D7.3 – Roadmap of Automotive Assurance Frameworks – Beyond V2I

Security Assurance Framework for Networked Vehicular Technology

Abstract

SAFERtec proposes a flexible and efficient assurance framework for security and trustworthiness of Connected Vehicles and Vehicle-to-I (V2I) communications aiming at improving the cyber-physical security ecosystem of "connected vehicles" in Europe. The project will deliver innovative techniques, development methods and testing models for efficient assurance of security, safety and data privacy of ICT related to Connected Vehicles and V2I systems, with increased connectivity of automotive ICT systems, consumer electronics technologies and telematics, services and integration with 3rd party components and applications. The cornerstone of SAFERtec is to make assurance of security, safety and privacy aspects for Connected Vehicles, measurable, visible and controllable by stakeholders and thus enhancing confidence and trust in Connected Vehicles.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

DX.X & Title:	**D7.3 Roadmap of Automotive Assurance Frameworks – Beyond V2I**
Work package:	WP7
Task:	T7.1 Dissemination and Exploitation
Due Date:	31 July 2017 (Approval by the Project Officer to be shifted to 31 October 2017)
Dissemination Level:	PU
Deliverable Type:	R

Authoring and review process information	
EDITOR	**DATE**
Panagiotis Pantazopoulos / ICCS	18-10-2017
CONTRIBUTORS	**DATE**
Sammy Haddad / OPP	03-11-2017
Panagiotis Pantazopoulos / ICCS	07-11-2017
REVIEWED BY	**DATE**
András Váradi / COMM	06-11-2017
Elana Copperman / AUT	07-11-2017
LEGAL & ETHICAL ISSUES COMMITTEE REVIEW REQUIRED?	
NO	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Document/Revision history

Version	Date	Partner	Description
V0.1	18/10/2017	ICCS	First draft (ToC) and subsections 1.2-1.4
V0.2	23/10/2017	ICCS	Section 3
V0.3	27/10/2017	Oppida	Section 2, 4
V0.4	30/11/2017	ICCS	Section 1, 5, Appendices
V0.5	03/11/2017	Commsignia	Peer review
V0.6	03/11/2017	Autotalks	Peer review
V1.0	08/11/2017	ICCS	Final version

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Table of Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Table of Figures

List of Tables

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Acronyms and abbreviations

Abbreviation	Description
CC	Common Criteria
Dx.y	Deliverable x.y
HW	Hardware
ICT	Information and Communications Technology
ISO	International Organization for Standardization
KPI	Key Performance Indicator
OEM	Original Equipment Manufacturer
SAE	Society of Automotive Engineers
SoA	State-of-the-art
SW	Software
WPx	Work Package x
V2I	Vehicle-to-Infrastructure

Table 1: List of Abbreviations

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Executive Summary

This document constitutes a brief report of the organisation, the activities-included and the outcome of the first SAFERtec workshop. For the sake of completeness, an overview of the available assurance frameworks is firstly presented to set the scene for the topics that were discussed in the workshop. Then, the deliverable elaborates on the way that the workshop served the SAFERtec communication plan and collected valuable feedback for the open challenges that are involved in the security assurance thread of research. The outcome of the workshop will be considered in the project's planning and the upcoming technical decisions, most notably in the design of the SAFERtec assurance framework.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

1 Introduction

The deliverable at-hand presents one part of the results achieved in the context of Task 7.1 which is entitled Dissemination and Exploitation. To serve the purposes of communication and dissemination (see the SAFERtec D7.1) the project has planned the organization of two workshops. The first one described here helped the project to meet with groups of experts and also establish new communication channels with relevant (academic) researchers. Most notably, it was an excellent opportunity to gather respective stakeholders and provide the consortium with valuable feedback. In parallel, the SAFERtec team had the opportunity to disseminate the project to a large audience of experts.

