DIAS

DIAGNOSTIC ANTI-TAMPERING SYSTEMS

N E W S L E T T E R

E D I T O R I A L

We are tampering with tampering!

Pollutant emissions of road vehicles have been reduced significantly thanks to the development and application of effective emissions control systems. However, tampering with these systems causes elevated tailpipe emissions to as much as the uncontrolled levels of vehicles decades ago. The numbers speak for themselves:

- Up to 10% of EU5/V and EU6/VI vehicles in the EU have suspiciously high emissions, mainly due to tampering with their exhaust aftertreatment system.
- Tailpipe emission levels for NOx-tampered vehicles can be more than 10 times higher than the limit. Tailpipe PM and PN emissions levels for DPF-tampered vehicles can be more than 100 times higher than the limit.

Ultimately, this leads to poor air quality, adverse effects on human health and inaccurate emissions data, with which regulations and protocols are established.

DIAS aims to harden a vehicle's EPS against tampering via prevention and detection solutions. This is achieved using a two-step approach. The first step involves developing measures that take early action against tampering ("low hanging fruits"). The second step prepares methodologies for dealing with tampering attempts in the future that are currently unknown.

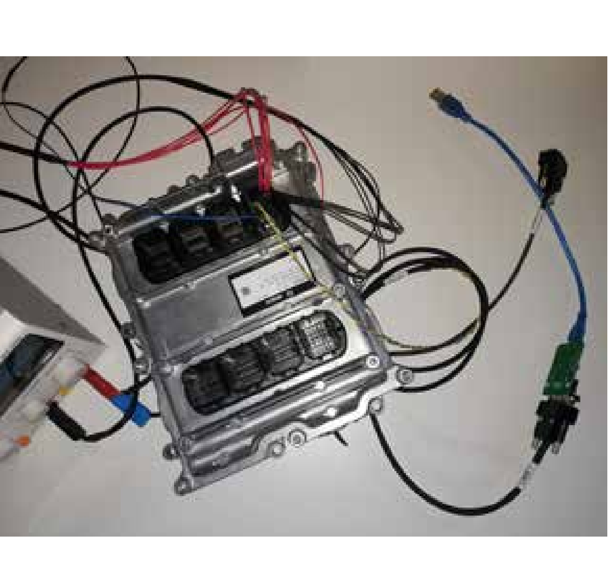
Up to now, we have successfully developed i) enhanced diagnostic solutions and ii) in-vehicle anti-tampering security techniques. This was feasible only after a thorough market review of tampering devices and practices, the testing of several of them, and the identification of the attack vectors and threats. Demonstration setups, including a demonstrator vehicle, have been built in parallel, which contain the proposed counter-measures. Effectiveness is judged by open competitions organized within the project (Hackathons). You can read about it in the "Hack-a-truck" article in this newsletter.

Currently and in the following months, we are focusing on future tampering and the development of relevant countermeasures. The knowledge gained will be leveraged to recommend regulatory provisions for effective anti-tampering. The proposals will be reviewed by several stakeholders including the advisory board, the associated industry as well as drivers' and consumers' associations.

The story so far

As the DIAS project is nearing its completion date of August 2022, the work on several of the tasks has started to come to fruition. These past months, three major public deliverables have been published.

1. For the deliverable D3.2 "Status quo of critical tampering techniques and proposal of required new OBD monitoring functions", a market assessment has been conducted and subsequently it has been determined which types of tampering devices pose the largest environmental risk. So far, 34 pieces of tampering equipment have been purchased and evaluated in lab and road tests. The tampering devices that were evaluated showed mixed results that ranged from successful to ineffective tampering. Based on the test results, the deliverable proposes the main directions for the development of required new functions which detect and prevent tampering.



2. The deliverable D4.2 "In-vehicular antitampering security techniques and integration" aims to reduce or totally eliminate tampering techniques that relate to vehicle emissions, by means of protective hardware and software solutions. This report serves as a description of the security techniques explored within the DIAS project, which could be used to alleviate tampering attempts. It provides an overview of security techniques and identifies three security directions: communication security, component security, and firewall & intrusion detection systems.

3. The deliverable D3.4 "Hackathon and security resilience evaluation of the level 1 concept: Outcome of the evaluation with the hackathon" provides an overview of the design and execution of the first hacking event that was executed in the DIAS project. The hackathon was an online event where five teams competed to come up with the best tampering plan. The five tampering plans presented contained six different types of attack vectors. However, no high-risk tampering solution was developed and proposed.

T H E 1 S T H A C K - A - T R U C K

To find out how the hackers do it we did it ourselves!

To get the participants up to speed, three training sessions were hosted by experts from industry-leading companies and knowledge institutes, such as Ford Otosan, Bosch and TNO. The participants learnt about the latest and the greatest new environmental protection systems, ECU and communication systems, tampering methods and the newly developed state-of-the-art countermeasures by the DIAS consortium. In between, the participants were assigned to a group of people with complementary skills and worked together on finding attack vectors in a defined truck set-up. Together, they worked out a business plan as if they were going to commercialize their new tampering product on the EU market.

The participants, despite their diverse backgrounds (ranging from mechanical engineering to computer science, electrical engineering and automotive engineering) had an avid interest in and experience with exhaust gas aftertreatment systems, automotive electronics and communication and security protocols.

The results of the Hackathon proved to be invaluable for the DIAS project: The hacking plans contained six different types of attack vectors. New attack vectors were found and also new methods were proposed for exploiting environmental systems.

Due to the restrictions imposed by the global pandemic, the tampering plans contain theoretical virtual attacks, which means that it was not physically demonstrated if an exploit would work. Nonetheless, the feedback on DIAS' proposed solutions from the participants proved to be equally as valuable.

Meet the partners

BOSCH Robert Bosch GmbH Germany

In 1886, Robert Bosch founded the "Workshop for Precision Mechanics and Electrical Engineering" in Stuttgart. Since then, the Bosch Group has been a leading global supplier of technology and services for the automotive sector. With regards to the DIAS project, Bosch's talented engineers have been tackling, along with the rest of the consortium, three of the most fundamental objectives for the DIAS project: Firstly, the development of systems that are able to detect malicious tampering. Secondly the creation of a cloud- based emissions certification system and finally, the preparation of a demonstrator vehicle that will incorporate all the innovations developed for the DIAS project.

FEV

FEV is a leading global engineering and digital mobility company. It was founded in 1978. Ever since, FEV has become a major supplier of advanced testing and instrumentation products and services to some of the world's largest OEMs. With regards to the DIAS project, FEV is the leader in the development of security mechanisms for hardened and tamper-proof vehicular systems. From the security analysis and requirements identification to the verification and validation of the proposed solutions, FEV's experts are playing a critical role in the success of the DIAS project.

MORE INFO

INTERNET SEARCH CHALLENGE!

Do you drive a diesel vehicle? Try searching for "EGR delete kit" followed by the brand and model of your car. Are there any kits available for your car? If yes, what promises do they make? Probably better fuel economy, better performance, higher power, better throttle response, increased lifespan for the engine, decreased maintenance costs, absence of Malfunction Indicator Light...

The list of promises sometimes seems never-ending! Well, if you've fallen for it, unfortunately for you, here at the DIAS project we've come to learn that not all those claims turn out to be true! So, would you risk removing a vital part of your environmental protection system now that you know the facts?

DIAS

Call: H2020-MG-2018-TwoStages

The DIAS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 814951