Risk Analysis on C-ITS pseudonymity aspects

Farah Haidar, Arnaud Kaiser, Brigitte Lonc, Pascal Urien

Risk Analysis on C-ITS pseudonymity aspects

Farah HAIDAR[1,2,3], Arnaud KAISER[2], Brigitte LONC[1], and Pascal URIEN[3]

[1]*Renault*, Guyancourt, France, Email: firstname.lastname@renault.com
[2]*IRT SystemX*, Palaiseau, France, Email: firstname.lastname@irt-systemx.fr
[3]*Telecom ParisTech*, Paris, France,Email: firstname.lastname@telecom-paristech.com

***Abstract*—In the near future, vehicles will communicate with their environment by broadcasting Vehicle to everything (V2x) messages over the vehicular network (IEEE 802.11p). The exchanged messages contain data related to driver's privacy. As the laws in Europe require the privacy protection, the solution is to use pseudonym identities (certificates) in the communication. However, the use of these certificates can create new vulnerabilities that must be taken into account. In this paper, we do a state of art on the existing vulnerabilities, we applied the TVRA method and propose new vulnerabilities. Finally, we propose new countermeasures that could be implemented.**

***Keywords*—C-ITS, security, TVRA, Risk assessment, pseudonym certificate.**

I. Introduction

Tomorrow vehicles will communicate and cooperate by exchanging V2X messages in order to improve road safety and traffic efficiency. Enabling the communication in Cooperative intelligent transportation system (C-ITS) will create new vulnerabilities that must be taken into account. Standards in Europe and US propose to use a Public Key Infrastructure (PKI) in order to deal with security issues. The role of the PKI is to distribute and manage digital certificates. Despite the use of the PKI, some vulnerabilities remain feasible. In other words, the PKI protects against the external attackers, but vehicles with valid key materials may be also misbehaving.

One of the challenge of the C-ITS is the privacy protection. Safety applications rely on the kinematic data like position, velocity, identity etc ... Such data are considered private, they provide geo-localization of the driver. Indeed, these information can be collected and used by an attacker to track the vehicle and generate drivers profiles potentially. Standards organizations thus propose to use pseudonym identities in order to protect the privacy of the vehicles. However, the use of pseudonym certificates may create new vulnerabilities.

In this paper, we present some existing vulnerabilities on the C-ITS, we apply the Threat vulnerability risk assessment (TVRA) method and we proposed new vulnerabilities from the use of pseudonym certificates not existing in the literature. The results of our analysis is a list of vulnerabilities with their risk and finally, we propose some countermeasure in order to deal with these vulnerabilities.

The rest of paper is organized as follow: Section II presents the related work, section III presents the security architecture of the C-ITS, section IV presents the motivation of our work, section V presents the detailed method with application and proposed vulnerabilities, and section VI conclude the paper.

II. Related works

A risk assessment is used to identify and analyze potential threats and vulnerabilities. The risk assessment is important to understand and measure the impact of the risk involved and hence to decide on the appropriate measures and controls to manage them. Many risk assessment methods exist in the literature such as Expression des Besoins et Identification des Objectifs de Securite (EBIOS), TVRA, etc ...

Berrehili et al. [1] applied the EBIOS method on the internet of things (IOT) domain. The motivation of their work is to determine the most security risks on the IOT applications. This will help the developers to build applications in a secure way.

The Threat, Vulnerability and Risk Analysis (TVRA) method is proposed first by the ETSI standardization body [2]. It is used to identify risks of the system based upon the product of the likelihood of an attack, and the impact that such an attack will have on the system. The output of the TVRA is a quantified measure of the risks to the assets and a set of detailed security countermeasures that will minimize that risk [3] . The importance of the TVRA method is that it is designed and adapted for the intelligent transportation system (ITS) technologies.

The difference between EBIOS and TVRA is that EBIOS is a generic method However TVRA is a detailed method and it is usually used to determine specific vulnerabilities for example: using EBIOS, we find a vulnerable interface that should be protected, otherwise using TVRA we should go more in the details (vulnerable interface permit to an attacker to do buffer overflow). Obviously the difference will impact the countermeasure, using EBIOS we will propose to use a firewall to protect the vulnerable interface, on the other hand using TVRA we will propose to resolve the problem of the buffer overflow.