The workshop was entitled "*Designing a security assurance framework under V2I connectivity use cases: the SAFERtec approach and vision*" and was organised in the framework of the 1st ESORICS Workshop on Security and Privacy Requirements Engineering (SECPRE 2017). Our workshop consisted of two parts, one that highlighted the SAFERtec vision and elaborated on associated technical issues; a second part included a round-table where project partners, an invited expert and the audience discussed the latest updates on V2I security issues.

The collected feedback and the pointers to open issues will be considered in the upcoming technical activities of the project. On a step further, some of the most relevant comments will be also in the SAFERtec exploitation activities (that will mostly take place during the final stage of the project).

1.1 Purpose of the document

The document seeks to present all the activities that took place in the first SAFERtec workshop and highlight what lessons the consortium has learned from it.

1.2 Intended readership

Besides the project reviewers, this deliverable is addressed to any interested reader (*i.e.*, PU dissemination level)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

1.3 Inputs from other projects

No input from other projects was considered during the compilation of this deliverable.

1.4 Relationship with other SAFERtec deliverables

There is no direct dependency of the content included in this document on other SAFERtec deliverables. However, some indirect relation exists with the deliverable D7.1 that describes the SAFERtec communication and dissemination strategy; one tool to implement such strategies is the presented workshop. Finally, what was taken out of the workshop as feedback is going to be considered in the project work-plan and therefore shape (to some extent) the relevant SAFERtec deliverables.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

2 Brief overview of existing assurance frameworks

For the sake of completeness we briefly discuss the current status in the area of the ICT assurance and security evaluation methods pointing to the multitude of the so-far proposed approaches.

Certification framework	Type of product	Certification Authority	ST	Assurance components / Evaluation scope	Evaluator	Tests on the TOE	Recognition	Assurance continuity	Duration and Cost
ITSEC	Any	National certification body	Defined by the level of evaluation	Security target evaluation, Life cycle, Development, Guidance documents, Functional Testing, Vulnerability testing	ISO 17025 accredited labs	Functional and vulnerability tests done by experts	Some EU members	Reevaluation	6 months to several years
TCSEC	With the required functions	National certification body	To be written for the product	Development, Guidance documents, Functional Testing	-		US	Reevaluation	6 months to several years
CC	Any	National certification body	To be written for the product. Using CC standardized format	Security target evaluation, Life cycle, Development, Guidance documents, Functional Testing, Vulnerability testing	ISO 17025 accredited labs	Functional and vulnerability tests done by experts	CCRA signers up to EAL 2 SOG-IS members up to EAL 4	Reevaluation	6 months to several years
CSPN	Any	ANSSI	To be written for the product. Including all CSPN requirements	Guidance documents, Functional Testing, Vulnerability testing	Labs accredited by the ANSSI	Functional and vulnerability tests done by experts	France	Reevaluation	25 days
EcoTaxe	ETS OBU	French DoT	No	Functional Testing, Vulnerability testing	ISO 17025 accredited labs	Conformance tests and security tests done by experts	France	Reevaluation	1 year
FIPS	Cryptographic products	NIST and CSE	No	Development, Guidance documents, Functional Testing	Accredited as Cryptographic Module Testing laboratories by the National Voluntary Laboratory Accreditation Program.	Conformance tests	US and Canada	Reevaluation	3 months to more than one year

Figure 1: Security certification methods

Security assurance is mainly about establishing trust that a product fulfils its security requirements. Evaluating and assessing security has been the focus of systematic research in the last 3 decades (public agencies, academic, industrial). Interestingly enough, very few of them have reached the level of global or at least national or regional consensus (see Figure 1 for what is to our knowledge the exhaustive list). The most widely recognized-one is the Common Criteria for Information Technology Security Evaluation (CC) standardized in ISO/IEC 15408. Even if regularly criticized, this is to be considered as a reference for the SAFERtec security assurance framework that will be tailored-made for application over V2I communication use-cases. As discussed in the SAFERtec workshop, security assurance, no matter what approach is chosen, is timely, costly, and thus the CC which is the most extensive approach providing the highest level of confidence suffers of these criticisms more than all the others.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

