DIAS

Smart Adaptive Remote Diagnostic Antitampering Systems

EUROPEAN COMMISSION

HORIZON 2020

LC-MG-1-4-2018

Grant agreement ID: 814951

Deliverable No.	D3.5
Deliverable Title	Hackathon and security resilience evaluation of the level 2 concept: Outcome of the evaluation with the hackathon
Issue Date	17/07/2022
Dissemination level	Public
Main Author(s)	Q. Vroom (TNO) I. Riemersma (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.

Document log

Version	Description	Distributed for	Assigned to	Date
V0.1	Draft version	TNO internal content review	Iddo Riemersma, Robin Vermeulen	21-5-2022
V0.2	Draft version	Consortium internal review	WP leader	15-6-2022
V0.3	Draft version	GA check + Internal review	GA members+ Internal independent reviewers	17-06-2022
V1.0	Final version			15-7-2022

Verification and approval of final version

Description	Name	Date
Verification of the “Final content of deliverable” by WP leader	Ann Delahaye (TNO)	15-07-2022
Check of the “First final version” before uploading by coordinator	Zissis Samaras (LAT/AUTh)	17-07-2022

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.

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 verification and validation methods , 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 second hacking event that was executed in the DIAS project to evaluate the prototype heavy-duty truck employed with DIAS Level 2 countermeasures.

Detailed results of the second 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 test bed mentors who observed the work, by means of 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.

Despite the Covid-19 pandemic, a mostly physical two day hacking event was organized. The event was called ‘Hack-a-Truck part 2’. The goal of the event was for participants to work in groups on finding potential vulnerabilities within the DIAS level 2 countermeasures. Participants were invited to an online information session in advance of the event, where they were provided with information in a number of technical presentations by experts from the DIAS consortium about tampering, DIAS developed countermeasures and the Ford Otosan prototype truck with Level 2 countermeasures. To speed up the hacking process during the event the level 2 countermeasures were split into two sub-systems and two separate test beds were developed, one for each sub-system. Each test bed was accompanied by test bed mentors, providing participants with answers to their questions as well as guiding and documenting the hacking process, meanwhile consortium experts were also available to assist in technical questions. On the second day of the event the groups of hackers presented their findings with respect to hacking attempts and outcomes, as well as participated in a central discussion session.

In total, four groups were formed with 15 independent hackers with an expertise in the field of cyber security with different levels of experience ranging from students to professional hackers. Each group was constructed under the guidance of the team captains, where participants with similar test bed preference got together in a group. In the end, one group focussed on test bed 1, one group focused on test bed 2 and the other two groups focused on both test beds. All four teams showed one or more hacking approaches and several hacking attempts:

- For test bed 1 there were 6 different attack vectors of which 1 had the potential of being a successful hack.
- For test bed 2 there were around 4 different attack vectors of which 1 had the potential of being a successful hack.

During the event, no system security breaching hacks were discovered. Further analysis and evaluation of the presented and documented attack vectors within the consortium is needed. The outcome of this evaluation will be direct input for the recommendations to make the DIAS level 2 anti-tampering countermeasures more robust.

Contents

List of Abbreviations

CCU	Communication Control Unit
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
EU	European Union
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	Set of points, system elements or endpoints (attack vectors) whereby an attack could potentially breach, effect 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 involve: • 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 as 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 which can be exploited by 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 (EPS) that have brought significant reductions to the actual emission levels. However, due to the additional costs for replacement and/or consumed reagent of the environmental protection systems (EPS) there is increasing evidence of illegal manipulation of these systems by vehicle owners and widespread usage is observed in the market. Such 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.

In the DIAS project, countermeasures have been developed to prevent or to detect and report tampering at two levels: level 1 constitutes the development of detection algorithms and security measures on the vehicle level and level 2 constitutes the development of a secure communication system that can report a possible tampering suspicion to the cloud. Level 1 was assessed in a first Hacking event 'Hack-a-truck' which has been reported in Deliverable D3.4: *Summary of the hackathon and security and resilience evaluation of the level 1 concept*. In a second hacking event the developed level 2 shall be assessed.

This report describes the work that has been conducted on task 3.4 of the DIAS project, which is to test the ability of the DIAS concept to harden against and detection of tampering in a hacking event.

1.2 Objectives and scope

The objective of task 3.4 of DIAS is to provide proof of the ability of the whole DIAS system concept (both Level 1 and 2) to prevent or detect and report tampering, which is to be independently tested in a hacking event. During this event, the DIAS concept level 2 is assessed for possible remaining vulnerabilities that allow deactivation of the EPS without being detected.
The scope of the second hacking event is on the DIAS level 2 demonstrator, the extra-vehicular (remote) communication. The attack surface is formed by two test beds, one on the in-vehicle communication of the in-vehicle control units relevant for wireless communication and one on the wireless communication between these control units and the cloud.

1.3 Approach

The approach for realising the objective is to perform an external open assessment by independent experts (ethical hackers) to find possible remaining weaknesses. Creative working sessions in the form of a hackathon are organized where the whole vehicle and sub-systems may be attacked. The plan is to take the following steps:

- Organization of an ethical hacking event after completion of DIAS level 2 anti-tampering measures.
- Supplying the demonstrator platform with developed tampering security solution (level 2) to ethical hackers.
- Allowing all possible methods to try to attack the system, including methods to erase detected tampering attempts.
- Monitoring and evaluation by the consortium of the attack methods, possible exploits, successful security defence and tampering detection, and possible detection erasure throughout the hacking event.

