DIAS

Smart Adaptive Remote Diagnostic Antitampering Systems

EUROPEAN COMMISSION

HORIZON 2020

LC-MG-1-4-2018

Grant agreement ID: 814951

Deliverable No.	D3.4
Deliverable Title	Hackathon and security resilience evaluation of the level 1 concept: Outcome of the evaluation with the hackathon
Issue Date	05/10/2021
Dissemination level	Public
Main Author(s)	Q. Vroom (TNO) R. Vermeulen (TNO)
Version	V1.0

DIAS Consortium

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

Executive summary

Pollutant emissions of road vehicles have reduced significantly thanks to the development and application of effective and often complex emissions control systems. Tampering of these systems by vehicle owners leads to elevated tail-pipe emissions, up to uncontrolled levels of vehicles of decades ago. Tampering poses a large environmental risk because a small share of tampering potentially can lead to a significant increase of the EU fleet average emissions. A market assessment has shown that tampering mainly targets environmental protection systems (EPS) of diesel engines as equipped in heavy and light commercial vehicles, passenger cars, non-road mobile machinery and agricultural vehicles. Tampering methods are classified into four main categories: emulators, ECU flashing, sensor modification and OBD deletion devices.

The main objective of the DIAS project is to develop countermeasures to prevent or detect tampering of environmental protection systems on-board of vehicles. Countermeasures are developed consecutively at two levels: Level 1 enhanced OBD, Level 2 cloud-based adaptive diagnostics. How tamperproof each level is, needs to be thoroughly tested by means of traditional pen(etration) testing, but also by means of a hacking event by a team of independent experts, to search for possible remaining vulnerabilities. This report provides an overview of the design and execution of the first hacking event that was executed in the DIAS project to evaluate the prototype heavy-duty truck employed with DIAS Level 1 countermeasures.

Detailed results of the first hacking event are confidential since they contain valuable information on new anti-tampering measures and potential vulnerabilities. Consequently, the results are not documented in this public report. Detailed results are made available to the consortium members of the DIAS project in the form of presentations as made by the teams of expert hackers, notes made by the team mentors who observed the work, through a presentation describing the working principles of the proposed attacks and by providing a list of internal recommendations for assessment of vulnerabilities in the DIAS project.

Due to the Covid-19 pandemic, a physical hacking event could not take place. Alternatively, an online hackathon was organized. The event was called ‘Hack-a-truck’. The main mode of the event was a Team contest with monetary awards for the teams that developed the best tampering plans. The teams were provided with information in a number of technical presentations by experts of the DIAS consortium about tampering and the tampering object, the Ford Otosan prototype truck with Level 1 countermeasures. In working sessions, the Teams were asked to brainstorm for possible attack vectors, work out the attacks in detail and work out a simple business plan as if the tampering was to be commercialized on the EU market. The teams were supported by mentors from whom additional information could be gained from a pool of experts from the Consortium. Teams could propose attacks and the pool of experts responded by providing new information or by providing the result of an attack. The drawback of this iterative process of trial and error through online working sessions is that the process is a virtual one and no physical attacks were performed. This means that it could not be tested if the proposed attacks would have been successful, i.e. would have led to the successful deactivation of a (part of) an EPS without being detected. The limited amount of time and information might have caused the teams to not fully explore the more complex parts of the EPS to search for potential vulnerabilities. . The main advantage is that without the actual trouble of making things work, such as connecting instruments, writing code, there was a lot of room for creativity of the participants to propose new kinds of attacks, which could be evaluated by the DIAS Consortium afterwards. The combination of the hacking event and in-depth penetration tests that are performed in the DIAS project ensures that the concept is tested for known attacks and that new ones can be discovered in a very efficient way.

The hackathon was an online event where five teams competed to make the best tampering plan:

"…Your challenge is to find an attack vector or attack vectors, exploiting it to deactivate or remove an environmental protection system of a truck and develop a tampering device or service to commercialize the tampering product on the EU market…".

Each Team consisted of one expert hacker and four students with a mix of expertise ranging from Automotive engineering to IT security. Each Team performed brainstorming and working sessions to work out tampering plans, containing details of the approach with the attack vector, the exploit and a simple business plan to show impact and market potential. At the end of the event, the tampering plans were evaluated and ranked by a jury based on the following criteria:

- tampering success and impact
- detection on-board and at technical inspection
- complexity and costs
- market potential

This goal of the jury ranking was to award the teams, but not to assess to determine whether the tampering could pose an actual threat. The five plans received 29 to 49 points out of the maximum of 52 from the jury, see Table 1. Team 5, 'the Emulators' won the event by a small margin over Team 4 the 'Nikites'. The obtained tampering plans are confidential and have been shared within the DIAS Consortium.

Table 1: Teams, points and ranking of the tampering plans by the jury.

Team #	Team name	Points, max. 52	Rank
Team 1	Kronos	38	4
Team 2	CAN-U-BREAK-IT	29	5
Team 3	Tinker thunders	39	3
Team 4	Nikites	48	2
Team 5	The Emulators	49	1

After the hacking event, the attacks were evaluated by the Consortium with regard to the possible impact on tailpipe emissions, the working principles of the exploit, detection on-board and by inspection and market potential, and thus if a tampering plan poses a potential threat. The five tampering plans contain six different types of attack vectors. No high-risk tampering solution was developed and proposed, i.e. tampering with high impact, low costs and complexity and hard to detect by on-board systems or at technical inspections and with high market potential. However, new attack vectors were found and also new methods were proposed for making an exploit.

Three of the tamperings that were developed could only have a low impact, for instance, a small reduction of AdBlue consumption. One tampering had limited market potential. Three of the

tamperings proposed new advanced approaches which are considered complex, costly and detectable. Tampering plans also contained new alternative attack vectors. For these new attack vectors, further assessment is recommended and therefore additional penetration tests and an update of the Threat Analysis and Risk Assessment (TARA) will be performed in WP4.

The results of the event have shown that the level 1 countermeasures:

- made it harder to tamper with the EPS,
- lead to tampering with lower impact on emissions due to only partial tampering potential with lower attractiveness for the market,
- increased tampering complexity,
- made detection of tampering appears faster on the OBD and easier to spot during roadside or periodic inspections.