3 The first SAFERtec workshop

3.1 Scope and relevant audiences

The initial idea as mentioned in the SAFERtec documents was to mainly use the workshop in order to provide the consortium with up-to-date user requirements. As such, the most relevant audience would be OEMs, hardware manufactures and automotive security professionals. Indeed, the consortium negotiated the organization of the workshop in conjunction with a major international industry-oriented conference [1] gathering top specialists in automotive cyber security (i.e., automakers and their suppliers). The SAFERtec workshop was agreed to be integrated into the conference programme. Three weeks before the conference dates (and while preparations where almost concluded) the consortium was notified that due to cancellations of some of the key-speakers, the organizers could not deliver the kind of comprehensive, high quality programme they aimed-at and therefore they decided to cancel the conference. The consortium was forced to identify another possible event (during the unfavourable summer period).

The consortium managed to ensure the collocated organization of the SAFERtec workshop with the largest cyber-security conference in Europe, the 22nd European Symposium on Research in Computer Security (*ESORICS*), held in September 2017, in Oslo Norway. One of the ESORICS workshops, i.e., the workshop on Security and Privacy Requirements Engineering (SECPRE 2017) was the host for the SAFERtec event. The general audience of the ESORICS conference reaching up to 100 persons mainly consisted of academics and cyber-security researchers. As such the project could mainly benefit from their expertise and research ideas, however their contribution to the collection of a complete set of user requirements was found to be rather limited.

To reach the required stakeholders, the SAFERtec partners have identified a set of key industrial events where the project will be presented and feedback will be collected by individual discussions and/or interviews with OEM experts[2].

[1] The 2017 Cyber Secure Car Europe conference was scheduled to place on 23-24 May 2017 in Munich, Germany

[2] A SAFERtec questionnaire has been already compiled and used in events such as the TU Automotive 2017, held in Detroit USA

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

3.2 Organizational activities and workshop structure

The organization of the SAFERtec workshop in the context of ESORICS conference was negotiated and agreed with the conference organization team. The support of the Workshop Chair prof. Sokratis Katsikas (from the Norwegian University of Science and Technology) needs to be highlighted here. Relevant preparations for the SAFERtec presence in ESORICS were mainly carried-out by ICCS and started already during summertime of 2017. Apart from having the organizational overview, defining the role of each partner in the workshop and the corresponding agenda, ICCS produced a special roll-up banner (see Figure 2) as well as a number of SAFERtec leaflets to promote the project.

Figure 2: The SAFERtec poster at the ESORICS registration desk

The title of the SAFERtec workshop "*Designing a security assurance framework under V2I connectivity use cases: the SAFERtec approach and vision*" was selected to best reflect its scope and the considered topics. It took place on the 14th of September and gathered around 20 attendees. Its programme (see the agenda in the Appendix A 1: Agenda of the first SAFERtec workshop) consisted of two main parts:

The first one (see Figure 3) highlighted the SAFERtec vision and elaborated on associated technical issues through a number of presentations, delivered by consortium members. The main objective of these presentations was to inform and educate the attendees about the project itself (1), its technical background (2) and the innovation it aims to develop (3):

- The SAFERtec concept and the automotive use-cases of interest. The first presentation of the workshop included a brief introduction to the scope, objectives and work-plan of the

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

project. An overview of the considered SAFERtec use-cases to serve as the basis for the SAFERtec assurance framework was also presented.

- The current landscape of V2X security and the SAFERtec choices for the infrastructure and vehicle components. The first technical presentation discussed the general characteristics as well as the security attributes of the V2X communication paradigm. The security features to be implemented in the context of the SAFERtec '*connected vehicle system*' were also briefly discussed.
- The SAFERtec innovative modeling of security and privacy threats in connected vehicles. The SAFERtec approach to threat modeling was introduced discussing its application over a SAFERtec use-case. There, the integration of EBIOS [1], SecureTropos [2] and PriS [3] (requirements engineering methodologies) was explained[3].