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 organized hackathon.

Chapter 3 describes the results of the hackathon.

Chapter 4 discusses the evaluation and recommendations.

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 detection of tampering, is tested in a hacking event and evaluated by IT security specialists.

- 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 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 road-side 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."

There were no deviations in the execution of the work from the DoW.

1.5.2 Time deviations from original DoW

There has been a delay of 3 months since the delivery date scheduled in the Grant Agreement. This delay was already communicated to and agreed upon by the EC officer.

2 Method: Hackathon (Hack-a-Truck part 2)

2.1 Mode of the event

The second hackathon was organised on 30-31 March 2022 and was titled Hack-a-Truck part 2. At that time, the Covid-19 pandemic was still ongoing, hence there were restrictions in place for cross-border travel and for organizing a physical event. To mitigate possible (last minute) travel or attendance complications, the event was setup in a hybrid manner by allowing both physical as remote participation. Physical attendance was the preferred option, both for hackers and consortium members. Furthermore, to support efficient remote participation additional facilities were arranged such as SharePoint folders and conferencing equipment.

Where the first hackathon was limited to theoretical development of attack vectors and working exploits due to its online format, in this second event they could be tested for real. One of the drawbacks with a live event is that it is restricted in time, especially since finding a successful attack vector and developing a working exploit may take years of lead time. To speed up the hacking process the level 2 countermeasures were split into two sub-systems and two separate test beds were developed, one for each sub-system. This provided the hackers with a system that was better to understand and easier to access. In addition, the hackers were instructed with detailed information about the testbeds in an information session prior to the hackathon. Questions on the architecture, software and communication protocols could be asked to the developers afterwards.

To attract and recruit skilled and experienced hackers the event was organized as a team challenge, with technical training during an information session in advance of the event and working sessions for brainstorming on attack vectors. During the hackathon the group members worked together to develop exploits and putting them to the test. They had access to the event logs of the anti-tampering systems and they could consult the (system) experts of the consortium. Where in the first hackathon the focus was on attracting students and organizing an event as a contest with prizes, this time the aim was to attract IT specialists which were all compensated for their time using a fixed daily fee. This allowed for drawing in skilled and experienced (professional) hackers for this event.

> *"…Hack-a-Truck part 2 revolves around a new system that reports information about a possible tampering suspicion wirelessly to a cloud or a supervising entity, to enable fast and easy detection and reporting of tampering of connected vehicles. The goal is to find possible vulnerabilities which allow tampering while remaining undetected…"*

Hack-a-Truck part 2 was a two-day physical hackathon, with an online preparation session a week in advance. The online session was hosted from a studio by a Microsoft TEAMS livestream. During this session several presentations were given:

- on the general background of the DIAS project,
- more specifically on the DIAS level 2 countermeasures, and
- highly detailed on the two separate test beds.

At the end of the preparation session four groups were formed consisting of four people. Four team captains were appointed prior to the session and they were responsible for forming groups with the other participants.

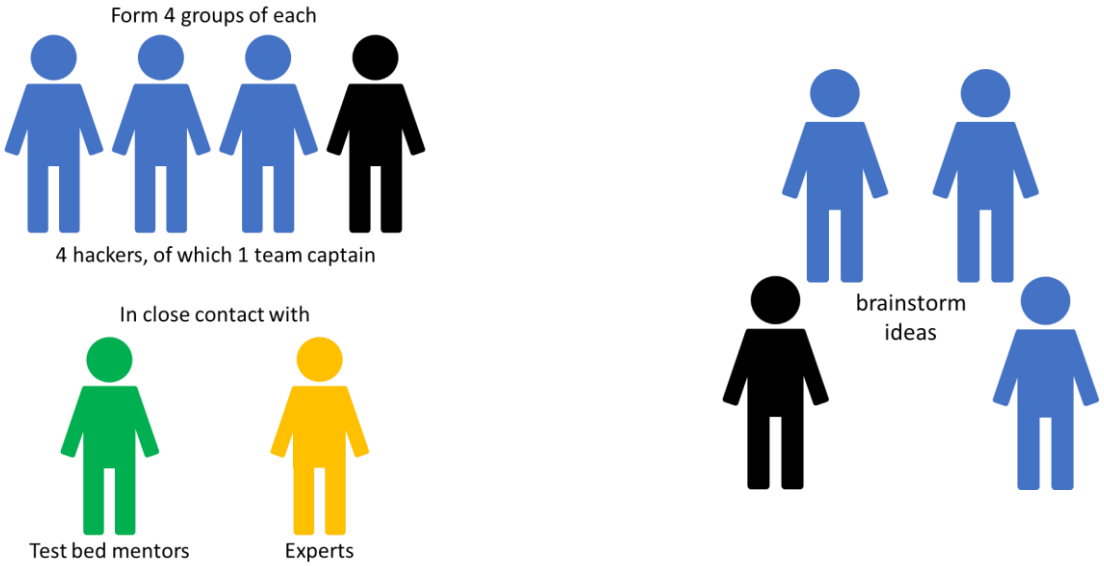
The two-day physical event was held in an old shipyard building in Rotterdam, the Netherlands. There was a Microsoft Teams stream involving multiple camera angles both on the host and the two test beds. Most of the participants were able to physically join the event, only one participant and a few consortium members joined remotely. During the event, teams had to brainstorm and develop new attack vectors and put them to the test on the available test beds. Each test bed was accompanied by

a test bed mentor who helped with team questions and hacking attempts, as well as to document the hacking process and findings. At least two experts per testbed were also available to assist the teams with questions and brainstorming. The interaction between hackers, mentors and experts are visually represented in Figure 2.

