Towards a Security Assurance Framework for Connected Vehicles

Panagiotis Pantazopoulos*, Sammy Haddad †, Costas Lambrinoudakis‡, Christos Kalloniatis‡,
Konstantinos Maliatsos‡, Athanasios Kanatas‡, András Varádi§, Matthieu Gay¶ and Angelos Amditis*
*Institute of Communication and Computer Systems (ICCS)
Iroon Polytechniou Str. 9, GR-15773, Athens, Greece
Email: {ppantaz, a.amditis}@iccs.gr
†Oppida, Montigny-le-Bretonneux, France
Email: sammy.haddad@oppida.fr
‡University of Piraeus Research Centre, Piraeus, Greece
Email: {clam, chkallon, kmaliat, kanatas}@unipi.gr
§Commsignia Ltd, Budapest, Hungary
Email: andras.varadi@commsignia.com
¶Airbus CyberSecurity, Elancourt, Ile-de-France, France
Email: matthieu.gay@airbus.com

***Abstract*—Security assurance is defined as the degree of confidence that the security requirements of an IT system are satisfied. In view of the emerging paradigm of *connected vehicles i.e.*, dynamic Cyber-Physical systems of highly-equipped infrastructure-connected vehicles, specifying the involved assurance becomes highly-critical yet challenging; vehicles increasingly exploit various communication means to exchange rich data of relevance with the infrastructure resulting in a large attack surface. Both the complexity and uncertainty are increased rendering the so-far generic methods for security assurance costly-to-apply.**

In this position paper we introduce a security assurance framework *tailored for* connected vehicles, as explored by the EU-funded H2020 SAFERtec project. We put under the microscope two instances of vehicle-to-infrastructure communications and relying on an innovative modeling methodology we identify the involved security and privacy requirements. We then present the way to enhance the processes of the credible yet generic Common Criteria approach to gain evidence that the above requirements are met. The experimental evaluation of the framework is carried-out over a reference implementation of a prototype vehicle connected to road-side units and cloud-based services. The expectations are that our work assists to effectively construct assurance arguments increasing trust in connected vehicles.

I. Introduction

The *connected vehicles* paradigm [1] whether referring to tech-assisted manually-driven or vehicles of higher automation level [2], has emerged over the last decade(s) as a prominent example of a dynamic cyber-physical system seeking to significantly improve traffic safety and efficiency. Indeed, vehicles have witnessed a shift from electro-mechanical artifacts to complex systems integrating numerous third-party software and sensor/hardware components and notably, constituting nodes of a dense connectivity layer. The latter provides real-time links to the Internet, infrastructure and the rest of the fleet. Thus, connected vehicles are enabled to access rich data of relevance, collaboratively sense the surroundings and even take informed decisions leading to new (automated) driving functions such as the cost-effective vehicles' platooning.

The successful adaptation and market penetration of vehicular technology relies on the extent to which challenging security concerns are efficiently addressed. Furthermore, when considering the critical-information exchange mainly between the vehicle and infrastructure, the corresponding attack surface becomes larger as numerous actors (*i.e.*, hardware and software modules) and rapid changes (*i.e.*, software updates) are involved; the resulting *connected vehicle system* (CVS) is likely to become highly vulnerable [3]. Security, privacy, data integrity (which can become a pivotal aspect of safety) are already open challenges for "traditional" ICT systems when involving multi-entity interactions, let alone the vehicular ecosystem of high dynamicity. The later environment entails considerable security, privacy and safety risks and thus, poses a multitude of requirements that may be hard to identify [4]. The main goal is then two-fold: on the one hand to devise security measures that will mitigate the identified threats and on the other to establish effective procedures for the assurance that the system satisfies its intended security behavior.