Contents

List of Abbreviations

CO_2	Carbon Dioxide
DEF	Diesel Exhaust Fluid
DIAS	Smart Adaptive Remote Diagnostic Antitampering Systems
DoW	Description of Work
DPF	Diesel Particle Filter
DTC	Diagnostic Trouble Code
EC	European Commission
ECU	Electronic Control Unit
EGR	Exhaust Gas Recirculation
EPS	Environmental Protection System
HD(V)	Heavy-Duty (Vehicle)
LD(V)	Light-Duty (Vehicle)
NDA	Non-Disclosure Agreement
MI(L)	Malfunction Indicator (Light)
NO_x	Nitrogen Oxides
OBD	On-board Diagnostics
OEM	Original Equipment Manufacturer
PTI	Periodic Technical Inspection
SCR	Selective Catalytic Reduction

Definitions

Attack surface	is a set of points, system elements or endpoints (attack vectors) whereby an attack could potentially breach, affect or control systems, and extract or manipulate information for malicious purposes
ECU	Electronic Control Unit, Embedded system in automotive electronics that controls one or more of the electrical systems or subsystems in a vehicle.
Environmental protection system	System fitted to a vehicle that is designed to reduce any (pollutant) emissions of that vehicle, e.g. EGR, DPF and SCR.
Exploit	An exploit (from the English verb to exploit, meaning "to use something to one's own advantage") is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behaviour to occur on computer software, hardware, or something electronic (usually computerized)
Hacking Event	Event organised within this project which allows hackers to tamper with (parts of) the environmental protection systems of vehicles to show and explain how they approach these systems.
Hacker	A person who uses computers to gain unauthorised access to data. With regard to environmental protection systems a hacker typically is a computer expert or vehicle technician that can, using his technical knowledge, make (unauthorised) changes to (secure) automotive ECUs or sensor communication, with either good or bad intentions.
Heavy-Duty	Vehicles that meet the requirements of vehicle categories M2, M3, N2 and N3 as defined in directive 2007/46/EC which involves: • M2 and M3: Vehicles designed and constructed for the carriage of passengers, comprising more than eight seats in addition to the driver's seat, and having a maximum mass not exceeding 5 tonnes for M2 and exceeding 5 tonnes for M3. • N2 and N3: Vehicles designed and constructed for the carriage of goods and having a maximum mass exceeding 3,5 tonnes but not exceeding 12 tonnes for N2 and having a maximum mass exceeding 12 tonnes for N3.
Light-Duty	Vehicles that meet the requirements of vehicle categories M1 and N1 as defined in directive 2007/46/EC which involves: • M1: Vehicles designed and constructed for the carriage of passengers and comprising no more than eight seats in addition to the driver's seat. • N1: Vehicles designed and constructed for the carriage of goods and having a maximum mass not exceeding 3,5 tonnes.

NRMM	Non Road Mobile Machinery. Any self-propelled vehicle which is designed and constructed specifically to perform work, which, because of its construction characteristics, is not suitable for carrying passengers or for transporting goods, as defined in directive 2007/46/EC. Machinery mounted on a motor vehicle chassis shall not be considered mobile machinery.
Tamperer	A person who for whatever reason deliberately tampers with the environmental protection systems of a vehicle.
To tamper	Interfere with something to cause damage or make unauthorised alterations.
Tampering Device	Also known as a cheating device. A systems, component or separate technical unit that, when fitted to a vehicle, actively or passively tampers with an environmental protection system of a vehicle with the purpose to (partly) deactivate or bypass it. This typically includes the removal or deactivation of systems in a vehicle that monitor the status of those environmental protection systems and give feedback about malfunctions, i.e. the OBD system of the vehicle.
Tampering Service	A service provided by a supplier or tamperer to make changes to an environmental protection system or ECU with the purpose to (partly) deactivate or bypass it. This typically includes the removal or deactivation of systems in a vehicle that monitor the status of those environmental protection systems and give feedback about malfunctions.
Vulnerability	A weakness that can be exploited by a threat, such as an attacker

List of Figures

List of Tables

1 Introduction

1.1 Background

With the EU emissions standards for vehicles becoming increasingly stringent, manufacturers have managed to introduce state-of-the-art environmental protection systems that have brought significant reductions to the actual emission levels. However, there is increasing evidence of illegal manipulation of environmental protection systems by vehicle owners and widespread usage is observed in the market [1, 2]. These manipulations, also known as tampering, can substantially affect the emissions of the tampered vehicles by bringing them back to uncontrolled or partially controlled conditions and therefore may constitute a significant threat to the efforts to regulate the emissions and improve air quality.

1.2 Objectives

The objective of task 3.4 of DIAS is to prove the ability of the whole DIAS system concept to harden against and detect tampering, which is to be tested in a hacking event.

1.3 Approach

- Organization of a successful ethical hacking event after completion of DIAS level 1.
- Supply the demonstrator platform with a developed tampering security solution (1st level) to ethical hackers.
- Allow all possible methods to try to attack the system and methods to erase detected tampering attempts.
- The attack methods, possible exploits, successful security defence and tampering detection, and possible detection erasure will be monitored and evaluated by the consortium.
- After completion of level 2, the hacking event will be repeated for the DIAS level 2 system.

1.4 Document structure

Chapter 1 presents the background, purpose, approach and structure of the current document and deviations from the DoW (Description of Work). Chapter 2 describes the methodology of the hackathon organized. Chapter 3 describes the results of the hackathon. Chapter 4 discusses the evaluation and recommendations. Finally, Chapter 5 presents the conclusions.

1.5 Deviations from original DoW

1.5.1 Description of work related to deliverable as given in DoW

In the DoW, Task 3.4 has the following description, as stated in *Grant Agreement-814951-DIAS*: Proof of ability of the whole DIAS system concept, the ability of the DIAS concept to harden against and detect tampering, is tested in a hacking event and evaluated by IT security specialists.

- The organisation of a successful ethical hacking event for real-world testing after completion of each of the two DIAS levels. Supply the demonstrator platform with a developed tampering security solution (1st level) to ethical hackers. After completion of level 2 repeat the hacking event for the 2nd level system. Allow all possible methods to try to breach the system and methods to erase detected tampering attempts. The latter is important for the possible use

of ‘tampering detection indicators’ at periodic inspections or roadside inspections. The hacking methods, possible breaches, successful security defence and tampering detection and possible detection erasure will be monitored. The outcome can be that still vulnerabilities are found and lead to recommendations for the development phases of the concept that follow after each of the two hacking events.

- Thorough DIAS concept evaluation. Provide the blueprint of the system concept to IT security experts for the assessment of the DIAS concept. The assessment addresses initial hardening against tampering (security), the ability to detect tampering and the resilience of the system concept to adapt to new future tampering attempts. Cases are developed for current as well as possible future tampering (from task 3.1) and used for fault injection to assess vulnerability and test detection of tampering.

Due to the pandemic, a physical hacking event was not possible. Instead, an online hackathon was organized. The drawback is that the prototype system and components with security upgrades could not be approached physically and attacked. However, such attacks take a lot of time and a few-day-event would only allow few real attacks. Instead, the online hackathon was designed to brainstorm freely about possible attacks and thus allows to obtain insight into the broadest range of possible attack vectors to determine whether the current level 1 countermeasures would be sufficient to counter these attacks.

1.5.2 Time deviations from original DoW

There has been a delay of 7 months since the delivery date scheduled in the Grant Agreement. This delay was already communicated to and agreed upon by the EC officer.

1.5.3 Content deviations from original DoW

The report describes an online hackathon instead of the intended live hacking event.

2 Method: online hackathon (hack-a-truck)

2.1 Objectives and scope

- Assess DIAS concept level 1 after completion (and later level 2) for possible remaining vulnerabilities that allow deactivation of the EPS
- Scope: in-vehicular security and diagnostic system.
- Attack surface: The entire demonstration vehicle with developed countermeasures.

2.2 Approach

After completion of level 1 and implementation of the countermeasures, perform an external open assessment by independent experts to find possible remaining weaknesses by means of hosting creative working sessions where the whole vehicle and sub-systems may be attacked. Organize a hackathon to facilitate this.

