European Commission

JRC TECHNICAL REPORTS

Vehicles Odometer and Emission Control Systems

Digital Tampering and Countermeasures

Version 1.00

May 2021

Joint Research Centre

Contact information
Email: JRC-VECSEC@ec.europa.eu

JRC Science Hub
https://ec.europa.eu/jrc

JRC 125025

Title: "Vehicles Odometer and Emission Control Systems - Digital Tampering and Countermeasures"
Authors: José Luis Hernández Ramos (JRC), Luigi Sportiello (JRC)

Acknowledgments: the authors would like to thank Prof. Georgios Kambourakis (JRC) for his contributions and comments in several sections of the present report. The authors thank Panagiota Dilara (GROW) for providing useful information and for the review of this study. The authors are also grateful to Philipp Troppmann (MOVE) for his review of this report.

Ispra: European Commission, 2021

Abstract

Vehicle odometer tampering is a malpractice that involves the unauthorised manipulation of mileage readings shown on odometers. Its aim is to create the impression that the motor of a vehicle has a lower mileage than it does in reality, which in turn leads to a higher re-sale price of the vehicle. The tampering of vehicle emission control systems (ECS) pertains to illegally removing, manipulating, or making dysfunctional any system or component used to manage emissions from a motor vehicle engine. The final goal is to get an economic benefit saving operational and maintenance costs linked to ECS. Such a malpractice raises environmental and health concerns and directly threaten the efforts toward reducing air pollution. In this report we specifically focus on digital tampering practices affecting odometers and ECS, so concerning the manipulation of the software and the hardware somehow involved in the functioning of such components. We summarize the legal framework adopted to hinder such practices. Digital tampering techniques affecting such components are presented and the technical countermeasures adopted to oppose to them are discussed. All elements are put in perspective drawing some considerations and recommendations.

Audience

This publication is intended to be read by all those stakeholders involved in the technical specification, manufacturing, installation and monitoring of odometers and emission control systems in vehicles. The document is a source of information for those involved in the design and implementation of these components to make them robust against tamperings. This encompasses legislators defining legal technical requirements and manufacturers. The information of the study can be also relied upon by those entities in charge of verifying the proper functioning of these components, like inspectors and law enforcers. This publication is intended to be of support both in the usage of robust odometers and emission control systems and in the detection of possible tamperings affecting them.

Contents

1 Introduction 2
1.1 Scope of this Report 3
1.2 Methodology 3
1.3 Structure 3
2 Legislation 4
2.1 Key Considerations 8
3 In-Vehicle Digital Architecture and Components of Interest 10
3.1 Odometer 13
3.2 Emission Control Systems 14
4 Digital Tampering 18
4.1 Motivations and Categories of Tamperers 18
4.2 Tampering Techniques 20
4.2.1 ECU flashing 20
4.2.2 Hardware Emulators and In-Vehicle Communication Manipulation 22
4.2.3 Tuning 24
4.3 Odometer Tampering Practices 25
4.4 Emission Control Systems Tampering Practices 28
4.5 Key Considerations 34
5 Digital Security Measures 35
5.1 Relevant Standards 35
5.2 Security Techniques 37
5.2.1 Authentication to ECU 37
5.2.2 Multiple and Protected Data Storage 39
5.2.3 Hardware Modules 40
5.2.4 Complementary Measures Against Unauthorised ECU Programming 41
5.2.5 Physical protection 44
5.3 Key Considerations 44
6 Recommendations and Final Considerations 46
7 Conclusion 52
References 53
List of abbreviations and definitions 59
List of figures 60

1 Introduction

According to the Cambridge dictionary, the term "tampering" is defined as "The action of touching or making changes to something that you should not, usually when you are trying to damage it or do something illegal". With regard to vehicles, tampering activities can be associated to many different components. This report is focused on the main tampering techniques and countermeasures for odometers and emission control systems.

According to a report from the Committee on Transport and Tourism (TRAN) of the European Parliament [2] odometer tampering is "a malpractice that involves an unauthorised manipulation of mileage readings shown on odometers. Its aim is to create the impression that the motor of a vehicle has a lower mileage than it does in reality, which in turn leads to a higher re-sale price of the vehicle." This practice is especially relevant in the second-hand market and cross-border trades, and represents between EUR 5,6 and 9,6 billion in economic damage in the Union. The consequences of odometer tampering are beyond economic aspects. Indeed, it could represent a safety concern for road users, as the manipulated cars could require more maintenance tasks according to actual mileage values.

The tampering of vehicle emission control systems (ECS) pertains to illegally removing, manipulating, or making dysfunctional any system or component used to limit emissions from a motor vehicle engine. Naturally, the installation of a new certified ECS or component that is at least equally effective in lowering vehicle emissions does not consist tampering. Therefore, tampering involves the violation of legislations and/or manufacturer's specifications regarding any component of a vehicle's ECS. Such malpractices raise environmental and health concerns and directly threaten the efforts toward reducing air pollution. Tampering is also connected to economic issues given that "environment-friendly" vehicles may enjoy considerable tax/toll reduction. From an owner's viewpoint, the most obvious economic benefit is not replacing a faulty ECS or not using consumable products with savings to the owner.

From a vehicle's owner viewpoint, the side-effects caused by digital tampering techniques may include missed service intervals, reduced safety, wrong statistics pertaining to the operational condition of the fleet, increased risk due to unwanted changes in other behaviours, which in turn may result in failure in case of emergency or even in normal operation, wrong or misleading information displayed in the vehicle's dashboard, and so on.

As detailed in Section 2, such vehicle tamperings directly violates the EU legislation.

In the following, the terms "tampering", "odometer tampering", and "vehicle emission control tampering" will be used interchangeably depending on the section they refer to. Tampering practices may include:

- digitally or physically installing a replacement part, including hardware/software, that is not approved by the manufacturer;
- removing or altering mechanical, electrical, or hardware/software parts;

Specifically in this report such practices are considered when they prevent the odometer or the ECS from functioning properly.

1.1 Scope of this Report

The aim of this report is multiple. First, it summarizes EU legal initiatives to address Odometer and ECS tampering. Second, after presenting the key components of in-vehicle architecture, it presents a basic adversarial model with the purpose of profiling the tamperers and identifying their motivations. Third, it offers a succinct, but full-fledged review of the basic methods used by tamperers to (a) tamper with the readings and stored values of the odometer, and (b) manipulate the settings of the emission control computer sometimes in parallel with specific hardware of interest. This means that the focus of the current report is on methods and weaknesses that allow the tamperer to directly or indirectly manipulate or replace the software running on a vehicle unit or specific hardware parts, e.g., unit memories. Forth, it provides insights on the current methods followed by vehicle manufactures to contrast digital tampering practices, concentrating among others on authentication services against vehicle units, hardware modules, and physical protection. Lastly, as a side-contribution, the report puts forward a list of key considerations and delivers recommendations.

1.2 Methodology

This study is the result of analysis on documentation available at DG Grow, desktop research and consultations of manufacturers and associations through a survey.

1.3 Structure

The report is structured as follows. The next section details on key parts of the EU legislation regarding vehicle tampering. Section 3 identifies in-vehicle components of interest, while section 4 presents the adversarial model, and elaborates on mainstream digital tampering techniques. Basic anti-tampering techniques and countermeasures against digital manipulations are addressed and exemplified in section 5. The last section puts forward key considerations and recommendations that directly stem from the current study.

2 Legislation

This section summarises key provisions of the EU legislation against tampering.

In the case of *odometer tampering*, different legislative instruments have been introduced to fight against this malpractice. As described by [2] one of the first initiatives is represented by the *Roadworthiness Package* of 2014, which is composed by the *Directives 2014/45/EU* [3] *2014/46/EU* [4] and *2014/47/EU* [5]

The *Roadworthiness Package* requires Member States to make sure that at every Periodic Technical Inspection (PTI) the mileage reading of the previous inspection is made available. However, *Directive 2014/45/EU* stipulates that the first PTI should not be performed later than four years, so a potential attacker could roll back the odometer during this period before the PTI.

*Directive 2014/*45/EU sets several actions of procedural nature to cope with odometer tampering. In particular, it states the need "to link the existing national systems with a view to facilitating exchanges of information on data relating to roadworthiness testing and odometer readings between the competent authorities of Member States responsible for testing, registration and vehicle approval, testing centers, test equipment manufacturers and vehicle manufacturers". Indeed, the recording of mileage in the roadworthiness certificate and access for inspectors to that information should facilitate the detection of odometer tampering or manipulation. In case where an odometer is found to have been manipulated, such manipulation "shall be punishable by effective, proportionate, dissuasive and non-discriminatory penalties." Another aspect is the need to collect and store information from vehicles that were involved in accidents. In this regard, the text highlights the possibility of making information on accident history and odometer readings available in anonymized form to vehicle inspectors, holders of registration certificates and accident researchers. It should be noted that the European Commission, with the cooperation of the Member States, has created in 2020 a web platform to display the different models of vehicle registration and roadworthiness documents [6] This initiative could help citizens to know if the document model is appropriate for a certain country when they buy a second-hand car from abroad, and authorities when they have to re-register an imported car.

Moreover, as described by [7] *Directive 2014/46/EU* introduces a principle of mutual recognition according to which Member States should recognize validity of a roadworthiness certificate issued in another Member State, even if there is an ownership change. This way, the mileage information can be shared across different Member States, in case it is included in the roadworthiness certificate and to the extent that the information is still available in the archives of the issuing Member State (information to be retained at least for 36 months). Furthermore, *Directive 2014/47/EU* foresees an odometer check during a roadside inspection as "visual inspection and/or using electronic interface" and reasons for failure include the odometer being "obviously manipulated (fraud) to reduce or misrepresent the vehicle's distance record" or if it's "obviously inoperative".

In addition to the Roadworthiness Package, *Regulation (EC) 2017/1151* [1] describes several aspects to be considered for protecting odometer readings. In particular, Section 2.3.6 of Annex I recites:

> ***Manufacturers shall effectively deter reprogramming of the odometer readings, in the board network, in any powertrain controller as well as in the transmitting unit for remote data exchange if applicable. Manufacturers shall include systematic tamper-protection strategies and write-protect features to protect the integrity of the odometer reading. Methods giving an adequate level of tamper protection shall be approved by the approval authority.***

These methods have to be approved by the corresponding type approval authority. In that regard the following provision is adopted in Article 5, Section 3(f), of the same Regulation

> ***The manufacturer shall submit the following information:***
>
> ***a description of the provisions taken to prevent tampering with and modification of the emission control computer, odometer including the recording of mileage values***

In addition to previous legislative instruments, a recent text adopted by the European Parliament about odometer manipulation [8] describes the current situation regarding odometer tampering in the EU, including the main consequences associated to this malpractice, as well as existing measures addressing odometer fraud. Furthermore, such documents highlight several loopholes of current legislation, including the need to define effective and dissuasive penalties, or the consideration to interconnect national platforms allowing cross-border data exchange including odometer readings. The already mentioned document [8] also provides several guidelines on the future development in the automotive sector in general, and on odometer tampering in particular, including the use of blockchain as a potential approach for odometer data stores, or the use of technical solutions, such as the Hardware Security Module (HSM) and Secure Hardware Extension (SHE) to protect odometer readings.

Regarding *emission control systems tampering*, we recall that European emission standards specify the tolerable limits for exhaust emissions of new vehicles sold in the EU and Member Countries of the European Economic Area (EEA) Member States. For latest vehicle models, the Euro 6d levelapplies [9] That is, this certification is mandatory for (a) categories M, N1 class I from Jan. 2020 onwards, and (b) categories N1 class II and III, and N2 from Jan. 2021 onwards. For heavy-duty diesel engines, the Euro VI certification is in force from Jan. 2013 onwards [12] with the final Step E coming into force only on Jan. 2021.

First off, *Regulation (EU) 2017/1151* [1] supplementing *Regulation (EC) 715/2007* [10] on type-approval of motor vehicles with respect to emissions from light passenger cars and commercial vehicles (Euro 5 and 6), addresses tampering from a manufacture's viewpoint in Article 5, Section 3(f), stating that the manufacturer shall submit "a description of the provisions taken to prevent tampering with and modification of the emission control computer ..." to the pertinent type approval authority, similarly to odometers as described above.

The same regulation in Annex I, points 2.3.1. and 2.3.2, as amended by Annex I of *Regulation (EU) 2018/1832*, concentrates on provisions for electronic system security stating that

Any vehicle with an emission control computer shall include features to deter modification, except as authorised by the manufacturer. The manufacturer shall authorise modifications if those modifications are necessary for the diagnosis, servicing, inspection, retrofitting or repair of the vehicle. Any reprogrammable computer codes or operating parameters shall be resistant to tampering and afford a level of protection at least equivalent to that afforded by the provisions of the standard ISO 15031-7:2013. Any removable calibration memory chips shall be potted, encased in a sealed container or protected by electronic algorithms and shall not be changeable without the use of specialised tools and procedures. Only features directly associated with emissions calibration or prevention of vehicle theft may be so protected.

Computer-coded engine operating parameters shall not be changeable without the use of specialised tools and procedures (e.g. soldered or potted computer components or sealed (or soldered) enclosures).

Similarly, the following provisions, respectively from Annex I point 2.3.4 and Annex XIV point 2.2, are specifically introduced about the programming of the systems

Manufacturers using programmable computer code systems shall take the necessary measures to deter unauthorised reprogramming. Such measures shall include enhanced tamper protection strategies and write-protect features requiring electronic access to an off-site computer maintained by the manufacturer, to which independent operators shall also have access using the protection afforded in point 2.3.1. and point 2.2. of Annex XIV. Methods giving an adequate level of tamper protection shall be approved by the approval authority.

Access to vehicle security features used by authorised dealers and repair shops shall be made available to independent operators under protection of security technology according to the following requirements:
(i) data shall be exchanged ensuring confidentiality, integrity and protection against replay;
(ii) the standard https//ssl-tls (RFC4346) shall be used;
(iii) security certificates in accordance with ISO 20828 shall be used for mutual authentication of independent operators and manufacturers;
(iv) the independent operator's private key shall be protected by secure hardware.
The Forum on Access to Vehicle Information provided for by paragraph 9 of Article 13 will specify the parameters for fulfilling these requirements according to the state-of-the-art.

For independent operators, the requirements for getting access to security-related functionalities are further refined in a scheme provided by the SERMI association [89] Among other specifications, independent operators have to receive a secure hardware token containing a digital certificate and its associated PIN. Such equipment is used to access some vehicle units security-related functionalities.

Moreover, Appendix 1 of Regulation (EU) 2018/1832, point 3.1.3 pertaining to penalties in Regulation (EC) 715/2007, addresses the manufacturer, but not the vehicle operator, or the owner. It is explicitly stated that:

> ***Non-compliance with the requirements of paragraph 7.1.6. of Appendix 1 to Annex 11 to Regulation No 83 established by tests described in point 3.1.2 of this Appendix or paragraph 7.1.9 of Appendix 1 to Annex 11 to Regulation No 83 shall be considered as an infringement subject to the penalties set out in Article 13 of Regulation (EC) No 715/2007. This reference does not limit the application of such penalties to other infringements of other provisions of Regulation (EC) No 715/2007 or this Regulation, which do not explicitly refer to Article 13 of Regulation (EC) No 715/2007.***

Regulation (EU) 2017/1151 also provides links to Annex 11 of UN/ECE Regulation No 83, which mentions the requirements for the On-Board Diagnosis system (OBD) to monitor the total failure or removal of critical components linked to the ECS.

On the other hand, *Regulation (EC) 595/2009* [11] on type-approval of heavy-duty vehicles defines tampering as the:

> ***inactivation, adjustment or modification of the vehicle emissions control or propulsion system, including any software or other logical control elements of those systems, that has the effect, whether intended or not, of worsening the emissions performance of the vehicle.***

Precisely, tampering is addressed in Article 5 (provisions to guarantee the right operation of NOx control measures), Article 7 (Manufacturers, repairers and operators of the vehicles shall not tamper with systems which use a consumable reagent), and Article 11 (relevant penalties to be determined by the Member States). It is to be noted that Article 11 specifically refers to infringements by repairers and vehicle operators stating that

> ***The types of infringements by manufacturers, repairers and operators of the vehicles which are subject to a penalty shall include tampering with systems which control NOx emissions. This shall include, for example, tampering with systems which use a consumable reagent. The types of infringements committed by operators of the vehicles which are subject to a penalty shall include driving a vehicle without a consumable reagent.***

Also, Regulation (EU) 582/2011 [12] which implements and amends 595/2009, explicitly addresses tampering of the emission control systems in Articles 5 and 6.

The above analysis leads to an important observation. That is, opposite to heavy-duty vehicles, the legislation for light-duty ones does not take measures against the main responsible for such tampering, i.e. the owner or operator of the vehicle.

The table below summarises all European legal initiative to deal with Odometer and Emission Control System tampering.

Odometer tampering	
Roadworthiness Package	Directives 2014/45/EU, 2014/46/EU, 2014/47/EU.
Regulation	*Regulation (EC) 2017/1151. It supplements Regulation (EC) 715/2007, amends Directive 2007/46/EC, Regulation (EC) 692/2008 and 1230/2012, and repeals Commission Regulation (EC) No 692/2008.*
Regulation	Regulation (EU) 2018/1832. It amends Directive 2007/46/EC, Regulation (EC) 692/2008, and Regulation (EU) 2017/1151.
Emission control systems tampering	
Regulation	*Regulation (EC) 715/2007.*
Regulation	*Regulation (EC) 595/2009. It amends Regulation (EC) 715/2007, Directive 2007/46/EC, and repeals Directives 80/1269/EEC, 2005/55/EC and 2005/78/EC.*
Regulation	*Regulation (EU) 582/2011. It implements and amends Regulation (EC) 595/2009, and amends Annexes I and III to Directive 2007/46/EC.*
Regulation	*Regulation (EU) 2017/1151. It supplements Regulation (EC) 715/2007, amends Directive 2007/46/EC, Regulation (EC) 692/2008 and Regulation (EU) 1230/2012, and repeals Regulation (EC) No 692/2008.*
Regulation	Regulation (EU) 2018/1832. It amends Directive 2007/46/EC, Regulation (EC) 692/2008, and Regulation (EU) 2017/1151.

Table 1. Milestones in EU legislation regarding Odometer and ECS tampering in chronological order

2.1 Key Considerations

In the table below we summarise some remarks about the provisions mandated in EU legislation (they are marked as L.X) to withstand digital tampering of Odometers and ECS. The considerations stem from our analysis of the technical content of the different legislations and standards summarized in the previous section.

	Consideration	Description
L.1	Lack of detailed requirements	Most of the requirements are generic, missing a clear identification of the components concerned and their security requirements for stored, processed and communicated data and their physical anti-tampering provisions. This is common for both internal vehicle components and operators equipment. In addition the range of application of provisions is not always clear, e.g. not clarified if Annex I point 2.3.4 in Regulation 2017/1151 applies to Odometers as well.
L.2	Reference to standard not really prescribing concrete solutions	The ISO 15031-7 referenced in Annex I point 2.3.1 in Regulation 2017/1151 gives generic indications without specifying any concrete security solution, simply delegating the manufacturers for the design and implementation of such measures.
L.3	Lack of uniform and common accepted type approval scheme	The kind of information to be provided and the procedure to assess the validity of the security solutions is at discretion of the different approval authorities, without any common guideline, minimum requirement or reference standard, see for instance Article 5, Section 3(f) in Regulation 2017/1151.

Table 2. Key considerations about current EU legislation with regard to protection against Odometer and ECS tampering

3 In-Vehicle Digital Architecture and Components of Interest

Figure 1 shows an overall digital architecture of a vehicle.

