EUROPEAN CONGRESS
LISBON, PORTUGAL
22-24 MAY 2023
ITS: The Game Changer.

15th ITS European Congress, Lisbon, Portugal, 22-24 May-2023

Paper ID #

Information System for Vehicle Antitampering based on OBD Data

Nikos Dimokas[1,3*], Dimitris Margaritis[1*], Andrew Winder[2]

1. Centre for Research and Technology Hellas/Hellenic Institute of Transport, 6th km Charilaou – Thermi, 57001, Thessaloniki, Greece (dimokas@certh.gr, dmarg@certh.gr)

2. European Road Transport Telematics Implementation Co-ordination Organisation, Avenue Louise 326, 1050 Brussels, Belgium (a.winder@mail.ertico.com)

3. University of Western Macedonia/Department of Informatics
Fourka area, 52100, Kastoria, Greece

Abstract

Recent days the tampering procedure, often known as unauthorized and deliberate alteration of vehicle parts, has an impact on many vehicle functions. In reality, contemporary tampering methods are becoming more sophisticated and are able to mimic authentic signals using unique control mechanisms. The main motivations among others of tampering is the increase of engine output and the manipulation of the Emission After Treatment System in order to save money by preventing the need for costly repairs for malfunctioning diesel engine emissions control systems. Along with numerous other nations, the European Commission predicted an increase in the number of modified vehicles. An information system for identifying and notifying potential tampering or inadequate engine performance/maintenance issues with a vehicle is presented in this paper. The basic idea is based on comparing vehicle parameter values retrieved from On-Board Diagnostic with factory values or vehicle performance values recorded by independent agencies.

Keywords

Information Systems, Tampering, On-Board Diagnostic, Vehicle Antitampering

Introduction

Protection of the environment and improvement of air quality is an important objective of the European Commission. In the automotive industry, EU legislation and standards aim to reduce the emission of CO_2, NO_X and particulate matter [1]. To that aim vehicles manufacturers have installed the Emission After Treatment System (EATS) to the vehicles. This System is fitted to a vehicle and it is designed to reduce any (pollutant) emissions of that vehicle. Examples of such systems are the Exhaust Gas Recirculation (EGR), the Diesel Particulate Filter (DPF), the Selective Catalytic Reduction (SCR), Three-Way Catalyst (TWC), Diesel Oxidation Catalyst (DOC), NO_X absorber, Evaporative Emission Control System (EECS) and others. The use of EATS has brought significant reductions to the actual emission levels.

Nowadays, there is increasing evidence of illegal manipulation of environmental protection systems by vehicle owners and widespread usage is observed in the market [2, 3]. The manipulation of these systems is called tampering [4, 5] and it is very common for many vehicle owners to manipulate the EATS for various reasons with the most important the money savings by avoiding repair costs of malfunctions of the emissions control systems of diesel engines. Other motives mentioned are: costs for consumables, costs for downtime, performance tuning and exhaust sound level. Today, there is a big market where tampering is offered for both light- and heavy-duty vehicles and non-road mobile machinery (NRMM). In general, there are four tampering techniques that used today for manipulating the EATS: i. Electronic Control Unit (ECU) re-flashing, ii. Emulators, iii. Modifiers and, iv. On-Board Diagnostic (OBD) suppressors.

The paper presents an information system for identifying and notifying possible tampering or insufficient engine maintenance issue or higher engine horsepower of a vehicle. The basic principle is based on comparing vehicle parameter values as available from OBD with factory values or vehicle performance values recorded by independent agencies/sources.

The remaining of the article is organized as follows: the second Section describes the relevant work, while the third one presents the information system. The fourth Section describes the evaluation of the system. Finally, the last Section concludes the article.