The second thread typically enjoys less attention than the first. The requested evidence is gained through carefully-designed evaluation processes attesting to the correctness and quality along the development, deployment and operation of the considered IT system, called Target of Evaluation (ToE). There are three main evaluation approaches: i) conformity checks, ii) vulnerability tests, iii) and assurance frameworks. The first (also called compliance assessment) is a form of evaluation that validates a system's compliance to a specific reference [5]. A reference conformity list has to be kept up to date and needs to be relevant to the considered system's needs in terms of functionality and security. Typically, this is the fastest and cheapest evaluation scheme however the definition and maintenance of relevant conformity lists can become cumbersome. Moreover, anything not conformant to a subset of this list cannot be validated. Vulnerability tests [6]

first require a quick perimeter definition *i.e.*, the product, the tests environment and relevant limitations. Then, experts runs tests of their choice during a predefined time-period seeking to reveal (potential) security vulnerabilities. This method allows to validate the system's security compared to the state of the art, providing low to medium assurance levels. Finally, the assurance framework approach [7] is the most complete and exhaustive one providing the highest assurance levels. It requires a precise description of the evaluation objectives and requirements to prescribe dedicated and extensive evaluation activities. However, it comes at the expense of considerable cost and time-to-complete while it requires rare and expensive accredited evaluators to define appropriate test-suits.

Many approaches falling under the three categories have been proposed and very few have reached any kind of global consensus. Two are so-far the only recognized and standardized for security certification. NIST FIPS 140-X [8] and the ISO Common Criteria for Information Technology Security Evaluation 3.1 R5 [9] which is the most accepted one. However, when moving to the ITS domain and the connected vehicle eco-system, none of them suits all relevant aspects. They are rather generic and typically expensive to apply on the highly-complex automotive setting.

In this paper we present the SAFERtec project's [10] approach to *automotive* security assurance. Our research aims to introduce an assurance framework to assess the level of confidence that the involved security-, privacy- and safety- needs of the connected vehicle system are satisfied. The focus is on both V2R (Vehicle-to-Roadside station) and V2C (Vehicle-to-Cloud) communication instances realized in carefully selected use cases of automotive information exchange such as the real-time traffic-hazard information (V2R) or the navigation data (V2C). Due to their large attack surface and/or trust-establishment processes among numerous involved entities, the challenging vulnerability assessment and the elicitation of the security requirements has been addressed introducing an innovative combination of three methodologies. With those requirements at hand, our framework relies on the so-far most credible approach *i.e.*, the Common Criteria (CC) [9] and aims to provide high assurance level for the CVS with lower cost than the usual CC certification process. Finally, the framework's experimental evaluation (and refinement) will be carried-out over a reference implementation that includes a prototype vehicle, dedicated hardware and instances of third-part services, integrated to realize the considered use-cases.

The remainder is structured as follows: In Section II, we mark the scope of our study discussing the considered vehicle-to-roadside station (V2R) and vehicle-to-cloud (V2C) use-cases. In Section III we present an innovative combination of methodologies that allows us to identify the involved security and privacy requirements. Our proposal for the design of the SAFERtec security assurance framework is detailed in Section IV while in Section V we present a reference implementation to act as a test-bed for the framework's experimental evaluation. Section VI concludes highlighting the expectations for the effectiveness and usage of the introduced framework.

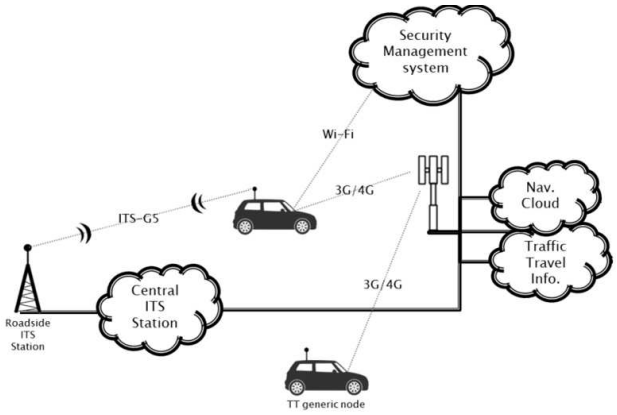

Fig. 1. Vehicle connected to roadside stations and cloud services

II. The V2R and V2C considered setting

Out of a broad set of relevant automotive scenarios of infrastructure-connected vehicles we have selected a limited yet challenging set of use cases on the basis of safe-criticality, usefulness, and problem-tractability. Having them realized using a prototype vehicle, dedicated hardware and a number of relevant applications, we seek to create a realistic environment to test and validate the introduced security assurance framework. Those use-cases involve the vehicle's communication either with the roadside station or with a cloud-based service. An effort to identify use-cases that lend to both above communication types has been taken; their comparative study can provide useful insights on the way that different technologies influence the involved levels of security assurance.