Moalla el al. [4] applied the TVRA method on ITS communication architecture. The results of their work is an analysis on the impact of threats related to wireless communications and threats specific for the ITS. In our work, we go a step further by proposing and analyzing new attacks related to the use of the pseudonyms certificates in the C-ITS.

III. System architecture

Usually the risk analysis is applied on a part of a system called target of evaluation (TOE). To position the TOE inside the overall system architecture we present the system architecture depicted in figure 1. It is composed of the vehicle

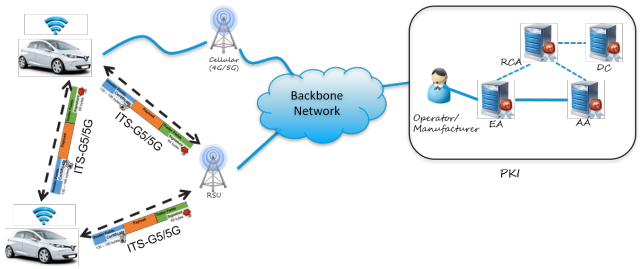

Fig. 1: PKI architecture

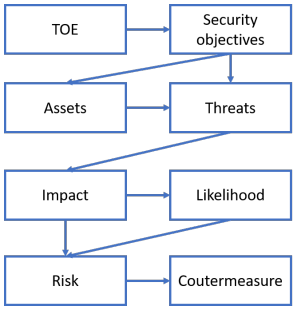

Fig. 2: TVRA steps

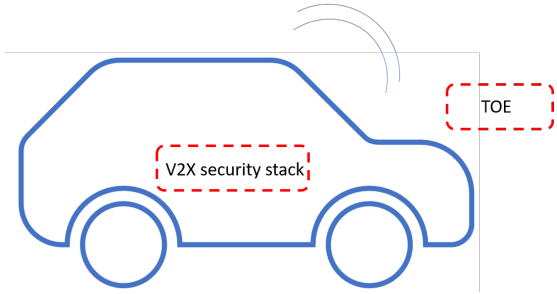

Fig. 3: Target of evaluation

and the Public key infrastructure (PKI). The PKI is a set of entities that create, manage and distribute digital certificates. We implemented a PKI that is compliant with the European Telecommunications Standards Institute (ETSI). It consists of the following entities:

- **Root Certificate Authority (RCA)**: The Root CA is the highest level CA in the certification hierarchy. It provides EA and AA with proof that it may issue enrolment credentials, respectively authorization tickets
- **Enrolment Authority (EA)**: Security management entity responsible for the life cycle management of enrolment credentials. Authenticates an ITS-S and grants it access to ITS communications.
- **Authorization Authority (AA)**: Security management entity responsible for issuing, monitoring the use of authorization tickets. Provides an ITS-S with authoritative proof that it may use specific ITS services.
- **Distribution Center (DC)**: Provides to ITS-S the updated trust information necessary for performing the validation process to control that received information is coming from a legitimate and authorized ITS-S or a PKI certification authority by publishing the Certificate Trust List (CTL) and Certificate Revocation List (CRL).
- **Operator**: installs and updates necessary information for security management in ITS-S during operation
- **Manufacturer**: installs necessary information for security management in ITS-S at production
- **ITS-S**: end-entity of the system that requests certificates to the PKI and communicates with other end-entities.

IV. Work motivation

This work is done as part of the research project Secure Cooperative Autonomous systems (SCA) [5] lead by IRT SystemX. The main objective of the project is to look into the question of making intelligent transport system (ITS) communications more secure and privacy preserving.

In this paper, we propose to apply a risk analysis method on some selected use cases issued from our previous work [6]. The use cases are the pseudonym reloading and pseudonym change. The use of the pseudonym certificates is crucial for privacy protection and it is adopted by different standards such as ETSI [7], IEEE and working groups such as Car2Car communication consortium [8]. We believe that a risk analysis on the pseudonym life-cycle use cases (pseudonym reload, pseudonym change etc...) is crucial.

V. Threat vulnerability risk analysis (TVRA)

In our analysis, we will use the TVRA method. It consists of the steps presented in figure 2 and described below.