2.3 Mode of the event

Initially, a live hacking event was foreseen. But due to the Covid-19 pandemic and the travel restrictions between countries hosting a live event proved to be problematic. Therefore, it was decided to organize an online event instead. This way it would be possible to invite independent experts and use their creativity and expertise to work in teams in cooperation mode on finding possible new attack vectors and develop exploits to tamper the EPS of the demonstration truck. The difference with a live event is the lack of a physical platform that can be used to find attack vectors, try and develop exploits. Also, it cannot be determined whether or not the attacks are successful. A drawback of a live event on the other hand is that it is too short in time because it became known during the initial course of the DIAS project that finding a successful attack vector and developing a working exploit actually can take years of lead time. An online hackathon could enable the gathering of new and creative concepts for attacking an EPS. Instead of trying the attacks on a physical platform in the live event, the virtual concepts should be evaluated afterwards to determine whether or not the attack could be successful.

To attract and recruit enthusiastic, creative and skilled people the event was organized as a team contest, a challenge with technical trainings at the start of the event, working sessions for finding attack vectors and developing virtual exploits and a tampering plan and with prizes to be awarded at the end for the team that developed the best tampering concept. TNO designed a unique online event where hacking enthusiasts and experienced hackers work together in groups for two days on developing new tampering concepts. This all while being witnessed by experts of the consortium to monitor the developments made by each team.

> "…Your challenge is to find an attack vector or attack vectors, exploiting it to deactivate or remove an environmental protection system of a truck and develop a tampering device or service with a goal to commercialize the tampering product on the EU market…"

Hack-a-Truck was a two-day hackathon with one open day in between. It was hosted with a studio live stream via Microsoft TEAMS. 5 teams were formed, each consisting of 4 hacking enthusiasts (mainly students), 1 experienced hacker and 1 group mentor from the DIAS consortium.

Various information was supplied to the groups. At the beginning of the event, an introduction presentation of DIAS was given. During the first day, three trainings were given on the topics of truck aftertreatment technologies, tampering techniques available on the market and anti-tampering measures.

Teams had to brainstorm new tampering ideas, work on a technical plan and a business plan in working sessions, and present these plans to a jury. The mentor was there to guide them in this process, answer (simple) questions as well as monitor and document the process. A pool of experts was available to answer in-depth questions from the teams throughout the working sessions.

The final presentations with the tampering plans of each group were given at the end of the second day and were ranked by a jury. The teams got awarded based on the jury decision in the award ceremony afterwards.

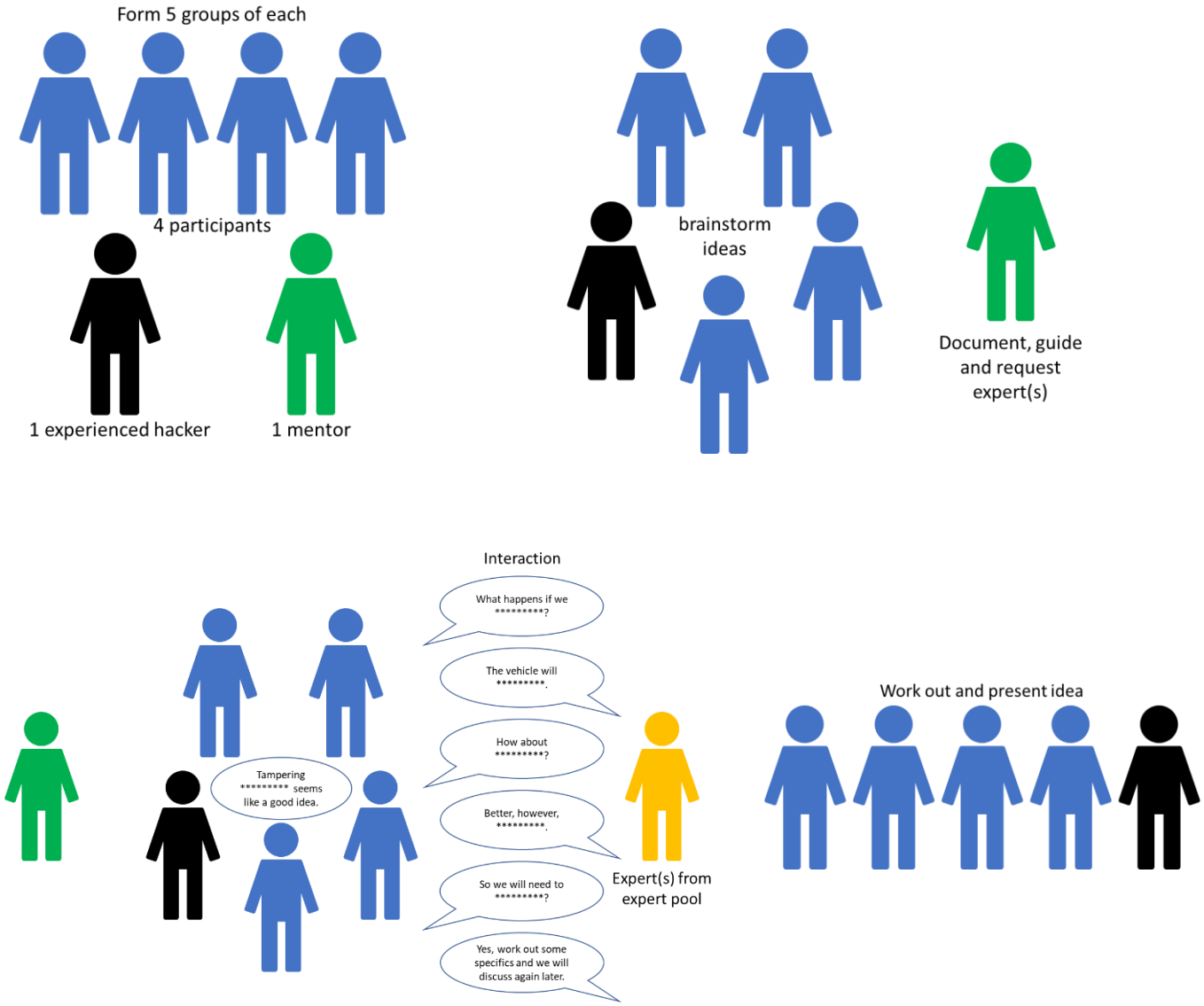

Figure 1: Visual representation of the online hackathon concept with brainstorm and iterative working sessions

A storyboard was made to organize and plan the event in terms of timing, tasks, facilities and personnel needed to run the event smoothly.