- *The vehicle-to-roadside (V2R) station case:* Information originates from the infrastructure back-end (*e.g.*, Traffic Management Center), reach the roadside station (see left part of Fig. 1) and become relevant in the use-cases of optimal driving speed advice, provision of real-time traffic information (*e.g.*, a traffic-jam ahead notification) and priority request in supervised intersection crossing.
- *The vehicle-to-cloud (V2C) case:* Information originates from the cloud-based services and through cellular networks (see right part of Fig. 1) becomes relevant for similar use cases like before *i.e.*, optimal driving speed advice and provision of real-time traffic information. Moreover, personalized driving-advices from the cloud can help us study how to secure personal data.

Without harming the generality of the proposed assurance framework, we next focus our study on those use-cases.

III. An innovative risk-based approach for reasoning about Security, Privacy and Safety

Security, privacy and safety are three fundamental concerns that upon satisfaction provide the necessary assurance in every context. Thus, in the automotive context, the initial step was the design of a process that would assist software engineers in reasoning about security, privacy and safety under a unified

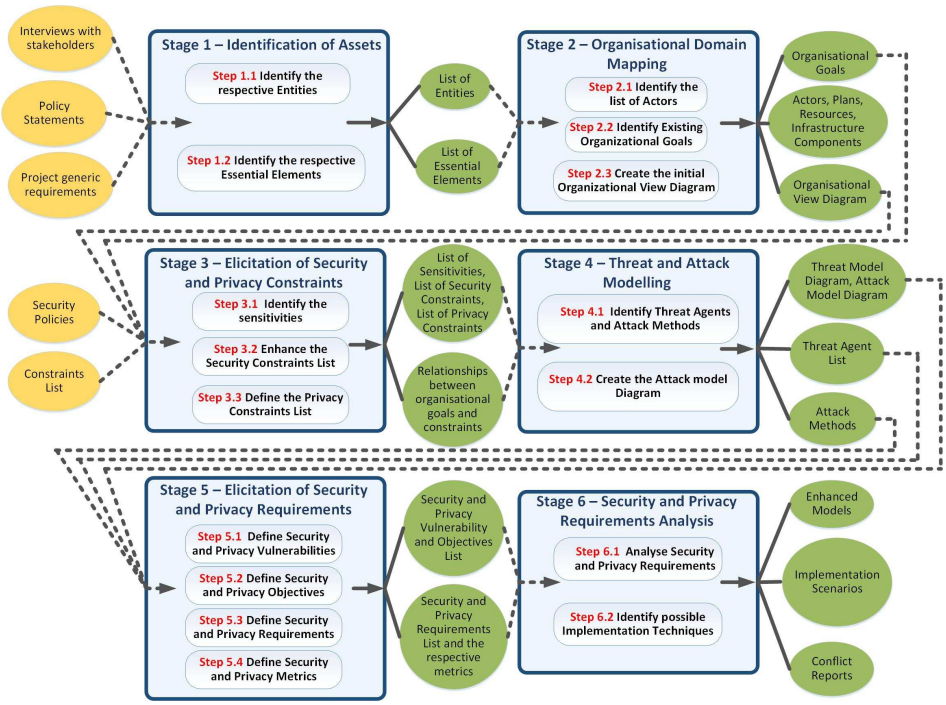

Fig. 2. The SAFERtec 6-stages modeling approach

approach. The proposed approach combines the fundamental characteristics of three well-known methods, EBIOS [11], Secure Tropos [12], [13] and PriS [14], [15]. Their combination provides an innovative approach for software engineers; it bridges the gap between the design and implementation phases through a six stages process starting with the elicitation of high-level objectives and ending with the suggestion of specific security, privacy and safety measures to be exploited in the proposed framework (see Section IV). The introduced process (see Fig. 2) combines risk analysis and attack modeling techniques for performing a successful transformation of high level security, privacy and safety requirements into specific technical requirements and respective measures. Even if studied in the automotive setting, it is generic enough for risk-based security and privacy analysis of every system. Each of the involved stages consists of several steps that assist the designers in eliciting and modeling the security, privacy and safety requirements of the studied system.

Specifically, in stage 1 EBIOS is introduced in order to proceed with the identification of the respective entities that correspond to the main players of the system to be. In parallel with the significant entities the essential elements will be identified. In stage 2 the main effort is to understand the current organizational structure and based on the identified entities and essential elements of stage 1 to identify actors, organizational goals, plans, resources, services and infrastructure.

In stage 3 the identification of security and privacy constraints related to the organizational needs are identified. Security and privacy needs are identified based on the security and privacy concerns that the organization has. Thus, it is important to identify, initially, the security concerns of the organization and understand their linkage with the identified organizational goals. Identification of sensitivities will provide the first set of candidate security and privacy concerns per use case. These constraints will be the set of concerns that should be fulfilled along with every identified functional requirement. Note that the input source for identifying the system's sensitivities and constraint lists can also be the organization's policy. Relevant laws and regulations can also be considered to identify the set of security and privacy goals.