A. Target of evaluation

In the initial phase, the target of evaluation (TOE) is defined as an interoperable vehicle implementing the ETSI V2X (Vehicle to everything) security stack [9]. Figure 3 presents the TOE considered in our analysis. Cameras, radars, and lidars and other sensors are not part of our TOE.

B. Security objectives

The security objectives that needs to be guaranteed in C-ITS are:

- Availability: ITS applications require a high level of availability for data and services
- Authentication: It ensures that communicating entities are authentic.
- Integrity: It ensures that exchanged information and data used inside the vehicle (sensor data, data used by softwares etc...) are not modified.
- Confidentiality: It consists of preventing sensitive information from reaching the wrong people.
- Privacy: Privacy is one of the main requirements and challenge for C-ITS. It consists of the protection of the information related to vehicle's identity.

C. Assets

Assets can be physical, logical, functional and human. Physical assets are the equipment that we want to protect such as the hardware security module (HSM), communication unit that implement V2X stack. Logical assets are the information stored in and handled by the physical assets, logical assets considered in our analysis are listed below:

- Pseudonym certificate: It is a pseudonym identity used by the vehicle for communication. It prevents attacker to link the exchanged messages by changing the identity depending on a pseudonym change strategy. Each vehicle has a pool of valid and certified pseudonyms that could be used during the vehicle's trip.
- Enrollment certificate: It is the long term identity. It is not used during the communication. It is used by the vehicle only for requesting a new pseudonym to the Authorization Authority (AA).
- Root certificate: It is the certificate of the Root authority.
- EA/AA certificates: The certificate of the enrolment authority and the certificate of the authorization authority should be protected to prevent any manipulation.
- Certificate Revocation List (CRL) and Certificate Trust List (CTL): A Certificate Revocation List (CRL) is issued and signed by the RCA verification key. It contains the CA certificates identifiers that are no longer worthy of being trusted. CTL contains the valid access point for security services
- Cryptographic keys: the keys that are used for encryption and decryption.
- ITS Messages: Exchanged messages such as Cooperative awareness message (CAM) and Decentralized Environmental Notification Message (DENM).

In our analysis We do not consider neither human assets nor functional assets.

D. Vulnerabilities

In this study, the following threat agents are considered:

- Eavesdropper with programmable radio receivers
- Threat agent with keying material and posing as a valid ITS-S

The list of attacks presented in table I and described below:

- Sybil attack: Sybil attack was proposed first by Douceur [10]. A vehicle possesses usually multiple valid identities (pseudonyms certificates) at the same time called also pool of pseudonyms. The sybil attack consists of using one or more valid identities by a vehicle at the same time. The threat agent can be a vehicle with valid keying material. An example of this attack could be an attacker who wants to enjoy the road alone or empty the street next to his house, to this end, he creates a sybil attack to simulate a congestion in an area, in order to cheat the info-traffic applications, so they redirect all traffic to other roads.
- Location tracking attack: It consists of collecting all the exchanged messages in a specified area or multiple areas, and analyzing their contents to identify which messages are sent by the same vehicle. This enables the attacker to track the vehicle and build drivers profiles profiles for vehicles. The threat agent can be an eavesdropper with programmable radio receivers to receive CAM messages exchanged in a area.
- Alteration of trust anchor information: Modification of the RCA certificate or/and the EA/AA certificate could impact all communication information received for the compromised vehicle.
- False message injection: There is no mechanism to detect that the received Cooperative Awareness Message (CAM)is plausible or not (position plausibility, other)

In the rest of this section we will present our proposed attacks:

- Pseudonym change strategy inhibition : changing the pseudonym is triggered by a pseudonym change strategy implemented in the vehicle. If a vehicle does not change its pseudonym identity for a while, it will be traceable and thus impact the privacy of the users. An attacker can block the pseudonym change.
- Exhaust of the pseudonym pool: when a vehicle sends a CAM, it is possible for an eavesdropper to send a CAM with the same ID. The originated vehicle receives this message and believes that another vehicle is using the same ID as it and thus, changes directly its pseudonym. The repetition of this act may exhaust the pseudonym pool of the targeted vehicle.