Table 2: Snapshot of a part of the storyboard that was made to plan the event

Date	Time		Event	Description	Responsible	All necessary attendee	What is in screen?	Participant local	Actions	Document/presentation
	07:00	'00 - '15	Free	Each participant needs to get access to the sharepoint. Groups separated. Perhaps other way is better.		Host presents all transitions				
		'15 - '30								
		'30 - '45								
		'45 - '00								
	08:00	'00 - '15	Studio startup		Director	LP team, Ann, Akshay		Main feed	Director starts up live studio feed and creates 7 TEAMS breakout rooms.	
		'15 - '30								
		'30 - '45	Welcome and coffee Mentimeter to energise people	Small talk between host and participants	Host, TNO	Akshay	Host and Mentimeter	Main feed	TNO is responsible to let in the attendees from the lobby TNO checks attendance of applicants	https://www.mentimeter.com/app/folder/1082036
		'45 - '00								
	09:00	'00 - '15	Day start	Day start by host (practical considerations and agenda)	Host, TNO	Akshay, all team members	Host	Main feed		Presentation: 00.Agenda, introduction and outline of the problem
		'15 - '30	Introduction	Presentation from LAT/Commission (Introduction)	LAT	Dimitris, all team members	Video LAT	Main feed	Check main room chat for possible questions	Video LAT: DIAS - Hackathon - Introduction - LAT-Kontses.mp4
		'30 - '45	Playing rules and group forming	Host explains the schedule, the playing rules and announces the groups. Participants can ask their questions about the event.	Host, TNO	Akshay, all team members, including mentors	Host and powerpoint	Main feed	Host explains that the groups will be placed in their specific break-out room and that after 45 minutes, they will be automatically moved back to the main room.	Playing rules presentation: 0. DIAS-Hackaton_playing_rules_Host
		'45 - '00								
	10:00	'00 - '15	Group-members getting to know eachother	Participants are placed in breakout rooms, together with hacker and guide. Group members introduce themselve to the team and exchange contact information (which?) and skills. Think of a name for the group and group pitch.	Mentor	All team members, including mentors	Hack-a-Truck Screensaver	Breakout room	Director places participants in correct TEAMS breakout rooms. Mentor make whatsapp groups for each group (or similar communication means) - TEAMS chat can also be used.	
		'15 - '30								
		'30 - '45								
		'45 - '00	Group pitches	Groups present themselves to everyone / group pitch. Each group has 3 minutes. Host guards the time.	Host, TNO	All team members, including mentors	Presenters	Main feed	Director places participants back in main TEAMS meeting.	
	11:00	'00 - '15	Training 1: Ford	Ford gives a presentation about their heavy-duty truck and aftertreatment system.	Ford	Dincer	Video Ford	Main feed	Check main room chat for possible questions	Ford training video: 1. DIAS-Hackaton training1_Ford_v2_Voiceover.pptx
		'15 - '30								
		'30 - '45	Q&A training 1	Participants can ask their questions about the training.	Ford	Experts Ford	Powerpoint presentation and presenter	Main feed	Answer and discuss questions Dincer to check and answer the questions.	Ford presentation: 1. DIAS-Hackaton training1_Ford_v2
		'45 - '00								
	12:00	'00 - '15	Lunch break				Screensaver			
		'15 - '30								
		'30 - '45								
		'45 - '00								
	13:00	'00 - '15	Training 2: TNO	TNO gives a presentation on current tampering; emulators, temperature sensors, ECU flashing etc.	TNO	Joep, Experts TNO	Video TNO	Main feed	Check main room chat for possible questions	TNO training video: 2. DIAS-Hackaton training2_TNO.pptx 2. DIAS - Hackaton - TNO Training.mp4 2. DIAS - Hackaton - TNO Training.mp3
		'15 - '30								
		'30 - '45								
		'45 - '00								
	14:00	'00 - '15	Q&A training 2	Participants can ask their questions about the training.	TNO	Experts TNO	Powerpoint presentation and presenter	Main feed	Answer and discuss questions TNO experts to check and answer questions	TNO presentation: 2. DIAS-Hackaton training2_TNO
		'15 - '30								
19 May		'30 - '45	Group Brainstorming	Groups will start brainstorming ideas on how to tamper with the EPS of the truck. In parallel, host visits each group to chat about their brainstorming.	Mentor	Host	Screensaver	Breakout rooms	Director places participants in correct TEAMS breakout rooms. Director places participants back in main TEAMS meeting.	
		'45 - '00								
	15:00	'00 - '15								
		'15 - '30								
		'30 - '45								
		'45 - '00								
	16:00	'00 - '15	Training 3: Bosch	Bosch gives a presentation on ECU and security countermeasures	Bosch	Thomas K./Björn/Andreas	Presentation + presenter	Main feed	Check main room chat for possible questions	Bosch presentation: 3. DIAS-Hackaton training3_Bosch

2.4 Roles, role description and recruitment

2.4.1 Roles and role description

According to the overall set-up as described above, the following roles were foreseen for the event:

- 20 selected participants of various relevant technical backgrounds
- 5 hackers of various relevant technical backgrounds
- 5 mentors
- Pool of experts
- Presenters for introduction and 3 workshops
- 1 host
- 5 jury members
- Coordinating team
- Studio personnel
- Participants
  - The participants work in a team together with a hacker and actively contribute to the process of finding new attack vectors, and developing an exploit to create a new tampering concept, presenting the concept as a technical business plan, describing how the tampering works, what resources are needed to make the exploit and develop a tampering product to commercialize it on the EU market.

- Hackers
  - The hackers work together with the team of participants on finding new attack vectors, and developing an exploit to create a new tampering concept, presenting the concept as a technical business plan, describing how the tampering works, what resources are needed to make the exploit and develop a tampering product to commercialize it on the EU market.

- Mentors
  - The mentors guide the Teams and answer (simple) questions.
  - Monitor and document team progress.
  - Forward team questions to the pool of experts and receive answers.
  - Stimulate when there is a lock-in.
  - Assist with practical issues.
  - Report issues to the coordinators.

- Pool of experts
  - The experts have extensive knowledge and understanding of the EPS of the demonstration truck, tampering techniques available on the market and/or anti-tampering countermeasures.
  - Provide answers to questions from Teams and additional information during the group working sessions.
  - One chairman divides the incoming questions and is in direct contact with the studio.

- Host
  - The host leads the whole event. He opens, narrates and closes each day.
  - Presents introduction, agenda, playing rules
  - Leads Q&A at the end of each training; collect and answer questions.
  - Provides practical information regarding the facilities.

- Small talk in between.

- Coordinating team
  - The coordinators make sure everything runs smooth and as planned.
  - Keep everyone on track in and outside the studio and assure everyone is without (connectivity) issues.
  - Solve unforeseen practical issues on the spot.

- Studio personal
  - Studio personal controls the studio equipment and the Microsoft TEAMS stream.
  - Perform TEAMS logistics such as making hacking teams, teleporting experts to teams, etc.

- Jury
  - The jury members listen to final presentations, judge and rank the tampering plans.
  - One jury member awards the groups winning third, second and first place.

2.4.2 Participant recruitment

A total of 20 participants had to be recruited for the event. Since each group was assisted by a white-hat hacker, the preference went for students and recently graduated hacking enthusiasts.

Event attendance was not open but 'invite only'.