Related Work

In recent years, the rapid evolution of vehicles has resulted in the advancement of tampering techniques. Table 1 describes the main tasks performed in each technique. The most common method of tampering in vehicles is to disable the EGR or DPF system. The reason is that in case of malfunction it costs less to disable the system than repairing it. Furthermore, because of the lack of control on tampering and a low chance of getting caught, this is the frequently chosen solution for emission control problems. An example of such tampering is a large scandal in Netherlands where the Bo-rent company has removed diesel particulate filters from their Mercedes-Benz Sprinter vans to save on maintenance costs [6]. In order to avoid similar situations, the Government of the Netherlands added an additional check in the roadworthiness test. A visual inspection is performed during the periodic inspections to check for the presence of the DPF [7]. However, with a simple visual inspection, even during Periodic Technical Inspection (PTI), the presence of the filter in the DPF system can hardly be checked and thus, this measure turned out to be ineffective. Although the visual inspection turned out to be ineffective, also other EU countries have adopted this technique for the investigation on the removal of DPF's [8, 9].

Similar to the DPF removal, another common technique is the EGR tampering by removing the EGR system and making changes to the vehicle's software. Although tampering with the EGR system is illegal in Europe, normally only the fault codes of the vehicle are checked during periodic inspections [10]. Finally, the last but not least emission control system that is commonly tampering on light-duty vehicles, is the SCR system. Today, in the Netherlands alone over 30 companies can be found on the internet that advertise with the removal of certain systems, guaranteeing a permanent solution and giving a life time warranty [11].

Table 1: Tampering techniques

Tampering technique	Work description
ECU re-flashing	A workshop alters the ECU flash and checks using test drives or dyno tests if any errors or problems arise. In the end, the workshop alters the ECU code in such a way that the requested EPS is deactivated, and no MILs are activated or OBD fault codes are stored. (Mostly LDs)
Emulators	The majority of the emulators offered for HD vehicles are devices that attack the SCR system. Most of these SCR or NO2 sensor emulators are CAN only, meaning they only communicate with the vehicle through the CAN-bus.
Modifiers	Specific hardware solutions that are simpler to emulators in design and mainly aim to alter the control state of an EPS.
OBD Suppressors	These devices sent specific CAN-bus messages to suppress the onboard diagnostics of the vehicle (by periodically erasing the fault code storage).

In case of heavy-duty vehicles (HDV), the most common system that is tampered is the SCR. For that reason, the Europe has enhanced the road inspections which are focused in this type of tampering [12]. In addition to SCR, DPF tampering is also another common technique for heavy-duty vehicles, however, the focus of Europe on DPF tampering via inspections is less compared to SCR tampering. Some common reasons that push the owners to tamper the DPF system are that the DPF removal increases fuel efficiency, improves the engine performance, increases the service life of the engine and reduces vehicle repair costs. Moreover, there is not much information and data that deals with the inspection of NRMM. However, it is highly likely that especially non-road mobile machinery used for agriculture and construction work are being tampered with on a similar scale as are HDV [13].

The main motivation for tampering is the avoidance of repairing cost and the increase of the engine power. Thus, new innovative measures have to be taken by authorities to prevent tampering. As far as the ECU re-flashing tampering method is concerned, the current security techniques have proven to be insufficient to prevent unauthorised flashing of an ECU. In order to prevent the re-flashing of the ECU the improvement of security has to be enhanced through encryption with secure key generation and storage, intrusion detection, code signing, authentication and data integrity checks [14]. In case of emulators, they can inject false digital signals via the CAN or via SENT protocol to the ECU. For digital signals, it is recommended to consider secure communication e.g. through message authentication. To prevent tampering of sensor and actuator signals, advanced algorithms should be developed to check the integrity of the signals. Analog sensor signals can not be protected by authentication. This means that these signals need to be checked by an advance integrity/plausibility/rationality check.

There are research efforts that have been carried out in order to detect and address tampering. The DIAS research project [15] tried to harden vehicle environmental protection systems (EPS) against tampering. As a result, any modifications to the hardware or software that reduce the performance of the EPS will be avoided or discovered. The CARES research project [16] aimed to investigate contactless measurement of vehicle exhaust emissions and provide results. Through these measurements, the researchers tried to detect the vehicles' tampering. In [17], the authors proposed "VetaDetect" a methodology for the detection of vehicle tampering. More precisely, the Dempster-Shafer (D-S) theory of evidence is used to combine an ensemble of multiple-input single-output (MISO) Auto Regressive Moving Average models (ARX) into VetaDetect.