In stage 4 the identification of every threat per organizational goal is conducted. Threat elicitation is of vital importance for capturing the external and internal sources that can cause harm to the assets of the system but also for validating that the identified security and privacy constraint lists are complete. Attack models are also constructed for every identified threat per security and privacy constraint for every functional goal (organizational goal).

In stage 5 the vulnerability analysis is conducted based on the identified threats and attack methods. Security and privacy vulnerabilities detection will lead to the identification of the security and privacy objectives, which are the way that vulnerabilities are mitigated thus reducing the potential risk on the identified entities. Next, is the definition of the security and privacy requirements that basically describe in a specific way the realization of the identified objectives.

Finally, in stage 6 the security and privacy requirements analysis is conducted. The specific stage is of vital importance since all the information collected from previous stages will be modeled under a unified model in order to proceed in the

identification of possible conflicts among security and privacy, threat mitigation and vulnerability satisfaction *etc.* Also, the identification of possible implementation scenarios for every security and privacy requirement will be realized in order for the stakeholders and developers to select the most appropriate solution per use case.

IV. Optimizing Common Criteria (CC) Evaluation

All existing IT security evaluation schemes address the following three dimensions: i) What has to be evaluated?, ii) Which evaluation activities to choose?, iii) Who should have the competences and responsibilities for what is in the evaluation process? These three dimensions correspond to what is generally called:

- The Security Target (ST)
- The assurance components
- The evaluation scheme

Each IT security evaluation scheme identifies in its own way the importance of those dimensions. It is to be noted that there is no universal solution for the problem of IT security evaluation and all available solutions can be criticized. Common however is the need to trade-off the cost with the achievable (final) level of confidence. Evaluating security is difficult and costly regardless the approach; this is mainly due to the continuously evolving technologies, the relatively short products' lifespan and the lack of universal measurement scale. The most complete and exhaustive evaluation scheme is the Assurance framework (see Section I). It provides the highest assurance levels and essentially includes both conformity verification and vulnerability tests together with specification and architecture reviews, life-cycle evaluation *etc.*

The Assurance framework background is rather limited to TCSEC [16], ITSEC [17] and the flagship Common Criteria (CC) [9]. The latter is in fact a merge of the two aforementioned ones that were developed in parallel. CC keeps the main concepts of ITSEC: i) the need of a proper Security Target (ST), ii) the decomposition of the evaluation in generic tasks independent of any product or security requirements, iii) the definition of several assurance levels, each providing a set of more stringent evaluation tasks. Eventually, CC provides a complete description and a reference set of security requirements (to write formalized STs) together with the most extensive list of evaluation tools. CC is the only approach officially recognized by several countries and therefore adopted as a base for our work. Precisely, our starting point is the CC adaptation proposal of [18] that we further enhance to effectively cope with the characteristics of the connected vehicle system.

