOM project addresses the security and the privacy of V2X communications. In [7], Kargl et al. present the SEVECOM system architecture composed by four modules that address secure V2X communications and identity and key management. These modules rely also on HSM for cryptographic operations and storing sensitive data.

B. In-Vehicle communications

Several works have been carried-out identifying the lack of security in the in-vehicle networks [8] but a few projects deal with security solution for in-vehicle communications.

EVITA project [9] aims at securing automotive on-board networks. It developed its own secure platforms. In fact, it defined and implemented three different variants of HSM (high, medium and low) for securing on-board networks. Depending on the security requirement of each ECU, one of these HSM is integrated on the ECU. For external communications, the high HSM is required. EVITA project does not consider the Internet Protocol (IP) for in-vehicle communications between ECUs unlike SEIS project [10]. Moreover, the SEIS project defined a security middleware extension providing modular security services. It consists of three layers: a security decision layer, a security communication layer and a cryptographic processing layer.

C. Secure crypto module

The proposal of using a Hardware Security Module (HSM) for securing vehicular systems has already been introduced. In fact, in [5] authors propose the integration of HSM which is the basis of trust in both vehicles and roadside units. In [7], authors present the SeVeCom architecture which includes an HSM. The main requirements that an HSM implementation should meet in order to be applicable for securing vehicle communication systems are detailed. The EVITA project [9] has already defined and implemented three different variants of HSM for securing on-board networks.

Previous works deal mainly with the security of vehicle communications which is part of the ITS-S vehicle but do not address the complete system. In this paper, we propose a security functional framework for the whole ITS vehicle system; a real-time embedded and connected system. Compared to previous works and ETSI security architecture, we introduce boundaries protection functionalities, widely deployed in connected information system, for ITS vehicle system. In addition, we consider ITS applications and associated data, independently of their sources, as the main feature in securing such system. We adapt the “Defense-in-Depth” model for securing ITS vehicle system and designing our security framework based on security requirements and risks that we identify in [11].

III. SECURITY CONSTRAINTS AND REQUIREMENTS

There are several security challenges and constraints in ITS-S compared to classic connected devices such as computers. Differences connected to the very constrained environment, the applications features and the production processes induce specific ITS-S security constraints that we present on the following:

- Critical time constraints: alerts related to road safety applications and received by the ITS-S vehicles must be processed on real time. It is a very challenging task for application to send, to process and to receive messages on real time. Consequently, security mechanisms should be optimized to meet critical time constraints.
- Very low tolerance for errors: as errors on alerts, based on received information, could lead to physical damage and may affect the human life, ITS need trusted, exact and fresh information. Therefore, ITS applications are intolerable for errors.
- ITS-S vehicle is involved in a large scale of heterogeneous system: a large number of vehicles and road infrastructures will be communicating. Different manufacturers and automotive constructors will use different implementations.
- High mobility: vehicles move at a fast velocity changing the reception area of vehicles. Thus, ITS are highly dynamic environments.
• ITS-S vehicles have a long life that make hard to change the ITS-S devices as a reaction to new threats. Procedures to update and manage security mechanisms during the vehicle life cycle have to be defined to ensure the operation of ITS system. Moreover, security measures have to operate autonomously assuming that vehicle user has not technical interaction with the security system.

In [11], we present in detail the risk analysis study that we carried-out in order to evaluate risks in the ITS-S communication system. This study is very important to define an efficient security framework. In the following, we present the most relevant ITS security requirements. These security requirements and security challenges should be considered during the definition of both security architecture and protocols.

- **Availability**: ITS applications, particularly safety applications, require a high availability of the system.

- **Authentication and Authorization**: Authentication ensures that entities involved in communication are correctly identified and authentic. Entity authorization is necessary for the applications requiring the definition of the rights that an entity (vehicle or infrastructure) has.

- **Integrity**: Integrity is a main security requirement for ITS applications; especially for the Road Safety applications. It is ensuring the non-alteration of the information exchanged between sender and receiver.

- **Confidentiality**: Some ITS applications require that the content of a message should be accessible only for the sender and the receiver.

