MEDDOCS
Open Access Publisher

Annals of Forensic Science and Research

Open Access | Case Report

Digital Forensic Readiness in Internet of Vehicles: The Denial-of-Service on CAN bus Case Study

Christina Katsini[1]; George E Raptis[1]; Kristina Livitckaia[2]; Konstantinos Votis[2]; Christos Alexakos[1]*

[1]Industrial Systems Institute, Athena Research and Innovation Information Technologies, Patras, Greece.

[2]Information Technologies Institute, Centre of Research and Technology Hellas, Thessaloniki, Greece.

***Corresponding Author(s): Christos Alexakos**
Industrial Systems Institute, Athena Research and
Innovation Information Technologies, Patras, Greece.
Email: alexakos@isi.gr

Received: Jul 29, 2022
Accepted: Sep 05, 2022
Published Online: Sep 07, 2022
Journal: Annals of Forensic Science and Research
Publisher: MedDocs Publishers LLC
Online edition: http://meddocsonline.org/

Keywords: Internet of Vehicles (IoV); Digital forensics; Post-incident investigation; Cybersecurity; DoS CAN bus.

Abstract

In the era of connected and autonomous vehicles (CAV), cyber-attacks can impose a hazard on passenger's life given that security incidents may lead to accidents in case they are not timely mitigated. It is therefore essential not only to quickly detect an attack and actively respond to it, but also to gather information that can be used for remediating future similar attacks. To do this, it is crucial to define forensic plans for such incidents before they happen, to ensure that the Internet of Vehicles ecosystem is ready to mitigate any risks with the minimum cost and disruption. Aiming to provide safer transportation on the roads and increase people's trust in CAVs, we proposed a framework of digital forensic readiness for the Internet of Vehicles which provides a process for acquiring and preserving digital evidence in case of an incident and supports the post-incident investigation. In this paper, we present a case study of the proposed framework for a specific to the Internet-of-Vehicles ecosystem attack, the Denial-of-Service CAN bus attack. We briefly present the implemented digital forensic framework of the IoV ecosystem and we report an attack specific to the Internet of Vehicles. We discuss the benefits of using the proposed framework for investigating an incident based on automatically collected evidence and providing a report that can be used for mitigating similar attacks in the future, and thus improving the safety of CAVs and providing better and uninterrupted transportation services.

Introduction

The introduction of Connected and Autonomous Vehicles (CAVs) in today's road transport is expected to reduce the frequency and severity of accidents. However, with cyber-attacks on information systems presenting a growing threat, the Internet-of-Vehicles (IoV) ecosystem is also at risk. Ensuring the security of CAVs is of critical importance, and it requires not only an active response to cyber-attacks (e.g., to stop the CAV when an abnormal behavior is detected), but also a post-incident investigation that will enable the transport companies and the CAV manufacturers to identify the cause of the attacks, and remediate vulnerabilities both of the CAVs and the IoV ecosystem.

The purpose of the post-incident investigation is to learn from incidents, turn problems into progress and build trust with passengers and other stakeholders. To this end, it is important to prepare the IoV ecosystem for an incident, the occurrence of which cannot be predicted. This is done by setting a forensic readiness policy that allows the maximization of the IoV ecosystem's ability to collect evidence during and after an incident, and minimization of the cost of forensics in an incident response. The policy is implemented through forensic readiness plans that are activated in case of an incident. These plans are responsible for managing the acquisition, identification, evaluation, and admission of the forensic evidence.

Cite this article: Katsini C, Raptis GE, Livitckaia K, Votis K, Alexakos C. Digital Forensic Readiness in Internet of Vehicles: The Denial-of-Service on CAN bus Case Study. Ann Anat Res. 2022; 1(1): 1004.

The IoV ecosystem is susceptible to the most common types of cyber attacks, such as denial-of-service (DoS) on the network between the vehicle and the supervision centre, which is responsible for monitoring the status of the CAVs. Apart from these types of attacks, the IoV ecosystem is also susceptible to IoV-specific types of attacks. In this case, CAV-specific sensors (e.g., GNSS sensor, odometer, OBU, etc.) are the targets. In CAVs, the sensors communicate through the Controller Area Network (CAN) bus. Any disruption on the CAN bus may lead to inability of these sensors to communicate which can affect the safety of the CAV.

In this paper, we present a case study of using a novel framework for post incident investigation. We discuss the forensic readiness plan steps, outline the collected evidence, and present the process of the investigation. Thus, the paper is organized into the following sections: in Section 2, we briefly present the nIoVe framework and discuss digital forensics in IoV. In Section 3, we present the DoS on CAN bus attack case study and in Section 4, we discuss the findings. Finally, in Section 5 we provide the concluding remarks.

Background and related work

nIoVe Framework

The nIoVe framework provides a holistic cyber-security solution for IoV ecosystem, with a primary focus on CAVs [1]. It enables the detection of the attacks on the IoV ecosystem in real time, the activation of both active (e.g., block IP of the attacker) and passive (e.g., inform the manufacturer about the vulnerability that was exploited by the attacker) response based on the type of the attack, and supports post-incident investigation. The post-incident investigation is implemented through the Attack Attribution and Digital Forensics Readiness Tool (i.e., AAFRT), which has been developed to support the forensic investigators during the post-incident analysis of an incoming attack and ensure the minimum interruption to the transportation services [2]. AAFRT provides two functionalities:

- Attack Attribution [3], which automatically detects indicators of compromise that can be then used by the forensic investigators to perform an accurate attribution of the attack (e.g., identification of threat actors, identification of tactics, techniques and procedures), and
- Digital Forensics Readiness [2], which automatically acquires, preserves and pre-processes evidence, and creates a report that can be used for post-incident analysis by the forensic investigators through a graphical user interface.