In front of the building a truck with integrated prototype DIAS Level 2 countermeasures was on display. On the first day a tour to the prototype truck was given to demonstrate the relation of the test beds to the entire prototype.

Figure 1: DIAS prototype truck shown in Rotterdam, the Netherlands.

During the morning of the second day the final presentations were given by the groups on their hacking attempts and the outcomes. The program finished with a central discussion involving participants, test bed mentors and consortium experts.



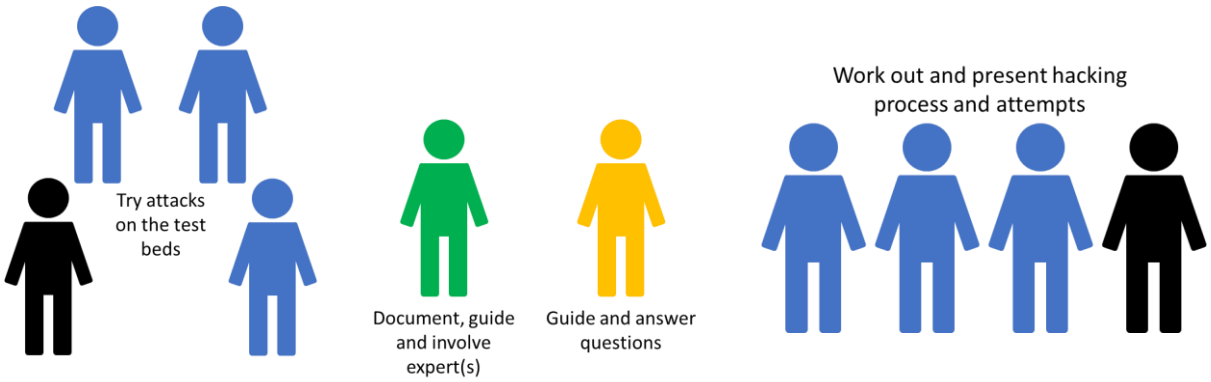


Figure 2: visual representation of the hackathon concept with brainstorm sessions and interaction between hackers, test bed mentors and experts.

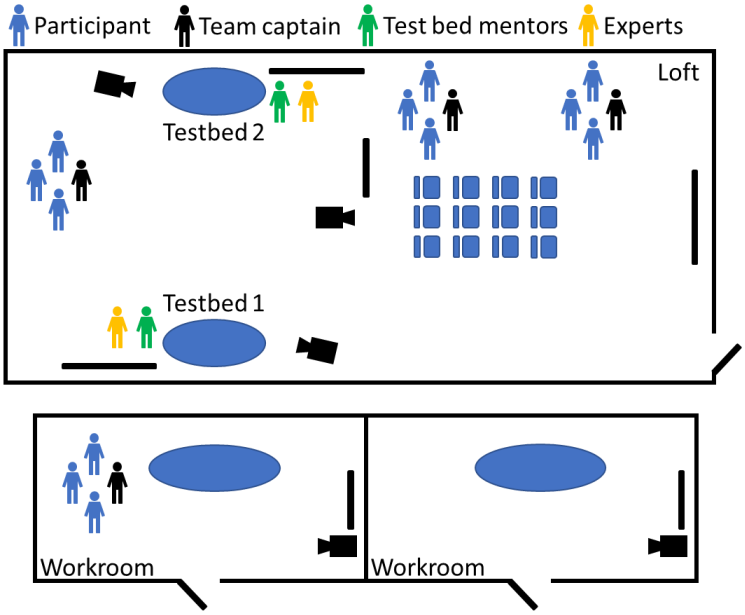


Figure 3: Floor map of the location during the two day physical event.

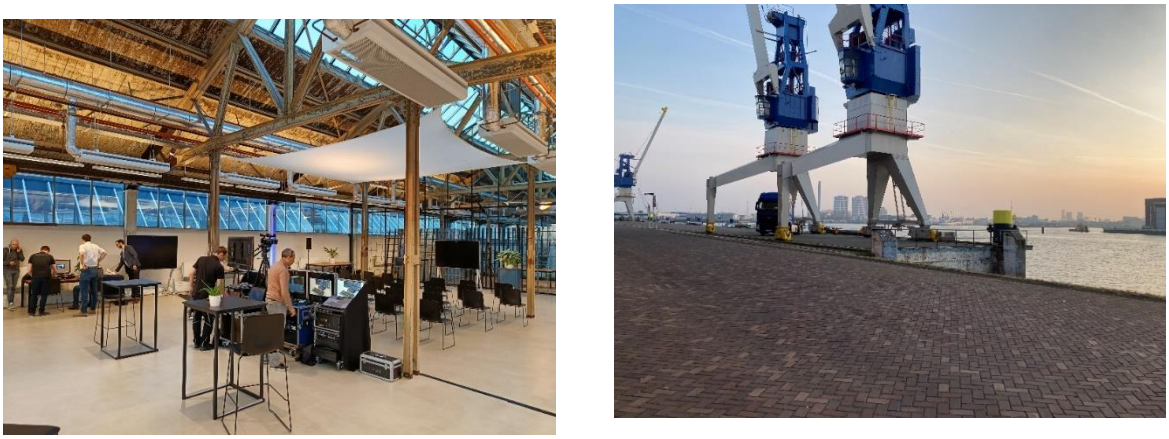


Figure 4: Impression of the location in Rotterdam, inside (left) and outside (right).