A. The SAFERtec Assurance Framework (SAF)

The SAFERtec Assurance Framework (SAF) combines in an innovative way existing standards and tools to achieve high assurance levels *at system level* for connected vehicles. A first refinement of the CC approach towards ITS product evaluation appears in [18]. The latter relies on regular CC evaluation tasks but proposes to execute them in parallel. The idea is that different actors can be identified to work in parallel on the different evaluation tasks. This is an important improvement on the time and cost needed to run the complete CC evaluation process. SAF proposes to rely on this concept and further enhance it by providing dedicated tools and knowledge bases; they are to ease and speed-up the generation of the developer's inputs or evaluation tasks. In fact, for every evaluation task CC defines specific inputs to be provided by the (considered software module's) developer together with the corresponding evaluation points to validate those inputs.

Fig. 3 summarizes our enhancements. For each CC evaluation task we present in the "developer" and "evaluator" boxes the proposed enhancement (*e.g.*, for the CC ADV evaluation task SAF proposes the methodology to help developers provide more appropriate system architecture descriptions to be used as the evaluation task input). More importantly, we have added to the regular CC framework an extra assurance component named AOP standing for OPerational Assurance component. This is to provide operational assurance metrics that will be used in the complete connected vehicle system to demonstrate its security features within its full operational environment.

In what follows, we only summarize the proposed enhancements due to space limitations: i) tools (*i.e.*, the integrated methodology of Section III) to precisely and efficiently specify more evolved security requirements, ii) knowledge bases to help the developer's implementation task, iii) adapted tools to help the developer and the evaluator for both functional and vulnerability tests, iv) definition of Key Security Performance Indicators to provide security assurance at system level, which CC do not include. All those enhancements contribute to the faster production of the developer's evidences required by the evaluation process. Moreover, they help the developer reach a higher security maturity for his software by supporting the fast integration of security requirements in the software modules. Finally, it eases the evaluation process by providing adapted tools and therefore lowering the cost of the global evaluation.

B. Introducing a Modular Protection Profile for Connected Vehicles

CC defines two documents: Protection Profile (PP) and Security Target (ST). Both describe a set of security functions and assurance requirements (as part of the certification process) for an IT product or system, called Target of Evaluation (ToE). PP describes requirements that are implementation-independent, while ST describes requirements, mechanisms and measures that are implementation-dependent. A PP is a combination of threats, security objectives, assumptions, security functional requirements (SFRs), security assurance requirements (SARs) and rationales.

The PPs applicable to the complex and modular connected vehicle system should be adjustable, easily extendable and cover all possible cases. These requirements led us to the adoption of a modular approach with three main notions. These are the Base Protection Profile (base-PP), the Protection Profile Module (PP-module) and Protection Profile Configuration (PP-Configuration). In this context, a base-PP is defined and used as a basis to build a Protection Profile