- **Non-repudiation**: it may be crucial in some cases (such as wrong information that can cause accident) not only to identify the sender but also to get the proof of the originator of the message (for accountability).

- **Privacy**: privacy is a major security requirement as ITS applications exchange personal data in particular location data over wireless communications. The design of ITS security solution must take into consideration some measures to ensure the protection of the personal data privacy. ITS applications must comply with European Directives relevant to the protection of privacy and data protection: the Directive 95/46/EC on data protection.

- **Plausibility**: plausibility checks are used to validate the correctness of the vehicle mobile data and can be performed in the received message information. For example, the claimed information state sent from vehicles must reflect their actual physical state.

### IV. COOPERATIVE ITS VEHICLE APPLICATION ORIENTED SECURITY FRAMEWORK: CIVAS

Our new functional security architecture (CIVAS) aims at securing ITS vehicle system. As ITS vehicle is a connected system to an internal vehicular network and to an external hybrid network. We choose to apply the “Defense-in-Depth” wireless approach widely deployed in the domain of network security for securing ITS vehicle system.

#### A. “Defense-in-Depth” model

“Defense-in-Depth” is an Information Assurance (IA) strategy developed by the National Security Agency (NSA) that involves multiple layers of defenses for networked electronic and systems security [12]. “Defense-in-Depth” approach consists in multiple layers of protection so that a breach in one layer only leads the attacker to the next layer of countermeasures. It helps to prevent direct attacks against critical systems and data, increases the likelihood of the attacker being detected. In automotive industry, applying security using the “Defense-in-Depth” principle is proposed in [13]. The suggested layered security solution consists on prevention, detection, deflection, and forensics approaches.

We choose to apply the “Defense-in-Depth” model for ITS vehicle system security because it is well adapted. Indeed, the vehicle is becoming more and more as a mobile information system. In fact, modern vehicles offer novel connected services which are based on interconnected embedded ECUs and wireless communication. Taking benefit from “Defense-in-Depth” model layers, we define a cross layered security framework for the connected automotive systems. Moreover, the defined functional layered framework covers security services like authentication, access control and integrity and security management functions such as system monitoring. The proposed security framework interacts through all levels of the system from applications, operating systems to hardware components. It covers also the security management functions during the system life cycle. In fact, the outer layers assure security management functions and policies while security mechanisms for system and data protection are in the innermost layers. We detail in the next section each layer of our CIVAS framework.

#### B. CIVAS functional layers

The functional architecture presented in figure 2 describes the decomposition of the ITS vehicle security system into a security services functionalities and a security management services functionalities. We place the data protection in the center of our security functional framework. Indeed, the main target of the attackers in the ITS-S vehicle system is to access to the system and its associated data. Nonetheless, the outer layers are concerned with the system operation and security management mechanisms. CIVAS takes into account a complete view of the connected ITS-S vehicle system.
The central layer is the data protection responsible for assuring the security of the stored, sent and received data. ITS data can either be a native software existing in the system or an exchanged information over wireless links with other ITS stations. This is important to deal with, since there are different data sources in ITS-S that provide different information which will be used by critical applications. In fact, the data can be generated by software and communications components and vehicle sensors. The ITS data protection layer deals with different tasks: secure software management, secure communications, secure storage, data plausibility and privacy protection. By securing software management, we target at the secure delivery, installation and removal of software components like road safety applications and secure wireless firmware update. For example, in [14], authors explain security challenges in automotive software update. Moreover, an ITS-S exchanges information and communicates either internally or externally with sensors and calculators or other ITS stations and devices respectively. Securing communications includes security of V2V, V2I, V2D and internal communications. To achieve this goal, we propose to support the security communication standards like IEEE 1609.2 and ETSI 103097 in securing V2X communications based on G5 technologies. We include also IPv6 security solution for ITS as defined in [15].

