DIAS

Smart Adaptive Remote Diagnostic Antitampering Systems

EUROPEAN COMMISSION

HORIZON 2020

LC-MG-1-4-2018

Grant agreement ID: 814951

Deliverable No.	D4.1
Deliverable Title	Security analysis, requirements identification and applicability of security solutions for tamper protection
Issue Date	18/05/2020
Dissemination level	Confidential
Main Author(s)	Obaid Ur-Rehman, FEV
	Bela Genge, UMFST
	Sofia Terzi, CERTH
	Andreas Hastall, Robert Bosch GmbH Germany
	Dominic Woerner, Robert Bosch AG Switzerland
Version	V1.0

DIAS Consortium

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 814951.

Executive summary

A vehicle of today consists of many advanced features made possible through electronic control units equipped with software and communication capabilities. Typically, a vehicle consists of different sensors such as sensors for emission protection system, like NO_x and PM sensors, and environmental sensors like radars and cameras for advanced driver assistance. These control units and sensors are grouped into multiple domains, such as powertrain and advanced driver assistance systems, and each domain typically has its own communication network. These domains are in turn interconnected via a gateway. A telematics unit such as the connectivity unit then connects the vehicle to the extra-vehicular networks and systems using external communication interfaces such as Bluetooth, Wi-Fi and mobile communications.

These new technologies have an impact on the protection of the vehicle's environmental protection systems (EPS) from tampering. As identified in the deliverables D2.1 and D3.1, currently the sensors can be emulated on the in-vehicle communication networks such as controller area network. Additionally, it is also already possible to reflash the relevant control units, such as the engine control unit or the sensor control unit, with unauthorized data and possibly software. This leads to tampered and false emissions being reported by the vehicle and contributes to environmental pollution for monetary gains.

This deliverable is the outcome of task T4.1. In this task, the objective was to approach the problem of emission tampering and protection of the EPS from cybersecurity perspective. In order to understand the problem, a generic vehicle architecture is defined for reference which includes most of the important sensors, control units and communication protocols typically found in a modern vehicle. This reference architecture also includes important elements of the demonstrator vehicle to be used in the DIAS project. This generic architecture and the inputs from D2.1 and D3.1 are evaluated from security point of view to understand the tampering possibilities and develop security requirements for protection against them.

Security threat analysis and risk assessment are performed on this generic vehicle architecture. This process also takes into consideration the tampering methods identified in D2.1 and D3.1. Through the process of risk assessment, the identified threats are rated and assigned a security level in order to prioritise them. The most critical threats are the ones that need highest security considerations. The output of the task is high-level security requirements which are derived based on the threats and risk assessment. Certain solutions already proposed in literature might fulfil the most trivial security requirements. These solutions are studied and listed. Some of these solutions can be integrated into the vehicular technologies used in practice. In order to fulfil the remaining requirements, new innovative security solutions will be needed. They will be developed and integrated during the project in the follow up tasks T4.2 and T4.3 and tested through the task T4.4 as well as the Hackathon events.

The current vehicular systems lack security protection mechanisms required to protect the vehicle's EPS from tampering. The currently observed practices of tampering through sensor emulation and ECU re-flashing can be addressed in the early phase of DIAS project if appropriate security mechanisms are in place. The security mechanisms for protection against tampering will be developed and integrated in the demonstrator vehicle in two phases. The security mechanisms for protection against emulation and ECU flashing will be developed and integrated in the first phase of the DIAS project. Their effectiveness will be tested through the first Hackathon event. In the second phase, any short comings of the security based

tamper protection methods identified through the Hackathon will be addressed. The second phase will also focus more on the future tampering possibilities that might result from the evolution of the modern vehicles. The protection of external connectivity, anomaly detection and blockchain mechanisms will be integrated in the second phase and validated by the project partners. Additional validation and verification of the developed concepts will be performed through the second Hackathon event.