The final presentation delivered by an invited expert Dr. Per M. Gustavsson (Senior Advisor Cyber Security at ATEA Sweden) elaborated on:

- Trends, vulnerabilities, stakeholders' requirements and open challenges in V2I (data storage). The presentation discussed the transition from traditional to connected vehicles and the relevant requirements that need to be met (in order for it to be successful). It also elaborated on the vulnerabilities caused by the involved technologies residing both in the vehicle and the infrastructure. Finally, the challenges in the emerging V2I communication landscape were analyzed.

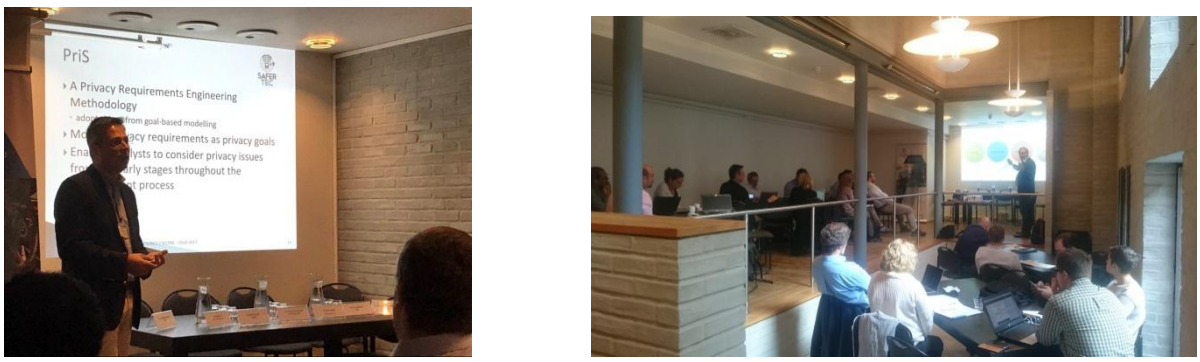

Figure 3: Snapshots of the SAFERtec workshop presentations' session

After the first part, the audience had been given the required information and momentum, thus the experts were familiar with the project and also with the open issues related to its scope. This assured that relevant key topics could be brought up and discussed.

[3] Relevant details to appear in the SAFERtec deliverables D2.2 and D2.3.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

The second part (see Figure 4) included a round-table where project partners, our invited expert and the audience discussed a broad set of V2I security issues including:

- A review of the considered problem and its importance
- The approaches to the quantification of ICT security and privacy assurance levels
- How the automotive setting can shape the above approaches
- Relevant standards and validation methods

The panellists and the workshop participants exchanged their know-how, commented-on the SAFERtec vision and highlighted the relevant challenges and issues that remain open for further research (see the following subsection).

Figure 4: Snapshot of the SAFERtec workshop round-table discussions

What is worth mentioning as a final remark is the responsiveness and vivid interest of the attendees. Some of the researchers expressed the request to be regularly updated about the project's achievements; moreover, a couple of them stated in private conversations their willingness to be somehow involved in the project. They agreed to have their names considered in case a SAFERtec Advisory Committee is deemed necessary to be formed for advising the project.

The consortium was represented in the workshop by UPRC, Oppida, SWARCO, Commsignia and ICCS while Autotalks and CCS contributed to the preparation of the presentation slides.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

3.3 Raised open issues, challenges and lessons learned for SAFERtec

In this paragraph we provide more details on the issues raised during the first SAFERtec workshop. We mainly focus on those that were discussed during the round-table and highlight the take-home conclusions for the project in the following list of points.