E. Impact analysis

The steps to establish risk of an attack are as following : 1) calculate the value of attack potential. It is the sum of the values mapped with factors presented in table III Time + Expertise + Knowledge + Opportunity + Equipment. 2) Attack potential values are mapped with attack potential required to exploit attack as presented in table IV. 3) map the vulnerability rating with the threat level to identify likelihood of attack as presented in table II. 4) The overall impact, shown in table VII, is determined by summing the asset impact value from table VI and the attack intensity value form table VIII. 5) Establishment of the risk (see equation 1). The value is then mapped using table V.

$$Risk = likelihood * impact \tag{1}$$

F. Countermeasures

In order to protect against the sybil attack, we propose some countermeasure: limit the number of valid pseudonyms at the same time could help to minimize the likelihood of occurrence. The implementation of misbehavior detection could help to detect sybil vehicles

Misbehavior detection can be a countermeasure for the exhaust of pseudonym pool attack.

The countermeasure of the tracking attack is using a robust pseudonym strategy. Our next step will be the study of the robustness of the pseudonym change proposed by the Car2car

Threat	Attack	Range	Value	Potential	Likelihood	Impact	Risk
Sybil attack	time	$\leq 5months$	15	25 (Beyond high)	2 (Possible)	3	6 (Critical)
	Expertise	Expert	6				
	Knowledge	public	0				
	Opportunity	Unlimited access	0				
	Equipment	specialized	4				
	Threat level	Critical	-				
	Asset impact	High	3				
	Intensity	Heavy level of multiple instances	2				
Location tracking attack	time	$\leq 6months$	17	27 (Beyond high)	2 (Possible)	3	6 (Critical)
	Expertise	Expert	6				
	Knowledge	public	0				
	Opportunity	Unlimited access	0				
	Equipment	specialized	4				
	Threat level	Critical	-				
	Asset impact	High	3				
	Intensity	heavy level of multiple instances	2				
False message injection	time	$\leq 1day$	0	7 (Basic)	3 (Very likely)	6	2 (Critical)
	Expertise	Proficient	3				
	Knowledge	Public	0				
	Opportunity	unlimited access	0				
	Equipment	specialized	4				
	Threat level	Critical	-				
	Asset impact	medium	2				
	Intensity	single instance of attack	0				
Alteration of trust anchor information	time	$> 6months$	19	57 (Beyond high)	3 (Possible)	3	9 (Critical)
	Expertise	Multiple experts	8				
	Knowledge	Critical	11				
	Opportunity	Difficult	10				
	Equipment	Multiple bespoke	9				
	Threat level	Critical	-				
	Asset impact	High	3				
	Intensity	single instance of attack	0				
Pseudonym change strategy inhibition	time	≤ 5 months	15	42 (Beyond high)	1 (Very unlikely)	2	2 (Minor)
	Expertise	Expert	6				
	Knowledge	sensitive	7				
	Opportunity	Difficult	10				
	Equipment	specialized	4				
	Threat level	moderate	-				
	Asset impact	medium	2				
	Intensity	single instance of attack	0				
Exhaust the pseudonym pool	time	≤ 3 months	0	7 (Basic)	3 (Very likely)	3	9 (Critical)
	Expertise	proficient	3				
	Knowledge	public	0				
	Opportunity	Unlimited access	0				
	Equipment	specialized	4				
	Threat level	Critical	-				
	Asset impact	High	3				
	Intensity	moderate level of multiple instances	1				

TABLE I: Risk determination

The countermeasure of false message injection attack is plausibility checks(PC). PC are crucial and it can help to filter not plausible messages. Kamel et al. [11] proposed a list of checks that could be implemented in order to detect a misbehaving entity.

VI. CONCLUSION AND FUTURE WORKS

In this paper, we realized a risk analysis with focus on the pseudonymity mechanisms used for V2X communications aspects of C-ITS by following the TVRA methodology. We studied potential vulnerabilities that may apply on pseudonym certificate life-cycle. We then propose several countermeasures that could handle these privacy attacks. Future work consist of studying more deeply the tracking problem, by implementing our tracking attacker and applying it on existing pseudonym change strategy to evaluate their robustness.

ACKNOWLEDGMENTS

This research work has been carried out in the framework of the Technological Research Institute SystemX, and therefore granted with public funds within the scope of the French Program *Investissements d'avenir*.

REFERENCES

[1] Berrehili Fatima zahra, Belmekki Abdelhamid, "Risk analysis in Internet of Things using EBIOS," in *IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, 2017.