A storyboard was made to organize and plan the event in terms of timing, tasks, facilities and personnel needed to run the event smoothly. A simplified overview is presented in the table below.

Table 1: Hackathon schedule overview

Information session *March 23rd*	**Hack-a-Truck day 1** *March 30th*	**Hack-a-Truck day 2** *March 31st*
Welcome and day start	Welcome and day start	Day start
Presentation on DIAS project	Group formation finalized	Short working session for the groups
Presentation on DIAS level 2 countermeasures	Working session for the groups	Presentations kick-off
Presentation on Test bed 1	Lunch and prototype truck showcase	Group presentations and Q&A
Presentation on Test bed 2	Working session for the groups	Lunch
Participant round the table and group forming	Day ending	Central discussion
Day ending	Dinner at the restaurant	Day ending

2.2 Roles, role description and recruitment

2.2.1 Roles and role description

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

- 15 selected hackers of various relevant technical backgrounds
- Test bed mentors
- Consortium experts
- Presenters for presentations on the DIAS project, the DIAS level 2 countermeasures and the test beds
- Host
- Coordinating team
- Studio personnel

The role description for each of these is as follows:

- Hackers
  - Work in a team and actively contribute to the process of finding new attack vectors.
  - Develop exploitations to create a new tampering concepts.
  - Present the new tampering concepts, describe the working principles and what resources are needed to make the exploits effective.
- Test bed mentors
  - Responsible for the test beds.
  - Answer questions about the testbeds.
  - Monitor and document hacking concepts and attempts.
  - Guide teams with hacking attempts and provides feedback on successful hacking attempts.
  - Forward team questions to the experts.
  - Stimulate participants (e.g. when there is a lock-in situation).

  - Report issues to the coordinators.
- Consortium experts
  - Share their 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.
- Host
  - Host the whole event by opening, stating announcements and closing each day.
  - Present introduction, agenda, playing rules, etc.
  - Leads Q&A at the end of each presentation; collects and answers questions.
  - Provide practical information regarding the facilities.
  - Small talk in between.
- Coordinating team
  - Make sure that everything runs smooth and as planned.
  - Keep everyone on track
  - Solve unforeseen practical (connectivity) issues on the spot.
- Studio personal
  - Studio personnel controls the studio equipment and the Microsoft Teams stream.

2.2.2 Participant recruitment

A total of 15 participants was recruited for the event. The participants were expected to be able to perform hacking attempts on the physical test beds, the main focus was on attracting experienced (professional) white hat hackers[1].

Every suitable candidate could apply for the event, however the event attendance was only open for those applicants that were invited after a thorough review of their CV.

The set of internally drafted requirements for participants is as follows:

- You should have extensive knowledge on and experience with (automotive) electronics, (automotive) communication and/or security protocols, in particular cryptography.
- You should have experience with Raspberry Pi.
- Knowledge on and experience with AUTOSAR SecOC, man-in-the-middle attacks on CAN-bus, HTTP and/or SSI are preferred.
- Your communication skills in English are excellent.
- You should deliver added value with your expertise and skills during the Hack-a-Truck 2 event.

During the direct participant sourcing this set was incorporated into the text describing the proposed challenge for the event:
Both testbeds are Raspberry Pi based setups, with added encryption.
These testbeds involve:

- *(man-in-the-middle attacks on) CAN-bus and AUTOSAR SecOC*
- *HTTP and SSI*

If you can hack one (or both) of these challenges and if you have excellent English communication skills, then please do apply!

Recruitment of staff from actual tamperers was discussed beforehand within the consortium. It was decided not to invite tamperers as there was a risk that they will retrieve the information of the

[1] According to Wikipedia, a white hat hacker is an ethical security hacker. Ethical hacking is a term meant to imply a broader category than just penetration testing. Under the owner's consent, white hat hackers aim to identify any vulnerabilities the current system has.

hackathon and use the information for their business to develop new tampering concepts while providing little to no input.

To assist with the recruitment of white hat hackers with the right experience for the job, the company 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 to assist the DIAS project team for the event. With their help, and by using the network of the DIAS partners, a total of 16 participants with expertise in the field of cyber security were recruited for the Hack-a-Truck 2 event, ranging from students to professional hackers.

2.2.3 Participant sourcing

For the recruitment of the participants multiple sources were used and participants of the previous hackathon event were made aware of Hack-a-Truck 2. Consortium partners reached out to their cyber security departments and also to various universities and colleges in their member states which were also contacted during the first hackathon.