Antitampering Information System

The system works as follows: a vehicle data collection and control unit send information to a central server in which comparison routines run between OBD and manufacturer performance values in order to identify any significant discrepancies per vehicle. If discrepancies are large and occur on an ongoing basis, the vehicle authority information manager is notified of the discrepancies. From there it is up to the local bodies to decide how to manage the notifications. They could call that particular vehicle for immediate inspection at a random PTIs centre. Should the PTI center confirm the tampering or engine maintenance issue, it would inform the local authority of the findings and accordingly recommendations to the owner could be made for compliance or give fines commensurate with the severity of the problem. The system compares the raw data collected per second of the engine power, the engine torque, the engine speed, the vehicle speed and the vehicle acceleration with values that are available either from the vehicle manufacturers or other reliable sources such as testing authorities. Uncertainly factors can also be introduced that will enable an alarm when the logged data exceed the manufacturer's values above a threshold. In our case, the alarm is triggered when the measured values are above 10% of the thresholds/manufacturer's values.

The system architecture follows the three-tier architecture. The presentation tier, or user interface, the application tier, where data is processed, and the data tier, where the application's associated data is stored and managed, are the three logical and physical computer tiers that make up the well-known three-tier architecture. Although, the system implements an OBD data recording and transmission system application and a website, the presentation tier contains only the website. The system exploits the web services in the application tier for providing data from/to the database. The web services have been built according to the most popular architectural styles that is Representational State Transfer (REST) architecture. Moreover, the application tier exploits the software application (in this case for mobile) developed to collect data from the vehicles. The data tier includes the database that stores the raw data.

The system architecture consists of 4 major components (Figure 1). The first component is the

On-Vehicle Unit (OVU) or a mobile application, in case there is no possibility of placing an application in the OVU, is responsible to read the data from the Controller Area Network (CAN) bus, pre-process it and then transmit it to the server. Due to the many different vehicle models from different manufacturers, developing an application that is capable of operating in different OVU environments is a very difficult task. For this reason, we developed a mobile phone application that receives vehicle data via OBDLink MX+ dongle device and is responsible of sending it to the server. More precisely, the application receives the data collected by the OBDLink application in CSV format. After that our application pre-processes the data and transmit it to the server.

