DIAS

Smart Adaptive Remote Diagnostic Antitampering Systems

EUROPEAN COMMISSION

HORIZON 2020

LC-MG-1-4-2018

Grant agreement ID: 814951

Deliverable No.	D2.1
Deliverable Title	Tampering, current practices and potential challenges for the (near-term) future
Issue Date	21/03/2020
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 documents an overview of current and (near-term) future tampering techniques. The methodology followed to achieve the target of this work included a literature review and extensive communications with tamperers. Following the introduction in chapter 1 regarding the background of DIAS and the purpose of this document, the study is structured around the chapters below:

- Chapter 2: Methodology
- Chapter 3: Tamperers
- Chapter 4: Current tampering practices
- Chapter 5: Future issues

The study concludes with the summary in chapter 6.

Chapter 2 discusses the methodology and sources which were used in the current deliverable.

Chapter 3 categorises the tamperers into 4 main levels:

- Level 1: Inexperienced individuals
- Level 2: Moderately experienced individuals
- Level 3: Highly experienced mechanic specialists
- Level 4: Highly experienced programmer specialists

Levels 1 and 2 have limited capabilities and the target-area is mainly tampering with older vehicles and simpler systems compared to the specialists. Levels 3 and 4 are usually in close cooperation with each other and work in tampering workshops.

Chapter 4 focuses on the current tampering practices (until early Euro 6/VI vehicles). The analysis shows that emulators and ECU (Electronic Control Unit) flashing are the prevailing general practices for all EPS. Emulators are considered low-cost but questionable solutions concerning reliability and are mainly applied in old vehicles from inexperienced individuals whereas specialists prefer the ECU flashing techniques as the only reliable solution. The options for gaining access to the ECU are also described and a few typical examples are presented. The next part of this chapter provides details for each of the main exhaust aftertreatment components that are tampered with, i.e.: SCR (Selective Catalytic Reduction), DPF (Diesel particulate Filter), EGR (Exhaust Gas Recirculation) and TWC (Three-Way Catalyst) systems. Finally, the effect and the techniques related to vehicle tuning are presented in the last part of this chapter.

Chapter 5 contains the future issues that will affect tampering practices. More advanced vehicle security systems i.e. secure CAN (Controller Area Network) will require new approaches for access to the ECU and smarter emulators. The available information is limited, though and continuous updates will be provided in the future when tamperers will be confronted with the new advanced vehicle systems.