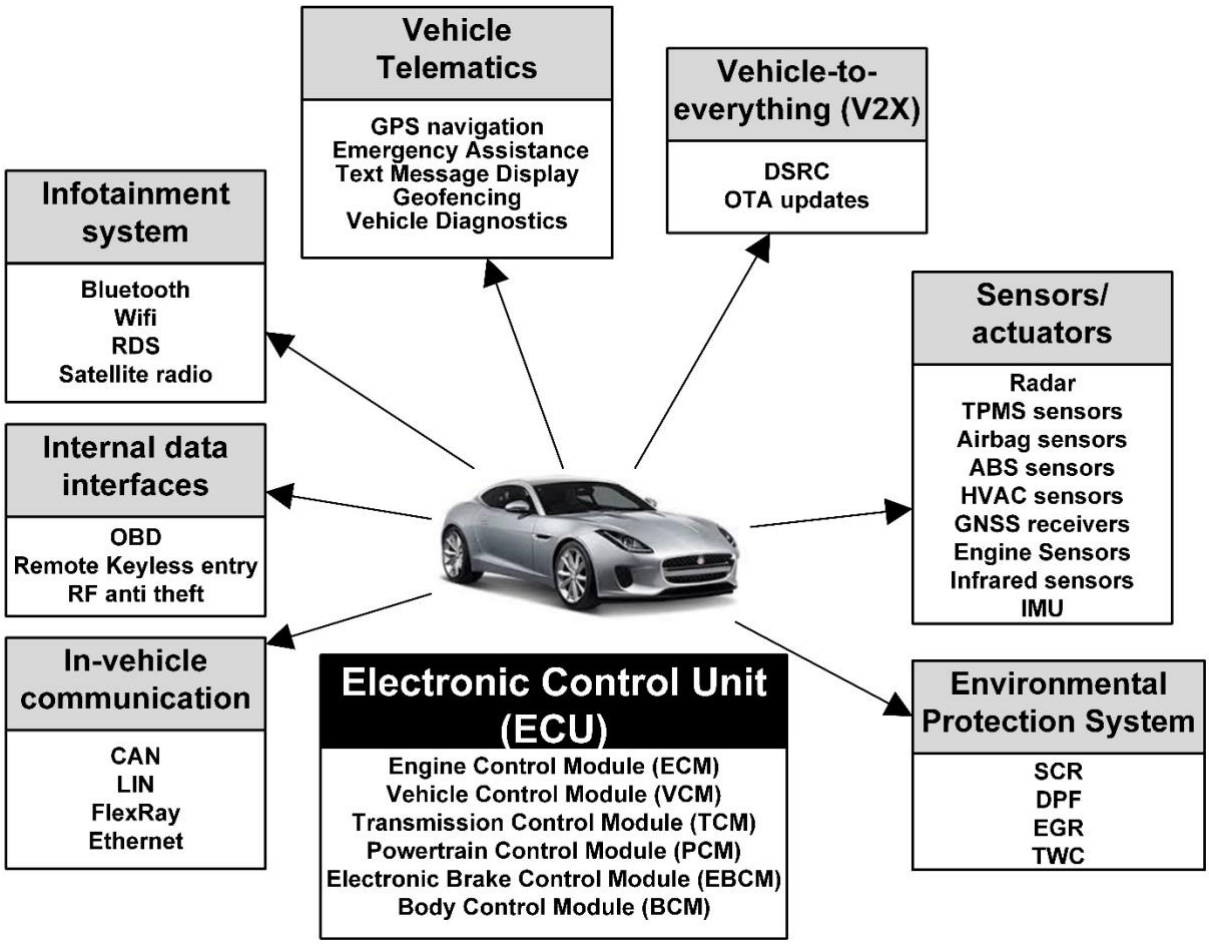

Figure 1. In-Vehicle Digital Architecture

Taking into account such architecture, the main components are:

- *Electronic Control Unit (ECU)*: a single or a collection of electronic control modules that prioritize, control, and manage the requirements for the engine and other major vehicle subsystems. Generally, an ECU receives signals from sensors or other ECUs, process them, and provides signals to actuators or other ECUs. Typically, the term ECU may refer to the following modules: Engine Control Module (ECM), which controls the actuators of the engine, including air to fuel ratios, Vehicle Control Module (VCM), which controls the engine and vehicle performance, Transmission Control Module (TCM), Powertrain Control Module (PCM), which is typically a combination of an ECM and a TCM, Electronic Brake Control Module (EBCM), which is responsible for the anti-lock braking system, and Body Control Module (BCM), which controls power windows, power seats, etc. Depending on the fuel used, additional ECUs may also exist, i.e., a dedicated Selective Catalytic Reduction ECU for diesel vehicles, which operates based on input stemming from a number of sensors. According to a recent report [13] a modern vehicle can integrate as many as 150

ECUs. In modern vehicles, one can roughly discern between two categories of ECUs: (a) those in charge of advanced driver-assistance systems and controlling car operations like steering, switching gears, braking, fuel consumption, and so on. These ECUs are typically controlled by a real-time operating system, like QNX Neutrino [14] and VxWorks [15] and (b) ECUs responsible for audio/video infotainment systems and relevant applications. These ECUs can be operated by operating systems quite like those that run on a personal computer, say, Linux. The term "ECU flashing" pertains to the reprogramming of ECU memory, which is non-volatile, but a kind of Electrically Erasable Programmable Read-Only Memory (EEPROM). Authorised "reflashing" is necessary to recover faulty ECUs or to upgrade firmware as per manufacturer's instructions. The interconnection of ECUs is achieved by diverse type of architectures and protocols depending on the manufacturer. In the following, the term "ECU" will generally refer to any electronic control module (microprocessor) that oversees millage tracking or emission control.

- *On-board diagnostics (OBD)*: it comprises an on-board computer system, which uses a network of sensors to monitor vehicle's operating conditions, including those responsible for controlling emissions. Any error found by the OBD protocol triggers the illumination of the Malfunction Indicator Lamp (MIL) – also referred to as Check Engine Light (CEL) - in the dashboard, and the generation of a Diagnostic Trouble Code (DTC) that corresponds to the problem. Furthermore, in modern vehicles, additional information (called freeze frame data) is stored, along with the trouble code, when a fault occurs. These data are stored by the units concerned by the fault and they are essentially a snapshot from a number of components and sensors somehow involved in the fault. A 16-pin port (connector) is offered by the OBD system, and specific tools can be connected to it to read DTCs, freeze frame data, or to interact with ECUs; indeed via such a connector it is typically possible to get access to the vehicle network, say, the CAN bus. Typically, the OBD port is located under the driver's side dash. Note that as per Regulation (EU) 2017/1151, article 4, "The manufacturer shall ensure that all vehicles are equipped with an OBD system".
- *In-vehicle communication*: such networks are used to interconnect the different ECUs and use different protocols, namely automotive Ethernet (IEEE 802.3bw-2015 [17] also known as 100BASE-T1), Flexray (defined in ISO 17458-1 [18] to 17458-5 [19] , Controller Area Network (CAN), and Local Interconnect Network (LIN) [20] The CAN bus protocol is hitherto by far the most widely used, so it is briefly discussed hereunder. The lower two layers of the protocol stack, namely PHY and Data Link, of CAN are defined in ISO 11898 [21] while other standards, including CANopen [22] and SAE J1939 [23] extend the CAN standard by defining upper layers, say, layers 3 (network) and 7 (application) with reference to the OSI model. CAN bus employs two dedicated wires for communication, namely CAN high and CAN low. When the bus is in idle mode, both the low and high lines carry 2.5V. When information is transmitted, CAN high line switches to a higher voltage (3.75V) and CAN low to a lower one (1.25V). Given this voltage differential of 2.5V between the two lines, CAN becomes a reliable choice for networked communications in noisy environment, i.e., it is highly insensitive to inductive spikes, electrical field, or other sources

of noise. The Data Link Layer enables all the relevant vehicle's components to transmit and receive data on the bus. In the same CAN bus network, each message carries a unique message ID, either 11-bit or 29-bit for CAN 2.0A (StandardCAN) or CAN 2.0B (ExtendedCAN), respectively. That is, an 11-bit ID allows for 2^{11} different messages, while a 29-bit ID for 2^{29}. Note that the CAN standard per se does not support node addressing. On the other hand, in SAE J1939, the last 8 bits of the message's ID represent the transmitting node's source address, thus allowing for 2^8 unique addresses. The CAN messages are broadcasted, meaning that all nodes can listen to every transmission. The CAN controller of each ECU filters each message and decides if it is interesting or not, e.g., checking if they are addressed to the ECU itself. As per the standard, the maximum data throughput is 1Mbit/s, but common rates are 125Kbits/sec for CAN Open and 250Kbits/sec for J1939. Communication relies on frames, either data, error, remote (carries no data and it is solely used to solicit the transmission of data from another node), or overload (it is transmitted by a node if it becomes too busy). Depending on its type, a frame can carry start and stop bits, frame type, a unique CAN message ID, data (at most eight bytes), a 15-bit checksum (CRC), and an acknowledgement slot. Note that the unique message ID is contained in the so-called arbitration field, which specifies the priority of the frame for contention resolution, i.e., which frame will be transmitted on the bus (critical frames, as for instance those related to the ABS ECU, are assigned IDs granting high priority on the bus). CAN bus messages are neither authenticated nor encrypted, and as expected, there is plethora of CAN readers and other tools dedicated to CAN manipulation available on the market. In addition, access to the CAN bus can be easily achieved via the installation of, say, a scotch-lock wire connector. For obtaining more information on CAN and relevant hacking techniques, the interested reader may refer to the work in [24]

- *Sensors and actuators*: a sensor is a device that detects and responds to some type of input from the physical environment both inside and outside the vehicle. For example, a sensor can monitor the temperature of the water in the car engine. Actuators are components that act on the environment on the basis of a specific request (e.g., from an ECU). In the automotive environment, actuators are used to regulate the behaviour of a vehicle component (e.g., the fuel injection).

In addition, the following key assets are of high interest to a cyber attacker. This is because such assets are well related to tampering, for instance by hacking the infotainment one might obtain access to the CAN bus, or a mileage freezer might interfere with vehicle telematics.

- *Vehicle telematics*: they combine telecommunication and informatics, bringing navigation, safety, security, and communication services into the vehicle's dashboard. GPS navigation, Automatic Collision Notification, Emergency Assistance, Text Message Display, Geofencing, Vehicle Diagnostics, Over-the-Air (OTA) updates, and others are examples of a telematic service.
- *Infotainment systems*: they may be a part of the vehicle telematics or an autonomous subsystem. These systems provide driving information and entertainment for passengers and drivers. Such a system typically offers a

graphical user interface displayed via a specialised monitor. Passenger smartphones can potentially connect to the infotainment system.

- *Vehicle-to-everything (V2X) communication*: it includes Vehicle-to-Vehicle (V2V) and vehicle-to-Infrastructure (V2I) communications, which are part of the Intelligent Transportation System.

3.1 Odometer

According to [7] an odometer can be defined as "an instrument measuring the distance travelled by a vehicle", and it is structurally integrated with a speedometer, which indicates the speed of a vehicle at any given moment. The odometer represents a very relevant device in a vehicle as it could determine the actual conditions of that vehicle, and the need for maintenance tasks, such as changing the engine oil.

The basic operation principle of an odometer is based on measuring the number of revolutions made by the tyre and transform this number into a distance magnitude, which is shown to the driver via the vehicle's dashboard. Based on this principle, there are two main type of odometers: mechanical and electronic. The *mechanical* odometer is composed by set of gears and numbered tumblers, as well as a coaxial cable that is connected to the front wheel-hub and the odometer itself. In the vehicle, a gear engages the output shaft of the transmission, thus turning the odometer cable as well. This cable is specifically connected to the input shaft of the odometer, this way the tumblers are turned to reflect the changes in the travelled distance on the vehicle's dashboard. Every 10 turns, the adjacent tumblers are rotated by one digit. Figure 2 shows an example of this.

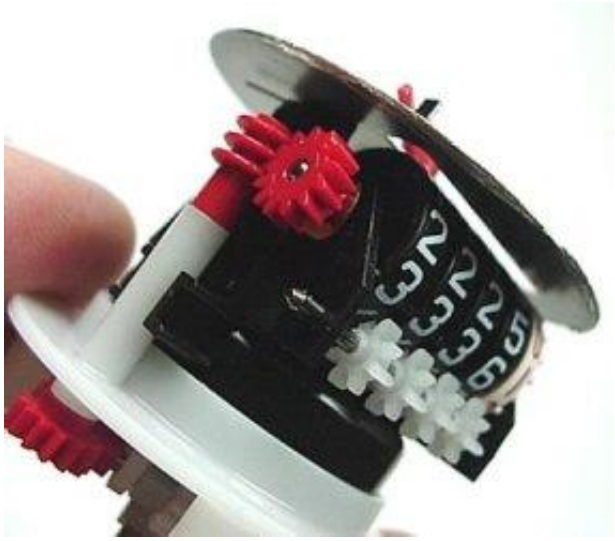

Figure 2. Example of mechanical odometer [56]

However, contemporary vehicles make use of *electronic* odometers, which replace mechanical devices by electronic components. These odometers are smaller, more accurate and require fewer components (e.g., the cable is not required) to operate.

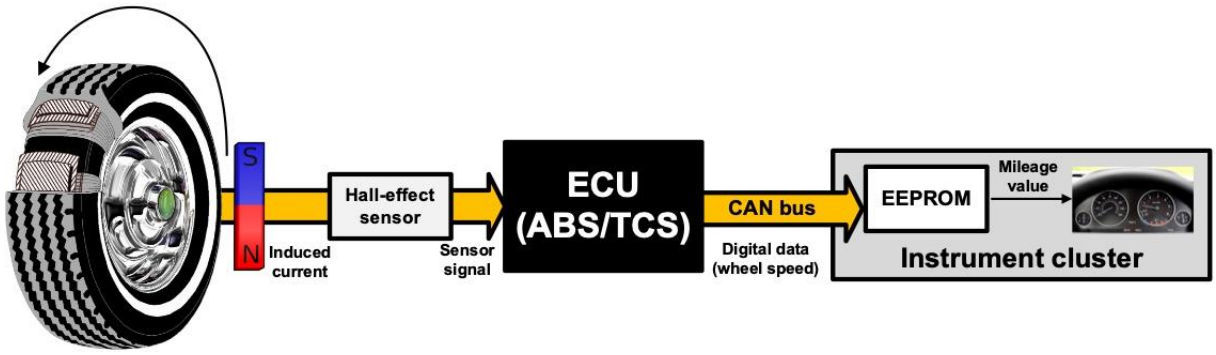

Figure 3. Basic operation of a digital odometer

For electronic odometers, one can distinguish between *electromechanical* and *digital* odometers. While the former combines electronic with mechanical components in the instrument cluster (e.g., tumblers), the later integrates basically only several electronic components to obtain the mileage values.

Figure 3 shows the basic operation of a digital odometer in which a magnet is attached to a rotating driveshaft, which in turn, is connected to a wheel. For each wheel revolution, the magnet produces a magnet field, which passes through a Hall-effect sensor. This sensor is connected to the Antilock Braking System (ABS) or the Traction Control System (TCS), which are two ECUs provided by the vehicle's Electronic Stability Program (ESP). Then, this ECU translates the sensor signal in digital data representing the wheels speed. This information is sent out on the CAN bus, and consequently, received by other vehicle's components. In particular, the instrument cluster (which can be considered as an ECU itself) reads the wheel speed value from the bus and converts it in vehicle speed and vehicle mileage. The mileage is stored in the EEPROM of the instrument cluster. This value is shown on a display of the instrument cluster that is visible to the vehicle driver.

Based on this description, and according to the report provided by [54] the way in which the odometer value is then managed by a vehicle varies among different manufacturers. For instance while in some vehicles the odometer value is not transmitted over the CAN bus, in most of contemporary vehicles the instrument cluster ECU can send the mileage value out on the CAN bus for making it available to other ECUs (for instance for backup or checking purposes).

According to the odometer architecture, as described in Section 4.3, several considerations must be taken into account to cope with potential tampering techniques for odometer devices.

3.2 Emission Control Systems

Depending on the vehicle type, ECS used to monitor and lower vehicle emissions typically comprise Selective Catalytic Reduction (SCR), Diesel Particle Filter (DPF), Exhaust Gas Recirculation (EGR), Gasoline Particle Filter (GPF) and Three-Way Catalyst (TWC). The first three systems are specific to diesel vehicles, while the latter two to gasoline ones.

As shown in Figure 4, DPF is a device destined to remove diesel particulate matter or soot/ash from the exhaust gas of a diesel engine. In fact, normally, the

particulate matter is removed up to 98% or more. Similarly, Gasoline Particle Filters remove a big part of particles emitted from Gasoline Direct Injection engines. Both DPF and GPF may be completely or partially damaged by cracks created due to thermal ageing, or by clogging. The following are equally relevant for DPF and GPF. l Cleaning the filter substrate or even replacing it induces considerable costs, hence tampering seems an alluring alternative for the user. As detailed in Section 4.4, filter-specific sensors, including differential pressure sensor throughout the filter, temperature sensor of the filter exhaust gas, and mass air flow sensor, as well as the the ECU in charge of monitoring the filter functioning is of high interest to a filter tamperer.

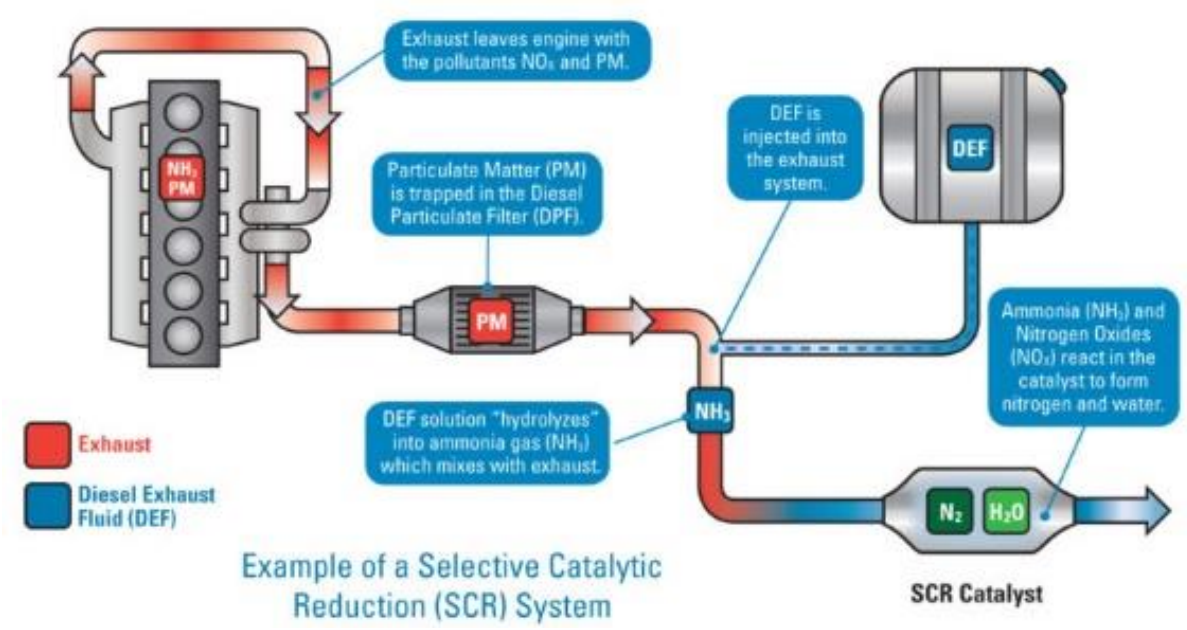

Figure 4. Basic operation of the SCR process [57]

The Selective Catalytic Reduction (SCR) is technology system to reduce the emissions of nitrogen oxide produce by diesel engines. To this end, the system injects a reductant agent (usually ammonia or a urea solution) into the exhaust stream of the engine in a catalyst. Such reductant agent converts nitrogen oxides into other elements, including nitrogen, water and carbon dioxide, which are expelled through the vehicle's exhaust pipe. Figure 4 shows the basic operation of the SCR system combined with the use of the particle filter, which was previously explained. SCR improves fuel efficiency, in addition to emission control. As shown in Figure 5, several electronic are employed to control the SCR system. Basically, an SCR ECU monitors the catalyst process through some sensors and according to their measures doses the agent to be injected. Such an ECU is connected to the CAN bus and communicate with the engine ECU about the SCR system behaviour. As detailed in section 4.4, the CAN bus, SCR specific sensors, and the ECM attract the attention of SCR tamperers.