[2] ETSI , "ETSI TR 102 893, Intelligent Transport Systems (ITS), Security, Threat, Vulnerability and Risk Analysis (TVRA)," 2017.

[3] ETSI, "ETSI TS 102 165, CYBER, Methods and protocols, Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA) ," 2017.

[4] Rim MOALLA, Houda LABIOD, Brigitte LONC, Noemie SIMONI, "Risk Analysis Study of ITS Communication Architecture," in *Third International Conference on The Network of the Future (NOF)*, 2012.

Vulnerability rating	Threat-level				
	Negligible	Low	Moderate	Severe	Critical
Basic	Possible	Likely	Very Likely	Very Likely	Very Likely
Enhanced	Basic	Unlikely	Possible	Likely Very Likely	Very Likely
Moderate	Very Unlikely	Unlikely	Possible	Likely	Very Likely
High	Very Unlikely	Very Unlikely	Unlikely	Possible	Likely
Beyond High	Very Unlikely	Very Unlikely	Very Unlikely	Unlikely	Possible

TABLE II: Mapping of vulnerability rating with Threat level to identify likelihood of attack

Factor	**Range**	**Value**
Time	$\leq$ 1 day	0
	$\leq 1week$	1
	$\leq 2week$	2
	$\leq 1month$	4
	$\leq 2months$	7
	$\leq 3months$	10
	$\leq 4months$	13
	$\leq 5months$	15
	$\leq 6months$	17
	$> 6months$	19
Expertise	Layman	0
	Proficient	3
	Expert	6
	Multiple experts	8
Knowledge	Public	0
	Restricted	3
	Sensitive	7
	Critical	11
Opportunity	Unnecessary/unlimited access	0
	Easy	1
	Moderate	4
	Difficult	10
	None	999
Equipment	Standard	0
	Specialized	4
	Bespoke	7
	Multiple bespoke	9

TABLE III: Factor and values

Attack potential values	**Attack potential required to exploit attack**	**Resistant to attacker with attack potential of**
0 to 9	Basic	No rating
10 to 13	Enhanced-basic	Basic
14 to 19	Moderate Enhanced	basic
20 to 24	High	Moderate
> 24	Beyond High	High

TABLE IV: Attack potential

[5] SCA project, "https://www.irt-systemx.fr/en/project/sca/," 2017.

[6] Farah Haidar, Arnaud Kaiser, Brigitte Lonc, Pascal Urien, Richard Denis, "C-ITS Use Cases: Study, Extension and Classification Methodology," in *IEEE 87th Vehicular Technology Conference (VTC Spring)*, 2018.

[7] ETSI, "TS 102 941, Intelligent Transport Systems (ITS),Security, Trust and Privacy Management," 2018.

[8] C2C, "FAQ regarding Data Protection in C-ITS," 2018.

[9] ETSI, "TS 102 731 Intelligent Transport Systems (ITS); Security,Security Services and Architecture," 2010.

[10] J. Douceur, "the Sybil Attack," in *First International Workshop on Peer-to-Peer Systems, 1st ed, USA, Springer*, 2003.

[11] Joseph Kamel, Arnaud Kaiser, Ines Ben Jemaa, Pierpaolo Cincilla, Pascal Urien, "CaTch: A Confidence Range Tolerant Misbehavior Detection Approach," in *IEEE Wireless Communications and Networking Conference (WCNC)*, 2019.

Value	**Risk**
1,2	Minor
3,4	Major
6,9	Critical

TABLE V: Risk

Impact	**Explanation**	**Value**
Low	The concerned party is not harmed very strongly; the possible damage is low.	1
Medium	The threat addresses the interests of providers/subscribers and cannot be neglected.	2
High	A basis of business is threatened and severe damage might occur in this context	3

TABLE VI: Asset impact

Asset impact	**Attack intensity**	**Resulting impact**
1	0	1
1	1	2
1	2	3
2	0	2
2	1	3
2	2	3
3	0	3
3	1	3
3	2	3

TABLE VII: Result on overall Impact of varying attack intensity

Attack intensity	**Value**
Single instance of attack	0
Moderate level of multiple instances	1
Heavy level of multiple instances	2

TABLE VIII: Attack intensity levels