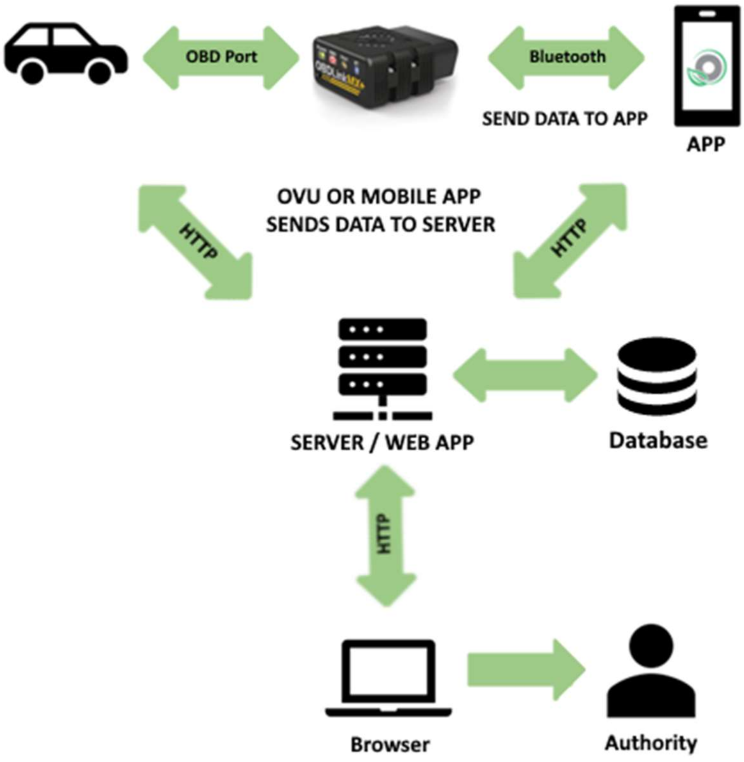


Figure 1: System Architecture

The mobile application has been developed on Android operating system. After the application reads the data, it stores it locally in csv format. The application has a background thread that runs continuously and every time a new file is created, it sends it to the server according to the HTTP protocol. At the same time, the application sends along the VIN, make, model and variant information for each vehicle. The core parameters that are used as a reference for the identifications of potential issues are the vehicle speed and acceleration, engine power and torque, engine speed (RPM) and the MIL indication on.

The second component is the server or else the web application that has been developed. The web application implements the following functionality:

- Implements the web services / Application Program Interface (API) in order to receives the data from the mobile application and stores the csv in the file system (Table 2)
- Processes the data (e.g. type casting, missing values)
- Transforms the data in the appropriate format according to the database

- Loads the data to the database
- Implements the web services / Application Program Interface (API) in order to serve the requests coming from the Presentation Layer

Additionally, the application tier exploits the Grafana open-source analytics and visualisation software. Grafana offers an open-source tool for building dashboards, query data sources, explore, monitor and visualise metrics. The application tier implements data analytics inside the Grafana and a dashboard that is incorporated in the user interface.

Table 2: API for receiving data (csv file) from the mobile application or the OVU

Operation Description	The web service module is responsible for receiving the raw data, process and store it in the database. The mobile app or the OVU sends to the server a multipart form data containing the information from a trip. The app or the OVU receives an HTTP code.			
Input	**Format**	**Name**	**Type**	**Comments**
	Multipart /form-data (HTTP POST)	brand	String	The vehicle's brand
		model	String	The vehicle's model
		variant	String	The vehicle's variant
		fuel	String	The vehicle's fuel type (e.g. Petrol)
		vin	String	The vehicle's identification number (VIN)
		file	CSV	The CSV file containing raw data for a specific journey
		filetype	String	The file's type
		filename	String	The file's name

The third component is the database where the raw data are stored. Additionally, the database contains the appropriate stored procedures for processing the data and producing the aggregated information. The data model developed as a relational schema consisting of various tables and the corresponding relations among them. The database schema (Figure 2) below presents the tables and the corresponding attributes.

The "vehiclecharacteristics" table stores the unique characteristics (reference values) of all different vehicles. Among other things, the table stores information on vehicle's brand, model, variant, engine power, engine torque, top speed, acceleration, etc. On the other hand, the "vehicle" table stores information only for the vehicle running our system. The table contains information about VIN, brand, model, fuel type, etc. The table "tamperingdata" contains the raw data.