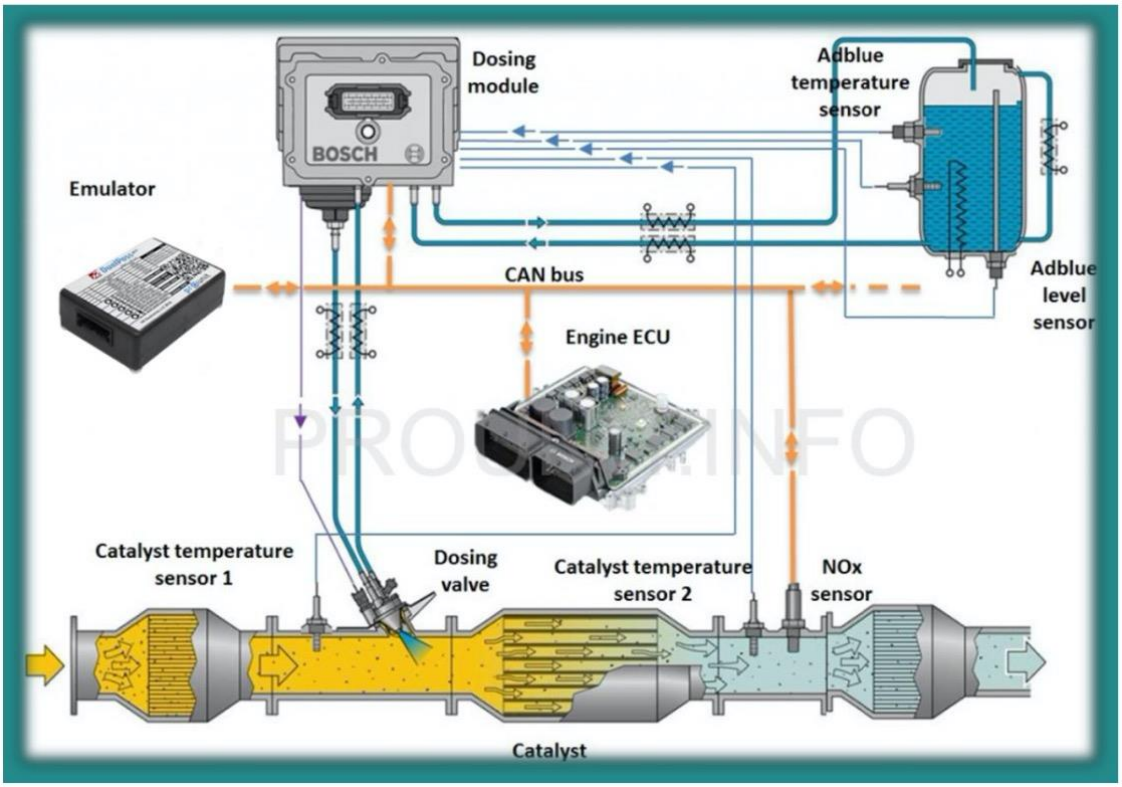

Figure 5. Basic components of the SCR emission reduction system of a diesel vehicle [25]

The Exhaust Gas Recirculation (EGR) is a technique to recirculate part of the exhaust gas to the intake manifold.

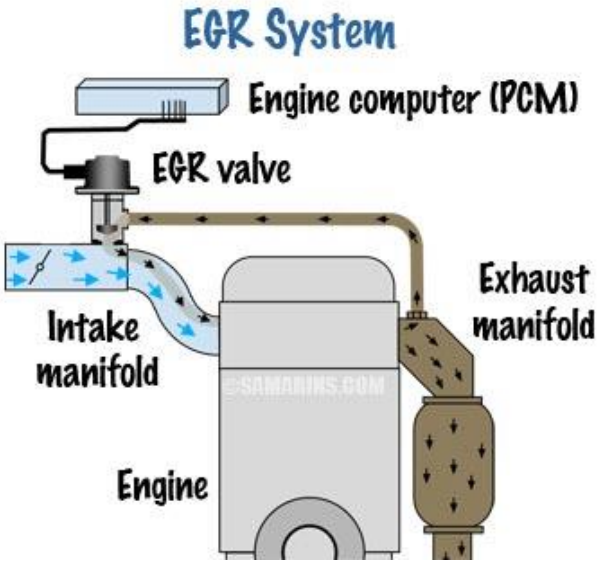

Figure 6. Basic Operation of the EGR system [58]

Figure 6 shows the basic operation of the EGR system, in which the PCM (which typically incorporates the ECM) is intended to control the flow of the system by opening/closing the EGR valve. Generally, the EGR valve is electronically (modern vehicles) or mechanically (pneumatic) controlled [60] The valve connects the intake manifold with the exhaust manifold. On the downside, the

EGR valve, especially if of bad quality, may get clogged up with carbon deposits, which can make it fail or even stuck in the open/close position. Naturally, this situation causes error codes, and in principle may stall the engine. As explained in section 4.4, the ECU controlling the valve (ECM) and components monitoring the gas flow comprise the systems of interest when EGR tampering is considered.

Three-Way Catalysts (TWC) are the basic technology employed to control emissions from petrol (gasoline) engines. The catalyst incorporates a ceramic or metallic substrate with an active coating incorporating alumina, ceria and other oxides and combinations of the precious metals, namely platinum, palladium, and rhodium. TWC operates in a closed-loop system including a lambda sensor, also called an oxygen (O2) sensor, to regulate the air-to-fuel ratio [16] That is, the oxygen concentration data are sent to the ECU (ECM), which regulates the amount of fuel injected into the engine to compensate for surplus fuel or surplus air. The catalyst can then simultaneously oxidise CO and HC (hydrocarbons) to CO2 and water, while reducing NO_x to nitrogen. The basic components of a TWC are depicted in Figure 7. Typically, as explained in section 4.4 the lambda/oxygen sensor and the ECU controlling the TWC process attract the attention of tamperers.

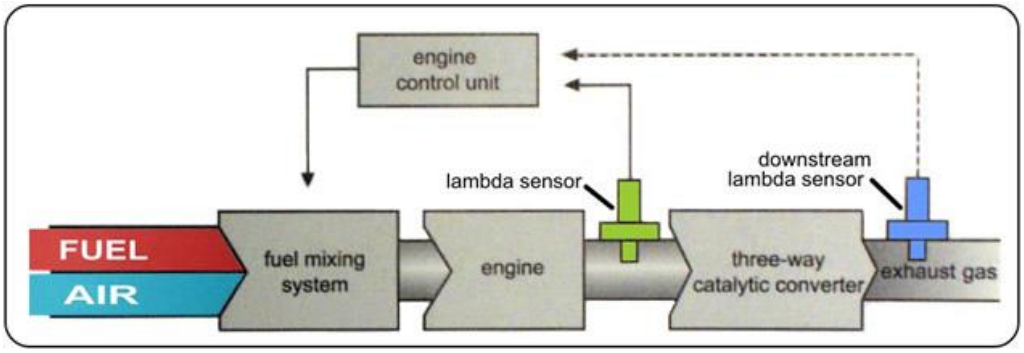

Figure 7. Three-way catalyst closed-loop system [59]

4 Digital Tampering

4.1 Motivations and Categories of Tamperers

From a cybersecurity viewpoint, we must distinguish between a "tamperer" and a "cyber attacker" (attacker). The latter category of actors attacks the electronic components of a vehicle without the owner's permission, while the first collaborates with the owner and is typically being paid by them. So, the tamperer has physical and directly "authorised by the owner" (root) access to the vehicle, and therefore its OBD interface and physical components. This also means that the tamperer may be able to reprogram the ECU or install, modify, or remove, say, a sensor or any other system at will.

An attacker on the other hand typically exercises their attacks remotely, except in the case where the vehicle is hijacked or stolen by the attacker or an accomplice of them. Broadly speaking, attackers are more interested in stealing, high-jacking, damage, or paralyse specific subsystems of the vehicle, modifying the cyber-physical capabilities of the vehicle, confuse or harass the driver, and compromise passengers' location-privacy, rather than manipulating the vehicle's odometer and ECS. Therefore, the major components in their focus are anti-theft systems, vehicle-to-everything (V2X) communications, telematics, infotainment, anti-lock braking systems, tire-pressure monitoring systems, airbag control units, and heating, ventilation and air conditioning systems.

An attacker may participate in a tampering incident, but in this case, their motive is different; it may include self-reputation, revenge, activism, fraud and e-crime, industrial espionage, opportunism, obsession, anger, ego, self-promotion, curiosity or boredom, worldview, etc. Monetary gain is also not to be ruled out, say, in case the attacker attempts to obtain a piece of software, having it reverse engineered, and then sell it to tamperers or any other interested party, including brokers. Conversely, given that emission standards are becoming stringent, the root motivation of a tamperer is basically anchored to the lowering of vehicle's maintenance costs, namely the expenses for consumables, the improvement of fuel economy, the skipping of regular service or necessary repair, and the reduction or avoidance of toll payments[1]. Another reason may be related to increasing the horsepower of the vehicle.

The vast majority of odometer and ECS tampering incidents today involve a tamperer. However, next-generation tamperers may take advantage of the available vehicle cyber attacking tools and methods and/or closely collaborate with cyber attackers with the purpose of exercising their activities remotely and in anonymity. This may be feasible by exploiting wireless interfaces, say, Bluetooth, IEEE 802.11, and others mostly offered by the telematic systems installed in current and future vehicles.

Given the above-mentioned observations this report concentrates on the "tamperer" type of adversary. However, for the sake of completion, we also detail on possible attack points and vectors, which can be possibly exploited by cyber attackers to tamper with the vehicle electronic systems, including the odometer and the ECS ones. The following types of tamperers, either individuals or groups, are considered in the context of this report.

[1] For instance, in Switzerland there is a significant toll saving associated with the "performance-dependent heavy traffic tax" [25] .

- Non-tech-savvy: mostly the vehicle owner or other inexperienced individuals who do not have technical knowledge on tampering methods. They exploit off-the-self and straightforward-to-use solutions and devices;
- Automotive hobbyist or enthusiast: they have some knowledge on tampering techniques mostly acquired by searching and reading manuals, seeking advises from specialists, participating in relevant forums, and self-experimentation. They can perform basic, low-risk tampering;
- Automotive mechanic expert: they are tampering-savvy and have several years of experience in the technical and mechanical aspects of vehicles. They are typically professionals specialized in repairing and modifying vehicles, and thus they can carry out complex tampering tasks. Also, they are able to tamper the Electronic Control Unit (ECU) by using ready to deploy software tools and files acquired externally;
- Automotive software expert: they are computer engineers specialized in automotive software and electronic equipment. They can read, interpret, analyse, and possibly manipulate pieces of data extracted from ECU. To this end, they may use custom-made software tools. Typically, they are interested in producing ready-to-use software tools and ready-to-flash modified versions of ECU data files and sell them to any interested party. This type of adversaries has also the knowledge and skills to remotely attack and compromise any electronic system on a vehicle in the existence of a vulnerability. Therefore, some of them may act as "attackers" as well.

Adversaries are assumed to potentially possess the following capabilities depending on the specific category they belong to:

- have physical or can obtain remote access to the vehicle;
- can team up, built communities, and share their knowledge either in the premises of a brick-and-mortar workshop or remotely, say, via the Internet; think of blogs, forums, chat rooms, etc. Forums may be closed or open. It may also be hierarchically structured, based on the contribution made by the tamperer; greater contribution means elevated access. Indicatively, two of the most popular forums are ECU Connections [26] and ECU Tuning Performance [27]
- have the technical expertise to reverse-engineer any system and protocol either by themselves or by seeking the help of a third party;
- have the necessary resources, such as, money, software, and hardware equipment to fulfil their task;
- have access to publicly available automotive vulnerability database systems;
- can collude with law enforcement or automotive authorities and exfiltrate information about, for instance, vehicle inspections, think of bribery, corrupted employees, etc;
- can lure hesitant vehicle owners to grant them access to vehicle by, for instance, promising the owner extra benefits over a certain modification;
- can covertly operate black markets via the dark web, e.g., over the Tor overlay;
- adhere to all cryptographic assumptions, that is, they are unable to decrypt a properly encrypted file without knowing the decryption key, and they cannot impersonate others without knowing the private key of an asymmetric key pair;
- especially for attackers, they can intercept, block, modify, inject, or replay any message in the public communication channel. They can exercise the

same attacks in the in-vehicle communications channel if they have physical access to the vehicle.

4.2 Tampering Techniques

This section succinctly describes the main tampering techniques that are applicable to different vehicle's components and, in particular, to odometers and ECS. Also, a high-level categorisation of the discussed methods is given in Figure 12.

4.2.1 ECU flashing

The ECU EEPROM is segmented to arrange information. We discern between the "program flash" (PFLASH), which pertains to the area where the control logic, i.e., the software code resides, and "data flash" (DFLASH), which accommodates the constants, maps (matrix variables), curves (vector variables), and calibration (scalar) variables that the program code uses. This abstraction aids in reusing the code for several variants of the same system with tiny tweaks. Below we present techniques adopted by tamperers to modify such EEPROM areas.

4.2.1.1 OBD Flashing

The flashing operation requires a flashing tool to be connected to the OBD port and controlled by the respective software installed on a computer, allowing the user to choose the corresponding firmware file to be installed on the ECU or to modify some ECU parameters. A short video presenting such a plug & play tool is given in [28] OBD Wi-Fi or Bluetooth adapters also exist [29] which allow for ECU flashing conducted via a laptop, tablet, or smartphone wirelessly connected to the adapter. Actually, there already exist a plethora of smartphone apps for vehicle monitoring via the OBD interface [30] and some of them may be exploited for flashing operations too. On the other hand, prominent examples of professional ECU flashing tools are the "Volvo Premium Tech Tool PTT 2.7 Development Mode & Dev tool" [31] the "LAUNCH X431 V PRO" [32] "Autotuner" [33] "CMD Flash Master plus OBD II" [35] and FLEX [36]

It is to be noted that such tools can come into two versions, namely "Master" and "Slave". The first does reading and writing in a cleartext format, so its operator can alter the files by themselves or send it to a third party. Any editing software, say, EVC WinOLS [37] that supports binary file can be used to modify a file read by such a tool (see Figure 8). Put simply, the master can read the files stored in the ECU, then, the parameters of interest can be edited and be rewritten back in the ECU. On the other hand, a slave tool only reads and writes off the shelf encrypted files, meaning that these files can be only modified by a Master, i.e., a file provider associated to the tool. The file received by the Master can be written in the ECU by the Slave. This also means that any Slave tool is linked to its Master, and a Slave owner must turn to its Master for tuned files. The Slave tool can be remotely transformed into a Master if the Master specifically approves the shift, and the price difference is payed.

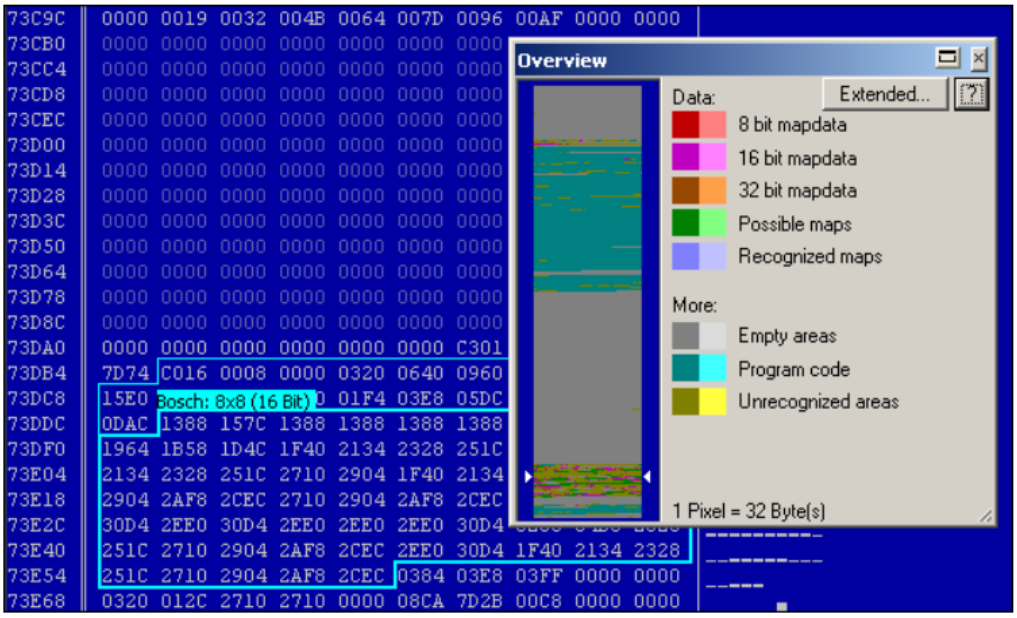

Figure 8. A screenshot of the WinOLS application. As observed, the application can automatically recognise program code, empty areas, maps, etc. [37]

4.2.1.2 Debug and Boot Modes

Specific interfaces are leveraged to reprogram the system. For instance, the Background Debug Mode (BDM) interface allows debugging of embedded systems by offering in-circuit debugging functionality in microcontrollers. This means that BDM-oriented vehicle tampering mandates the removal of the ECU from the vehicle for accessing the BDM port, which, as already pointed out, is provided by the manufacturer for debugging proposes. This allows the flashing of the ECU and this method is suitable if the chip cannot be flashed using other tools, as for instance OBD flashing solutions. As shown in Figure 9, a prominent example of such a tool is the BDM100 [38] by EVC electronic GmbH. The JTAG is another example of debug interface that can be used for the same scope.

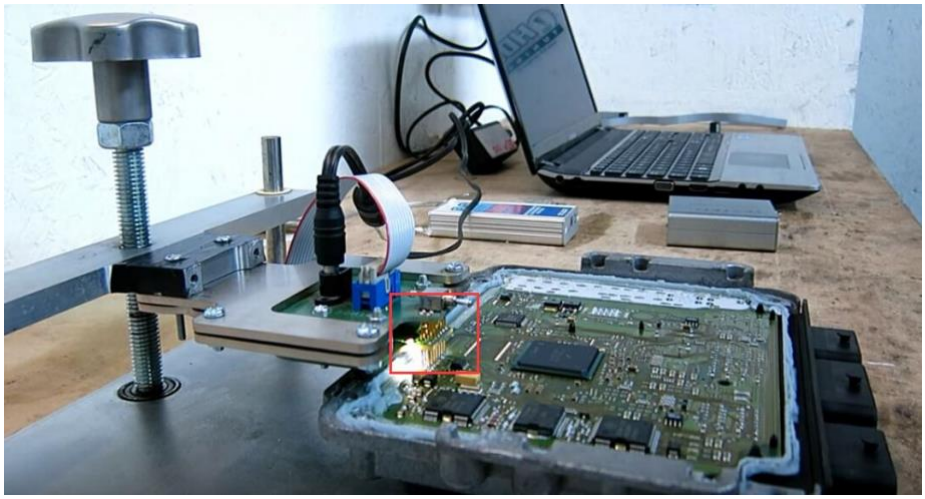

Figure 9. A BDM testbed [38]

A similar approach can be followed with the Bootstrap Loader (BSL). A BSL is a small piece of code which can be triggered soon after a microcontroller has been powered up with the aim of loading and executing another program. The bootstrap loader is hardcoded in the microcontroller and is exploited to update

the device's firmware. Specifically, after enabling the microcontroller's bootstrap mode, a loader program can be employed to store a number of routines on the microcontroller. Next, these routines are used to update the firmware. For vehicles, BSL flash programming requires both the removal of the concerned ECU and some soldering operations. Specifically, several microcontrollers like the Infineon XMC4000 microcontroller family [40] provide a built-in BSL mechanism, actually an equivalent to the BDM port called "bootmode", that can be used for flash programming. Some microcontrollers support both an asynchronous serial BSL interface and a CAN-based BSL approach. For acquiring a more detailed understanding of these two types of BSLs for Infineon XMC4000 family microprocessors, the interested reader may refer to [42] and [43] respectively. BSL100 [44] by EVC electronic GmbH is a typical tool used for BSL programming. Several ECU manufacturers try to restrict BSL access by setting a bootmode password.