The secure platform layer is concerned with system protection enabling ITS-S to detect malicious manipulations on complete or critical parts of ITS-S. This layer acts as trust anchor for data protection layer. In fact, it performs secure boot and cryptographic operations and ensures secure storage of secret cryptographic keys. It provides also secure time base and secure random generation. We consider that a dedicated hardware module is needed to meet security performance requirements of ITS and to support this functional layer.

The boundaries protection layer presents prevention measures. It ensures that unwanted access, modifications and injections of messages on ITS-S are prevented. In fact, its main functions are the networks traffic monitoring, intrusion detection and system supervision. It protects ITS vehicle systems from other ECUs in vehicle and external devices. Firewalls, Intrusion Prevention System (IPS), Intrusion Detection System (IDS) and Honeypot can be deployed to support functions of this layer. These mechanisms and components for vehicle system protection are presented in [16, 17]. However, no integration and evaluation of these mechanisms in vehicle systems are given.

To meet different security requirements, an ITS-S security system should offer security management services in addition to the security services supported by functional layers described above. Our CIVAS framework is composed also by three functional layers related to security management. Indeed, an ITS vehicle security system interacts with security infrastructure components like Public Key Infrastructure (PKI) and transportation authorities.

Security policies layer is the first layer related to the security management services. It describes the rules for basic tasks of different security system functionalities. For instance, this layer regroups access control rules and it defines also security procedures for the system. As security policies are specific for each ITS-S system and each automobile constructor, the documents described security policies are confidential.

Analysis, audit and monitoring layer consists in logging information related to system security in order to analyze them. It is also responsible for auditing and monitoring the ITS-S system. Its main objectives are to verify the status of the whole security system, to detect system misbehaviours and to evaluate security policies. This layer collects and analyzes logging data and alerts the system administrator whenever a problem occurs. For detecting an abnormal or faulty system behavior, local misbehaviour detection mechanisms are also included. Following misbehaviour detection mechanisms, for example those presented in [18], the decision to initiate the revocation process is taken in this layer. Local detection and reaction is necessary to minimize the impact of malicious or malfunctioning ITS systems and ECUs. Security policies are then updated based on security events reporting.

Security management layer is responsible for managing identities and credentials, its related processing such as identities update. An ITS-S vehicle has usually two security identities types: a long term certificate and a set of pseudonyms certificates. Pseudonyms certificates are short term certificates that do not reveal the real vehicle identity. Moreover, pseudonyms certificates change frequently to ensure privacy protection. Pseudonyms certificate loading is essential function of credentials management for securing V2X communications. This layer is also in charge of security system management. The different security functionalities cited through previous layers are managed by this layer. For example, re-configure the firewall components and part of boundaries protection layer with new filtering rules. Security management layer includes PKI protocols for certificates updates, revocation and refilling and security procedures description like ITS-S parts certification.

C. Example

In this section, we present an example to illustrate the interaction between the different functional layers as shown in figure 3. To detail the security processing and exchanges
hold flows between functional layers of our designed CIVAS framework, we consider “stationary vehicle” use case. This road safety use cases consists in sending Decentralize Environmental Notification Basic Service Message (DENM) by a stationary vehicle with activated hazard lights in the defined relevance area.

To be able to send and receive V2X messages, ITS-S must be turned on and during the start-up step the secure platform layer perform a secure boot. This step is crucial as it ensures that ITS-S is a trusted device with secure software. If the secure boot is not completed, the ITS-S is not activated in order to avoid introduction of malicious devices. Procedures must be defined to remotely detect, assist and update ITS-S vehicle like remote diagnostic. After a successful boot, the security management layer checks if there are enough valid pseudonyms certificates stored in the ITS vehicle system. If no valid pseudonym certificate is stored, the secure platform layer generates a new short term key pairs and request security management layer to certify keys. Once the ITS vehicle system has valid security credentials, it is able to send ITS messages over ITS channels. In the stationary use case, the hazard lights activator sends internal message to the ITS-S vehicle. The boundaries protection layer verifies the access rights of this activator. The data protection layer checks the authenticity and plausibility of the received in-vehicle data. If information is erroneous, the event is signaled to analysis, audit and monitoring layer in order to inform the administrator and update the system. Otherwise, ITS-S vehicle checks the plausibility of vehicle dynamic data and constructs the DENM message related to signaled event. Before sending the message to vehicle neighborhood, the data protection layer formats a signed DENM message. This message is signed with a valid vehicle short term private key which is securely in the secure platform layer. The signature operation is then performed on this layer.