- Vehicles being connected (i.e., exposing numerous interfaces) means that they will be increasingly targeted by cyber-attacks; then, intrusion and tampered data should be expected. In that sense, three axes in the connected vehicles technology are becoming relevant: prevention, detection and response. The first one refers to the way that connected vehicles make it as hard as possible to attack. The second one refers to the need for real-time knowledge about a cyber-attack while the third points to the mitigation of the damage, once an attack has occurred. The SAFERtec assurance framework is expected to somewhat provide guarantees about the level of assurance of V2I technology instances. Those can help the involved stakeholders (e.g., OEMs) assess their products (i.e., relevant to prevention) and consider possible security updates/improvements (i.e., relevant to response).
- The involved connected vehicles SW will be subject to very frequent updates. In near future it is foreseen that SW updates will be released at a high rate and they should be assessed accordingly (in terms of their impact on security assurance). In the SAFERtec context and considering the lifetime of the project as a constraint, the requirement of validating such SW updates mainly points to our modeling work. The challenge for the SAFERtec is to derive an easily extendable security assurance framework that would allow for the inclusion of new entities and/or functionality and be able to support (validate) vehicular systems accounting-for functional safety.
- The status of the existing standards for cyber-physical vehicle systems (e.g., ISO 26262 [4], SAE J3061 [5]) and the extent to which the project will use them. The state-of-the-art regarding standards will be studied in the context of (designing) the SAFERtec assurance framework (details to appear in D3.1). The challenge for the project is to re-use existing methodologies and already deployed good practices. CC (see Section 2 Brief overview of existing assurance frameworks) will be considered as reference but further details regarding the automotive setting will be incorporated to the framework to capture more accurately the involved levels of assurance.
- The use of standardized test suites. This can be addressed by the introduction of appropriate KPIs that can partially work on standardized parts of the architecture. However, this is considered as not sufficient to provide highly-confident levels of assurance for critical parts of the system. The relevant challenge for SAFERtec is to contribute-to (or extend) the available automotive standards.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- Evaluation of every HW and SW module/part of the considered system. It is deemed mandatory to consider all involved modules (in a given V2I use-case) in order to provide highly confident assurance levels. The completeness of the study constitutes another challenge for the SAFERtec project.
- Evaluating the cost of the SAFERtec assurance framework. This task which may be interesting remains out of the project's scope. SAFERtec aims to provide a dedicated and efficient assurance framework carefully tailored for the needs of the connected vehicles paradigm and therefore, cost-efficient. A relevant point to the involved costs relates to the consideration of the value (i.e., cost) of the infrastructure when estimating the corresponding assurance level. This task would call for the availability of a large piece of information that is subject to change in the course of time.
- The question of prioritizing the importance of safety, security and privacy (to be protected) in the setting of connected vehicles was addressed to the audience. The immediate yet expected response was that safety is the top-priority. However, through the discussions it became clear that safety is closely interconnected with both security and privacy and therefore, a holistic consideration should be sought after.

Finally, a number of other issues were discussed and largely remain open to for future research. A summary of these issues is as follows: The identification of the level of attack that the connected system or its individual component can tolerate. Which are the most appropriate players to decide about that, the OEMS, the drivers or the National Authorities? The involved thresholds in the security assurance estimation need to be determined. Is there a systematic way to do so? Who should set those thresholds (in order to maximise their acceptance)?

The project will seek for answers as the relevant (technical) work progresses.

In a nutshell, the workshop discussions have made clear that the 'Connected vehicles paradigm' will become a reality only if the involved security needs against a variety of 'new' threats are *confidently* satisfied. The SAFERtec project will significantly contribute towards this end.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

4 Towards the SAFERtec assurance framework

In this section we will briefly present the way that we expect the proposed SAFERtec assurance framework to be designed, in line with the discussions that took place in the workshop. We will first present what tools the current assurance evaluation approaches use and then discuss how the SAFERtec solution seeks to differentiate from them. Our target for the SAFERtec solution will be to go beyond the available frameworks and mark one of the first systematic approaches to the automotive security assurance methodologies [4] (as will be in-detail explained in the WP3 deliverables).