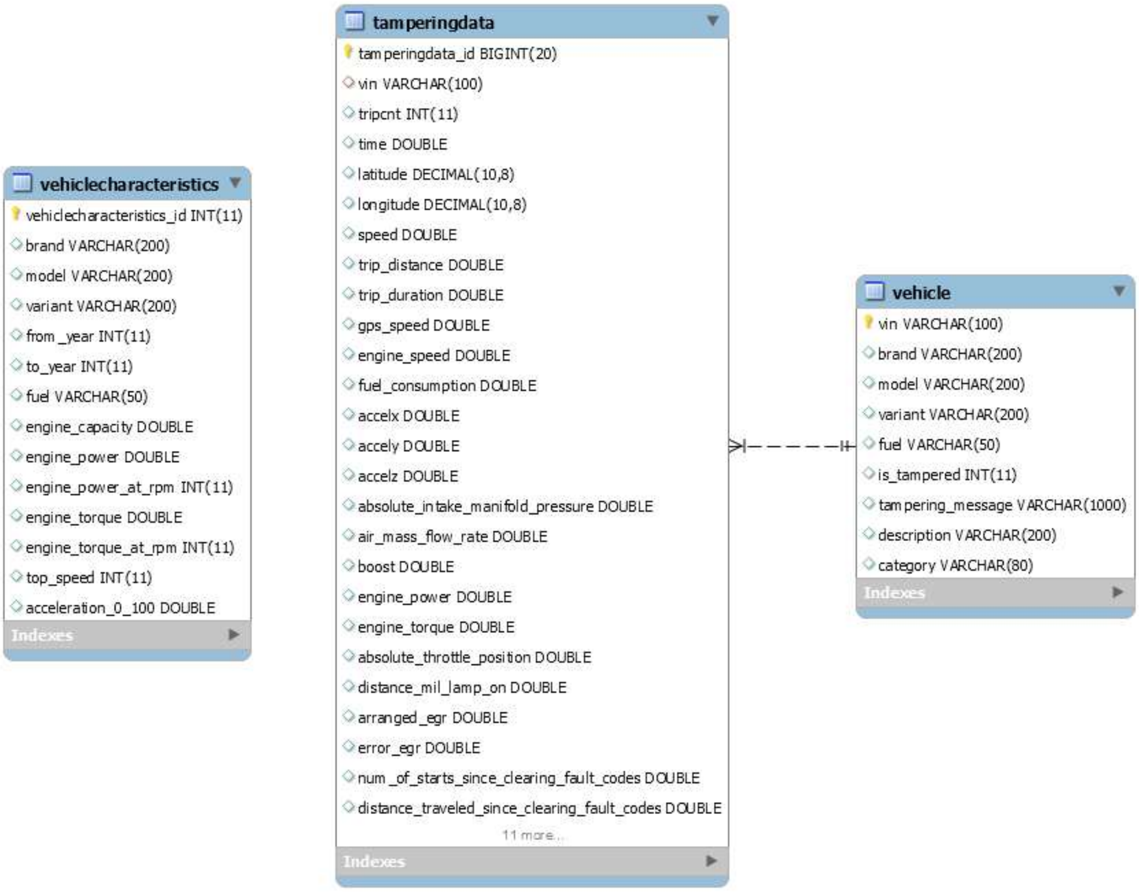


Figure 2: Database schema

Finally, the fourth component is the user interface (Figure 3). It has been implemented based on the Grafana open-source analytics and visualisation software, the HTML, CSS and JavaScript programming languages. The overall user interface, implemented for the overall dashboard web application, consists of three major sections/subsystems. The first, called dashboard, presents the overall dashboard. The second section, called region, provides also aggregated indicators according to the data gathered from a specific region. The third section, called warnings is related to the current system and provides valuable information about warnings.

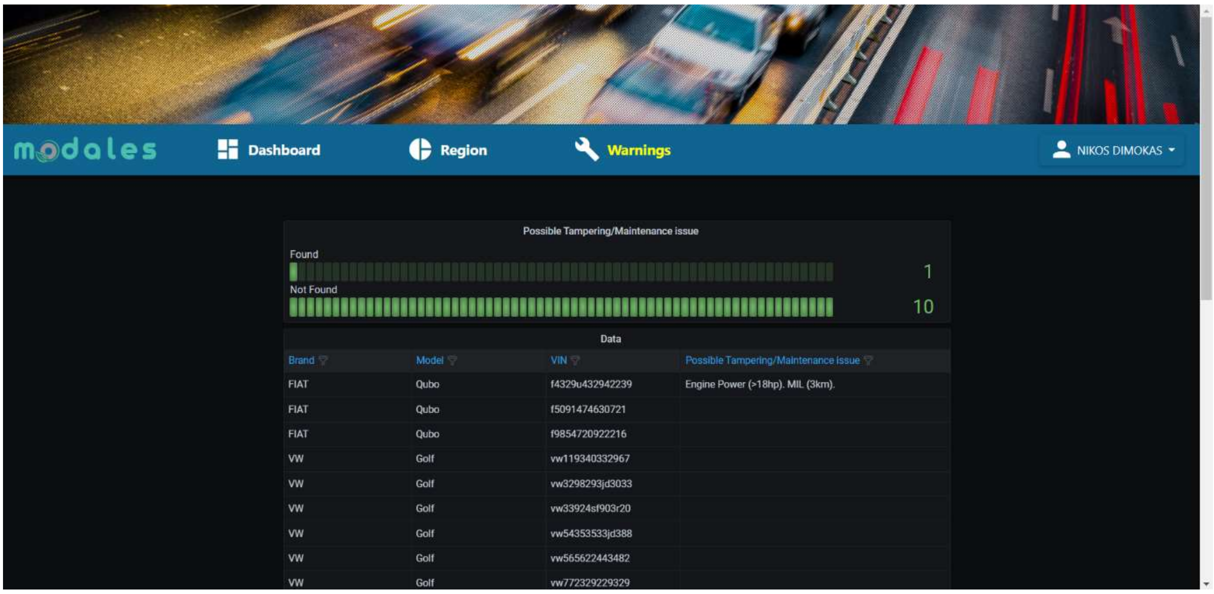
This warnings section provides aggregated information on how many vehicles are experiencing possible tampering and maintenance issues. The user accessing this section can view detailed information about the vehicle’s brand, model and the description for the warning. The warnings can only be accessed by authorized users belonging to an authority.