A neighbor vehicle controls received flow based on ITS-S boundaries protection mechanisms. Upon reception of the DENM message, the secure platform layer verifies the certificate of the sender and then the signature of the message. If the sender certificate is not included on the message and is not stored in the received vehicle, the security management layer is notified to send a request to the certificate sender. If the signature is verified, the data protection layer checks then the plausibility of the received data. If a sender misbehavior is detected, analysis, audit and monitoring layer notifies it in order to update security policies by prohibiting messages from this vehicle.

V. INTEGRATION AND IMPLEMENTATION

The standardized ETSI communication architecture presents security as a cross entity offering security services for ITS applications. This cross entity allows to instantiate security mechanisms suitable for each ITS use case. The communications security ensuring the security of data packets is also provided by this security entity. To integrate our designed security functional framework, we propose to implement a generic security functionalities in the cross security as shown in figure 4. A hardware security component assures functions of the secure platform layer and is a part of this entity. Other security functions require more information related to the application and communication environments such as plausibility checks, trust evaluation and pseudonyms certificates updates and changes. Facilities layer acts as a middleware for ITS applications and provides support for applications, information and communications in ITS-S. We propose to support this modular design for security requirements and to include a “security support module” in the facilities layer that ensures security related application functions cited above. Plausibility checks and trust evaluation, relevance for several ITS applications, are implemented into “security support module” within the facilities layer. Applications subscribe on the security support module if they require plausibility and trust evaluations services. This approach seems to be beneficial as plausibility check algorithms for example are independent to the application logic and diagram status. Security management services like pseudonyms certificates update and pseudonyms certificates change require also applications knowledge environment. As a first example, an ITS safety application can request a block of pseudonym change if the vehicle is in critical situation within the protection field area. Time and position information are supported by the facilities layer. As a second example that needs an application and management knowledge, we can cite pseudonyms certificate update over G5. We propose that ITS-S vehicle uses ITS-G5 free communication and takes advantage of the Internet Access Service (IAS) offered by ITS-S road side unit. In fact, ITS-S roadside broadcasts Service Announcement Message (SAM) to announce services that propose to neighbor ITS stations. ITS-S vehicle receiving SAM message announcing IAS can decide to securely download certificates from the security infrastructure using the ITS-S roadside as a relay.

The “security support module” that we propose to integrate into the facilities layer ensures plausibility checks, trust evaluation, pseudonyms certificates change and update. It is responsible of the interaction between security management services and ITS-S management entity. Moreover, the security entity supports this module via a security management application part of the security management layer.

To illustrate the flexibility of our integration approach, we propose a possible implementation based on the Score@F [19] platform prototype implementing the standardized ETSI ITS-S architecture. Actually, each module of Facilities layer is implemented as an OSGI Bundle. Bundles are activated to be available to different ITS use cases. We add a new security services related on plausibility check, trust evaluation, certificates change and certificates update in the facilities layer as new Bundles in the OSGI environment.
This work has been supported by the PRESERVE-PReparing SEcuRe VEHICLE-to-X Communication Systems-FP7 European project under grant agreement n°269994.

ACKNOWLEDGMENT

In this paper, we have presented our layered security framework for an ITS-S vehicle. The framework is based on a global system view of ITS-S vehicle as is common practice in system engineering. The proposed security architecture is inspired by the “Defense-in-Depth” approach in order to cover all parts of ITS-S. We propose the functional high level view, the dynamic view and the implementation view of the designed security framework. As next steps we will complete the CIVAS prototype implementation based on the integrated Score@F and PRESERVE platforms.

REFERENCES

[9] EVITA project Homepage: http://www.evita-project.org/
[19] Score@F project Homepage, https://project.inria.fr/score