Minimum requirements for participants:
- You are currently following or you have completed one of the following bachelor studies:
  - Mechanical engineering
  - Automotive engineering
  - Computer science
  - Electrical engineering
- You have an interest in and preferably experience with exhaust gas aftertreatment systems, (automotive) electronics, and/or (automotive) communication and security protocols.
- Your communication skills in English are excellent.
- You should bring expertise and skills to your team during the hack-a-truck.
- You have a computer with Microsoft TEAMS available

2.4.3 Hacker recruitment

A total of 5 white hat hackers was recruited. Recruitment of actual tamperers such as DIMsport was discussed by the consortium and it was decided not to invite tamperers as there was a risk that they will retrieve the information of the hackathon and use the information for their business to develop new tampering while providing little to no input. For this event hackers with a background in (automotive) electronics and security were recruited from UMFST in Romania, the Cyber Security department of TNO in the Netherlands, Wingmate in Australia and ERNW in Germany.

For help with the recruitment of white-hat hackers with the right experience for the job, ERNW was contracted. ERNW is an independent IT Security service provider based in Heidelberg, Germany who hosted the bug hunting event 'Car Manufacturer meets Security Community' and provided their services and network for the event to source the hackers and facilitated the drafting of an NDA between OEM and hackers.

2.4.4 Participant sourcing

For the recruitment of the participants, consortium partners reached out to various universities and colleges in their member states which offer the relevant studies as mentioned in the application requirements (Table 3). The faculty leaders were asked to distribute the flyers.

Table 3: Sources of participants (universities and companies)

Students	Hackers	Experts
TU Delft, The Netherlands TU Eindhoven, The Netherlands Han hogeschool, The Netherlands Hogeschool, Rotterdam, The Netherlands VU Brussel, Belgium COSIC, Leuven, Belgium UMFST, Romania RWTH (FEV), Germany Aristotle University of Thessaloniki, Greece Democritus University of Thrace, Greece University of Thessaly, Greece Faculty Hochschule Esslingen, Germany Technical University of Cluj-Napoca, Romania	ERNW TNO Cyber Security UMFST Wingmate	ERNW Consortium members (Ford Otosan, Bosch, FEV and TNO)

2.4.5 Recruitment website and flyer

For the recruitment of participants, a digital flyer was made by LAT. The flyer was distributed as well as posted online on the DIAS project website. The flyer served to recruit participants and inform them about the contents, timing and location of the event. On the website, there was a direct link to the application website. The application process was done via the recruitment department of TNO. This department is normally used for job applications and has a lot of experience with handling personal information securely. Below is an image of the flyer.

Figure 2:The flyer used for the recruitment process

The information text of the flyer:
Malicious tampering of environmental protection systems turns very clean vehicles into heavy polluters. In the European project DIAS, countermeasures are developed to harden vehicles against the malicious tampering and this needs to be thoroughly tested. That is why we invite creative, ingenious people to hunt for bugs. A hackathon is organized in which you will cooperate in teams containing people with various skills to work out a virtual plan, from finding a bug to making a business out of it.

Hack-a-truck is an online automotive hackathon which lasts two days in total. To get you up to speed, three trainings will be hosted by experts from industry-leading companies and knowledge institutes, such as Ford, Bosch and TNO. The experts will inform you 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. In between these trainings we invite you to some action: you will be assigned to a group of people with complementary skills and you will work together on finding bugs in a defined truck set-up. Together, you'll have to work out a business plan as if you were to commercially sell your bug as tampering on the internet. Other groups are your competition. Beat them and get rewarded.

- *Three trainings, hosted by experts from industry-leading companies and knowledge institutes.*
- *You will be assigned to form a group of 5 selected participants with complementary skills, 1 mentor and 1 professional hacker. You will work together on finding bugs in a defined truck set-up. Together, you'll have to work out a technical plan and a business plan as if you were to find a bug and commercially sell your bug as a tampering 'product' on the internet.*
- *The winning team receives 2000 €, the second team 1000 €, the third team 500 € (to be divided between the selected participants only).*
- *A certificate of being a laureate to the DIAS hack-a-truck 2021.*
- *An exclusive goodie package before the start of the event.*

The Hack-a-Truck is planned for week 20 (17-21 of May). Final dates will be announced soon.

To apply for this event, please enter your motivation letter and CV via the application form below before April 08th, 2021.

The selection procedure will be finished before the end of April 2021

If you are selected, you will be asked to sign an NDA.

For additional information and updates visit our website or send an e-mail to info(at)dias-project.com.

The selection procedure was finished before the end of April 2021. The hack-a-truck event was held in week 20 of 2021 from the 19th until the 21st of May.

2.4.6 Participant selection process and team formation

Via the application tool on the DIAS project website, we received 36 applications in total. Every candidate had provided a cv and most of them attached a motivational letter as well. The applications were used to make a ranking based on the applicants:

- Relevant skills, experience and expertise from education, degree, faculty, interest and work.
- Motivation and enthusiasm as described in the application letter

A prerequisite from the consortium was that candidates from competing companies and professional tamperers were to be excluded from the event. In the end, 20 candidates were selected and invited to the event. Group formation was done by the coordinating team, to spread the skills and expertise over the groups and balancing them as much as possible. A preliminary group formation was made in advance of the event, while the final one was decided at the start of the event. Fortunately, only one person was absent and group formation could remain as envisaged.

2.5 Hosting and facilities

The hackathon was hosted on the 19th and 21st of May. Due to the pandemic, the event took place in a digital environment using a studio set up at TNO in the Netherlands. A stream was hosted via a Microsoft TEAMS meeting, of which the link was shared with the entire party in advance. There was a host present during the entire event, specifically to greet the guests as they joined, kick off the event each day, announce transitions, guide the process and wrap it all up at the end of each day. Behind the scenes was a crew of studio personal working on sound and visuals of the studio, making sure online presenters were visible, and moving participants to and from separate group break-out rooms. Behind the scenes was also the coordinators making sure all participants were present, guiding the host and the studio according to the storyboard and keeping an eye on the timing, providing the host with answers to questions from the participants, coordinate questions directed at the pool of experts and making sure the correct expert went to the group to answer, and of course fix unexpected problems. Below are some pictures of the stream and the studio technicians.

Figure 3: Pictures of the stream and the studio technicians

To prepare for the event, there was a dress rehearsal in the studio on the 11th of May. Consortium members were invited to participate, the host could practice as well as the studio. Forming break-out rooms and assigning participants was tested.

SharePoint was used to provide a platform and tools for the participants. There was a general SharePoint in advance of the event, which contained general information on the DIAS project and preparation. On the first day of the hackathon, each group was given access to their own SharePoint. Here template PowerPoints were provided with explanations and room for brainstorming, working out tampering attacks and making a final presentation of the tampering business plan.

2.6 Information provided

Preparatory information was provided to the participants in advance of the event via a SharePoint site.Information needed to be provided to inform the participants about the scope, working principles of the EPS, current tampering and information of the prototype vehicle necessary for finding potential weaknesses and information to be provided during group sessions.

Three types of information are distinguished:

1. Documentation, available at the beginning.
2. Introduction objectives, playing rules and trainings (Ford Otosan, TNO and Bosch).
3. Pool of experts answers questions and provide information during group sessions.

To ensure that the confidential information on anti-tampering measures and possible vulnerabilities does not leak to the outside world, an NDA was drafted. With the confidential information coming from the presentations and the answers from the pool of experts. Both the participants and the white hat hackers have signed the NDA in advance of the event.