Evaluation

Considering that the system can be validated when the tampering or poor maintenance of the vehicle is known, the validation phase was limited at this stage but it will continue until the end of the project. In our cases, the system spotted an increased engine power of a vehicle for that variant. More specifically, the vehicle was a FIAT diesel with a Multijet engine which produces 75 hp at 4000 RPM. However, there were several logs with the engine power above 85 hp, with a maximum of 92 hp at 4300 RPM.

Looking at potential engine tampering of this engine type, the current performance of the engine matches with a software tuning that increases the engine power to 95 hp at 5000 RPM.

The owner of the vehicle was not aware of this issue because he had bought the vehicle as a second hand from the first owner who has bought it new from an official FIAT dealer. From this example, the parameter of the total ownership of the vehicle is also of importance. However, when vehicle data will be logged since the first date of registration (assuming that the data will not be manipulate by a tampering software), any tampering will be associated with the owner of that period.



Possible Tampering/Maintenance issue

Found 1

Not Found 10

Data

Brand	Model	VIN	Possible Tampering/Maintenance issue
FIAT	Qubo	f4329u432942239	Engine Power (>18hp). MIL (3km).
FIAT	Qubo	f5091474630721	
FIAT	Qubo	f9854720922216	
VW	Golf	vw119340332967	
VW	Golf	vw3298293jd3033	
VW	Golf	vw33924sf903r20	
VW	Golf	vw54353533jd388	
VW	Golf	vw565622443482	
VW	Golf	vw772329229329	

Figure 3: System's warnings

Conclusions

Tampering of all vehicle types as well as of NRMM is very common in many European countries and new innovative measures have to be taken by authorities to prevent it. The main motivations for tampering are the avoidance of repairing cost or the increase of engine output. The paper presents an information system for locating and alerting potential car tampering or inadequate engine maintenance issues. The system is based on comparing factory values or vehicle performance data recorded by independent sources with car parameter values available from OBD.

The system architecture consists of 4 major components: the mobile application, the server or else the web application, the database where the raw data are stored and the user interface. Through the interface, authorities can be notified for the discrepancies of the identified vehicles. Even though the evaluation period run for a short time (at the time of this paper), the system could identify a vehicle with 20% more engine power than the engine performance factory figures.

Acknowledgements

Research supported by MODALES project [18] that is funded by the European Commission under the Grant Agreement 815189.