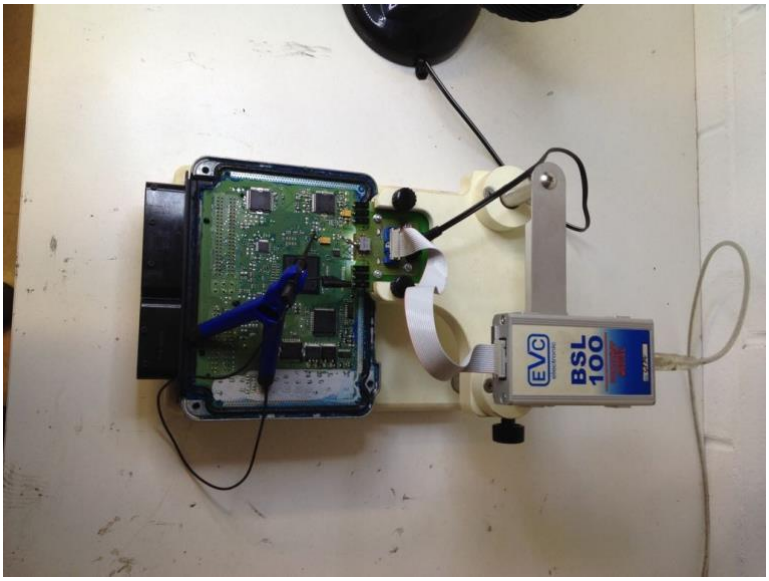

Figure 10. A BSL testbed [44]

4.2.1.3 ECU Soldering

To perform the flashing operation, it is required to remove the ECU from the vehicle and to unsold its memory chip. After unsoldering the chip, an EEPROM programmer is used to read and save the software. The software is then modified and re-installed in the memory. In some cases, the tamperer may solder a chip socket at the original location of the memory chip ("Chipable" ECU). In such a case the modified chip is plugged in the socket, which allows to easily repeat the tampering operation other times. Also, note that the tamperer may not flash the original chip, but directly replace it with a new one. A short video demonstrating such a procedure is available at [34]

4.2.2 Hardware Emulators and In-Vehicle Communication Manipulation

Generally, hardware emulation is the process by a certain hardware component is mimicked by a different hardware device. An emulator is destined to fool or usurp control of certain components and drive them to provide falsified information (signals) to another component. We can discern between three basic cases:

1. an additional resistor or controller intervens between a sensor and an ECU to feed the second with fake information and lead it to instruct the relevant actuator wrongfully or not at all;
2. a controller is placed between an ECU and an actuator to fake the signals provided originally by the ECU. By doing so, the actuator will receive counterfeited signals or no signal(s) at all.
3. a controller is placed in the communication channel between two ECUs, e.g., between the engine controller and the emissions controller to feed the second with fake signals. A controller may be also employed to replace subparts of ECUs, as for instance memory components.

Naturally, depending on the situation, the aforementioned cases can be combined with each other.

To be noted that all techniques adopted to simply alter electrical signals related with sensors and actuators (this typically goes under cases 1 and 2 above) are not part of the focus of this report, which is devoted to digital manipulations. Anyway they are mentioned for completeness and because they may have an influence on digital components behaviour.

They are mostly plug-and-play devices, and in some cases, relatively easy to detect during an inspection check. That is, while low-cost emulators are straightforward to use, more expensive models are sophisticated, programmable devices which are hard to detect. For instance, an emulator device for a Euro VI truck tested by the Danish Technological Institute showed that "the device works as intended and can even be remote-controlled from the steering wheel" [45]

Basically, there exist 4 basic types of emulators:

- OBD: a device is fitted in the vehicle's OBD connector and thus to the in-vehicle communication. Indeed recall that the OBD port provides direct access to in-vehicle communication. This is an example of emulation category 2 as explained above. An OBD emulator replaces the behaviour of another ECU originally connected to the vehicle bus. They are easy and quick to install, but in most cases also easy and straightforward to detect.
- Hardwired: a device is adjusted to the vehicles wiring harness and directly connected to some ECUs/sensors or to the CAN bus. They can be hidden anywhere, often in difficult to inspect or inaccessible places. The scope is to replace the behaviour of another component or of another ECU originally connected to the bus.
- EEPROM: memory emulators are used to replace the original EEPROM, which may be somehow specifically protected (e.g., with hardware countermeasures) against data modification. This process usually involves the removing of an ECU from the vehicle to pull out its memory chip, so that the emulator can be connected. An example of this emulator can be found at [63] that is usually employed to change the mileage value.
- Passive, non-programmable components: they are connected to sensors in the vehicle's wiring harness to influence their measurement values. An example of this situation is given in Figure 11.

Figure 11. Example of SCR temperature sensor manipulation using resistors

Expensive emulators are also combined with external or built-in DTC modifiers or erasers, say, for reporting only specific OBD parameters and erase or misrepresent the others for the sake of removing tampering evidences. That is, such emulators are hard to detect with standard OBD error code readers. Note that error code readers are typically portable devices, which car technicians or law enforcers may employ to scan the directory containing the vehicle's error code readings.

Note that devices plugged into the OBD port, or directly connected to the vehicle bus, may be also used for purposes different from emulation. For instance cheap and off-the-self equipment, like Raspberry Pi and Arduino boards, may be straightforwardly connected to a CAN bus module, like the PiCAN2 [46] and a CAN bus transceiver, like the CAN-BUS Shield [47] to be then physically attached to the bus. Then, the equipment can be exploited along with ready-to-use libraries [48] and custom made Python scripts to mount certain attacks, including message blocking (preventing a CAN frame to be circulated), replay (re-sending of already captured CAN frames), fuzzing (creating and sending arbitrary CAN frames), and malformed (creating and sending specially crafted CAN frames).

4.2.3 Tuning

Tuning refers to the alteration of ECU behaviour, i.e., the map configurations related to a combination of fuel consumption, performance, emissions, maintenance, and safety parameters, in an attempt to improve performance or/and fuel economy. The original map configurations programmed by manufacturers in ECUs consider a balanced mix of the aforementioned variables. On the downside, tampering with the ignition timing advance and/or the air-to-fuel ratio may augment performance or improve fuel economy, but as a rule of thumb, negatively affects the exhaust gas emissions and reduces the life expectancy of other components, including the catalyst.

The ECU may be reprogrammed via remapping or by installing a device, commonly known as tuning box, performance chip, tuning chip, power chip, power box, or piggyback. As already pointed out, the former method requires tampering with the ECU, say, flashing it, typically via the OBD interface or otherwise as detailed in subsection 4.2.1. On the other hand, a tuning box

commonly tampers with certain engine sensors, say, intake-air, coolant temperature, mass absolute pressure, and mass airflow, falsifying specific signals transmitted to ECU. Similar to the use of emulators, a tuning box is easily noticeable during visual inspection, but at the same time it is easily removable, say, before visiting a roadworthiness test centre. Tuning boxes are mostly available for modern diesel and turbo-charged petrol motors.

Overall, the manufacturers do include protective mechanisms to fight against chip tuning. However, such countermeasures are sometimes defeated quite shortly after a new vehicle model is introduced in the market[2].

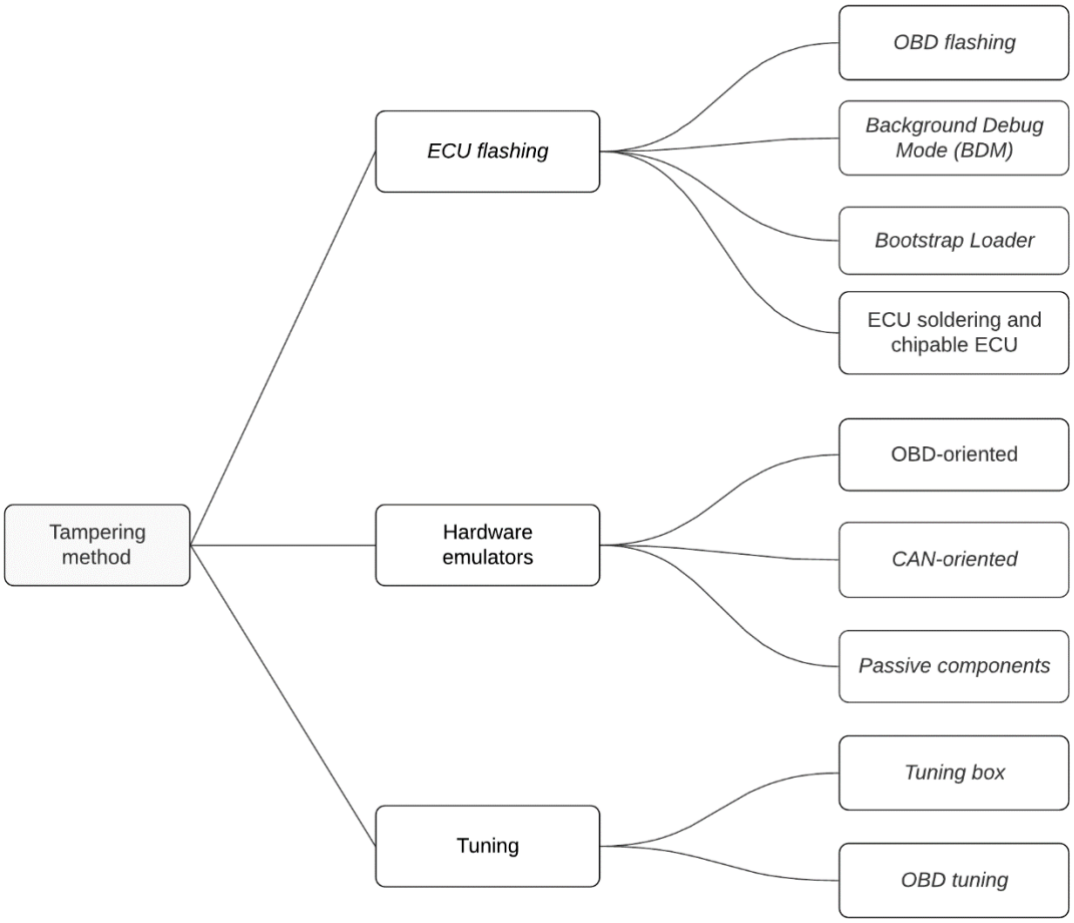

Figure 12. High-level categorization of vehicle tampering methods. Tuning methods can also be seen as subcategories of the other two methods, namely ECU flashing and hardware emulators

4.3 Odometer Tampering Practices

Based on the description provided in Section 3.1 about the odometer architecture, here, we describe some of the main tampering practices affecting this device. A summary view is also given in Figure 22.

- *Manipulation via the ODB port:* As already pointed out, the OBD port is usually situated near the dashboard, and it is wide open to anyone with

[2]https://www.racechip.de/?gclid=EAIaIQobChMI1t3h28iW7gIVQp7tCh2aHgN8EAAYASAAEgIjRfD_BwE, https://www.tuningkit.com/de?gclid=EAIaIQobChMI1t3h28iW7gIVQp7tCh2aHgN8EAAYAyAAEgIv8fD_BwE, https://www.chiptuning.com/?adwords=Chiptuning_Top&gclid=EAIaIQobChMI1t3h28iW7gIVQp7tCh2aHgN8EAAYBCAAEgJ_wPD_BwE.

the appropriate hardware and software. As described in Section 4.2.1, a certain hardware can be used to access the CAN bus of the vehicle, and consequently, other components. In particular, following the description in Section 3.1, it is possible to access the instrument cluster ECU, and thus its EEPROM where the odometer value is stored and the ABS/TCS ECU. For instance, once the tamperer has got access to the instrument cluster's EEPROM, he can modify specific memory areas storing the odometer value. Similarly the tamperer can access and modify ABS/TCS ECU memory areas, for example he could manipulate odometer information or delete fault data, such as the freeze-frame data, which represent a snapshot of data from vehicle's components when a fault is detected, and which may give insights about possible tamperings. Indeed these freeze-frame data could also contain mileage information and they are usually stored in an error memory. It should be noted that this kind of hardware can be found easily on the Internet with a price about 150€, so they are appealing for potential attackers. Furthermore, other more sophisticated devices can be also bought in the Internet for higher prices, such as the one shown in Figure 13, which represents a powerful hardware providing different functionality and a wider compatibility with several vehicles. In particular, it allows a user to perform several actions, as for instance engine oil inspection reset, programming of immobilizers and in general reading and writing of memory areas. Such a device is also constantly updated to guarantee compatibility with new vehicle brands and types introduced in the market. It seems able in some cases to successfully run the security protocol (see Sections 5.1 and 5.2.1) to unlock and access security-related functionalities of ECUs.

Figure 13. Example of hardware to manipulate the odometer value through the ODB port

So basically by using these devices, specific memory areas of an ECU can be modified. This is also usually called "OBD flashing", which has been described in Section 4.2.1.1. In the particular case of the mileage value, specific EEPROM areas with mileage values are modified in the ECUs containing this value. So while authorised reflashing is required to update ECU´s software, this practice is also used by an attacker to modify the mileage values, or other vehicle data, as previously mentioned.

- *Physical access and EEPROM emulators*: as already mentioned, odometer values are usually stored in the EEPROM memory of the instrument cluster. In this case, the vehicle's dashboard is pulled out and stripped down to obtain access to the EEPROM. Then, two alternatives are usually considered to modify the mileage stored in it. In the first case, the tamperer may rely on techniques like the ones of Sections 4.2.1.2 and 4.2.1.3 to interact with the EEPROM and modify the odometer values, so removing the EEPROM chip and then using a HEX editor (e.g., hex-works [55] Figure 14 shows a screenshot of this tool) to modify the mileage value or maybe without unsoldering it.

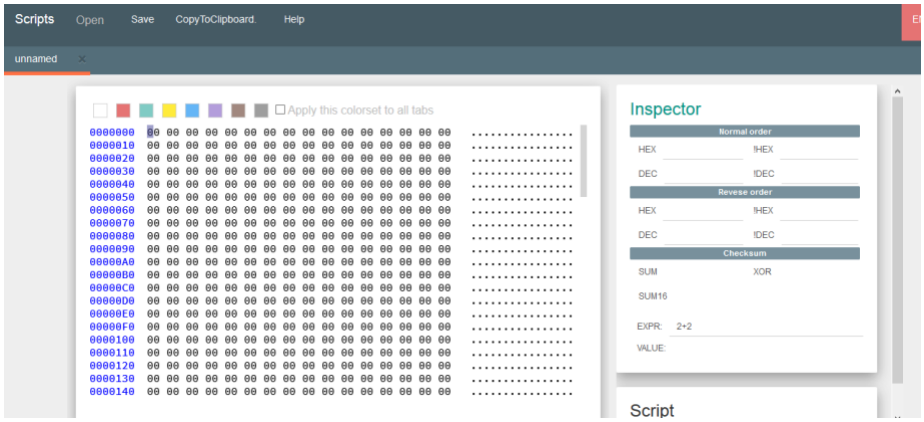

Figure 14. Screenshot of the hex-works website that can be used to modify odometer values

In the second case, the attacker can use an EEPROM emulator, which replaces the original EEPROM. This represents an example of hardware emulator as described in Section 4.2.2, in which the original EEPROM is replaced by a similar device with certain odometer values provided by the tamperer. Indeed, Figure 15 shows several images related to the installation based on the description provided by [63] The installation process usually requires to disassemble the dashboard from the car, and reading out the mileage values from the original EEPROM. Then, such values are stored and modified in the EEPROM emulator, which is soldered in the chip replacing the EEPROM.

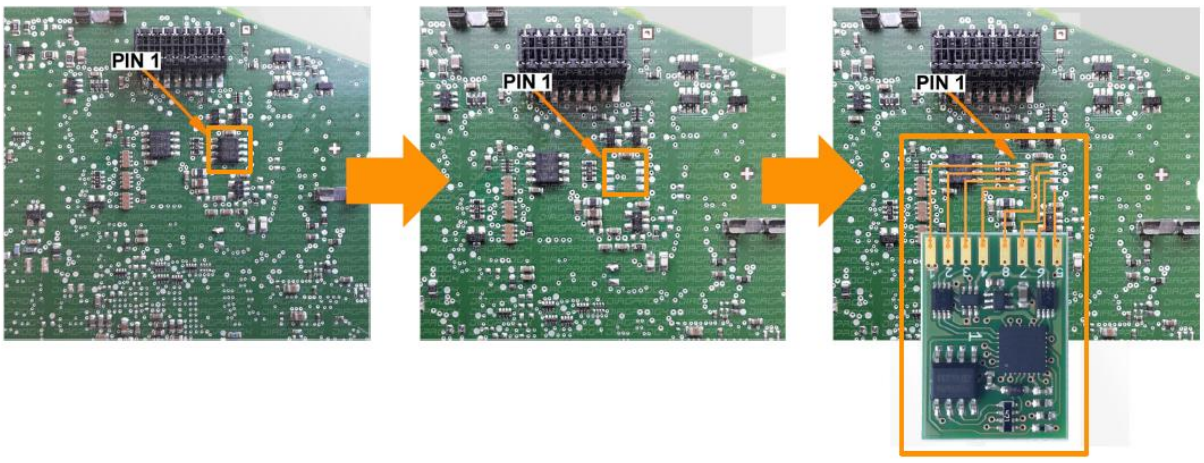

Figure 15. Snapshot of an EEPROM emulator installation [63]

- *CAN blocker or Odometer freezer/stopper*: this tampering technique is based on specific hardware (i.e., freezer), which is connected to the vehicle CAN bus and to the steering wheel. Then, the device is simply activated by using the buttons on the steering wheel. Basically, this device acts as a gateway, which filters the vehicle's distance that is communicated through the CAN bus. Therefore, the attacker activates the filter by pushing a button in the steering wheel, so that the correct distance travelled is no longer showed in the dashboard. The use of the odometer freezer seems to prevent the ABS/TCS ECU to communicate the updated value of the wheel movement to the vehicle's dashboard. Therefore, such information cannot be obtained while it is activated, so the traversed distance during this time will be lost. Furthermore, according to vendors, these devices do not generate DTC errors on the OBD system after their installation. This represents a specific example of tampering approach associated to the general technique described in Section 4.2.2. In particular, this CAN blocker can be considered a device that is placed in the communication channel between two ECUs (i.e., ABS/TCS and dashboard's ECU) to filter speed/mileage value. Figure 16 shows an example of odometer freezer hardware and connector that can be found on the Internet.

Figure 16. Example of odometer freezer hardware and connector

4.4 Emission Control Systems Tampering Practices

Thus far, tampering methods and practices are rather concentrated on hardware modification backed up with signal manipulation through ready-to-use or custom-made control devices. As already pointed out in section 4.2, from a high-level view, digital tampering strategies fall under two broad umbrellas, namely "emulators" and "ECU flashing", with the latter being exploited basically by experts. This section details on these techniques when applied for ECS tampering. A summary view is also provided in Figure 22.