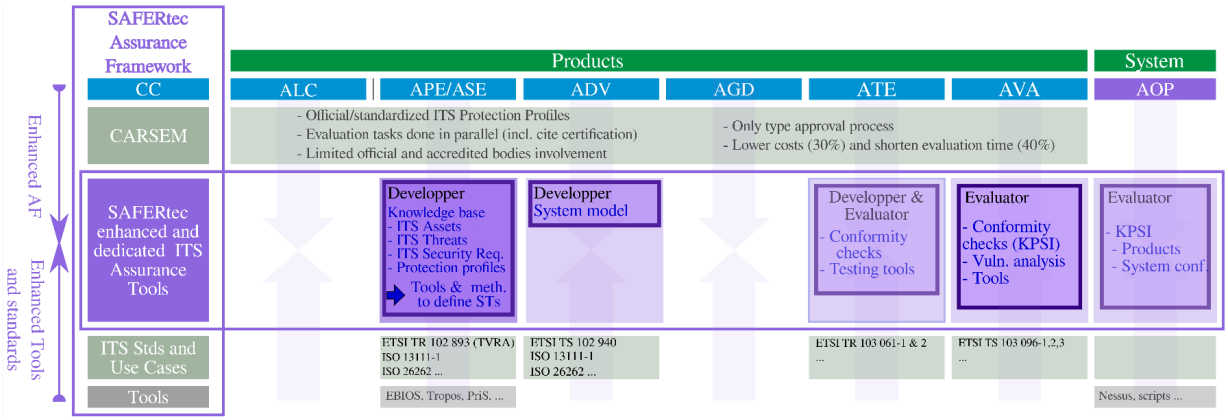

Fig. 3. The SAFERtec Security Assurance Framework (SAF): introduced evaluation tools beyond Common Criteria

configuration. The ToE addressed by base-PP is the base of a vehicle system (V-ITS-S), intended to be installed in all types of cars and will be referred as V-ITS-S Base. This base-PP includes those system components that are prerequisite by all possible envisioned system functionalities. PP-module is an implementation-independent statement of security needs for a ToE, complementary to one or more Base Protection Profiles. PP-module refers to a set of optional security features for a certain type of ToE and has to be used together with one or more base-PP(s). A PP-module is a consistent set of elements (threats, assumptions, organizational policies, objectives and security requirements) with a unique reference. Unlike PPs, PP-modules address optional security features of a given type of ToE that cannot be required uniformly for all products of this kind. Furthermore, a PP-configuration results from the combination of at least one PP-module with its base-PP.

Based on the above conceptual approach, the base-PP and the optional PPs have been identified for V-ITS-S system. The base-PP includes the service control subsystem which has embedded the applications and the related databases. The optional PPs that have been identified are the Sensor Monitor PP, the Communication Control Monitor PP and the HMI PP.

V. Experimental Evaluation over a Reference Implementation

To enable the proposed framework's validation we develop and integrate the connected vehicle system (CVS). We have specified the architecture and all the involved mandatory components *e.g.*, hardware security unit (HSM), on-board units (OBU), standard software blocks of the three main parts of the CVS: the vehicle platform, the roadside station (R-ITS-S) and the cloud infrastructure (see also Fig. 1).

The first part includes the in-vehicle components (see Fig. 4). V2I communication is done by a dedicated OBU connected to the vehicle's Controller Area Network (CAN bus) following the standards ISO 11898-1,-2 [19]. Basic transmission service is realized via the on-board units' access to vehicular sensors information, while functional safety parts remain isolated by a CAN gateway. The integrated ETSI ITS

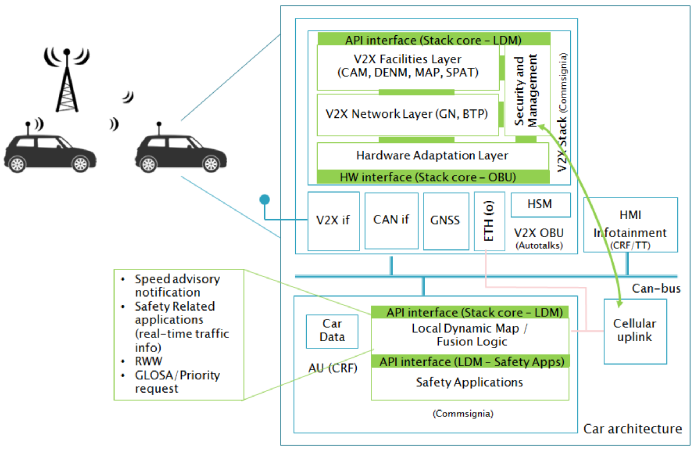

Fig. 4. The SAFERtec in-vehicle software architecture

G5 [20] protocol stack processes and verifies received data from R-ITS-Ss or other vehicles. Data is made accessible over the internal network via a secured and authenticated channel to be temporarily stored in a Local Dynamic Map (LDM) and later handled by safety applications. The latter identify dangerous traffic situations and trigger notifications to the driver provided by the HMI module.