Table 2 Organisations and companies that were contacted for recruitment of participants

Educational institutions	Partners and companies
1. TU Delft 2. TU Eindhoven 3. Han hogeschool 4. Hogeschool Rotterdam 5. VU Brussel 6. COSIC, Leuven 7. UMFST 8. RWTH 9. Aristotle University of Thessaloniki 10. Democritus University of Thrace 11. Faculty Hochschule Esslingen 12. Technical University of Cluj-Napoca, Romania	ERNW TNO Cyber Security CERTH Cyber Security FEV

2.2.4 Recruitment website and flyer

For the recruitment of participants a digital flyer was designed by LAT. The flyer was distributed as well as posted online on the DIAS project website. The flyer served to recruit participants and to inform them about the contents, timing and location of event. On the website there was a button with a direct link to the application. The application process was done via the project office department of TNO, where they have a lot of experience with handling personal information securely. Below is an image of the flyer.

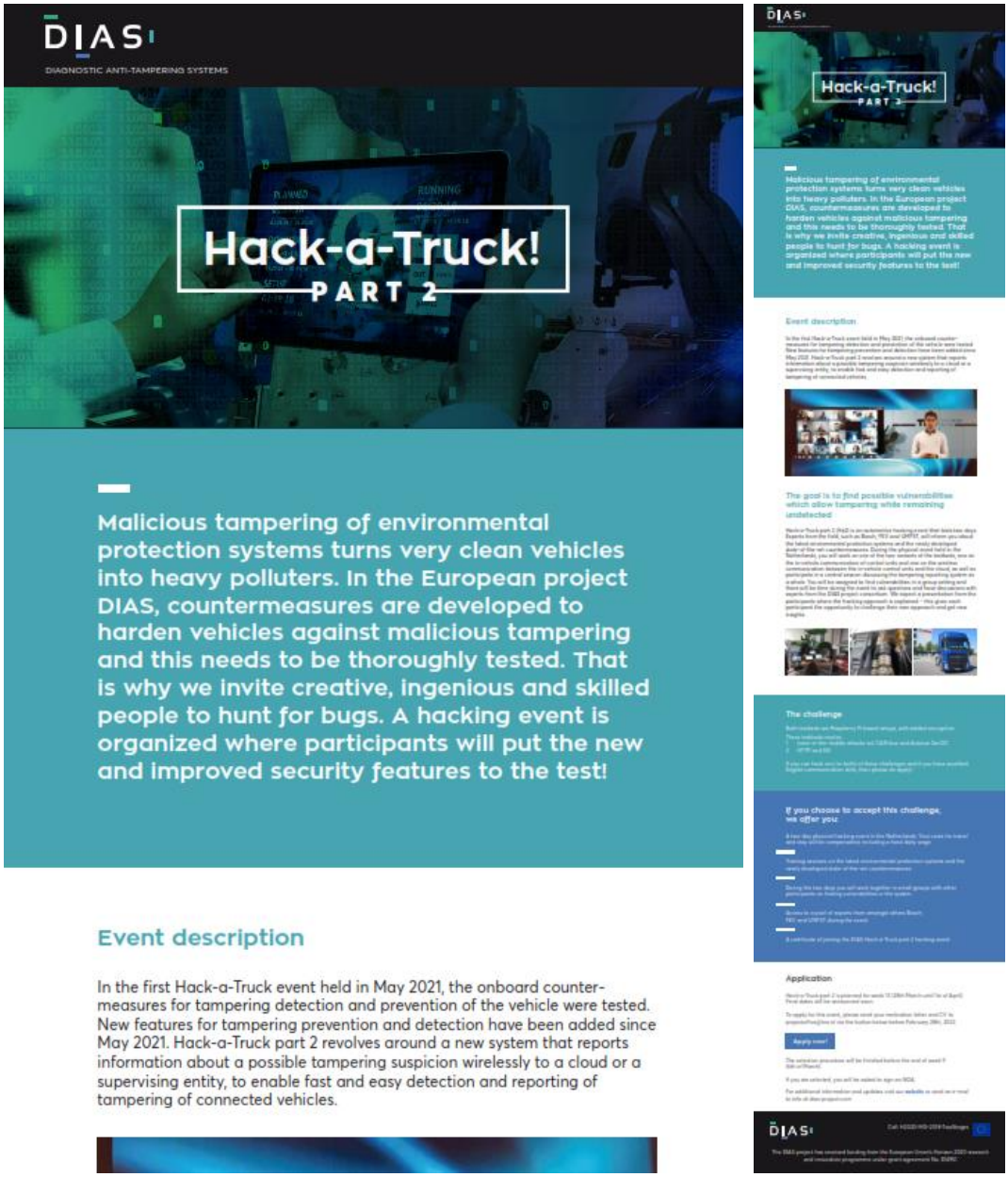


Figure 5: Image of the Hack-a-Truck part 2 flyer, zoomed in (left) and in its entirety (right).

The information session of the Hack-a-Truck 2 event was held in week 12 on the 23rd of March, and the physical event a week later in week 13 on the 30th and 31st of March.