- *SCR-oriented tampering*: It pertains to diesel vehicles. The goal here is to reduce the cost for the Diesel Exhaust Fluid (DEF)[3] and to minimise service costs regarding SCR components. Given that cost savings on AdBlue depend on mileage, assuming an annual mileage of ~150,000 km, a truck owner can save more than €2,000 per year [45] In addition, after diagnosing a failure in the emission control system, the ECU of modern

[3] DEF, commonly known as AdBlue, comprises a chemical liquid used to decrease the amount of air pollution created by a diesel engine. That is, as illustrated in Figure 4, DEF is consumed in SCR to reduce NOx concentration in the diesel exhaust emissions from the engine. Simply put, without AdBlue, the SCR system does not function, resulting in a severe augmentation of the NOx emissions.

trucks will put the vehicle into the so called "limp mode"[4], a highly undesirable situation for the truck owner/driver. Tampering with a SCR system typically requires the disconnection of the SCR ECU from the CAN line and involves an AdBlue/NOx emulator placed on the CAN bus, mimicking the SCR ECU and NOx sensors functionalities towards the Engine ECU. That is, the emulator simulates the reagent level and a NOx sensor and passes falsified data to the Engine ECU deluding it into believing that the system works as intended. Also, the emulator may block error codes and messages, including (a) deactivating the main diagnostics light in the vehicle's dashboard, (b) deactivating the AdBlue indicator lights, (c) manipulating the AdBlue tank gauge, (d) deactivating the limp mode, and (e) blocking the reading of error codes concerned with the engine emission control through an OBD error code reader. Moreover, some emulators can be programmed to automatically be deactivated if the vehicle's speed falls below a pre-defined limit, say, when idling, thus making tougher the detection of tampering during a road-side inspection. According to [45] an AdBlue manipulated Euro VI vehicle may generate emissions equal to the level of a 20-year old Euro I vehicle. Typically, two types of emulators are used for this task, differing for the way they are connected to the CAN bus (see also Section 4.2.2): OBD ones, plugged to the OBD port, or CAN ones, physically wired to the CAN lines. The work in [49] reports up to 100 different providers of AdBlue emulators, most of them being Chinese manufacturers, but also a significant number from vendors residing in the European continent. Software-wise SCR tampering is also possible via re-flashing the Engine ECU and/or the SCR ECU for instance relying on debug or boot modes and OBD-based programming (see [97] for an example of a tool available for this purpose), in addition to or without additional hardware modifications, including the removal of the particulate filter, the disabling of the AdBlue pump unit and the conditioning of values produced by sensors like temperature and NOx ones. Software-wise tampering is the most difficult tampering to detect, as it may leave no traces at all. Figure 17 illustrates the different basic ways the SCR system can be tampered. According to [45] strong indicators of AdBlue manipulation include: missing fuses in fuse box, lack of fluid in or unusual smell from the AdBlue tank, the AdBlue level indicator displays either exactly ¼, ½, ¾ or full, corrosion on AdBlue tank filler cap, inconsistent display of AdBlue level gauge, lack of AdBlue purchase receipts, the temperature indicator on the dashboard shows a value that does not match the current ambient temperature, excessive soot in the exhaust pipe on models fitted with particulate filter, and after-market wiring and connections as well as connectors and hidden switches in the vehicle's wiring. Notably, by manipulating the engine emission control is a very inexpensive option instead of replacing the SCR catalytic converter. This also means that numerous manipulated vehicles have problematic emission systems and are kept functional solely via the use of an AdBlue emulator or modifying ECUs software. Lastly, it is pertinent to note that

[4] Typically, limp mode" is enabled when one or more signal values transmitted by one or more sensors to the Engine ECU lie outside the pre-programmed range specified by the manufacturer. This countermeasure is destined to safeguard from further damages. In the case of a truck, limp mode means bounding engine performance and lessening the driving speed, thus forcing the driver to service the vehicle.

the European Automobile Manufacturers' Association (ACEA) has taken several actions toward scrutinising the AdBlue emulator market [49] and the emulators utility [50] in diverse model of trucks.

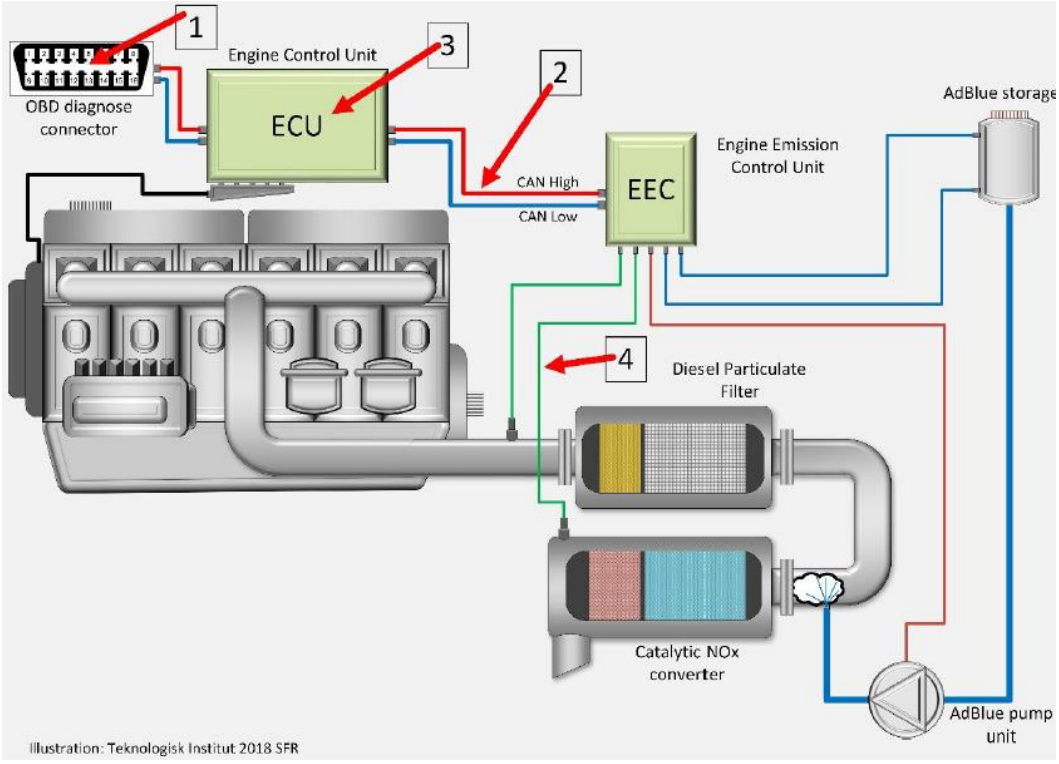

Figure 17. Tampering of the SCR system via (1) OBD emulator, (2) CAN emulator, (3) ECU flashing, and (4) manipulation of temperature, level, or NOx sensors [45]

- *Particle filter-oriented tampering*: Recall from subsection 3.2 that this method pertains to both gasoline and diesel motors. Such practices typically require replacing the filter with an exhaust pipe (known as "filter delete"), chopping the filter canister to detach the filter and soldering the canister back together. Another method known as "filter drilled" is to drill out the filter substrate. Such methods in addition require either (i) the modification of the differential pressure sensor, using, say, a resistor, to mislead the ECU (ECM) in charge of monitoring the filter functionality, or (ii) the remapping of the ECU for erasing the pressure sensor from the OBD scanning field, or (iii) the use of a filter emulator as illustrated in Figure 18. The latter device is fitted under the car bonnet and generates (mimics) signals from sensors that oversee the operation of the particle filter, i.e., differential pressure sensor, exhaust gas temperature sensor, and mass air flow sensor, thus fooling the ECU (ECM) monitoring the filter system into believing that the non-existent filter is clean. The operation of such a device is given in Figure 18, while an example of a filter tampering practice can be seen in [51]

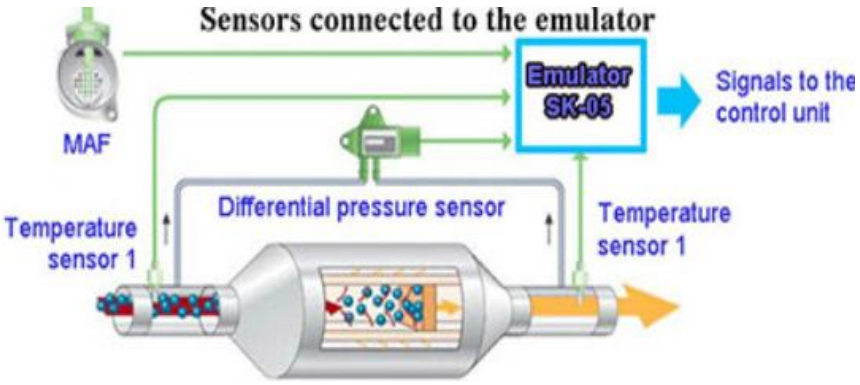

Figure 18. Typical operation of a particle filter emulator [52]

- *EGR-oriented tampering*: It also pertains to diesel vehicles. As already pointed out in section 3.2, EGR aims at the reduction of emissions of NOx. Excluding mechanical tampering, i.e., obstructing the EGR gas tube or sealing the hose to the vacuum actuator, EGR tampering practices are essentially classified in two categories: (i) Disconnection of the EGR valve associated with the use of an emulator, and (ii) EGR overriding ("deleting"). The first and more straightforward involves an external device connected to the wiring harness to emulate the EGR valve operation towards the ECM as given in Figure 19 and Figure 20. The latter mandates ECU (ECM) remapping, and thus it is typically exercised by experts. Specifically, in this case, the ECU is programmed to never open the EGR valve. This also means that there is no need to physically remove the valve, avoiding the associated cost as well.

Figure 19. An EGR pneumatic valve emulator [41]

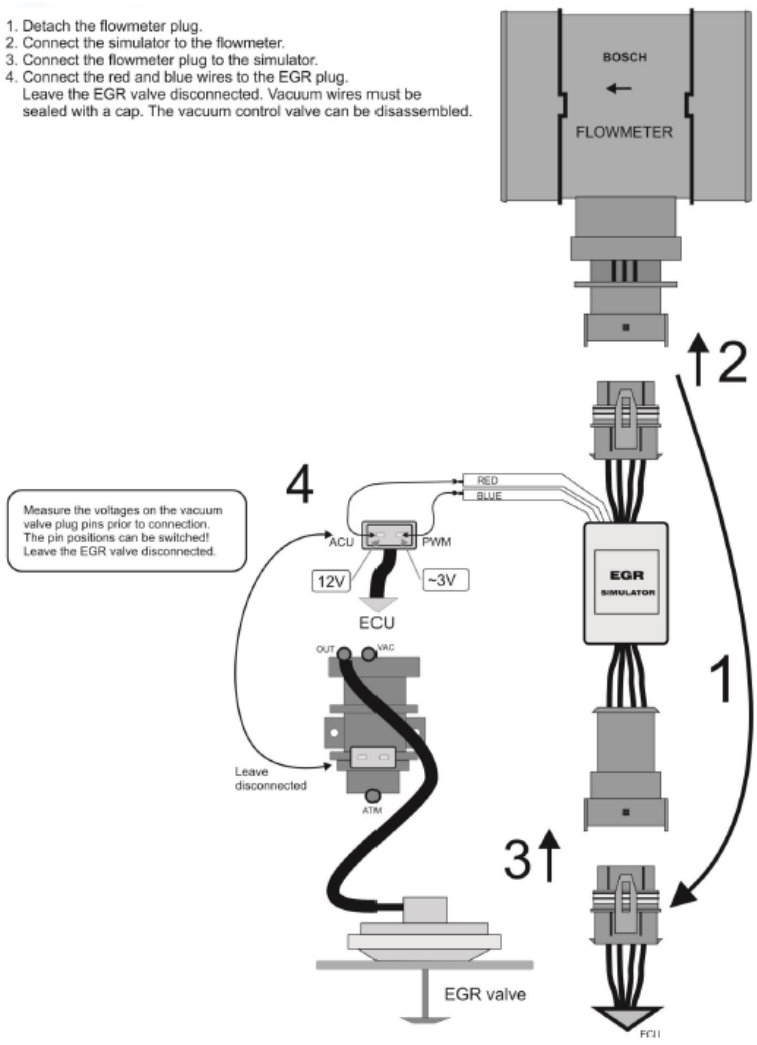

Figure 20. Connection diagram for the EGR valve emulator of Figure 19 [41]

- *TWC-oriented tampering*: As already pointed out in subsection 3.2, this technique is concerned with petrol (gasoline) vehicles. Typically, the tamperer removes the catalyst and replaces it with a legacy exhaust pipe, but this will be normally detected by the OBD and triggers a MIL. So, in addition, the lambda sensor needs to be altered, replaced, or removed, thus requiring ECU (ECM) remapping or the use of an "O2 spacer" as explained in the following. Specifically, contemporary vehicles rely on two Oxygen (O2) sensors, also called lambda sensors; the primary (upstream) one is placed before the catalytic converter and inspects the chemical composition of the exhaust gases before catalysis. The secondary (downstream) is placed after the catalytic converter, it measures the composition of the exhaust gases after catalysis and sends the information back to the ECU (ECM). The latter compares the measurements to decide if the TWC works as normal. That is, in case the data between the two sensors become quite similar the ECU may trigger a catalyst insufficiency check engine code, leading to a MIL. Given that, ECU remapping will modify ECM parameters regarding O2 emissions data. If, however, remapping is not the method of choice, tamperers may use an "O2 spacer", that is a modified lambda sensor with or without a built-in miniature catalytic converter. Such a device extends the gap between the

downstream O2 sensor and the exhaust gases (takes the O2 sensor out of the exhaust stream), with the goal of providing a lower O2 measurement in the exhaust pipe, which in turn restores the value expected from the ECU. Put simply, the tamperer removes the secondary O2 sensor, threads the spacer into the exhaust pipe, threads the sensor into the spacer and locks at the angle of preference. If used, the built-in catalyst in the spacer scrubs the exhaust, i.e., removes the last traces of pollution, to further reduce the possibility of a MIL. A couple of characteristic videos explaining the installation of a O2 spacer, also called "O2 defowler" are given in [61] [62]

Figure 21. Example of an installed O2 spacer [39]

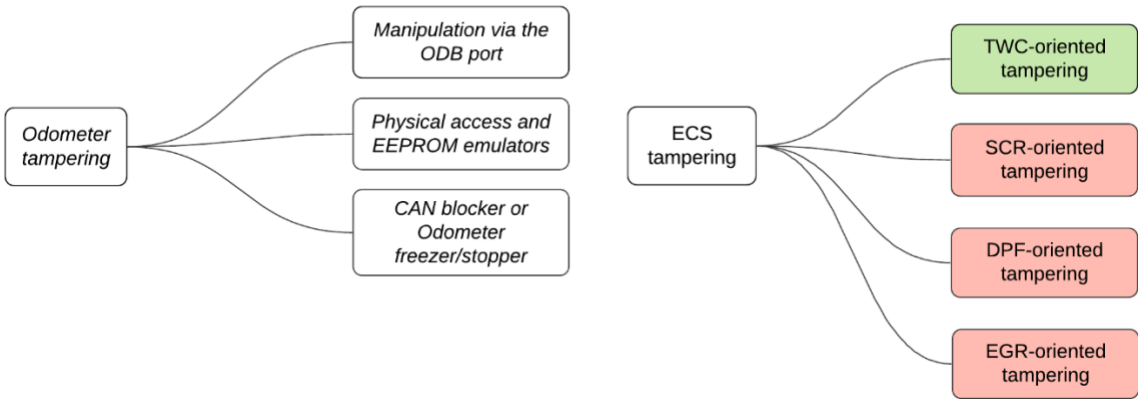

Figure 22. Odometer and ECS tampering practices

4.5 Key Considerations

In the table below we summarise some remarks about the digital tampering techniques (marked as T.X) employed against Odometers and ECS. The provided considerations directly stem from our analysis of the previous sections and recapitulate in a snapshot both some weaknesses affecting the current systems and the possible countermeasures to tackles them.

	Consideration	**Description**
T.1	OBD flashing is possible	It is possible to write memory areas of ECUs with commercially available tools simply connected to the OBD port. The credentials to update the ECU internal memory have to be adequately protected and their check has to be well enforced before granting sensitive rights. See Sections 4.2.1.1, 4.3, 4.4.
T.2	Debug and Boot modes available for reprogramming	Different ECU programming channels may remain available at the end of the vehicle manufacturing process, like the ones offered by specific debug and boot modes. A systematic assessment should be carried out to verify that no unauthorized channels remain open to write the ECU internal memory. See Sections 4.2.1.2, 4.4.
T.3	Unsoldering and soldering of ECU chips is possible	Chips from the ECU board can be unsoldered to be reprogrammed and resoldered or replaced by other ones. The ECU should prevent such operations from being possible and/or should detect any such an attempt reacting to it. See Sections 4.2.1.3, 4.3.
T.4	Emulators accepted by the systems	Emulators can be connected to the vehicle system and can interact with the other components. The messages they transmit are accepted by the rest of the system. Authenticity of the data transmitted in the vehicle system should be granted, allowing to detect unauthorised messages. See Sections 4.2.2, 4.4.
T.5	Message blocking/manipulation is allowed	Message blocking/manipulation devices can be installed preventing the correct receipt of messages by ECUs in the vehicle system. The possible absence of expected messages should be detected. The integrity and authenticity of such messages should be protected. See Sections 4.2.2, 4.3.

Table 3. Key considerations about digital tampering techniques currently adopted against Odometers and ECS

5 Digital Security Measures

In this section we summarize the main security solutions devised to withstand the digital tampering of Odometer and ECS in vehicles.

5.1 Relevant Standards

Regulation (EC) 2017/1151 and Regulation (EU) 2018/1832 explicitly mention the standards series ISO 15031:2013 and ISO 14229:2013 as the standards used for the transmission of OBD relevant information. In particular, ISO 15031 consists of seven main parts describing several aspects about the communication between vehicle and external equipment for emission-related diagnostics. It includes "Part 7: Data link security", which gives basic guidelines for the protection of road vehicle modules from unauthorized intrusion through a vehicle diagnostic data link. Such a standard is explicitly mentioned by European legislation to set some security measures, as pointed out in Section 2. Anyway for the concrete implementation of security measures, the standard references another standard to give an example of security implementation, namely ISO 14229-1.

The "ISO 14229-1:2020. Part 1: Application Layer" is intended to describe the Unified Diagnostic Services (UDS) that are used by diagnostic systems to communicate with ECUs in vehicles, including the diagnosis of potential errors and reprogramming of ECUs. This standard is part of the ISO 14229 series, which defines a set of common requirements for diagnostic systems by using the OSI Model as a reference. In particular, the ISO 14229-1 is focused on OSI Layer 7 (Application layer) by providing a set of requirements for diagnostic services in which a client (tester) communicates with an ECU (server) to control diagnostic functions.

Each different diagnostic service offered by an ECU is represented by a Service Identifier (SID), and the specific actions carried out by these services are further specified through subfunction levels (LEV) [64] Based on SID and LEV fields, the standard defines a basic application layer protocol in which a service request sent from the client is always answered by one or more responses from the server, with some exceptions in specific cases that requires the use of negative responses including an error code. An overview of these basic messages is shown in Figure 23.

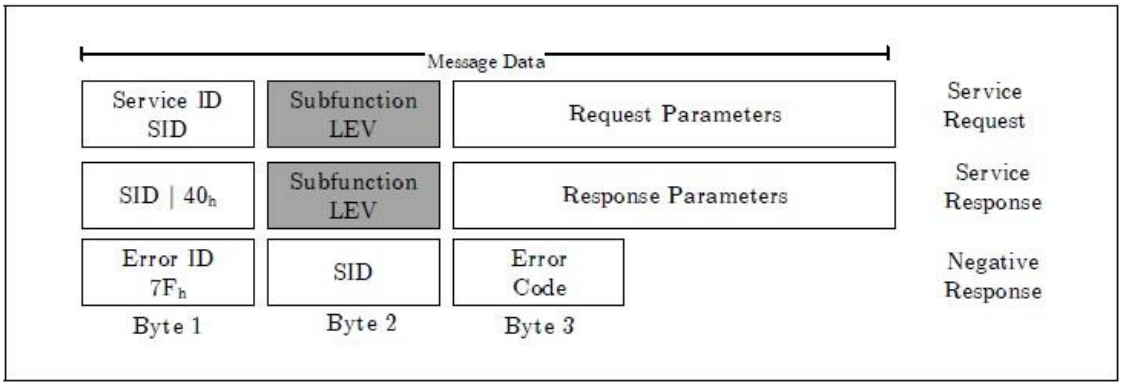

Figure 23. Simplified overview of the diagnostic protocol [64]

The standard defines a set of diagnostic services, which are grouped in several functional units. For the definition of each service, the standard describes the

parameters of requests and responses, as well as a set of error codes, which are used in the case of negative responses for a certain service. These aspects are further described in Section 9 of the ISO 14229-1:2020 standard. Furthermore, the standard defines the concept of diagnostic session as the "state within the server in which a specific set of diagnostic services and functionality is enabled". There shall always be exactly one diagnostic session active in a server, this means that some services will not be available until the system switches to the proper session. An ECU will start by default in the "default session" that will be running as long as it is powered. Then, a client request could trigger the start of a new session; for example, a "programming session" is used to upload software, or the "safety system diagnostic session", which is defined to enable all diagnostic services required to support safety system related functions (e.g. airbag deployment).