Typical security evaluation approaches are based on conformity checks or vulnerability tests. The former is subject to the feasibility of defining a reference conformity list. In many cases this is hard to obtain and even harder to maintain it up-to-date. Also the validation scope is limited to the elements of the considered list. Anything outside of it or different from it cannot be validated. But they are usually the cheapest and fastest approaches. Another regularly used tool is the vulnerability tests. The main drawback in that case, is the need for confidence to the tester and the lack of reproducibility; thus they can only yield low-to-medium assurance levels. Nevertheless, they are characterized by good adaptability to updated (product) requirements. When it comes to the ITS security validation, the former suffers the fact that ITS system are young, diversified and very fast evolving systems while the later suffers from its lack of reproducibility and common grounds for confidence in a specific evaluation.

Moving to somewhat more complete approaches categorized under the thread of assurance frameworks, the validation becomes then more exhaustive and provides more comparable results. They manage to provide results (i.e., levels) of the highest confidence but again at the expense of time and cost constrained by the requirement of external accredited evaluators and involvement of national supervising bodies.

Compared to previous approaches, the SAFERtec solution will be tailored-made for a V2I setting and automotive industry. The main objective will be to enhance the product (i.e., individual modules) together with the system evaluation. The envisioned approach is to define *global*- as well as *local*-scope requirements for the whole system and its elements (see the comment for an exhaustive evaluation in the previous section). In parallel, the involved automotive/V2I characteristics will be included in the definition of a knowledge base (with relevant threats, security requirement and tests). Then, going beyond the current standards tools to optimize the assurance evaluation will be proposed (see the comment for the enhancement of existing standards in the previous section). Also the evaluation approach will rely on a more distributed use of competences including directly the

[4] The title of this deliverable implies that the outcome of the SAFERtec workshop would lead to the introduction of a new 'road-map' for the research in security assurance frameworks. We have collected the required input/feedback to define and introduce the SAFERtec approach but we choose not to call it a 'road-map'; this term should be used in the cases of somewhat global acceptance and for our occasion, not without the approval/adoption of the auto-manufacturers. This essentially constitutes the greatest SAFERtec challenge.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

developers and car manufacturers (as global system integrator – the SAFERtec questionnaire becomes relevant here). The effort would be to not only rely on external accredited bodies.

The above sketch for the introduction of the SAFERtec framework will be systematically studied, updated and refined in the context of the WP3. The consortium aspires that the outcome of this work (to be presented in the second SAFERtec workshop) will set new 'standards' in the security assurance thread of research.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

5 Conclusions

The first SAFERtec workshop was successfully organized in conjunction with the largest European conference (ESORICS) in the area of cyber-security. On the one hand, the consortium had the opportunity to expose its vision and technical approach to an audience of security experts, mainly of academic background; on the other hand, in the context of the ESORICS conference, the SAFERtec partners had the opportunity to exchange know-how and disseminate the project activities to a broader audience. The feedback and the points raised in the SAFERtec workshop will be taken into account along the upcoming activities.

The SAFERtec workshop outcome will a) suggest an extendable attack-modelling approach; b) shape the design of the proposed assurance framework (advancing the so-far available approaches to meet the automotive setting requirements); c) direct much of the focus of the project to a combined consideration of security, privacy and safety; d) prompt towards the enhancement of the available standardization efforts. Finally, a more industrial point-of-view regarding manufacturers' requirements will be available to the consortium through other channels (e.g., the participation in congresses/forums, use of the SAFERtec questionnaire etc).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

References

[1] https://www.ssi.gouv.fr/archive/en/confidence/documents/methods/ebiosv2-methode-plaquette-2003-09-01_en.pdf

[2] Haralambos Mouratidis and Paolo Giorgini, "Secure Tropos: A security-oriented Extension of the Tropos Methodology " Int. J. Soft. Eng. Knowl. Eng. 17, 285 (2007). https://doi.org/10.1142/S0218194007003240

