Summary: How They Did It: An Analysis of Emission Defeat Devices in Modern Automobiles

1 Introduction

"How They Did It: An Analysis of Emission Defeat Devices in Modern Automobiles" was written by M. Contag, G. Li, A. Pawlowski, F. Domke, K. Levenchenko, T. Holz and S. Savage and published in 2017 in *Security and Privacy (SP), IEEE Symposium*. The objective of this paper is the examination of different types of so-called "defeat devices", used for example by Volkswagen, and the uncovering of their technical details. Based on these findings, the authors developed a prototype called "CurveDiff" to automatically detect defeat devices.

2 Exhaust scandals in the past

The paper is based on two case studies: Volkswagen Group and Fiat Chrysler Automobiles. Both are independent vehicle manufacturers that stand accused of cheating on emissions tests by using a defeat device. In September 2015, the US Environmental Protection Agency published a claim against the Volkswagen Group. The allegation: Volkswagen implemented defeat devices for over eight years in twelve different car models. In February 2016, the next emission scandal occured. This time it hit Fiat Chrysler Automobiles. Both cases show the high pressure automobile manufacturers are under and which trade-offs they must deal with: weak performances or heavy fines?

3 Relevant basics and fundamentals of automobile engines

Due to strict emission standards, performance and efficiency of diesel engines are in danger. Compared to gasoline engines, diesel engines are environmentally more harmful due to noise and higher emissions of particulate matters and nitrogen oxides (NO_x). This is caused by a different fuel injection timing in the combustion process. The combustion cylinder of diesel engines takes air and compresses it. When the time of the compression cycles demands it, fuel is added and ignited. One can see and hear the environmental impacts, which are black smoke and the so-called diesel knock. Vehicle manufacturers try to reduce those emissions by means of emission control devices, which have advantages as well as disadvantages. The Exhaust Gas Recirculation (EGR) and NO_x Storage Catalyst (NSC) decrease NO_x but increase particulate emissions. The Selective Catalyst Reduction (SCR) also decreases NO_x but requires urea injection. The Diesel Particulate Filter (DPF) decreases black smoke and particulate emissions but requires regeneration.

4 Relevant basics and fundamentals of test procedures

The US Environmental Protection Agency as well as the California Air Resources Board define US standards as maximum pollutant levels for vehicles. The maximum pollutant levels in Europe are defined by the EU standards (starting at Euro 1 and continuing up to Euro 6). To check if vehicle manufacturers obey those emission standards, emission test cycles are carried out. The emission tests in the US and Europe are done on a chassis dynamometer, which means the vehicle is lifted up for the wheels to turn while it stays on one spot. Test protocols are publicly available including details about standardize lab temperatures, vehicle conditions, speed, load, number of stops and the types of route (highway, rural road or urban). Emission compliance is confirmed when an automobile passes all test cycles, which imitate different typical driving scenarios. The so-called cycle beating happens when the exhausted emissions are different during test cycles than on the road.

5 Relevant basics and fundamentals of engine control units

Cycle beating is possible because of the complexity of the cyber-physical system of an automobile. There are more than 70 electronic control units that use sensors (e.g. speed and exhaust oxygen content) and control actuators (e.g. brake and engine). Any defeat device is not a hardware component but part of a car's software which is connected to the electronic engine control unit (ECU). The ECU is the most important embedded system. It can alter the engine power, fuel consumption and exhaust gases by influencing emission control devices. It requires sensor inputs to control the combustion process. Therefore, the ECU communicates status information with other electronic control units. The key component of many diesel light passenger vehicles is EDC17 ECU and manufactured by Robert Bosch GmbH. The German company builds the hardware and develops its software. Their customers are automobile manufacturers, i.e. Volkswagen Group and Fiat Chrysler Automobiles. Bosch calibrates all constants for each vehicle model which leads to the assumption that Bosch created said defeat devices, whereas Volkswagen and Fiat enabled them for their specific vehicle models.

6 Relevant basics and fundamentals of defeat devices

The defeat devices of Volkswagen and Fiat Chrysler Automobiles are of different kind. In the first case study concerning Volkswagen, defeat devices work as a mechanism for appropriate vehicle behaviour during emissions tests and environmentally worse behaviour on the road. After the defeat device does not recognize a test scenario, it alters the vehicle behaviour from emission friendly driving mode to "real" driving mode.