Among the services being provided, "Security Access" and "Authentication" provide certain functionality to ensure only legitimate and authorized entities get access to ECUs' services. Specifically, "Security Access" provides a mean to access data and/or diagnostic services that have access restrictions, such as reading specific memory locations from a server. The approach is based on the use of a "seed", which is sent by the server. Based on this seed, the client computes a "key", which is sent to the server to unlock certain services. The requests of seed and key parameters are associated to a certain security level defined by the manufacturer. As described by [65] the security level is a status that the client gains by unlocking features within the server. The standard allows the definition of 64 different levels that can unlock a whole service, a subfunction or the access to a specific value. Only one such level should be active at any instance of time and until another request seed command is triggered or the session expires due to, say, inactivity. The server may implement a protection mechanism to limit the requests of "Security Access" services, typically introducing a delay after a failed security access attempt. If the server supports a delay feature, then a separate timer may be implemented per security level.

It should be noted that the standard defines a sequence of services to be launched for certain diagnostic functions to be activated, e.g., Diagnostic Session Control to enter a specific session offering the target service, Security Access to gain the right to run the service and in the execution of the (secure) diagnostic services. For example, this procedure is used during the non-volatile server memory programming process (Section 17 of the standard), which includes the download of one or multiple application software/data modules into non-volatile server memory. In particular, this procedure is mandatory for emissions-related and safety systems. Indeed, according to subsection 17.3.1.2 of ISO 14229-1-2020, "all programmable servers that have emission, safety or theft related features shall employ a seed and key feature" and "… service replacement servers shall be shipped to the field with the security feature activated …". This is also confirmed by table 502 of the same ISO that defines the security service for "Programming phase #1 – Download of application software and/or application data" as "Optional: Required to be supported by theft-, emission-, and safety-related systems".

In the case of the "Authentication" service, it lies on top of the security access service and is used to allow a client to prove its identity to access data and/or

diagnostic services by using two main approaches: authentication with Public Key Infrastructure (PKI) certificate exchange (based on asymmetric cryptography), or authentication with challenge-response (based on symmetric/asymmetric cryptography). Note that there could be services requiring authentication together with the security access service. The authentication with PKI certificate exchange supports unidirectional and bidirectional authentication in which the client or the client/server are authenticated through a certificate and the corresponding private key. Furthermore, depending on the trust model of the PKI, the client and the server may need a certificate of the certificate authority (CA) which issued and signed the certificate client and certificate server. For the authentication with challenge-response the use of certificates and PKI is not considered, so a set of pre-established cryptographic material is assumed. In the case of symmetric cryptography, client and server already have pre-shared key, while for the asymmetric variant, client's and server's public key will be shared between both entities. Given that thus far no global PKI infrastructure has emerged, the first method implies that each manufacturer needs to either deploy its own PKI or rely to an external party. In any case, for proper certificate verification, the verifying party needs to possess or somehow obtain in a real-time fashion the certificate of the root certification authority which issued the other end's certificate. Also, the claimant needs to send the whole certificate chain to the verifier.

In general the "Authentication" service is intended to secure a certain diagnostic session, service or function and it is followed by any service that is secure or restricted by authentication. After being authenticated, an ECU will stay in an authenticated state until a certain security timeout or mileage offset (which is manufacturer specific) is reached, or explicitly by using a "deAuthenticate" request. Furthermore, as described in Section 10.6 of the ISO 14229-1, session keys can be obtained through this service to secure the communication between tester and ECU, for example through an asymmetric key agreement protocol or by deriving from existing pre-shared keys in the case of symmetric cryptography. In that regard, it should be noted that ISO 14229-1 defines a security sub-layer in order to perform diagnostic services in a secured mode. In general, as defined by the standard, "the task of the security sub-layer when performing a diagnostic service in a secured mode is to encrypt data provided by the "Application Layer", to decrypt data provided by the "Network Layer", to add an authentication code, to verify an authentication code, and to add, check, and remove security specific data elements".

5.2 Security Techniques

5.2.1 Authentication to ECU

To defend against unauthorized ECU flashing, i.e., the aftermarket reprogramming of the ECU's software and calibration data, manufacturers introduced security measures commonly referred to as "tuning protection". Excluding physical protection and other supplementary measures succinctly mentioned in subsections 5.2.4 and 5.2.5, first, they brought in controls against OBD-enabled flashing. This is typically referred to as "link layer security" and it is implemented as a "seed and key" scheme with reference to current ISO 15031-7:2013 and 14229-1-2020. The goal is to allow only authorized tools (entities) to reprogram the ECU.

Based on the aforementioned ISOs, the core idea of "seed and key" is that the ECU acting as server passes a pseudorandom n-byte seed to the flashing tool acting as client, and the latter needs to convert that seed into a key using a manufacturer-specific security algorithm. The ECU applies the same algorithm internally, and compares the key value given by the tool to its own value. If the two values are equal, the tool is implicitly assumed to know the secret algorithm, and access is granted. As a rule of thumb, manufacturers do not publicise the internal workings of the algorithm, but to ECU supplier. As already detailed in section 5.1, with specific reference to the "Security access" service, from a high-level view, the algorithm works as follows:

- the flashing tool issues a so called "request seed" command toward the ECU;
- the ECU issues a "request seed" response to pass the tester a n-byte "seed". Note that typically this seed is not retrieved from an external source, say, a server, but it is generated by the ECU itself;
- based on this seed, the flashing tool returns a "key" to the ECU via a "send key" command. The important thing here is that the "key" can be calculated by the flashing tool per se (this requires the tool to know the secret algorithm) or pushed by an external "bridge" server (typical case for modern implementations). In the latter case, as pointed out in section 2, the provisions of regulation 2017/1151 regarding "electronic access to an off-site computer maintained by the manufacturer" should apply;
- the ECU compares the received "key" with the one internally calculated or pre-stored, and it transitions to the unlocked state if the two keys are identical. Also, there may be a threshold restricting the number of subsequent unsuccessful authentication attempts. If this threshold is exceeded, then the mechanism introduces a considerable time delay as a penalty before replying to another "request seed" command. This delay, typically implemented as a delay counter, may be a constant value or depend on the number of failed attempts.

Some additional hands-on information about the "seed and key" are also given in [70] where rudimentary implementations of "seed and key" are reported, for instance based on static seed and key values or based on basic algebraic operations. However, keep in mind that both these works are published back in 2014, and therefore may include outdated information vis-à-vis contemporary implementations based on ISO 14229-1-2020.

On top of the "seed and key" unlocking function, an authentication can take place beforehand between the diagnostic tool and the ECU. Also in this case the authentication may go through an online process, where the flashing tool retrieves its role represented by a digital certificate based on public key cryptography, and authenticates itself towards the ECU. Commonly, such an architecture involves four parties, namely the ECU, the diagnostic tool (operated by the user), a main server, and a bridge server, which acts as a mediator between the main server and the diagnostic tool. The servers are assumed to be online and trusted, and the diagnostic tool is connected to the server(s) over a wired or wireless connection. Such an architecture demands (mutually) authenticated and secure connections among the parties, i.e., between the tool and the server, and between the servers, in case they run on different physical machines. In the procedure, the servers return to the tool its digital certificate

that specifies its authorized role. The certificate is forwarded to the ECU that checks its validity using pre-installed root certificates and replies to the tool with a challenge. The challenge is forwarded to the servers which in turn calculate, relying the corresponding certificate private key, and return the response that is finally sent by the tool to the ECU. The latter relies on public key of the received certificate to verify the response and authenticate the tool. It is plausible to think that such a scheme relies upon the "Authentication" service presented in Section 5.1.

Specifically with regard to the diagnostic tools, it has to be noted that in some cases this kind of official devices undergo multiple vulnerability assessments and penetration tests by security industry experts to identify security issues and suggest improvements. Modern diagnostic tools can also affords an encrypted file system, utilises secure boot, and stores cryptographic material in an HSM chip (see Section 5.2.3). In some cases, diagnostic tool to external server communications relies on UL-2900 compliant software for providing integrity and authenticity. Note that UL-2900 [95] is a series of standards which among others present general software cybersecurity requirements for network-connectable products. This points out that cybersecurity certifications are already taken into consideration in some automotive applications.

5.2.2 Multiple and Protected Data Storage

As described in Section 4.2.1, ECU flashing could be carried out by potential tamperers by using the ODB port and a suitable flashing tool to modify certain vehicle's values stored in EEPROM areas. This attack is especially employed in the case of the odometer (Section 4.3) in which the EEPROM of the instrument cluster ECU is accessed to modify the odometer value. To hinder this tampering, some manufacturers disable the possibility to manually write into certain memory registers and also enforce checks to control the access to debug interfaces to block other avenues for memory writing (see Section 5.2.4). In that regard it has been also reported that in some cases the modification of odometer values is only possible by using a debug mode with proprietary commands of the manufacturer.

Another approach to contrast odometer fraud is the distribution of the mileage to different control units in the vehicle that are forced to store the highest value being received. In particular, the instrument cluster may be in charge of distributing the mileage value to the other control units in the vehicle. In case of discrepancies among the different stored mileage values, an error may be displayed by the vehicle. This approach also allows to maintain the last mileage even if the instrument cluster is replaced. Anyway to be an effective measure a tamperer should not be able to alter all different mileage copies.

Other solutions make use of cryptographic algorithms to secure the odometer data storage by using cryptographic keys that are stored by the manufacturer in the vehicle. For instance the mileage may be stored in a dedicated instrument cluster's EEPROM. To detect the possible manipulation of the odometer data in this EEPROM, its content is compared by the instrument cluster software with other cryptographically protected mileage copies. To avoid that such a protection is circumvented, the software running in the instrument cluster can be also periodically checked (e.g., for each drive) to verify its integrity (see Section 5.2.4). The cryptographic keys may be stored and managed in a protected way relying on Hardware Secure Modules (HSM) as described in Section 5.2.3.

Furthermore, certain manufacturers consider the use of databases hosted at their premises where data mileage is taken from the vehicle. For example, for every inspection in a workshop, the mileage value could be read from the vehicle and stored in the corresponding manufacturer's database.

5.2.3 Hardware Modules

The storage of specific data, typically the mileage information held in the instrument cluster, may be protected using dedicated EEPROM modules that allow only the writing of higher values in special areas of their memory. Thus, if the odometer value is stored in such a component, it cannot be manually decreased. Note that this way even the software of the instrument cluster cannot bypass such a protection. The EEPROM is also typically featured by a unique serial number, and this number is routinely checked by the instrument cluster software to detect any replacement of the EEPROM module (e.g., it may be replaced with one containing a smaller mileage value). Unfortunately, as explained in Section 4.2.2, EEPROM modules may be replaced by emulators, which mimic the original hardware device returning the same serial number and presenting a reduced mileage value.

Moreover, the use of Hardware Security Module (HSM) and Secure Hardware Extension (SHE) components is already considered in several vehicle's components, such as immobiliser systems and infotainment and telematic ECUs. They basically represent a security extension of an ECU microcontroller. In the case of a HSM, it is a physical secure computing device, which is in charge of managing cryptographic material and performing certain cryptographic operations and algorithms. A HSM typically offers dedicated hardware accelerators for specific cryptographic algorithms, true random number generators (TRNG) and secured key storage. A SHE can be seen as a HSM but with reduced functionalities. As defined by AUTOSAR [68] a SHE consists of three building blocks, namely: a storage area to keep the cryptographic keys and additional corresponding information, an implementation of a symmetric key algorithm (i.e., AES) and a control logic connecting the unit to the CPU of the ECU microcontroller.

As said, both HSMs and SHEs have been considered in the automotive sector. Specifically, the "e-safety vehicle intrusion protected applications" (EVITA) project [82] established three HSM security levels (Light, Medium, and Full), with several features similar to the Secure Hardware Extension (SHE) and Trusted Platform Module (TPM) specifications. In particular, SHE's functionality is similar to the one provided by the "light HSM" that includes protecting cryptographic keys from software attacks and implementation of symmetric key algorithms. For the functionalities of Medium and Full HSMs look at Figure 24, which shows a comparison of the functionality provided by the HSMs defined by EVITA, SHE, TPM and smart cards (SmC).

	Full	Medium	Light	SHE	TPM	SmC
Cryptographic algorithms						
ECC/RSA	■/■	■/■	□/□	□/□	□/■	⊞/⊞
AES/DES	■/⊞	■/⊞	■/□	■/□	□/□	⊞/⊞
WHIRLPOOL/SHA	■/■	■/■	□/□	□/□	□/■	⊞/⊞
Hardware acceleration						
ECC/RSA	■/□	□/□	□/□	□/□	□/□	□/□
AES/DES	■/□	■/□	■/□	■/□	□/□	□/□
WHIRLPOOL/SHA	■/□	□/□	□/□	□/□	□/□	□/□
Security features						
Secure/authenticated boot	■/■	■/■	⊞/⊞	■/□	□/■	□/□
Key AC per use/bootstrap	■/■	■/■	■/⊞	□/■	⊞/■	□/□
PRNG with TRNG seed	■	■	■	■	■	■
Monotonic counters 32/64 bit	■/■	■/■	□/□	□/□	■/□	□/□
Tick/UTC-synced clock	■/■	■/■	■/■	□/□	□/□	□/□
Internal processing						
Programmable/preset CPU	■/⊞	■/⊞	□/⊞	□/■	□/■	⊞/⊞
Internal V/NV (key) memory	■/■	■/■	⊞/⊞	■/■	■/□	■/□
Asynchronous/parallel IF	■/⊞	■/□	■/□	■/□	□/□	□/□

Annotation: ■ = available, □ = not available, ⊞ = partly or optionally available

Figure 24. Comparison between hardware security components [69]

HSMs and SHEs can be used in vehicles to prevent non-authorised access (e.g., by running authentication protocols), protecting ECUs against manipulation (e.g., verify cryptographic checksums on installed software) and in general preserving the security and integrity of the systems [2] HSMs are also used in some cases to protect the access to debug or specific microcontroller boot modalities through strong passwords [73] Such modules are also already considered for the protection of odometer data, as presented in Section 5.2.2. Anyway, while some manufacturers already consider HSMs to protect the storage of odometer readings at rest, such components may be also employed to protect the internal communication of such values, or even when they need to be communicated with external entities (e.g., manufacturer's database). More in general they may be considered to protect the integrity and authenticity of vehicle communications.

5.2.4 Complementary Measures Against Unauthorised ECU Programming

On top of the authentication service and as an ECU's internal defensive mechanism, the ECU manufacturers use a number of checksums (fingerprints) to verify the genuineness of the ECU's memory content[5]. That is, a decade ago, they moved toward the use of cryptographic signatures (i.e., relying on RSA and ECDSA cryptosystems) to verify the integrity and authenticity of the ECU contents. As detailed next, this measure is in accordance with ISO 14229-1-2020.

A typical example is the digital signature that can be applied on ECUs software updates, which has to be verified before the installation of the received new software. Installed ECU software integrity may be also checked periodically by the unit itself, for instance at each boot time.

[5] Note that if a checksum is calculated via a software algorithm in the ECU and not by a dedicated hardware (e.g., HSM), this may entail that the software computing the checksum itself may be more prone to suffer from manipulations.

For tamperers, the cracking of such a signature is almost futile, if only relying on legacy brute force methods. So, they needed to devise alternative methods for reprogramming a protected ECU. For instance, when the Infineon TriCore TC-series 32-bit processors (used in Bosch MED17/EDC17 family ECUs) was released, tamperers realised that in the ECU programming routing there was a backdoor that could be leveraged to install unauthorised software. Naturally this bug is now patched, mandating signature validity check after every OBD reprogramming attempt. In case of discrepancy, a flag is set in the ECU memory immobilising the vehicle. Anyway advanced flashing tools can scan for this security functionality by reading the ECU via the OBD. In such cases of protected ECUs, as for ECUs equipped with Tricore TC17xx-series processors, a tamperer may leverage other techniques, for instance removing and opening the ECU for booting and programming it from pins on the motherboard in order to circumventing the protection. By doing so, the ECU may omit the signature validity check. This procedure is called "bench flash" [72] or "install a probe", and is basically exercised by BDM or BSL flashing as discussed in Section 4. To respond to this vulnerability, latest microcontrollers introduced a password-based method to prevent unauthorized access to the debugging resources. As mentioned in Section 5.2.3, the debug mode password-based access may be also enforced by a HSM module if it is embedded in the ECU.

Apart from the abovementioned countermeasures, some manufactures also rely on one or a mixture of the following safeguards:

- Watchdogs: use of a tuning protection watchdog to prevent bypassing tuning protection code [74] A watchdog may be implemented in hardware or software. Generally, the former comprises a piece of hardware that initiates code to continuously check the soundness of the underlying system, namely, the hardware and software components of interest. The system is reset or even shutdown in case one of the components - especially a hardware one - shows an unhealthy behaviour. On the contrary, a software watchdog can take a more intelligent decision about the way an abnormal condition will be tackled, say, the unhealthy process may be restarted or killed, or the hardware may be reverted to a sound state before restarting the relevant processes. In addition, a watchdog caters for debugging purposes as it collects/dumps any piece of data regarding the nature of the malfunction or failure.
- Security gateway (SGW): it oversees the routing of messages from one vehicle network bus to another, and acts also as a firewall separating between the in-vehicle network and the outside world, including the OBD socket and the infotainment system interfaces. Specifically, after receiving a message, the SGW will inspect the message's content and forward it only if it matches the SGW's internal pre-configured policy. The policy can be customised, say, to be fine or coarse-grained, e.g., permissions based on the tool's (user's) role, and thus, as already pointed out, its operation resembles that of a typical firewall. The tool's role can be inferred for instance on the base of authentication protocols as shown in Section 5.2.1.
- Locked diagnostic testers: a specific manufacturer tester can only be provided to and activated by users registered on the manufacturer's platform. This means that any ECU flashing operation must be done via this tool and is also tracked by the manufacturer. Any flashing operation is enabled by the tool only after an authentication to the manufacturer

systems, which can happen over a Virtual Private Network (VPN) connection or by using a secure-ID provided by the manufacturer. In this case, the way, say, the out-of-band method like email, telephone, etc., this secure-ID is communicated to the authorised user should be defined. In general it is likely that the adopted authentication solution is the one of the SERMI scheme [89] mentioned in Section 2, requiring the use of a security token and its PIN to authenticate to the manufacturer and unlock tester sensitive functions. After a successful authentication, the tester inspects specific unique properties of the vehicle, e.g., the Vehicle's Identification Number (VIN), and automatically chooses and flashes to the ECU the corresponding proper software.

No less important, section 17.3 of ISO 14229-1-2020 attempts to sort through the requirements for server (ECU) programming. Precisely, the following provisions are defined and exemplified:

- any server that allows programming of the application software "shall contain boot software in a boot memory partition". Recall that the term "boot software" refers to the software that runs after the server boots up;
- the boot software "can" be protected by hardware or software means against unintentional or intentional modification or erasure. This ensures that the server will be able to recover after, say, an abortive programming attempt or power disruption. As a suggestion, the boot software should not be modified using the same programmable modules that are utilised for application programming. A secure boot, a way to make sure that a device boots using only certified software, i.e., the one provided by the original equipment manufacturer, is also employed in some ECUs (e.g., infotainment systems and telematics);
- boot and application software and data "may" be uniquely identified by the corresponding identifiers (IDs) included in Table C.1, Section C.1, annex C of the ISO. The structure of such data records remains to the discretion of the manufacturer. These IDs shall not be allowed to be written directly and individually, but only jointly with the respective software or data, i.e., as an indispensable part of them;
- software and data fingerprints shall be used when erasing or reprogramming the application or data stored in the server. If used, a fingerprint serves a dual purpose. First, it uniquely identifies the tool used to modify the respective software module, and secondly uniquely identifies the module being altered, say, the specific application, data, or boot software. Fingerprints shall be kept in the non-volatile memory of the server and written prior to updating the target software or data. Again, these fingerprints are vendor specific, and table 502 of the ISO defines this service as "Optional: Required for writing the fingerprint and other identification data";
- in some modern vehicles some units (e.g., telematics) may also employ applications sandboxing, meaning that the execution of the different applications on the unit are logically isolated from each other. This reduces the possibility that malware running on the unit may negatively affect the execution of legitimate applications.