The second part of the CVS is the roadside station (R-ITS-S) shown in Fig. 5. It has been designed as the gateway between the central infrastructure where traffic-data are gathered and the SAFERtec prototype vehicle. Traffic management data is encapsulated in various standard messages (*e.g.*, ETSI-CAM) and broadcasted by an ETSI ITS G5-stack implementation [20]. Similar specifications and design rules (*e.g.*, each service to operate independently of the rest ones residing in the cloud stack) have been derived for the SAFERtec cloud infrastructure and the corresponding mobile communication to the vehicle. The above architecture coupled with ITS-G5 and cellular technologies as well as the appropriate hardware is integrated to realize the CVS functionality and serve the evaluation purposes of the SAFERtec assurance framework.

The prominent tool to identify the vulnerabilities of the

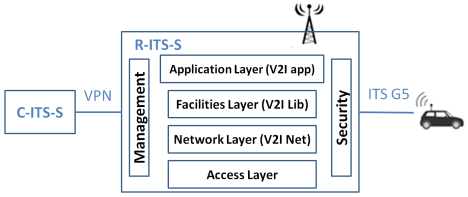

Fig. 5. Sketch of the SAFERtec roadside station (R-ITS-S) architecture

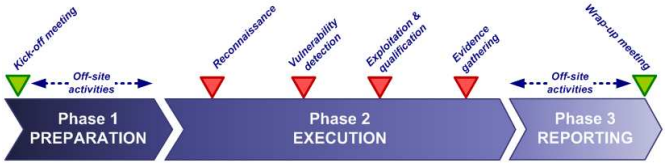

Fig. 6. The SAFERtec penetration testing process

implemented CVS is penetration tests *i.e.*, authorized simulated attacks. There are three types of penetration tests [21] depending on the level of the available information to the auditor: 'black box' where no information is given, 'grey box' where functional knowledge and system access are available; finally, 'white box' is the favorable case of full information availability. The more information is available, the deeper is the investigation and therefore the effectiveness of the test is increased. Given a level of information availability that allows grey and/or white box penetration testing, we plan to test the CVS following a three-step-process illustrated in Fig. 6.

Our first phase constitutes of the preparation used to anticipate the course of the penetration test. The second phase is the execution. It starts with the reconnaissance (*i.e.*, port scanning, protocol versions *etc.*). Then, vulnerabilities are detected and quantified using the standard Common Vulnerability Scoring System [22]. During this phase, we plan to analyze each exposed interface by running fuzzing tests to spot protocol/apps flaws. All parameters will be audited for misconfiguration. The robustness of the involved key infrastructure will be evaluated and credential compromise will be tested; thus, evidence to prove the CVS (potential) vulnerability will be gathered. The second phase is recursive: successful exploitation of vulnerabilities lead to new reconnaissance activities. The result of a penetration test will be reported in the last step including a list of security issues, an assessment of their criticality and recommendations. Those will be used to update and improve the SAFERtec Assurance Framework.

VI. Conclusions

As highly-equipped connected vehicles increasingly rely on data exchanged with the infrastructure, further cyber-security, privacy and safety concerns are raised; uncertainty about achieving the involved security objectives is increased. To gain confidence that automotive security needs are satisfied and reduce the associated (high) costs, we have first proposed an innovative combination of methodologies to elicitate the involved requirements. Then, relying on the most credible yet generic assurance methodology *i.e.*, the Common Criteria (CC), we have introduced targeted enhancements to ease the evaluation processes and notably extend the CC scope up to system-level. Accordingly, we propose the use of modular protection profiles to cope with integrated automotive communication systems. Our security assurance framework, to be experimentally validated on timely vehicle-to-infrastructure use-cases aims to increase trust in connected vehicles.

Acknowledgment

This work is a part of the SAFERtec project. SAFERtec has received funding from the EU Horizon 2020 research & innovation programme under grant agreement No 732319.