2.2.5 Participant selection process and team formation

In total, 25 applications were handed in at the TNO project office email account. Every candidate had provided a CV and most of them attached a motivational letter as well. The applications were used to evaluate the applicants based on their:

- Relevant skills, experience and expertise from education, degree, faculty and/or 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, 15 candidates were selected and invited to join in the event. Most participants had an expertise in the field of cyber security, ranging from

students to professional hackers. Group formation was done by appointing team captains in advance of the online information session and facilitating a short introduction round between the participants and team captains after the presentations in Teams break-out rooms. The participants were not only asked to introduce themselves, but also to state their preference to which of the two test beds (or perhaps both) they would like to focus during the physical event, based on the information in the presentations by the consortium members. This helped to naturally group the participants in such a way that similar interests and hacking goals were aligned in each group. A preliminary group formation was made at the end of the information session, and the final one was decided by the organisation shortly before the start of the physical event. One person was unable to travel to the Netherlands due to travel restrictions, but fortunately he was able to join the event remotely.

Groups were allowed to choose which test bed to focus their attention to. This led to the division given below.

	Focus on test bed no.
Group 1	2
Group 2	1
Group 3	1 and 2
Group 4	1 and 2

2.3 Hosting and facilities

In advance of the physical event an online information session was organised on 23 March 2022. A stream was setup via a Microsoft Teams meeting, which was hosted from a studio setup at TNO in the Netherlands. There was a host present during this session to welcome the participants as they joined, start off the event, announce transitions and presenters, guide the process and the Q&A's and to wrap it all up at the end of the day. Behind the scenes there was a crew of studio personnel working on sound and visuals of the studio, to facilitate multiple Teams meetings and making sure presenters and presentations were visible on the screens. There were also coordinators monitoring the meeting, making sure that all participants could join the meeting, guiding the host and the studio according to the storyboard and keeping an eye on the time. After the information presentations on the DIAS countermeasures and test bed specifications by the consortium members there was time for a short introduction round between participants. Four parallel Teams meeting streams were provided, each for one pre-appointed team captain. The remaining participants were encouraged to visit each of these separate meetings to meet up with the team captains.

As mentioned previously, the main event was hosted in the Netherlands in an old shipyard building in Rotterdam. It was setup in a hybrid manner to allow for remote participation, both for participants of the event as well as for consortium members joining the event. To accomplish this, an audio-visual company was involved to setup the livestream including multiple camera angles and multiple microphones, as well as conferencing units in the separate workrooms.

For each of the participants a hotel was booked near the event location and transportation to and from the hotel was arranged. On the location of the event there was all-day catering provided and at the end of the first day dinner was organised in a restaurant nearby. Participants were expected to bring their own laptops, but hardware required for connecting to the test beds was supplied.

Below are some pictures of the event to get an impression.

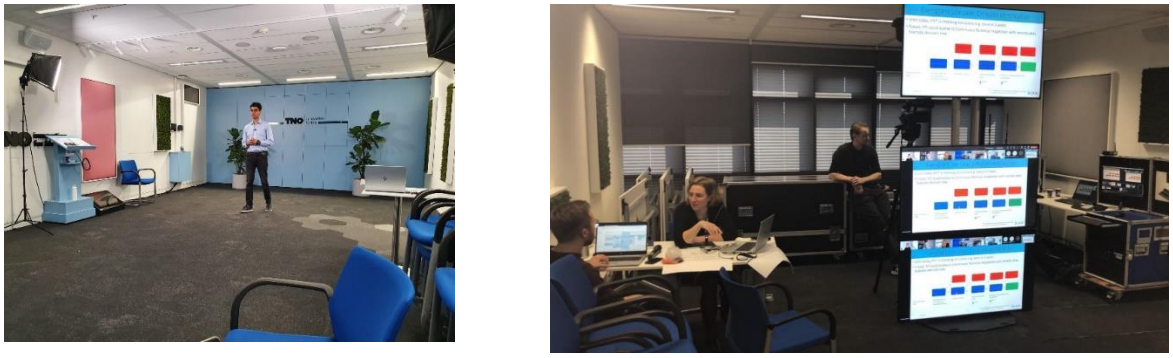


Figure 6: Pictures in the studio during the information session.

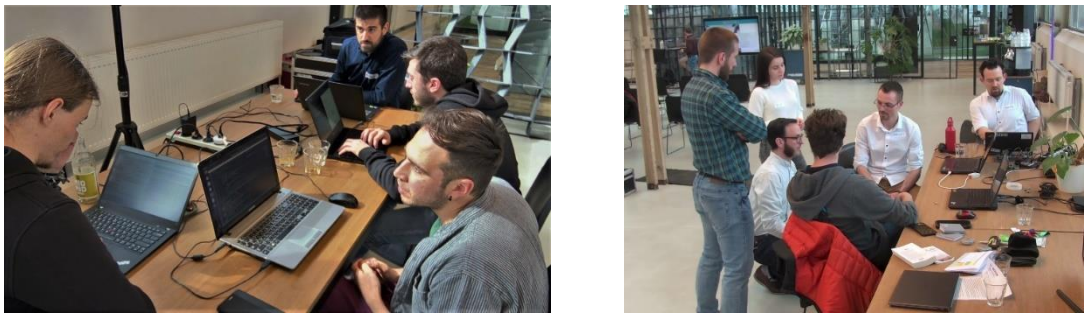


Figure 7: Pictures of the group working sessions during the physical event.