5.2.5 Physical protection

For denying unauthorized access to sensitive electronic components and to render tampering, device cloning, and reverse-engineering harder, some manufacturers employ physical protection measures on top of digital ones. For instance, in addition to the use of uniquely shaped screw heads, they seal the cover of the ECU with silicon or glue, or coop the sensitive component up in a special metallic case or use ultrasonic bonding. The latter term refers to a process in which ultrasonic sound waves are applied to a number of pieces that are being pressed together to create a single piece, and hence assembles a housing cumbersome to pry without a perceivable damage [75] In the case of adhesive, dissolving the substance, say, with acetone, may also harm the equipment or the printed circuit board itself, while in the case of reinforced housings, the tamperer needs to chop or dismantle the case with the aid of special equipment. Covering the BDM port with glue or epoxy resin (called also "potting") is also a typical practice [76] In other cases, the components hosting calibration memory chips (EEPROMs) and other sensitive electronic equipment may be coated by means of a conformal coating material (a thin polymeric film, typically epoxy or polyurethane) [77] [78] and thus cannot be easily peeled or broken into without damaging the assembly.

While such measures are in the positive side, and also serve as anti-theft features, they practically comprise a first line of defense; in many cases, the motivated and determined tamperer will finally find a way to obtain access to the component of interest. For example, in the case of glue or epoxy-protected components, the tamperer can employ several methods, including freezing the case for several hours, which may cause the adhesive to become brittle. Besides, modern solutions do not require even di-soldering the chip from the board to read/write its contents [79] [80] Lastly, similar physical protections are available in the market for use by vehicle owners as anti-theft measures. The most straightforward, is encasing the OBD port in a metallic box [81]

More promising measures may include switches or sensors, say magnetic or pressure contacts or light sensors, to detect removal of the cover or de-capping attempts against the integrated circuit itself. Once a tampering attempt is detected the unit logic has to react to protect itself, for instance erasing sensitive data (e.g., cryptographic keys), logging the event or permanently disabling itself.

5.3 Key Considerations

In the table below we summarise some remarks about the above-discussed security measures (marked as S.X) to hinder current digital tampering practices against Odometers and ECS. Again the provided considerations directly stem from our analysis of the previous sections and in particular recapitulate in a snapshot some limits concerning the security measures adopted so far to contrast digital tempering practices.

	Consideration	**Description**
S.1	Non-standard and non-commonly accepted security protocols are possible	The lack of precise specifications allow manufacturers to freely choice, and in some cases to design by their own, the mechanisms used to secure the access to ECUs for sensitive functions by

		diagnostic tools. This leaves open the possible adoption of non-state of the art solutions potentially susceptible to attacks. See Section 5.2.1.
S.2	Lack of systematic security requirements and lack of respective assessment for the adopted security solutions	Solutions to prevent ECUs digital data modification through alternative channels, like via debug and boot modes, are necessary. Anyway there is not any explicit requirement for them, which are introduced only at discretion of the manufacturer. Even when implemented there is not any assessment to evaluate their strength. Indeed even if (EU) 2017/1151 provides a set of tests, such list does not report any verification of the provisions taken to prevent tampering with and modification of the emission control computer and odometer, for which is only required a description to be submitted for a documental verification. See Section 5.2.4. Physical-protection measures can also provide some help. Anyway also these solutions are introduced just at discretion of the system designers and in addition they should be accompanied by other measures, for instance techniques to detect an unauthorized access to the ECU's electronics. The effectiveness of such measures should be duly assessed as well. See Section 5.2.5. Also the multiple storage of data can be of limited help if specific data protection solutions are not employed. See Section 5.2.2.
S.3	Secure hardware not offering full protection	Hardware explicitly introduced to secure some functionalities shall not be replaceable. See Section 5.2.3. It should be also able to withstand the publicly known attacks that can be of interest for tamperers. For instance hardware introduced to store and manage cryptographic keys should include countermeasures against side-channel attacks. In general today's vehicle digital systems are not properly protected against side-channel and fault injection attacks, and the "difficulty" to get access to the components is in some cases already considered as a sufficient protection.
S.4	Lack of solutions to secure inter-ECUs communications	Security protocols and authentication mechanisms are introduced only to regulate the access to ECUs by diagnostic tools (see Sections 5.1, 5.2.1), but according to the collected information no integrity and authentication mechanisms are in place to protect the communications among ECUs.

Table 4. Key considerations about security measures adopted to hinder the digital tampering of Odometers and ECS

6 Recommendations and Final Considerations

Based on our analysis, we propose here below some technical recommendations about security measures against current digital tampering practices on Odometers and Emission Control Systems. We link each recommendation to the different key considerations drawn in the previous sections. The idea is that following a recommendation also the issues described by the related considerations would be addressed.

Recommendation	**Addressed Considerations**	**Description**
Security protocols should address the different known tampering possibilities and should rely on standardized approaches	L.1, L.2, T.1, T.2, T.4, T.5, S.1, S.2, S.4	Security mechanisms are defined to access some ECUs sensitive diagnostic services, typically via the OBD interface. Anyway no standard protocols are mandated for this purpose leaving open the possibility of custom weak implementations. In addition no security mechanisms are prescribed for inter-ECUs communications. On top of this there are no security requirements about other ECUs access ports, like debug and boot modes. **Standard cryptographic algorithms should be adopted** to both authorize the access to ECUs functionalities and to assure the integrity and authenticity of inter-ECUs and ECUs-external components communications. Similarly, the access to other ECUs port should be protected, or they should be disabled if no longer needed at the end of the manufacturing process.
Adoption of secure hardware components	L.1, T.4, T.5, S.3	There are no clear requirements about the adoption of secure hardware components in ECUs and operators equipment. As suggested in the previous recommendation, the adoption of strong and standard cryptography is desirable. This requires the installation in ECUs, and operators equipment as well, of sensitive cryptographic material, which should be protected from unauthorised access with specific secure hardware. The vehicle tampering scenario exposes the cryptographic material to a high risk, as for instance the owner of a vehicle would be willing to grant unconditional access to the ECUs to possibly act on such material and make a tampering. For this reason the cryptographic material should be stored and managed in **hardware secure modules (HSMs), capable to withstand all known**

		attacks against cryptographic material. The cryptographic material stored in an HSM hosted in the ECU would prevent the replacement of the ECU itself and the tampering of its communications. Similarly, a sound protection of cryptographic material stored in operators equipment prevents the cloning of such a material and thus hinders unauthorized operations.
Need for a uniform effective assessment and type approval scheme	L.3, T.2, T.3, S.2	The scheme adopted for the type approval is discretionary for each approval authority. Above all there are no indications about the kind of testing to be carried out to assess the completeness and robustness of the employed anti-tampering solutions. In addition, if every use case is evaluated in isolation and different security concepts are mandated and deployed, this will open the door further for misuse by tamperers. On top of this, typically, the protection or mitigation measures taken by manufacturers are "risk-based", meaning they stem from their own risk assessment, which however may be subjective. **The type approval process should rely on a security certification scheme for all vehicle digital components, typically ECUs, playing a role in mileage storage and emissions control.** The standardized Common Criteria (CC) framework, internationally agreed for such a purpose, should be considered for adoption. Actually, other initiatives in the automotive sector, i.e., digital tachograph [92] and C-ITS [93] mandate the usage of CC certified devices; in fact, for instance digital tachograph components have proven that systems baring a successful CC certification are far less vulnerable to tampering. It has to be noted that the CC methodology can be also successfully adopted for assessments within the vehicle cybersecurity framework of ISO/SAE 21434 [90] and of the UN R155 regulation [91] Indeed, the use of a security certification approach such as CC would be an additional element underpinning the general vehicle cybersecurity management system. In this way the overall security of each ECU undergoing the certification would be systematically scrutinized against any known attack and tampering practice. Note that such a process wouldn't cover only the security of HSMs, but would also protect

		from other practices like soldering of ECU components or access by debug and boot modes. A security certification scheme is also advisable for equipment used by operators for sensitive ECU operations.

Table 5. Overall considerations about current digital tampering practices and effectiveness of the related countermeasures.

As self-evident in the description of each recommendation, they are almost in daisy-chain, meaning that all recommendations should be followed to provide an overall capability to withstand digital tampering practices. Note that the idea is to provide protection against current practices and possible future ones. For instance the introduction of standard cryptographic solutions would be immediately effective against some practices. Anyway, if the related cryptographic material wouldn't be protected in certified secure dedicated hardware, it would be just a matter of time for tamperers to focus their efforts in accessing such a cryptographic material to devise new tampering procedures. Indeed it has to be underlined that tampering can be a very profitable activity, so tamperers may be motivated in investing and engineering specialised attacks to access cryptographic data (e.g., side-channel and fault injection attacks [83] , thus the adoption of a rigorous security certification scheme (i.e., Common Criteria [84] [85] would be justified to prevent such possibilities. Such a certification should apply at least to those ECUs affected by legal requirements (i.e., concerned by mileage storage and emissions control) and to operators equipment used for sensitive operating (e.g., ECU memory programming). Of course the selection of the cryptographic solutions to be adopted, in particular with regard to inter-ECUs communications, should be orchestrated along with other typical vehicle technological constraints, like communication protocols specifications and real-time needs. An alternative may be represented by the introduction of more powerful ECUs [88] capable of performing different tasks that were traditionally assigned to different ECUs (e.g., engine control unit and emission control unit may be merged in a single unit). This way the communication among sensitive units disappears removing at the same time the need to secure their exchange of information. Anyway the requirement of security certification of the resulting ECU would persist, to prevent other tampering practices on the unit itself (e.g., physical access to the unit board, leverage of debug and boot modes), along with other requirements like a communication with diagnostic tools based on standard security protocols.

Here below some final general considerations stemming from our study, outlining the current and future status of digital tampering and related countermeasures:

- current odometer tampering affects the mileage information communicated and stored in the vehicle. Most of current countermeasures for odometer tampering (e.g., redundant storage) are not focused in preventing the tampering but instead attempt to detect the modification, even if their effectiveness is not clear. Furthermore, in some cases no automatic checks are in place to compare the different stored odometers values in the different ECUs, leaving this task up to operators. It has also been noted that some vehicles cannot detect a freezing of mileage counting. Therefore, it may be advisable to introduce odometer plausibility diagnostics that cross checks the logical increase of the odometer reading

within all control units on-board of the vehicle (e.g. crosschecking the wheel rotation speed sensor data against GPS and possibly a third odometer model based on other sensor sources like engine speed, combined with gear indicator, etc). Nevertheless, the establishment of a set of requirements for securing the odometer data in transit and at rest relying on cryptographic solutions is the concrete recommendation as this should prevent mileage modifications. These requirements should be monitored by considering clear specifications that should include a test methodology;

- the tampering or deactivation of emission control systems are possible due to vehicle hardware modifications and software security shortcomings. Current tampering practices focus on emission control devices of diesel vehicles, including SCR, DPF, GPF and EGR. On the other hand, TWC seems to be the mostly targeted petrol component. The installation of hardware emulators represents a widespread tampering practice. Their size is getting smaller, and thus they can be more easily hidden. Also, plug-and-play emulators can be swiftly removed by the vehicle operator. ECU remapping is far stealthier, and obtaining exploitable evidence normally involves the intervention of an authorised by the manufacturer technician to detect re-flashes via the use of original equipment and manufacturer's software. Also in this case the adoption of cryptographic protocols and of sound assessment schemes should allow to tackle the issue. On top of this, consistency and plausibility checks, e.g., conducted over the various relevant sensor values, can be of aid here. Anyway, such countermeasures are so far insufficiently addressed in approval legislation, and hence not put to use by manufacturers;
- even if the use of HSM and SHE components has been already considered by automotive manufacturers, apparently there is no clear evidence that such devices are widely employed in current vehicles. However, both HSM and SHE are strongly recommended as a potential approach for securing vehicles against digital tampering practices;
- modern tampering is focusing on digital techniques rather than on vehicle hardware modifications and can be exercised either after obtaining physical access to the vehicle or remotely, since vehicles are going to be more and more connected through telematic services. For this reason, in general, a more secure digital vehicle infrastructure is paramount. For instance the systematic adoption of robust and affordable authentication system through a PKI, such as the ones foreseen for the digital tachograph system and the C-ITS, would be recommended (e.g., enhancing the SERMI scheme);
- from a cybersecurity standpoint, the diverse, and sometimes proprietary, architectures and protocols used by vehicle manufacturers may seem to serve a security by obscurity and security by diversity strategy, but at the same time, lead to misconfigurations, which in turn magnify the attack surface and entail vulnerabilities. Simply put, often, the manipulations utilise not-documented and not or feebly protected instructions build-in by manufactures, thus pertaining to a security-by-obscurity-weakness. Nevertheless, while security-by-obscurity features, including undocumented commands, may be present for allowing functions during service and maintenance, they also create room for misuse after identification. Overall, it can be said that the manufacturers' response against tampering in particular and cyberattacks in general remains

fragmented and in constant flux. The adoption of standard security solutions and of commonly accepted certification scheme would be of help in that regard. In the same mindset, more details on odometer and ECS ECUs should be made public by manufacturers to support the fighting against tampering during PTIs;

- purely digital tampering is hard to immediately detect and patch. Actually, it pertains to zero-day vulnerabilities. This situation also calls for concrete vulnerability disclosure policies [86] [87] the existence of well-maintained vulnerability databases, and frequent software updates. If not properly addressed, the latter need creates more opportunities to tamperers and attackers. Note that attackers may be involved in such incidents for instance to provide ready-to-flash files and other ECU software tools to tamperers;
- it is expected that in the future the updates of software and perhaps also hardware will increase due to the more complex and comprehensive functions but also due to the higher amounts of security updates. Therefore, a process for updating the approval would be more and more important. This aspect is key for the certification process of vehicles' components, as software updates could require the re-certification process of certain components. To be noted that for the case of Common Criteria security certifications a re-certification or certification maintenance process [94] for assurance continuity is already available;
- the use of a EU-wide platform to enable the cross-border sharing of vehicle information could mitigate for instance the issues associated to odometer frauds. This platform would most ideally interconnect the national databases of the EU countries and, if applicable, databases of manufacturers that are already in place to store odometer readings. The target platform should be based on existing best practices to provide a timely and reliable collection of such data. Beyond the use of such databases, also the adoption of blockchain-based platform is advocated by some parties [2] , in particular to combat odometer tampering. The idea is that any vehicle sends and so stores its mileage values in a blockchain infrastructure. Anyway the added value of such solutions may remain questionable. Indeed the generation for instance of blockchain data would rely on the mileage information produced and stored by the vehicle. If vehicle mileage data remains susceptible to tampering, the blockchain data may be equally affected. Therefore, only when protection at the source is ensured it may be useful to apply a tracking database, or to rely on data offered via the Extended Vehicle concept [96] (i.e., vehicle data is transmitted to servers and then offered in the form of Web services) to check the enforcement of legislations. Indeed, without strong protection of the mileage inside the vehicle, the value can be "adjusted" before each external storage cycle and therefore may even document a wrong value officially;
- certain highly potent manipulation schemes are very costly too. So, a straightforward measure is to discourage tamperers by making the amortization and pay-back of such a tampering method unattractive in terms of investment payback and return on equity. In that regard, a Common Criteria certified ECU is likely to request a huge effort to be compromised, thus making any tampering probably unattractive;
- newest regulations on vehicle cybersecurity, namely UN R155 and R156 [91] allows for "self-certification" by the manufacturers (OEM). Indeed in

the current cyber security legislation there is the absence of harmonised test requirements and performance criteria against which the technical service shall test. The introduction of cybersecurity certification schemes like the Common Criteria one can reinforce the effectiveness of the new regulations;

- the protection of private data stored in the vehicle and possibly communicated to external parties, including the manufacturer itself, should be also regulated and ensured. At the same time the availability of certain sets of in-vehicle data for non-OEM organizations, e.g., PTI providers, shall be duly preserved.

7 Conclusion

Modern vehicles are featured by several digital components, the ECUs, and some of them can be tampered to modify the mileage produced and stored by the Odometer or alter the functioning of Emission Control Systems. In both cases such malpractices can be either directly pursued by the vehicle owner (or its operators), or commissioned to professional tamperers. The purpose of the tampering is to obtain financial benefits, namely to sell the vehicle at a higher price in the case of odometer tampering, or saving operational and maintenance costs in the case of emission control manipulations.

Vehicle digital tampering practices are reaching a high engineering level, relying on techniques which typically pertain to the information technology domain, and specifically to that of embedded systems. It is not rare, also browsing the web, to find sponsored tools to be simply connected to the vehicle network to program an ECU memory, or even tutorial and workshop services to directly act on the ECUs circuit board to carry out a tampering.

Such tamperings are typically made possible by weaknesses in ECUs software and hardware, as well as in the adopted interaction protocols. To prevent the introduction of such weaknesses, more specific security requirements should be adopted, underpinned by more stringent testing and approval schemes. This should be valid at least for all legally-mandated digital components employed in a vehicle.

The bottom line here is that security in this fast-evolving sector should be prioritised at the same high level as safety and environmental protection. Namely, a holistic, solid, and consistent way is required to safeguard vehicle's on-board and off-board security assets from manipulation.

References

[1] COMMISSION REGULATION (EU) 2017/1151 of 1 June 2017. Official Journal of the European Communities L175. http://data.europa.eu/eli/reg/2017/1151/oj

[2] Research for TRAN Committee – Odometer tampering: measures to prevent it. European Parliament. Directorate General for Internal Policies. 2017. https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2017)602012

[3] DIRECTIVE 2014/45/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 3 April 2014 on periodic roadworthiness tests for motor vehicles and their trailers and repealing Directive 2009/40/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0045&from=ES

[4] DIRECTIVE 2014/46/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 3 April 2014 amending Council Directive 1999/37/EC on the registration documents for vehicles. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0046&from=GA

[5] DIRECTIVE 2014/47/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCILof 3 April 2014 on the technical roadside inspection of the roadworthiness of commercial vehicles circulating in the Union and repealing Directive 2000/30/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0047&from=es

[6] EC launches a web tool for vehicle registration & roadworthiness documents. International Motor Vehicle Inspection Committee, 2020. https://citainsp.org/2020/04/10/ec-launches-a-web-tool-for-vehicle-registration-roadworthiness-documents/

[7] Odometer manipulation in motor vehicles in the EU - European Added Value Assessment Accompanying the European Parliament's legislative initiative report, 2018. https://www.europarl.europa.eu/RegData/etudes/STUD/2018/615637/EPRS_STU(2018)615637_EN.pdf

[8] Odometer manipulation in motor vehicles: revision of the EU legal framework European Parliament resolution of 31 May 2018 with recommendations to the Commission on odometer manipulation in motor vehicles: revision of the EU legal framework (2017/2064(INL)). https://www.europarl.europa.eu/doceo/document/TA-8-2018-0235_EN.pdf

[9] Commission Regulation (EU) 2016/646 of 20 April 2016 amending Regulation (EC) No 692/2008 as regards emissions from light passenger and commercial vehicles (Euro 6). http://data.europa.eu/eli/reg/2016/646/oj.

[10] Regulation (EC) No 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information (Text with EEA relevance). http://data.europa.eu/eli/reg/2007/715/oj.