2.6.1 Information provided in advance

- References to working principles of EPS and examples of tampering
  - https://en.wikipedia.org/wiki/Diesel_exhaust
  - https://en.wikipedia.org/wiki/Selective_catalytic_reduction
  - https://en.wikipedia.org/wiki/Diesel_exhaust_fluid
  - https://en.wikipedia.org/wiki/Diesel_particulate_filter
  - https://en.wikipedia.org/wiki/CAN_bus
  - https://en.wikipedia.org/wiki/On-board_diagnostics
  - https://en.wikipedia.org/wiki/Unified_Diagnostic_Services
  - https://en.wikipedia.org/wiki/Keyword_Protocol_2000
- Supported ECU's trucks
  - https://www.dimsport.it/en/applications-list/ecu/truck/
  - https://www.alientech-tools.com/k-tag/
  - https://ecutools.eu/publications/ktag-update-16122020/
- Examples for passenger cars:
  - https://www.autotuner-tool.com/en/bosch-md1-mg1
  - https://www.youtube.com/watch?v=kcVvqOSODes
- Pictures and a video of the demonstrator vehicle. AT box, sensors, actuators, an overview of the truck, workshop tester.

- Public reports D3.1 and D3.2
- Final presentation template in DIAS style
- Goodies

2.6.2 Trainings and presentations

The event was started by a welcome and outline of the problem of the tampering as well as an introduction to the DIAS project. Afterwards, the host explained the playing rules of the hackathon and the use of the facilities. Three trainings were given, hosted by experts from industry-leading companies and knowledge institutes: Ford Otosan, TNO and Bosch. After each training was sufficient time for questions and answers. Ford presented the Ford vehicle and aftertreatment system. TNO presented current tampering methods available on the market, and Bosch presented ECU and security countermeasures and communication.

2.6.3 Additional information and answers during the event

During the working sessions, the mentor of the group was there to answer simple questions. Additionally, a pool of experts was available for Q&A, judging ideas and providing further information. The questions to the pool of experts were managed via the mentors. Physical access to the truck was not possible in an online, digital setting. Instead, a pool of experts was available to answer technical questions and provide feedback on hacking attempts proposed by the groups.

The pool of experts was realized via a separate break-out room in the TEAMS stream. All of the experts were on standby in this meeting room, awaiting questions from the groups. The chairman of the expert pool received the questions and discussed within the pool what the answer was and who could best provide this answer to the group. The chairman was present in the studio, so once the decision was made on which experts were answering the question the chairman could directly coordinate the transition from one break-out room to another. As soon as the experts were finished with their questions, they were pulled back to the pool.

2.7 Guiding and monitoring the process

Each group had a mentor assigned, who was familiar with the project and the objectives of the hackathon. The mentor was responsible for guiding the group in their process and helping them to get answers to their questions efficiently since there was limited time available. At the same time, the mentor had the task of documenting the process. An important part of the hackathon was getting a look into the hacking process and the hacker mindset. Each mentor was provided with a mentor sheet to document all the important developments during the working sessions of the event. Especially the discussions between group members and visiting experts were extremely valuable in grasping the hacker mindset.

2.8 Final presentation and jury grading

Groups were asked to transform their findings into a final presentation, which was presented at the end of the second program day. A DIAS style PowerPoint template was provided so that groups could focus on the content and not have to spend time on the format. Each presentation was followed by a short round of questions, and after all of the presentations, it was time for the jury to discuss the grading of the groups. It was an independent jury consisting of experienced members who were not directly involved in the execution of the hackathon, although most were involved within the DIAS

project. Participants were informed in advance of the grading criteria and jury members were provided with a grading sheet. The criteria were:

The technical plan (40 points total):

a. Tampering success (equal points for SCR AdBlue off and DPF) meaning deactivation or removal of an EPS is possible and remains undetected by on-board systems **20**
b. Staying undetected at roadside inspection by a technical police squad. Think of (visible) signs of tampering a technical police squad could detect. Currently, a police squad is typically equipped with a generic scan tool, AdBlue quality tester (refractometer), multimeter, flashlight. **10**
c. Product complexity (vs. simplicity) and robustness, ease of installation/removal: Simple, robust designs which are easy to install and pose no risk for damage to the vehicle receive most points **10**

The business plan (12 points total):

d. Market potential: costs, added 'value', reach **10**

Bonus points:

e. Creative sketch e.g. of the product, brand name and label **2**

The technical plan is the most important result in this hackathon, however, the business plan is an essential part of ensuring the feasibility of the proposed technical plan with respect to time and resources.

3 Results

During the online hack-a-truck event all five teams made a tampering plan and presented the tampering plan at the end of the event to the mentors, experts and the jury. The team mentors administered the working process and important details of the process of making the tampering plans. The tampering plans were evaluated and ranked by a jury based on five important criteria for successful tampering (tampering success/impact, detection on-board, detection at inspection, complexity and costs and market potential, see Chapter 2.8 and Annex B: 'Playing rules' and information for the Hack-a-truck event 19 and 21 May 2021).

The five plans received 29 to 49 points out of the maximum of 52 from the jury, see Table 4.

Table 4: Teams, points and ranking of the tampering plans by the jury.

Team #	Team name	Success /impact (20)	Detection (10)	Cost and complexity (10)	Market potential (10)	Creative sketch/design (2)	Points (max. 52)	Rank
Team 1	Kronos	16	7	8	7	0	38	4
Team 2	CAN-U-BREAK-IT	9	5	5	7	1	29	5
Team 3	Tinker thunders	16	7	8	7	1	39	3
Team 4	Nikites	19	8	9	10	2	48	2
Team 5	The Emulators	20	8	9	10	2	49	1

The final plans contained six different types of attack vectors. New attack vectors were found and also new methods were proposed for making an exploit. The obtained information is confidential and has been shared within the DIAS Consortium. The tampering plans contain theoretical virtual attacks. This means that it was not physically demonstrated if an exploit would work, i.e. if an EPS could be deactivated or removed while remaining undetected.

Two teams proposed plans for tampering with a limited impact, i.e. only a partial shutdown of AdBlue dosing while in one case the MIL is activated and DTC are set, additionally detection is easy because of hardware being visible at inspections. One team proposed tampering for DPF removal of heavy commercial vehicles for which market potential is considered low. Two teams proposed new alternative attack vectors and also new advanced approaches for developing exploits.

4 Evaluation and recommendations

In this chapter, the results from the hackathon are evaluated as well as the event itself. Additionally, recommendations are made for future hackathon events.

4.1 Evaluation of results

After the hacking event, the attacks were evaluated by the Consortium with regard to:

- the possible impact on tailpipe emissions,
- the working principles of the exploit,
- detection on-board and by inspection,
- market potential,

and thus if a tampering plan poses a potential threat.

As mentioned previously, two teams proposed plans with limited impact and one team proposed DPF removal which has low market potential. Two teams proposed new alternative attack vectors and also new advanced approaches for developing exploits which however are considered complex and costly. For the new attack vectors, further assessment is recommended and therefore additional penetration tests will be performed in WP4.