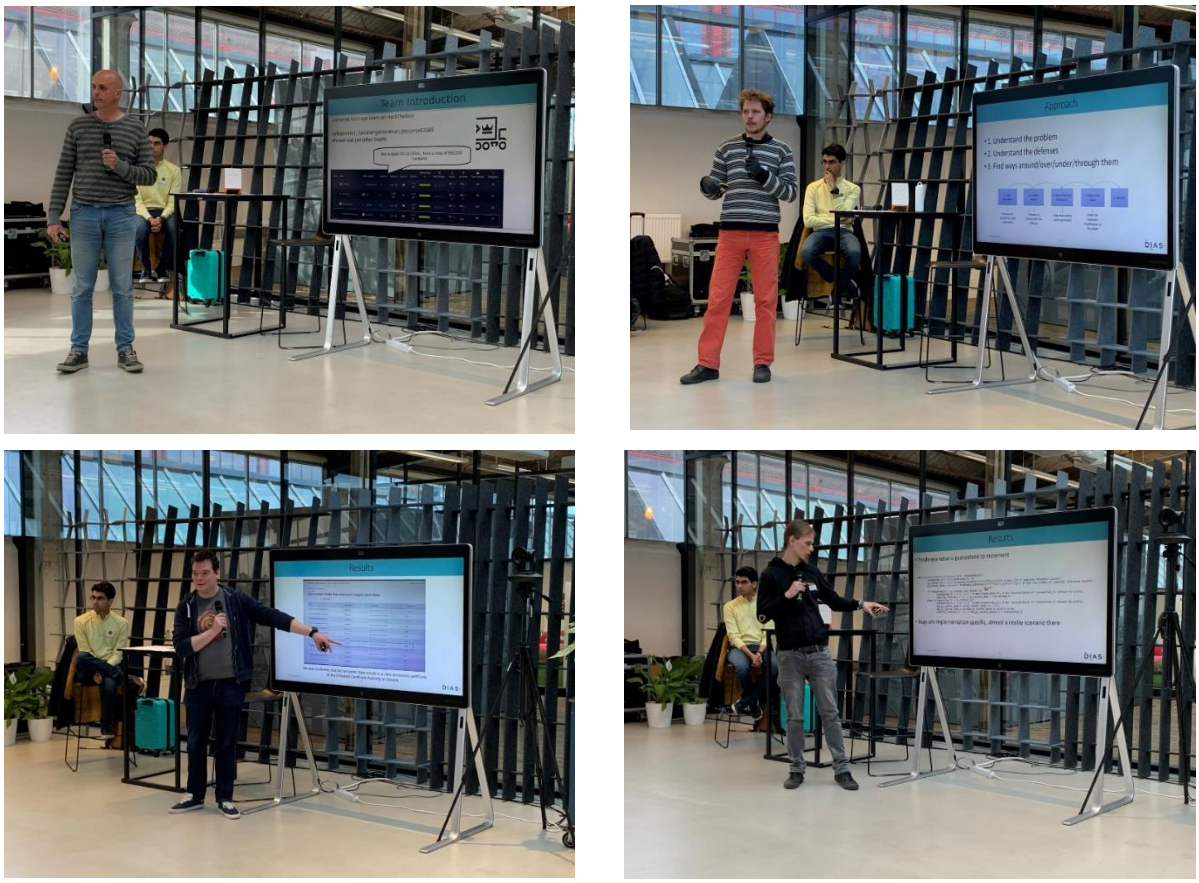


Figure 8: Pictures of the final presentations by the team captains of each group.

A SharePoint was setup especially for the Hack-a-Truck 2 event, to provide a platform and tools for the participants to work together. There was a general SharePoint folder available ahead of the physical event, which contained the presentations given by consortium members during the information session. Each group was also given their own partition on the SharePoint where they could work together and which contained a template for the final presentation.

2.4 Information provided

Preparatory information was provided to the participants in advance of the physical event via a SharePoint with documents and presentations. This consisted of information regarding:

- Scope of the hackathon and playing rules
- working principles of the EPS
- current tampering practices
- insight into the DIAS project anti-tampering countermeasures
- specifications of the test beds necessary.

This was seen as essential information to discover potential vulnerabilities in the system.

During the physical event participants could reach out to test bed mentors and consortium experts to acquire additional information and ask questions.

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

2.4.1 Information provided during the information session

The information session started by a welcome and a short introduction to the event by the host. Four presentations were given that day by multiple experts from industry leading companies and knowledge institutes such as: LAT, Bosch, UMFST and CERTH, which are all DIAS project partners. The first presentation contained an introduction to the DIAS project and a high level overview of the challenges against tampering and the proposed anti-tampering countermeasures within the project. The second presentation dived deeper into the DIAS project level 2 countermeasures. The third presentation contained the scope and specifications of test bed 1, focussing on the in-vehicle communication. The fourth and final presentation contained the scope and specifications of test bed 2, focussing on the remote communication with an external entity. After each presentations there was room for questions to the presenters and the experts.

2.4.2 Additional information and answers during the physical event

During the physical event, test bed mentors and experts were available to answer any questions the participants raised. The advantage of this being a physical event is that the participants, mentors and experts could easily reach out to each other and to the test beds. This allowed participants to receive an answer to questions and receive additional specific material related to a question on one of the test beds. At the same time this facilitated in-depth discussions with experts and mentors on hacking approaches and experts and mentors to observe hacking approaches while providing direct feedback on its success.