[11] Regulation (EC) No 595/2009 of the European Parliament and of the Council of 18 June 2009 on type-approval of motor vehicles and engines with respect to emissions from heavy duty vehicles (Euro VI) and on access to vehicle repair and maintenance information and amending Regulation (EC) No 715/2007 and Directive 2007/46/EC and repealing Directives 80/1269/EEC, 2005/55/EC and 2005/78/EC (Text with EEA

relevance). http://data.europa.eu/eli/reg/2009/595/oj.

[12] Commission Regulation (EU) No 582/2011 of 25 May 2011 implementing and amending Regulation (EC) No 595/2009 of the European Parliament and of the Council with respect to emissions from heavy duty vehicles (Euro VI) and amending Annexes I and III to Directive 2007/46/EC of the European Parliament and of the Council Text with EEA relevance. http://data.europa.eu/eli/reg/2011/582/oj.

[13] eeNews, Automotive, Number of automotive ECUs continues to rise [Online]. Available: https://www.eenewsautomotive.com/news/number-automotive-ecus-continues-rise, Accessed on: Jun 18, 2020.

[14] QNX Neutrino Real-time Operating System (RTOS) [Online]. Available: https://blackberry.qnx.com/en/software-solutions/embedded-software/qnx-neutrino-rtos, Accessed on: Jun 18, 2020.

[15] VxWorks [Online]. Available: https://www.windriver.com/products/vxworks/, Accessed on: Jun 18, 2020.

[16] AECC, Three-Way Catalysts (TWC) [Online]. Available: https://www.aecc.eu/technology/catalysts/, Accessed on: June 18, 2020.

[17] 802.3bw-2015 - IEEE Standard for Ethernet Amendment 1: Physical Layer Specifications and Management Parameters for 100 Mb/s Operation over a Single Balanced Twisted Pair Cable (100BASE-T1). https://standards.ieee.org/standard/802_3bw-2015.html

[18] ISO 17458-1:2013, Road vehicles — FlexRay communications system — Part 1: General information and use case definition. https://www.iso.org/standard/59804.html

[19] ISO 17458-5:2013, Road vehicles — FlexRay communications system — Part 5: Electrical physical layer conformance test specification. https://www.iso.org/standard/59809.html

[20] ISO 17987-1:2016, Road vehicles — Local Interconnect Network (LIN) — Part 1: General information and use case definition. https://www.iso.org/standard/61222.html

[21] ISO 11898-1:2015, Road vehicles — Controller area network (CAN) — Part 1: Data link layer and physical signalling. https://www.iso.org/standard/63648.html.

[22] CiA, CANopen history [Online]. Availbale: https://www.can-cia.org/can-knowledge/canopen/canopen-history/

[23] SAE International, Core J1939 Standards. https://www.sae.org/standardsdev/groundvehicle/j1939a.htm.

[24] C. Smith, The Car Hacker's Handbook: A Guide for the Penetration Tester, No Starch Press, 1st Edition, March 2016, ISBN 978-1593277031.

[25] Othmar Arnold, Cantonal Police Uri, AdBlue fraud: Manipulations on exhaust gas post-treatment.

[26] ECUCONNECTIONS forum [Online]. Available: https://www.ecuconnections.com/forum, Accessed on: Jun 18, 2020.

[27] ECU Tuning Performance forum [Online]. Available: https://forum.ecutuningperformance.com, Accessed on: Jun 18, 2020.

[28] COBB Tuning - COBB University Episode #16 - How To Use an Accessport [Online]. Available: https://www.youtube.com/watch?v=xDeNjPgqtAQ, Accessed on: Jun 18, 2020.

[29] MHD Wireless OBDII Wifi Flash Adapter'' [Online]. Available: https://burgertuning.com/products/mhd-wireless-obdii-wifi-flash-adapter, Accessed

on: Jun 18, 2020.

[30] Best OBD2 Android/iOS Apps For Cars Review in 2018/2019 [Online]. Available: https://magnetoitsolutions.com/blog/best-obd2-android-ios-apps-for-cars-review, Accessed on: Jun 18, 2020.

[31] PTT 2.7 Development & Dev Tool Plus [Online]. Available: https://www.amazon.com/Premium-Tech-Development-Volvo-Renault/dp/B07NZCND3T, Accessed on: Jun 18, 2020.

[32] LAUNCH X431 V PRO Bi-Directional Scan Tool [Online]. Available: https://www.amazon.com/LAUNCH-Diagnostic-Bi-Directional-Control-Warranty/dp/B01GRN4BRQ, Accessed on: Jun 18, 2020.

[33] Autotuner automotive tool [Online]. Available: https://www.autotuner-tool.com/en, Accessed on: Jun 18, 2020.

[34] Youtube, How To Chip / Socket A Honda OBD1 ECU [Online]. Available: https://www.youtube.com/watch?v=R02luOvJgFI, Accessed on: Jun 18, 2020.

[35] ECU Tools, CMD Flash Master plus OBD-II [Online]. Available: https://ecutools.eu/chip-tuning/cmd-flash-master-obd, Accessed on: Jun 18, 2020.

[36] Magic Motor Sport, FLEX tool [Online]. Available: https://www.magicmotorsport.com/flex/, Accessed on: Jun 18, 2020.

[37] EVC, WinOLS [Online]. Available: https://www.evc.de/en/default.asp, Accessed on: Jun 18, 2020.

[38] EVC, BDM100 [Online]. Available: https://www.evc.de/en/product/bdm/, Accessed on: Jun 18, 2020.

[39] K-Motor [Online]. Available: https://kmotorperformance.com/product/o2-oxygen-sensor-cel-fix-extender-adapter-check-engine-light-fix-spacer-m18x1-5/, Accessed on: Jun 18, 2020.

[40] Infineon, 32-bit XMC4000 Industrial Microcontroller ARM® Cortex-M4 [Online]. Available: https://www.infineon.com/cms/en/product/microcontroller/32-bit-industrial-microcontroller-based-on-arm-cortex-m/32-bit-xmc4000-industrial-microcontroller-arm-cortex-m4/, Accessed on: Jun 18, 2020.

[41] TAFMET, EGR valve simulator Ducato Iveco Boxer Jumper 3.0 JTD HDI (4-pins plug) [Online]. Available: https://tafmet.pl/english/egr-valve-simulators/206-egr-valve-simulator-ducato-iveco-boxer-jumper-30-jtd-hdi-4-pins-plug.html, Accessed on: Jun 18, 2020.

[42] Infineon, ASC Bootstrap Loader for XMC4000 [Online]. https://www.infineon.com/dgdl/Infineon-XMC4000_TOO_Bootloader-ApplicationNotes-v01_04-EN.pdf?fileId=db3a30433e4143bd013e46a58ebf40cb, Accessed on: Jun 18, 2020.

[43] Infineon, CAN Bootstrap Loader (BSL) [Online]. https://www.infineon.com/dgdl/Infineon-AP32269_XMC4000_CAN_BSL-AN-v01_00-EN.pdf?fileId=5546d4624933b875014936d188cd1659, Accessed on: Jun 18, 2020.

[44] EVC, BSL100 [Online]. Available: https://www.evc.de/en/product/bsl/, Accessed on: Jun 18, 2020.

[45] The Danish Technological Institute, Investigation of NOx manipulation in heavy duty vehicles, March 2018.

[46] PiCAN2 - CAN Interface for Raspberry Pi With SMPS'' [Online]. Available: https://copperhilltech.com/pican2-can-interface-for-raspberry-pi-with-smps/, Accessed on: Jun 18, 2020.

[47] CAN-BUS Shield V1.2 [Online]. Available: https://wiki.seeedstudio.com/CAN-

BUS_Shield_V1.2/, Accessed on: Jun 18, 2020.

[48] GitHub - Seeed-Studio / CAN BUS Shield [Online]. Available: https://github.com/Seeed-Studio/CAN_BUS_Shield, Accessed on: Jun 18, 2020.

[49] Paul Greening, ACEA market Survey into AdBlue emulators. AdBlue Emulator Workshop, 5 December 2017.

[50] Adblue Emulators Investigation Results. ACEA AdBlue Emulator Workshop, Brussels, 5 Dec. 2017.

[51] Dailymotion, Removal of particulate filter DPF Subaru (DPF Emulator SK-05) [Online]. Available: https://www.dailymotion.com/video/x7t66zz, Accessed on: Jun 18, 2020.

[52] SDS [Online]. Available: https://dpf-toyota.com/, Accessed on: Jun 18, 2020.

[53] Baldini Gianmarco, Daniele Borio, Raimondo Giuliani, Jose Luis Hernandez Ramos, Tania Martin, Ioannis Vakalis, Security & Privacy Challenges in cooperative and automated vehicles (CAV), JRC Report 113816. Publications Office of the European Union, 2018.

[54] Hacking the CAN Bus: Basic Manipulation of a Modern Automobile Through CAN Bus Reverse Engineering GIAC (GCIA) Gold Certification, 2017. https://www.sans.org/reading-room/whitepapers/threats/paper/37825

[55] Hex-works. Hex editor for EEPROM dump editing. http://hex-works.com/eng

[56] How Odometers Work, [Online]. Availbale: https://auto.howstuffworks.com/car-driving-safety/safety-regulatory-devices/odometer.htm#pt2

[57] Selective Catalytic Reduction | How it Works, [Online]. Available: https://www.tersusdef.com/about/how-selective-catalytic-reduction-scr-works/

[58] How Exhaust Gas Recirculation (EGR) system works , [Online]. Available: https://www.samarins.com/glossary/egr-system.html

[59] Lambda power – Technotes [Online]. Available: https://secure.lambdapower.co.uk/TechNotes/Tech-1.asp, Accessed on: Jun 18, 2020.

[60] Deplhi Technologies, Aftermarket, The basics of EGRs - what they do, how they work, how to troubleshoot [Online]. Available: https://www.delphiautoparts.com/gbr/en/resource-center/basics-egrs-what-they-do-how-they-work-how-troubleshoot, Accessed on: Jun 18, 2020.

[61] Youtube, How to Pass Emissions Without a Catalytic Converter, [Online]. https://www.youtube.com/watch?v=q1rJ2tJXhok, Accessed on: Jun 18, 2020.

[62] Youtube, How to Install a Defouler (Fix CEL Light) [Online]. https://www.youtube.com/watch?v=EuEsevIXE7Q, Acessed on: Jun 18, 2020.

[63] EEPROM EMULATOR EASY, [Online]. Available: http://www.diagprog4.co.uk/wp-content/uploads/2019/05/Emulator_EEPROM_eng.pdf. Accessed on September 16, 2020

[64] Ring, Martin, Tobias Rensen, and Reiner Kriesten. Evaluation of vehicle diagnostics security – implementation of a reproducible security access. SECURWARE 2014, 2014.

[65] Introduction to UDS, [Online]. Available: https://udsoncan.readthedocs.io/en/latest/udsoncan/intro.html

[66] Artificial intelligence: Bosch teaches cars how to learn and take appropriate action, [Online]. Availbale: https://www.bosch-presse.de/pressportal/de/en/artificial-

intelligence-bosch-teaches-cars-how-to-learn-and-take-appropriate-action-92352.html

[67] FCA Secure Gateway Module [Online]. Available: https://diag.net/msg/m1fsoznwl3nndqti9pxq9k4nz0

[68] AUTOSAR. Specification of Secure Hardware Extensions. https://www.autosar.org/fileadmin/user_upload/standards/foundation/19-11/AUTOSAR_TR_SecureHardwareExtensions.pdf

[69] Wolf, Marko, and Timo Gendrullis. Design, implementation, and evaluation of a vehicular hardware security module. International Conference on Information Security and Cryptology. Springer, Berlin, Heidelberg, 2011.

[70] M. Ring, T. Rensen and R. Kriesten. Evaluation of Vehicle Diagnostics Security – Implementation of a Reproducible Security Access, in proc. of The Eighth International Conference on Emerging Security Information, Systems and Technology, 2014.

[71] C. Valasek, C. Miller, Adventures in Automotive Networks and Control Units, Technical white paper, 2014. https://ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf, Accessed on: Dec 4, 2020.

[72] E90Post.com Forum, Late E-Series N55 MEVD1726 DME Removal/Benchflash Guide, [Online]. Available: https://www.e90post.com/forums/showthread.php?t=1433320, Accessed on: Dec 4, 2020.

[73] AURIX 32-bit microcontrollers for automotive and industrial applications [Online]. Available: https://www.infineon.com/dgdl/Infineon-TriCore_Family_BR-ProductBrochure-v01_00-EN.pdf?fileId=5546d4625d5945ed015dc81f47b436c7, Issue 2020, Accessed on: Dec 4, 2020.

[74] QNX, Software watchdog [Online]. Available: http://www.qnx.com/developers/docs/qnxcar2/index.jsp?topic=%2Fcom.qnx.doc.neutrino.sys_arch%2Ftopic%2Fproc_Watchdog.html, Accessed on: Dec 4, 2020.

[75] COHEN Daniel, TONKICH Vladimir. Tamper resistant case, Patent no. WO/2016/189523, Dec. 2016. https://patentscope.wipo.int/search/en/detail.jsf?docId=WO2016189523&tab=PCTDESCRIPTION, Accessed on: Dec 4, 2020.

[76] Gencoupe forum, ECU information [Online]. Available: https://www.gencoupe.com/threads/ecu-information.101736/, Accessed on: Dec 4, 2020.

[77] EEVblog Electronics Community Forum, Vehicle ECU - dissolving PolyUrethane, [Online]. Available: https://www.eevblog.com/forum/projects/vehicle-ecu-dissolving-polyurethane/, Accessed on: Dec 4, 2020.

[78] ELECTROLUBE, Electronics Control Unit (ECU), [Online]. Available: https://www.electrolube.com.au/products/automotive-electronics-ecu/2k850/ecu/, Accessed on: Dec 4, 2020.

[79] Advanced Diagnostics, CodeX Lite, Universal EEPROM Kit For Locksmiths & Auto Electricians [Online]. Available: https://www.advanced-diagnostics.com/CodexLite-EEPROM-Kit-Locksmith-Tools-Garage-Equipment, Accessed on: Dec 4, 2020.

[80] SecureLayer7, Reading data from EEPROM without desoldering, [Online]. Available: https://securelayer7.github.io/posts/reading-firmware-from-eeprom-easyway/, Accessed on: Dec 4, 2020.

[81] Van Lock Store, Red Box (OBD Protection), [Online]. Available: https://vanlockstore.co.uk/red-box-ecu-protection.html, Accessed on: Dec 4, 2020.

[82] Schweppe, Hendrik, et al. Securing car2X applications with effective hardware software codesign for vehicular on-board networks. VDI Automotive Security 27, 2011.

[83] Y. Li, M. Chen and J. Wang. Introduction to side-channel attacks and fault attacks, 2016 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC), Shenzhen, 2016, pp. 573-575.

[84] ISO/IEC 15408 Information technology — Security techniques — Evaluation criteria for IT security. https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

[85] ENISA. Cybersecurity Certification - EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS, Ver.1.0, 01/07/2020

[86] M. Schaake, L. Pupillo, A. Ferreira, G. Varisco. Software Vulnerability Disclosure in Europe Technology, Policies and Legal Challenges. Report of a CEPS Task Force. June 2018.

[87] ENISA. Economics of vulnerability disclosure. December 2018.

[88] G. Niedrist. Deterministic Architecture and Middleware for Domain Control Units and Simplified Integration Process Applied to ADAS. TTTech. https://www.tttech-auto.com/wp-content/uploads/TTTech_Deterministic-Architecture-and-Middleware_2016.pdf

[89] SERMI. Scheme for accreditation, approval and authorization to Access Security-related Repair and Maintenance Information (RMI), May 2016.

[90] ISO/SAE DIS 21434 Road vehicles - Cybersecurity engineering, https://www.iso.org/standard/70918.html, Accessed on: March 3, 2021.

[91] UNECE, Three landmark UN vehicle regulations enter into force, https://unece.org/sustainable-development/press/three-landmark-un-vehicle-regulations-enter-force, Accessed on: March 3, 2021.

[92] Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) No 165/2014 of the European Parliament and of the Council laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components. http://data.europa.eu/eli/reg_impl/2016/799/oj

[93] Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), Release 1, December 2017. https://ec.europa.eu/transport/sites/transport/files/c-its_security_policy_release_1.pdf

[94] Application for the Issuance of a Certificate (Deutsches IT-Sicherheitszertifikat) based on Common Criteria by the German Federal Office for Information Security (BSI), [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Product_certification_application_form.pdf;jsessionid=239106456F415A08CFBC1CA986DA0216.internet081?__blob=publicationFile&v=1, Accessed on: March 2021.

[95] UL Cybersecurity Assurance Program (UL CAP), [Online]. Available: https://www.ul.com/resources/ul-cybersecurity-assurance-program-ul-cap, Accessed: March 2021.

[96] ISO 20077-1:2017 Road Vehicles — Extended vehicle (ExVe) methodology — Part 1: General information. https://www.iso.org/standard/66975.html

[97] MyGenius – OBDII Remapping at any time, [Online]. Available: https://www.dimsport.it/en/race/my-genius/, Accessed: March 2021.

List of abbreviations and definitions

BCM	Body Control Module
CAN	Controller Area Network
DPF	Diesel Particulate Filter
DTC	Diagnostic Trouble Code
EBCM	Electronic Brake Control Module
ECS	Emission Control System
ECU	Electronic Control Unit
EEPROM	Electrically Erasable Programmable Read-Only Memory
EGR	Exhaust Gas Recirculation
EPS	Environmental Protection System
ERDF	European Regional Development Fund
HSM	Hardware Security Module
MIL	Malfunction Indicator Lamp
OBD	On-Board Diagnostics
OTA	Over-the-Air
PCM	Powertrain Control Module
PTI	Periodic Technical Inspection
SCR	Selective Catalytic Reduction
SHE	Secure Hardware Extension
TCM	Transmission Control Module
TWC	Three-Way Catalyst
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VCM	Vehicle Control Module

List of figures

Figure 1. In-Vehicle Digital Architecture....10
Figure 2. Example of mechanical odometer [56] 13
Figure 3. Basic operation of a digital odometer 14
Figure 4. Basic operation of the SCR process [57] 15
Figure 5. Basic components of the SCR emission reduction system of a diesel vehicle [25] 16
Figure 6. Basic Operation of the EGR system [58] 16
Figure 7. Three-way catalyst closed-loop system [59]....17
Figure 8. A screenshot of the WinOLS application. As observed, the application can automatically recognise program code, empty areas, maps, etc. [37] 21
Figure 9. A BDM testbed [38] 21
Figure 10. A BSL testbed [44]....22
Figure 11. Example of SCR temperature sensor manipulation using resistors....24
Figure 12. High-level categorization of vehicle tampering methods. Tuning methods can also be seen as subcategories of the other two methods, namely ECU flashing and hardware emulators....25
Figure 13. Example of hardware to manipulate the odometer value through the ODB port 26
Figure 14. Screenshot of the hex-works website that can be used to modify odometer values 27
Figure 15. Snapshot of an EEPROM emulator installation [63] 27
Figure 16. Example of odometer freezer hardware and connector....28
Figure 17. Tampering of the SCR system via (1) OBD emulator, (2) CAN emulator, (3) ECU flashing, and (4) manipulation of temperature, level, or NOx sensors [45] 30
Figure 18. Typical operation of a particle filter emulator [52] 31
Figure 19. An EGR pneumatic valve emulator [41]. 31
Figure 20. Connection diagram for the EGR valve emulator of Figure 19 [41]. 32
Figure 21. Example of an installed O2 spacer [39]....33
Figure 22. Odometer and ECS tampering practices 33
Figure 23. Simplified overview of the diagnostic protocol [64] 35
Figure 24. Comparison between hardware security components [69]....41

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

- at the following standard number: +32 22999696, or

- by electronic mail via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications from EU Bookshop at: https://publications.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

The European Commission's science and knowledge service

Joint Research Centre

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub

ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

EU Science, Research and Innovation

EU Science Hub

Publications Office
of the European Union