Although some teams received high points on the jury criteria, not one high-risk tampering solution was developed and proposed. The scores of the judges were provided in a relative way and are primarily used to create a ranking order of the presented ideas of the groups. High-risk tampering is considered by the Consortium to have a high impact on emissions, have low costs and complexity, is hard to detect by on-board systems and at technical inspections, and has high market potential (demand).

4.2 Evaluation of the event

At the end of the event, there was a Mentimeter quiz where participants and hackers were asked for their feedback. The event was rated between 7 and 8 out of 10 by 22 persons. When asked if they would attend a second DIAS hackathon 15 replied ‘yes’, 9 replied ‘maybe’ and 0 replied ‘no’. Despite the pandemic excluding the possibility of a live setting, there were several valuable outcomes. The teams were well balanced and delivered useful results. Each of the five groups presented a (slightly) different approach to tampering with the EPS. New attack vectors were identified and also new methods were proposed for making an exploit. There was a good interaction between the groups and the experts during the working sessions. Teams asked the experts in-depth questions on various topics and even inspired deep discussions with the experts on system working principles and possible vulnerabilities. The thinking process of the groups was observed and extensively documented by the group mentors. The lack of physical hacking sped up the hacking process significantly. However, the actual success of the proposed hacking solutions remains to be confirmed by the DIAS project at a later stage. There was a mix of automotive and IT expertise among participants and hackers, although a point for improvement was the scarcity of participants and hackers with dedicated automotive hacking experience. The jury consisted of experienced members of the consortium. Time after the event was foreseen to evaluate the tampering plans with attack vectors by the Consortium experts. The total time during the event, two days of the program with one day in between was somewhat restricted. This resulted in groups having to work hard and efficiently on their tampering plans and presentations. Looking at the high scoring results of all the groups indicates there was sufficient time

to work on a solid plan. That being said, the day in between offered a moment for clear thinking and extra time for carrying out work. Also, the short amount of time may have caused teams to choose the options that were least time consuming to understand fully and work out during the event. Performing the event in an online fashion also eliminated the need for travel, except of course for everyone available at the studio. This resulted in decreased travel costs as well as decreased CO_2 emissions. Overall the hackathon was successful.

With the experience gained from this event, various recommendations for future hacking events can be made. In short:

- An online setting speeds up the hacking process but requires hacking success to be evaluated by members of the project at a later stage.
- Quick interaction between groups and experts is essential in an online and time-restricted setting.
- Question-driven discussions between participants/hackers and experts are remarkably useful for finding vulnerabilities and grasping the hacking mindset and approach.
- A program free day (or section) within the event stimulates participants positively in their process.
- It is important to ensure that there is sufficient time and information for the participants to understand the main working principles of the EPS and the existing and new security features for detection or prevention of tampering of the EPS. Sufficient time and information are also needed to facilitate the search for possible new attack vectors and to work out a plan for an exploit for the purpose of tampering with the EPS.
- Acquiring dedicated automotive hackers requires hard to come by connections, an event-specific NDA and sufficient time to recruit.
- Jury grading on the technical feasibility of presented ideas requires sufficient time (at least 15 minutes per idea) and specialized experts for evaluating and judging the results.

5 Conclusions

Detailed results of the first hacking event are confidential since they contain valuable information on new anti-tampering measures and potential vulnerabilities. Consequently, the results and conclusions documented in this public report are limited.

Five teams were formed with independent hackers and students and (recently) graduated hacking enthusiasts. Each team performed brainstorming and working sessions to work out tampering plans that had to contain details of the approach with the attack vector, the exploit and a simple business plan to show impact and market potential. At the end of the event, the tampering plans were evaluated and ranked by a jury based on five criteria for successful tampering to be able to award the winning teams (3 prizes were awarded for 1st, 2nd and 3rd prize). The five plans received 29 to 49 points of the maximum of 52 from the jury, see Table 1. Team 5, 'the Emulators' won the event by a small margin over team 4 the 'Nikites'. The obtained tampering plans are confidential and shared within the DIAS consortium.

After the hacking event, the attacks were evaluated by TNO and experts of the DIAS consortium with regard to the possible impact on tailpipe emissions, the working principles of the exploit, detection on-board and by inspection and market potential, and thus if a tampering plan poses a potential threat. The five tampering plans contain six different types of attack vectors. No high-risk tampering solution was developed and proposed, i.e. tampering with high impact, low costs and complexity and hard to detect by on-board systems or at technical inspections and with high market potential. The hacking event was highly effective in gaining insight into new and undiscovered attack vectors, although the limited amount of time and information available might have influenced teams to not fully explore the more complex parts of the EPS to search for potential vulnerabilities. The combination of the hacking event and in-depth penetration tests that are performed in the DIAS project however ensures that the concept is tested for known attacks and that new ones can be discovered in a very efficient way.

Three of the tampering methods that were developed could only have a low impact, for instance, a small reduction of AdBlue consumption. One tampering had limited market potential. Three of the tamperings proposed new advanced approaches which were considered complex, costly and detectable. Tampering plans also contained new alternative attack vectors. For these new attack vectors, further assessment is recommended and therefore additional penetration tests and an update of the Threat Analysis and Risk Assessment (TARA) will be performed in WP4.

The results of the event have shown that the level 1 countermeasures made it harder to tamper, lead to tampering with lower impact on emissions, with lower attractiveness for the market, higher complexity or tampering that could be detected by OBD or roadside or periodic inspections.

Annex A: Practical information Hack-a-truck

Welcome!

We are happy to have you onboard the hack-a-truck event!

You are selected to work in a team as a creative expert to find possible attack vectors of environmental protection systems onboard a modern truck.

Q. When is Hack-a-truck?

A. 19 and 21 May 2021, the 19th starting at 8:30 CEST (Central European Summer Time). Be sure to be in time to solve possible start-up issues due to which you could miss the start of the event.

Q. Where is hack-a truck?

A. Hack-a-truck is an online event that largely takes place **in the TEAMS app**.

You will receive a link to the event per email after you have signed the NDA's.

Further details such as a link to a SharePoint to work in with your team will be given at the beginning of the event after teams have been formed.

When entering the TEAMS meeting, announce yourself by typing your name in the chat so that we know who you are!

Q. What do I need to do to prepare myself?

A. Return the 2 signed NDA's before noon (12 o'clock daytime) on Monday 17 May to:

quinn.vroom@tno.nl and cc: info@dias-project.com

A. Please make sure that the TEAMS meeting runs smoothly (browser or app) before the event.

A. Have a look at the information already available on the SharePoint: Hack-a-truck SharePoint

With your email address provided to us, you can obtain access to the SharePoint, but only after you have returned the signed NDA's.

The SharePoint contains the invitation, content material: of the prototype vehicle, technical information about the working principles of the environmental protection systems, reports of the DIAS project about tampering, the market of tampering, testing of tampering, high level working principles and guidelines for detecting or preventing tampering.