References

[1] N. Lu *et al.*, "Connected vehicles: Solutions and challenges," *IEEE Internet of Things Journal*, vol. 1, pp. 289–299, 2014.
[2] D. Watzenig and M. Horn, Eds., *Automated Driving: Safer and More Efficient Future Driving*. Springer International Publishing, 2017.
[3] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Transactions on ITS*, vol. 16, no. 2, pp. 546–556, 2015.
[4] E. Schoitsch, C. Schmittner, Z. Ma, and T. Gruber, "The need for safety and cyber-security co-engineering and standardization for highly automated automotive vehicles," in *Advanced Microsystems for Automotive Applications 2015*. Springer Publishing, 2016, pp. 251–261.
[5] IEEE Conformity Assessment Program (ICAP). [Online]. Available: http://standards.ieee.org/about/icap/index.html
[6] H. H. Thompson, J. A. Whittaker, and F. E. Mottay, "Software security vulnerability testing in hostile environments," in *Proc. of the ACM Symposium on Applied Computing*, NY, USA, 2002, pp. 260–264.
[7] K. Beznosov and P. Kruchten, "Towards agile security assurance," in *Workshop on New Security Paradigms*, NY, USA, 2004, pp. 47–54.
[8] National Institute of Standards and Technology, *FIPS PUB 140 Series: Requirements and standards for cryptographic modules*, May 2001. [Online]. Available: https://csrc.nist.gov/publications/fips
[9] "ISO/IEC 15408 part 1/2/3:2005-Information technology, Security techniques, Evaluation criteria for IT security," Tech. Rep., v3.1, Release 5. [Online]. Available: https://www.commoncriteriaportal.org/cc/
[10] H2020 SAFERtec project. [Online]. Available: https://www.safertec-project.eu/
[11] EBIOS 2010 Expression of Needs and Identification of Security Objectives. [Online]. Available: https://www.ssi.gouv.fr/archive/en/confidence/documents/methods/ebiosv2-methode-plaquette-2003-09-01_en.pdf
[12] H. Mouratidis and P. Giorgini, "Secure tropos: a security-oriented extension of the tropos methodology." *Int'l Journal of Software Engineering and Knowledge Engineering*, vol. 17, no. 2, pp. 285–309, 2007.
[13] M. Pavlidis and S. Islam, "Sectro: A case tool for modelling security in requirements engineering using Secure Tropos," in *CAiSE Forum*, 2011.
[14] C. Kalloniatis, E. Kavakli, and S. Gritzalis, "Addressing privacy requirements in system design: the PriS method," *Requirements Engineering*, vol. 13, no. 3, pp. 241–255, Sep 2008.
[15] C. Kalloniatis, "Designing privacy-aware systems in the cloud," in *Trust, Privacy and Security in Digital Business*, S. Fischer-Hübner, C. Lambrinoudakis, and J. López, Eds. Springer, 2015, pp. 113–123.
[16] United States Department of Defense, "Trusted Computer System Evaluation Criteria (Orange Book)," Tech. Rep., 1985.
[17] C. Jahl, "The information technology security evaluation criteria," in *13th Int'l Conf. on Software Engineering*, May 1991, pp. 306–312.
[18] S. Haddad *et al.*, "CARSEM: A Cooperative Autonomous Road-vehicles Security Evaluation," in *Proc. of the 25th ITS World Congress*, Copenhagen, Denmark, Sept. 2018.
[19] [Online]. Available: https://www.kvaser.com/can-protocol-tutorial/
[20] ETSI EN 302 663. [Online]. Available: http://www.etsi.org/deliver/etsi_en/302600_302699/302663/01.02.00_20/en_302663v010200a.pdf
[21] J. N. Goel and B. Mehtre, "Vulnerability assessment and penetration testing as a cyber defence technology," *Procedia Computer Science*, vol. 57, pp. 710 – 715, 2015.
[22] CVSS. [Online]. Available: https://www.first.org/cvss/