Volkswagen's test detection is based on the condition monitoring block, which is part of the function block. Depending on the status of the customer-specific acoustic condition, the "real" driving mode is set if computations equal 0 (and the acoustic condition is activated). Factors include the temperatures of coolant, fuel, oil and atmospheric pressure when the engine is started. If the acoustic condition is deactivated and computations equal 1, emission firendly driving mode is set. Here, factors such as time since start of engine, acceleration pedal position, engine revolution counter and distance play a role. Additionally, the defeat device compares time-distance profiles to known test cycle curves. If computed relation values are outside of determined lower and upper boundaries, the "real" driving mode is set while the acoustic-condition is activated. Furthermore, Volkswagen implemented a steering wheel check: In case the angle of the steering wheel differs by more than 20 degree from its neutral position, emission friendly driving mode is set while the acoustic-condition is deactivated. As there are two sets of calibration values for each driving mode, every Volkswagen diesel light passenger vehicle has two personalities. The customer-specific acoustic condition influences other components of a vehicle as well. On one hand, the acoustic condition alters fuel injection behaviour. In case it is set to true, there is an additional constant for emission friendly driving mode. If it is set to false, a value based on the engine speed for "real" driving mode is computed. The acoustic condition alters the recirculated amount of exhaust gasses. If it is true, a correction value for the total air mass is computed for emission friendly driving mode.

Compared to the discussed case study, Fiat 500X has a time-based defeat device built in. It has neither any acoustic condition in its function sheets nor any test cycle curves in firmware images. Fiat Chrysler Automobiles used the Bosch EDC17 ECU as well, but manipulated the regeneration of the NO_x Storage Catalyst. This way the frequency of regeneration is reduced to improve fuel economy. While demand logic decides when NSC regeneration takes place, release logic decides when NSC regeneration is allowed. Both depend on the NO_x load and catalyst temperature.

7 The beginning: Detecting defeat devices manually

The authors analysed three data sources to find out how defeat devices were implemented by the Volkswagen Group. The first data source are function sheets as already mentioned. They describe the functinal behaviour of the ECU firmware. The second data source comprises so-called A2L and OLS files. These files contain the calibration process of the ECU firmware images. While A2L state which elements are modified by manufacturers, OLS indicate which configuration values or calibration constants are set by the manufacturers. The third and last data source are the ECU's firmware images themselves. They can be officially obtained via the Volkswagen online platform.

8 Detecting Defeat Devices: CurveDiff

To detect active defeat devices like the ones used by Volkswagen, the authors developed a static binary analysis tool called "CurveDiff". It is a fully automated framework for EDC17 ECUs which analyzes given firmware images and looks for circumvention code as described in chapter 5. The general procedure of CurveDiff contains 4 steps: First the IDA database is generated and pre-processed. This involves accessing different data regions to resolve memory accesses. Secondly, the core structures are built. Here Static Single Assignment Form (SSA) is used to facilitate the process. SSA describes an intermediate language in which each variable has one single definition assigned that dictates its use. Thus, the transformation of functions into SSA form allows to design efficient data-flow analysis algorithms. The third step includes the analysis of curve function invocations. This is done by extracting all invocations and pairing them in order to determine the upper and lower boundary for a given data point. During the last step, the obtained curve checks are matched against known test cycles. If the data points of a driving profile (i.e. test cycle) lie within the determined boundaries, the driving profiles match.

To test their device, the authors used 963 firmware images by Volkswagen. The results according to the authors were 924 successfully analyzed firmware images, 20 timeouts and 19 failed analyzations. A total of 406 of the successfully analyzed images contained a defeat device of which 333 had one or more active profiles. The mean time necessary for a successful analyzation was 105 seconds. Compared to the chassis dynamometer, CurveDiff proved much faster.

Though a seemingly successful and viable product, the authors discuss some limitations of CurveDiff. It yet can only detect defeat devices that use an active detection approach (as described before). This means that the detection of passive defeat devices, i.e. ones that switch from emission friendly to normal mode after a certain period of time, is not included in CurveDiff. It further uses an intra-procedural analysis and excludes an inter-procedural approach which may enhance the reliability of its implementation.

The authors come to following conclusions: 1. Based on dated firmware images, a refinement of the defeat devices used by Volkswagen seemed to happen even though the company was already under investigation. 2. The authors are the first to present and evaluate an automatic approach to detect defeat devices in given firmware. 3. Furthermore, they are the first to openly document defeat devices used in Fiat 500X vehicles.

9 Conclusion

According to the authors, they are the first to reveal the defeat device in Fiat 500X vehicles. Yet on September 1st, 2016, the German Ministry of Transport sent a letter to Rome as well as the EU Commission in Brussels with initial findings obtained by the Kraftfahrt-Bundesamt that Fiat, similar to Volkswagen, installed defeat devices in their vehicles[1]. This included technical details. Since the paper "How They Did It: An Analysis of Emission Defeat Devices in Modern Automobiles" was first published in May 2017, their third statement cannot be confirmed. Nonetheless, they are the first to use the knowledge on defeat devices to build a system which can automatically detect emission circumventions. Seeing as “diesel gate” and defeat devices are still a hot topic and how easy emission tests can be manipulated due to their standardized nature, this paper makes a valuable contribution with CurveDiff and could help fight cheating car manufacturers in the future.

[1] http://www.wiwo.de/unternehmen/auto/fiat-500x-doblo-und-jeep-renegade-kommt-der-zweite-abgasskandal-aus-italien/14483066.html