Q. If I have any questions beforehand, where can I ask them?

A. You can send an email to TNO who is the organizer of the event. The contact person is: 'email TNO contact person'

Annex B: 'Playing rules' and information for the Hack-a-truck event 19 and 21 May 2021

The problem

Malicious vehicle owners are tampering environmental protection systems of their vehicles. They are flouting regulations and pollution is increasing. Tampering devices and services are offered via tuning workshops, websites, eBay, fora that exploit vulnerabilities of current vehicles to deactivate or remove (parts of) the environmental protection systems.

Help the DIAS project by testing the new and improved security features that are employed on a demonstrator truck a Ford Fmax tractor.

Figure 4:Ford F-Max truck used to tesu the new and improved security features

Your challenge

Your challenge is to find an attack vector or attack vectors, exploiting it to deactivate or remove an environmental protection system of a truck and develop a tampering device or service to commercialize the tampering product on the EU market.

Examples of Environmental protection systems of trucks in the EU which are targeted for tampering are:

AdBlue/Diesel Exhaust Fluid dosing as part of the SCR system. Shutting down this dosing of fluid or reducing it. The motivation for a vehicle or fleet owner is avoiding costs for consumables (called AdBlue or DEF) and/or avoid repair of the SCR system or components of this system and downtime of the tuck resulting from malfunctions of the system. AdBlue savings are up to (1000 EUR / y). Complete shut off of AdBlue dosing increases harmful nitrogen oxides emissions with at least a factor of 10!

DPF: Diesel Particle Filter removal. Most often for passenger cars, not for trucks, but possibly for construction equipment and agricultural tractors. This tampering results in a very large increase in harmful particle emissions. Removal prevents the replacement of the filter element in the case it breaks down or maintenance such as cleaning the filter. Also, the reduction of the fuel consumption of a few % is mentioned.

NOx (Nitrogen oxides) sensor tampering. To avoid replacement of the sensor. 150 EUR/pc

SCR: Selective Catalytic Reduction catalyst removal (a large increase of harmful Nitrogen oxides emissions). Motivations are not very clear. A reduction of fuel consumption is mentioned, or performance tuning or increasing the sound level.

EGR Off. Most often for passenger cars. Offered for trucks in ECU tunes/reflashes. To avoid costs for repair of engine parts due to fouling.

More information on how environmental protection systems work, what are the motivations and working principles to tamper the systems will be presented in the trainings, as well as the newest new countermeasures. Information can also be found in SharePoint. You are also free to search other information sources for tampering practices.

Work in Teams

Five teams will be formed before the event, with skills and expertise equally as good as possible divided over the teams. You will get to know your team members before you start to work together during the online hack-a-truck event. Each team consists of 3 or 4 students and one expert white-hat hacker. Each team is assisted by a mentor who helps with practical stuff, who is monitoring and administrating the teamwork and who can forward attack proposals to a team of experts. And that is what we are interested in, to see what creative technical ideas you will come up with, to find attack vectors that can be exploited to make tampering business out of it.

Trainings

You will attend three technical trainings and an introduction to the problem and receive more information about your challenge to get you up to speed. After the trainings there is time for Q&A so you can acquire valuable new information already here.

Working sessions

The action happens in a sequence of working sessions where you will work together with your TEAM to first brainstorm finding attack vectors that can be exploited to make a commercial tampering product or service.

Then you'll be asked to work out the most promising attack vectors from the brainstorm in a technical plan and a business plan. During the working sessions, you can reach out to a team of experts to gain information and test if the proposed attacks will work or not.

A PowerPoint template will be provided on a SharePoint where each TEAM can work out its plans.

This is how the TEAM working sessions look like:

1. **Brainstorms**: 2 parts, one on day 1 and one on day 2. Think of all possible attack vectors/bugs/vulnerabilities which can be exploited to deactivate or remove an environmental protection system of a truck. A template will be provided where each team can note its ideas. Select the most promising attack vector(s).

2. **Working sessions: make a tampering plan**

a. **Technical plan:** Attack the system, using the selected attack vector(s). Perform virtual attack(s), working out idea(s) in a technical plan: focus on making the exploit.

   You will propose attacks to a team of experts and you can ask questions via your TEAM mentor. The experts will provide you with the result of the attack or with further information that would be obtained as a result of your attack. If the first attack is successful you might meet new challenges…

   Work out the attack(s) in detail. Step-by-step, propose all the things that you think are needed to perform the attack to produce the exploit: tools, software, material, skills, people, processes needed.

b. **Simple business plan.** Develop a tampering business plan to commercialize the exploit: Using the technical plan as a basis, work out a simple business plan, estimating production costs describing what is needed for producing a tampering product or service. A template will be provided where each team can work out its plans.

A tampering business manager also needs to pay the monthly bills, so also add some profit to the costs. Market the product or service: define your claim, what will the tampering be able to do and why is it attractive taking account of the current market demand with the known tampering motivations.

What if you didn't find a bug? Well then, DIAS succeeded in developing very effective countermeasures and you will have big problems with your investor. Work out a plan to develop a bogus device hoping the investor wouldn't find out as he will be furious about it.

Presentation of the plan

Each team makes a presentation composed of the technical plan and the business plan based on the template that was used for the brainstorm and during the working sessions.

Send the presentations before 16:00 to: info@dias-project.com. Presentations received later than 16:00 will not be considered by the jury for the prize.

The jury will rank the tampering plans based on the technical plan and the simple business plan, see below for points.
Each team has 15 minutes to present the plan. The jury may ask one or two questions for clarification for 3 minutes so there is a total of 18 minutes for each team.

The whole tampering plan should contain the **technical plan** and the **simple business plan**:

- **Technical plan (main part), see template:**
  - **How the exploit works.** Describe the attack vector, vulnerability, logic, tools, material, software, personnel, facilities needed.
- **Simple business plan, see template:**
  - What market demand is satisfied? Who is the customer? What is the added value? Define your claim to the market.
  - Simple cost estimate: production + profit?
  - How do you reach out to as many potential customers as possible?
  - Creative sketch of the product, brand label

Jury criteria for judging tampering plans

DIAS aims to make tampering tough and expensive (prevention) and aims to detect tampering. Therefore the most important criteria for judging the plans are related to complexity/robustness, price and risk of detection.

Main criteria for ranking the bug-to-business plans. For each criterion, points can be awarded up to a total of 50 + 2 bonus points for a creative sketch of the product.

The technical plan (main part):

a. Tampering success (equal points for SCR AdBlue off and DPF) meaning deactivation or removal of an EPS is possible and remains undetected by on-board systems **20**
b. Staying undetected at roadside inspection by a technical police squad. Think of (visible) signs of tampering a technical police squad could detect. Currently, a police squad is typically equipped with a universal OBD tester, AdBlue quality tester (refractometer), multimeter, flashlight. **10**
c. Product complexity (vs. simplicity) and robustness, ease of installation/removal: Simple, robust designs which are easy to install and pose no risk for damage to the vehicle receive most points **10**

The business plan:

d. Market potential: costs, added 'value', reach **10**

Bonus points:

e. Creative sketch e.g. of the product, brand name and label **2**

Environmental impact is assumed equal for all tampering unless tampering has a reduced environmental impact e.g. due to a partial shutdown.

Figure 5: Danish police training Flemish police to detect tampering of environmental protection systems near E40 motorway in Belgium (source: TNO)