References

1. Bischof, O. (2015). Recent Developments in the Measurement of Low Particulate Emissions from Mobile Sources: A Review of Particle Number Legislations, *Emission Control Science and Technology*, vol. 1(2), pp.203-212.
2. Transport & Environment (2017). New truck diesel scandal in Europe twice the size of 'VW diesel gate' in US. Transport & Environment, 20 February 2017. Available: https://www.transportenvironment.org/discover/new-truck-diesel-scandal-europe-twice-size-vw-dieselgate-us/, last accessed January 2023.
3. Gallagher, J. (2017). Thousands of motorists are breaking the law by driving diesel cars without pollution filters. BBC, 29 October 2017. Available: https://www.bbc.com/news/uk-41761864, last accessed January 2023.
4. Baldini, G., Giuliani, R., Gemo, M. (2020). Mitigation of odometer fraud for in-vehicle security using the discrete hartley transform. In Proceedings of *11th IEEE Annual Ubiquitous Computing, Electronics Mobile Communication Conference (UEMCON)*, New York, USA.
5. Thirumalini, S., Malemutt, P. (2021). Investigations on anti-tampering of diesel particulate filter. In Proceedings of *International Conference on Advances in Materials and Manufacturing Applications*.
6. Vermeulen, G., Messelink, R. (2018). Autoverhuurder Bo-rent sjoemelt massaal met roetfilters dieselauto’s. EenVandaag. Available: https://eenvandaag.avrotros.nl/item/autoverhuurder-bo-rent-sjoemelt-massaal-met-roetfilters-dieselautos/, last accessed January 2023.
7. Messelink, R. (2019). Strengere controle op roetfilterfraude faalt, dus worden duizenden vuile diesels APK-goedgekeurd. EenVandaag. Available: https://eenvandaag.avrotros.nl/item/strengere-controle-op-roetfilterfraude-faalt-dus-worden-duizenden-vuile-diesels-apk-goedgekeurd/, last accessed January 2023.
8. Griffiths, H. (2017). Thousands of UK motorists removing diesel particulate filters. Auto Express. Available:https://www.autoexpress.co.uk/car-news/consumer-news/95410/thousands-of-uk-motorists-removing-diesel-particulate-filters, last accessed January 2023.
9. Kadijk, G., Spreen, J. (2015). Roadworthiness Test Investigations of Diesel Particulate Filters on Vehicles. TNO, no. Report TNO 2015 R10307v2.
10. DieselNet (2016). Conference report: 3rd conference on sensors for exhaust gas cleaning and CO2 reduction. Available: https://www.dieselnet.com/news/2016/07svsensors.php, last accessed January 2023.
11. AMT Chip Tuning, “Adblue uitschakelen,” AMT Chip Tuning, [Online]. Available: https://amtchiptuning.nl/adblue-uitschakelen/, last accessed January 2023.

12. Thürmer, J., Schuster, M. (2018). Illegale Fahrzeug-Manipulationen - Der Abgas-Wahnsinn auf Deutschlands Straßen. Bayerischer Rundfunk. Available: https://www.br.de/br-fernsehen/sendungen/mehrwert/illegale-fahrzeug-manipulationen-abgas-wahnsinn-deutschland-strassen-100.html, last accessed January 2023.
13. Stegeman, A. (2017). Fraude in de vrachtwagensector. SBS6: Undercover in Nederland. Available: https://www.sbs6.nl/programmas/undercover-in-nederland/videos/apDRs20Xhe1/undercover-in-nederland/, last accessed January 2023.
14. Meiracker, J.A., Vermeulen, R. (2020). Status quo of critical tampering techniques and proposal of required new OBD monitoring functions. DIAS-Smart Adaptive Remote Diagnostic Antitampering Systems. European Commission Horizon 2020. Deliverable D3.2, Version V1.0, 23/12/2020
15. DIAS European Union Research Project, "Diagnostic Anti-Tampering Systems", https://dias-project.com/, last accessed January 2023.
16. CARE European Union Research Project, "City Air Remote Emission Sensing", https://cares-project.eu/, last accessed January 2023.
17. Haller, P., Genge, B., Forloni, F., Baldini, G., Carriero, M., Fontaras, G. (2022). VetaDetect: Vehicle tampering detection with closed-loop model ensemble, *International Journal of Critical Infrastructure Protection*, vol. 37.
18. MODALES EU Research Project, https://modales-project.eu/, last accessed January 2023.