[3] C Kalloniatis, E Kavakli, S Gritzalis , "Addressing privacy requirements in system design: the PriS method"- Requirements Engineering, 2008

[4] https://www.iso.org/standard/43464.html

[5] http://standards.sae.org/wip/j3061/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Appendices

A 1: Agenda of the first SAFERtec workshop

Security Assurance Framework for Networked Vehicular Technology

H2020 Programme

Grant Agreement No: 732319

Agenda

SAFERtec project panel-session

at SECPRE 2017

"Safety and Privacy in Vehicle-to-Infrastructure communication use-cases:

The SAFERtec case"

14 September 2017 | 9.00 - 12.30 | Oslo

In conjunction with ESORICS OSLO 2017 11.-15. September

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Thursday, 14 September 2017

8.30-9.00	***Welcome – Registration***
Session 1 (9.00 – 10.30)	
9.00-9.20	**Dr. Panagiotis Pantazopoulos,** Technical Project Manager/Researcher, ICCS *'The SAFERtec project on V2I security assurance: concept and vision'*
9.20-9.40	**Mr. András Váradi**, Product Manager, Commsignia Inc 'V2X Security: State of the Art' *(A jointly-prepared presentation by Autotalks and Commsignia experts)*
9.40-10.00	**Dr. Costas Lambrinoudakis**, Associate Professor at the Department of Digital Systems, University of Piraeus / **Dr. Vasiliki Diamantopoulou**, Research Associate, University of Piraeus *'Identification and Modelling of Security and Privacy Threats in Connected Vehicles' (A jointly-prepared presentation by AIRBUS CyberSecurity and UPRC experts)*
10.00-10.30	**Dr. Per M. Gustavsson**, Senior Advisor Cybersecurity, Atea Sverige AB *'Cyber-security challenges in V2I data storage '*
Session 2 (11.00 – 12.30)	
11.00-12.30	**Roundtable discussion** (Moderator: Dr. Panagiotis Pantazopoulos, ICCS) Participants: 1. Dr. Per M. Gustavsson , Atea Sverige AB 2. Mr. András Váradi, Commsignia 3. Mr. Sammy Haddad, Oppida 4. Ms. Silvia Capato, Swarco mizar s.p.a 5. Prof. Lambrinoudakis, UPRC 6. Prof. Kalloniatis, UPRC

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Speakers Biographies

Dr. Panagiotis Pantazopoulos has been working on Intelligent Transport Systems (ITS) research along the last years. His interests lie in the areas of design, analysis and performance evaluation of ITS protocols and applications. In the context of the SAFERtec project he holds both technical and managerial roles. Prior to the ITS involvement he spent several years working on Internet protocols at the National & Kapodistrian University of Athens. He will be representing the SAFERtec coordinator.

Mr. András Váradi: Product Manager at Commsignia and also responsible for the coordination of research activities. He received his MSc in 2009 from the Budapest University of Technology and Economics (BME) in electrical engineering, followed by continuing to work in the automotive industry on sensor networks and communication technologies. He is currently chairing Hungary at ISO TC 204 and CEN TC 278, acts as sub-chair at the Car 2 Car Communication Consortiums Data Aggregation and Service Management sub-working group

Dr. Costas Lambrinoudakis holds a B.Sc. (Electrical and Electronic Engineering) from the University of Salford, an M.Sc. (Control Systems) from the University of London (Imperial College), and a Ph.D. (Computer Science) from the University of London (Queen Mary and Westfield College). Currently he is a Professor and head of the Department of Digital Systems, University of Piraeus, Greece. In parallel, he serves on the board of the Hellenic Data Protection Authority. His research interests are in the areas of Information and Communication Systems Security and Privacy Enhancing Technologies.

