DIAS

Smart Adaptive Remote Diagnostic Antitampering Systems

EUROPEAN COMMISSION

HORIZON 2020

LC-MG-1-4-2018

Grant agreement ID: 814951

Deliverable No.	D2.2
Deliverable Title	End-user requirement & use case definition
Issue Date	23/12/2020
Dissemination level	Confidential
Main Author(s)	Pavlos Fragkiadoulakis (LAT/AUTh) Dimitrios Kontses (LAT/AUTh)
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

The state-of-the-art vehicle environmental protection systems (EPS) can successfully retain the emissions at low levels. However, tampering attempts with these systems are increasing and this can significantly reduce their effectiveness. The reasons and motivations are related to the security of current On-Board Diagnostic (OBD) systems which need to be improved and the cost-benefit that can result for the vehicle owners.

This report, based on the assessment of representative tampering practices via laboratory and real-word testing as presented in deliverable D3.2, identifies and categorizes the end-user requirements towards a tamper-proof EPS. Additionally, the report includes the use-cases which are the verification of tampering practices based on experiments/measurements performed by several DIAS partners.

The study is structured around the chapters below:

- Chapter 1: Introduction
- Chapter 2: Sources and Methodology
- Chapter 3: Description of vulnerabilities and tampering methods for all EPS components
- Chapter 4: Use-cases
- Chapter 5: End-users requirements

The study concludes with the summary in chapter 6.

Chapter 1 contains the background of DIAS and the purpose of this document.

Chapter 2 discusses the methodology and sources which were used in the current deliverable. Methodology refers basically to two new important DIAS concepts, “end-users requirements” and “use-cases” that are fully analyzed in the following chapters.

Chapter 3 describes in detail each one of the structural concepts which form a tampering practice:

- Environmental Protection System (EPS)
- Component
- Vulnerability
- Tampering Method

A tampering attack firstly addresses the EPS and the components that need to be deactivated. The next step is the identification of the corresponding parameter/signal that needs to be modified (i.e. vulnerability e.g. NOx sensor signal). The final step is the modification of the EPS through hardware (physically and via an emulator) or software (through ECU/xCU re-flashing) changes.

Chapter 4 presents the testing activity for representative tampering practices verification (use-cases), including the steps that analyse the tampering process and the verified results correspondingly. This chapter’s material justifies the confidential scope of the current deliverable and is supported by detailed test reports (available in DIAS SharePoint).

Chapter 5 contains the suggested countermeasures (end-user requirements) categorized as follows:

- Manufacturers requirements
- Workshops requirements
- Regulators requirements
- Vehicle owners requirements

The chapter concludes with a summary table of end-user requirements sorted by EPS.