2.5 Guiding and monitoring the process

Each test bed was accompanied by one test bed mentor who helped with team questions and hacking attempts, as well as document the hacking process and findings. At least two experts per testbed were also available to assist teams with questions and brainstorming. An important objective of the hackathon was to get a better view into the hacking process and the hacker mindset. Each mentor

was provided a mentor sheet to document all the important observations near the test beds during the working sessions of the event. Especially the questions raised by the participants and the discussions between participants and experts and mentors were extremely valuable in grasping the hacker mindset. The participants and the mentors had a lot of interaction during the entire process from brainstorming possible hacking approaches up until implementation of the hacks.

2.6 Final presentation and discussion

Groups were asked to show their findings in a final presentation. A DIAS style PowerPoint template was provided to ensure that the presentations were complete and consistent while the groups did not have to spend time on the format. Each presentation was followed by a short round of questions from the participants and consortium members. Presentations were limited to 15 slides and 20 minutes of presentation time. The hacking approaches and discovered vulnerabilities were the most important results from this hackathon. After the lunch break there was a central discussion session involving participants and consortium members to elaborate on the (implications of) possible vulnerabilities and anti-tampering countermeasures.

After the event each participant received a certificate of participation.

3 Results

Since the specific results are confidential, this section is limited to a qualitative description of the main findings. Detailed information is only shared between the consortium partners of the DIAS project. During the Hack-a-Truck 2 event all four teams showed one or more hacking approaches and several hacking attempts. The test bed mentors administered all of these, as well as the discussions between participants, mentors and experts. The main outcomes of the central discussion session at the end of the event was documented by one of the team captains.

The results presented by the groups contained multiple attack vectors for each of the test beds, some of which were tried on the test beds during the event:

- For test bed 1 there were 6 different attack vectors of which 1 had the potential of being a successful hack.
- For test bed 2 there were around 4 different attack vectors of which 1 had the potential of being a successful hack.

Important to note is that none of the potential successful hacks presented during the event had the capacity to breach the system security.

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. Since the specific results are confidential, the evaluation of the results itself is not included in this report. Detailed evaluation of the results is performed by the consortium partners of the DIAS project.

4.1 Evaluation of the event

At the end of the program on the second day of the physical event participants were asked for their feedback. The overall responses of the participants were positive. There were compliments for the organization of the event, in particular on the location and the available facilities. People were happy with the overall program setup and had enjoyed the event. The proposed challenge and the topic were interesting and educational, although it was quite challenging for most participants to absorb the large amount of new information. The well-prepared test beds were much appreciated by the participants. They indicated that this saved them a lot of time and preparation and gave them a flying start during the event.

As learning points the participants mentioned that the time between the information session and the physical event was too short and that the amount of information to digest during the information session was far too much. Participants would have preferred to have the presentations distributed over multiple information sessions so as to have more time to get familiar with the presented topics and prepare hacking approaches between the information session and the physical event. The available time for hacking during the physical event was also found fall short. Participants would have preferred to have more hands-on time with the test beds.

Among the participants there was a mix in experience levels, ranging from students to professional hackers, mostly with a dedicated expertise in the field of cyber security. A point for improvement was the scarcity of participants with dedicated automotive hacking experience. A great advantage over the first hackathon was the physical aspect of it, allowing for hands-on hacking by the participants and direct feedback on the success of the hacking attempts. This also allowed for easy interaction between participants and test bed mentors or experts. This gave consortium members good insight into the tampering approaches and the hacker mindset. Overall the Hack-a-Truck event was successful and delivered very useful results.

With the experience gained from this event, the following recommendations for future hacking events can be made:

- Allow sufficient time for participants to digest the background information provided for the hackathon. It is important to check that there is no information overflow during the preparatory information session. If necessary, distribute the information over multiple sessions.
- Allow participants to get familiar with the topic, tools and protocols and to prepare hacking approaches well in advance of the hackathon. One week is not sufficient.
- Acquiring dedicated white hat hackers with automotive and communication security experience is very challenging. It is advised to start the recruitment process well ahead of the hackathon and to advertise it as wide as possible in relevant networks, possibly with assistance of dedicated service providers (e.g. specialised in IT Security).
- Question-driven discussions between participants/hackers and experts are remarkably useful for finding vulnerabilities and grasping the hacking mindset and approach.
- Preparing dedicated test beds for hackers to work on during the hackathon speeds up the process and reduces time and effort needed for the participants to understand the system.

- Having a physical event allows for hands-on hacking and direct feedback on the success of the hacking attempts, however it requires more time and effort for organizing than an online version.

5 Conclusions

The specific conclusions of the Hack-a-Truck 2 event are confidential since they contain valuable information on new anti-tampering measures and potential vulnerabilities. Therefore, this section is limited to a qualitative description of the main conclusions. Detailed conclusions are only shared between the consortium partners of the DIAS project.

During the event no system security breaching hacks were discovered. Further analysis and evaluation of the presented and documented attack vectors within the consortium is needed. The outcome of this evaluation will be direct input for the recommendations to make the DIAS level 2 anti-tampering countermeasures more robust.