Dr. Vasiliki Diamantopoulou is a Research Associate at the University of Piraeus and a Research Fellow at the School of Computing, Engineering and Mathematics at the University of Brighton. She holds a Diploma in Product and Systems Design Engineering, an MSc in Management of Information Systems and a PhD in Information Systems and Innovation, from the Department of Information and Communication Systems Engineering, University of the Aegean, Greece. Her public scientific work focuses on Privacy and Security of Information Systems, eGovernment and Interoperability Frameworks.

Dr. Per M. Gustavsson is Senior Advisor Cybersecurity at Atea Sverige AB, ex-Principal Research Scientist at Saab Training Systems, Sweden, Assistant Professor at C4I Center at George Mason University, USA, and Assistant Professor at Swedish National Defence College, Sweden. He holds a BSc (Systems Programming) and a MSc (New Generations Representations) in Computer Science. He received his Ph.D. (Simulation Engineering) in 2011 from De Montfort University, Leicester, UK.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

SECURITY ASSURANCE FRAMEWORK FOR NETWORKED VEHICULAR TECHNOLOGY

Project Facts

SAFERtec has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319.
Start date: January 2017
End date: December 2019
Total cost: EUR 3 819 380
EU contribution: EUR 3 819 380
Topic: DS-01-2016 – Assurance and Certification for Trustworthy and Secure ICT systems, services and components
Funding scheme: RIA – Research and Innovation action

Project Coordinator

Dr. Angelos Amditis
Institute of Communication and Computer Systems (ICCS)
9 Iroon Polytechniou Str.
Gr 157 73 Zografou Athens, Greece
a.amditis@iccs.gr

http://www.safertec-project.eu

A 2: List of participants in the first SAFERtec workshop

SAFERtec project panel-session at SECPRE 2017

"Safety and Privacy in Vehicle-to-Infrastructure communication use-cases: The SAFERtec case"

14 September 2017 | 9.00 - 12.30 | ESORICS Oslo 2017

No	NAME	AFFILIATION	E-MAIL	SIGNATURE
1	PAWEŁ RAJBA	UNIVERSITY OF WROCLAW	pawel@cs.uni.wroc.pl	Rajba
2	Budi Arief	University of Kent, UK	b.arief@kent.ac.uk	
3	HADDAD Sammy	OPPIDA	sammy.haddad@oppida.fr	
4	Majed Alshammari	University of Oxford	majed.alshammari@cs.ox.ac.uk	
5	ANDRAS VARADI	COMMSIGN LTD	ANDRAS.VARADI@COMMSIGN.COM	
6	SILVIA CAPATO	SWARCO MIZAR	silvia.capato@swarco.com	
7	Goitom K. Weldehawaryat	NTNU	goitom.weldehawaryat@ntnu.no	
8	Sibylle Fröschle	OFFIS & Uni Oldenburg	sibylle.froeschle@offis.de	
9	Katja Tuma	Gothenburg University	katja.tuma@cse.gu.se	
10	Vivien Rooney	IMT Atlantique	vivien.rooney@imt-atlantique.fr	

SAFERtec project panel-session at SECPRE 2017

"Safety and Privacy in Vehicle-to-Infrastructure communication use-cases: The SAFERtec case"

14 September 2017 | 9.00 - 12.30 | ESORICS Oslo 2017

11	Gaute Wangen	NTNU	GAUTE.WANGEN@NTNU.NO	
12	Simon Foley	IMT Atlantique,		
13	MARTIN KOLAR	UMA	KOLAR@UMA.ES	
14	VASILIKI DIAMANTOPOULOU	UPRC	vdiamant@unipi.gr	
15	CHRISTOS KALLONIATIS	UPRC	chkallon@unipi.gr	
16	Athanasios Kanatas	UPRC	kanatas@unipi.gr	
17	Costas Lambrinoudakis	UPRC	clam@unipi.gr	
18	Per Gustafsson	AFRA	PER.GUSTAFSSON@AFRA.SE	
19	Panagiotis Pantazopoulos	ICCS	ppantaz@iccs.gr	
20				

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319