IoV is a complex ecosystem with a wide variety of connected devices that process and share various sorts of information. This information is communicated through different protocols within the CAVs, among them, and between the CAVs, the infrastructure, the cloud, and the pedestrians. It is frequently critical for the safety of the CAVs, hence safeguarding such an ecosystem is critical. The nIoVe framework offers a complete cyber-security approach for IoV [1].

The complexity of the IoV ecosystem imposes the requirement not only of ensuring the active response in case of an attack but also of establishing forensic readiness policies for different types of attacks to enable **post-incident investigation** for discovering the root cause of the attack, the underlying motives of an attack, the vulnerabilities of the IoV with the ultimate goal of remediating the threat and improve the security of the IoV ecosystem. The forensic readiness policies are implemented through digital forensic plans. At a preparation stage, the forensic investigators must identify potential evidence that would be required in case of an attack and then create the plans that should be executed in the event of an attack. Such plans should enable the acquisition, preservation, and preliminary analysis of the attack related data. Collecting forensic evidence from an attack is essential not only for mitigating the attack but also for identifying vulnerabilities and notifying both the manufacturers and the transport authorities. Automating this process would be beneficial because the IoV ecosystem handles a large amount volatile data that could be lost or corrupted if the collection of the evidence was not done immediately after the attack. The process of handling IoV data that can be used as evidence is an integral part of the digital forensic readiness process and in the next section we discuss the research attempts related to forensics in IoV.

Digital forensic readiness for IoV

Digital forensics is an emerging interdisciplinary field where information systems expertise is met with legal knowledge to assess digital evidence that has been gathered, processed, and preserved in a legally permissible method. Digital forensics is mostly employed in legal or law enforcement investigations that are likely to wind up in court. As a result, there is a focus on legal acceptability. Given the volatility of digital evidence, which may be lost or corrupted, there is a need to manage (e.g., collect, preserve) digital evidence to ensure its integrity and soundness. As a result, researchers and practitioners have created digital forensic tools and procedures (for example, [4, 5]) to collect, store, and assess the evidence that may be utilized by forensic investigators.

Traditional forensics are not appropriate for the IoV ecosystem due to the mobility of the IoV entities, its distributed structure, and the vast quantity of possible evidence that may be created from such a complex environment [6]. Nilsson et al. [7] presented a set of prerequisites for in-vehicle network detection, data collecting, and event reconstruction.

The forensic investigation framework for IoVs, Trust-IoV [8], features a forensics gateway, integrated on each IoV entity which is responsible for logging incoming and outgoing interactions and an IoV forensic service, which stores evidence, including data from infotainment systems relevant to forensics investigation [9], and provides read-only access to them. Another model for acquiring and preserving evidence from CAVs was proposed by Feng et al. [10], who emphasized the issue of the ease with which evidence data may be altered in IoV forensics and advocated the use of hashing and encryption to ensure data integrity.

As discussed, research teams have proposed a few solutions for supporting the forensic readiness process in IoV. These solutions were theoretical frameworks. The nIoVe framework includes a tool, AAFRT [2], for automatically acquiring, preserving, and analysing evidence after the occurrence of an incident. The tool facilitates post-incident investigation through a graphical user interface for mitigating and remediating attacks and ensuring the safety of the passengers and the pedestrians. In the case of CAN bus related-attacks, it is essential to re-authenticate the devices connected to the CAN bus and perform post-incident investigation to identify the root cause of the attack to ensure that the CAVs can re-start the route without putting the passengers life at risk.

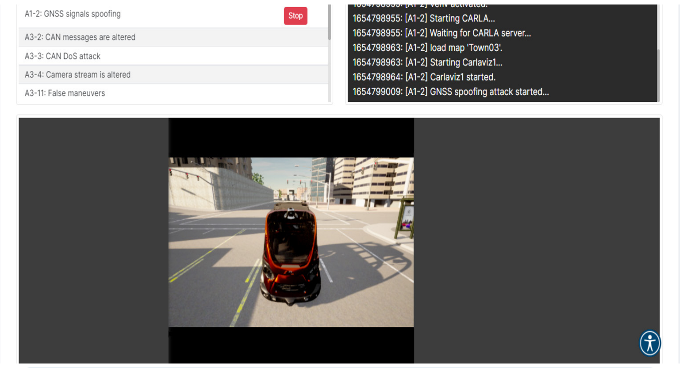
CAN protocol vulnerabilities

The CAN protocol allows sensors, micro-controllers, and any other devices connected to the bus to communicate with each other. Its vulnerabilities lie in i) any device connected to the CAN is allowed to read and write to the bus, ii) all data coming from the CAN are considered trusted, and iii) CAN messages cannot be distinguished from genuine, compromised, faulty, etc. As a result, the CAN bus is susceptible to DoS attacks. Detection of such attacks is based on detecting anomalies in the CAN traffic. Further investigation is required to identify the root cause of the attack, as it could be either because one of the existing devices connected to the CAN bus was compromised, or someone managed to directly access the CAN bus and has published messages aiming to increase the traffic and disrupt the communication. In this paper, we present the use of the AAFRT tool of the nIoVe framework for the post incident investigation of such an attack.

Case study: DoS CAN bus attack

DoS CAN bus attack scenario

This scenario assumes that the attacker can maliciously communicate on the CAV's internal network. The attacker, acting as a maintainer, has access to the CAN bus interface. We consider the flooding of the CAN network with messages with high priority (messages ID close to 0), yielding to the unresponsiveness of the CAN bus. CAN is no longer operational since all vehicle's connected devices cannot communicate. Unresponsiveness of the CAN bus leads to the inability of the CAV to receive critical information about its position, speed, brakes, etc., thus the vehicle is uncontrollable and may demonstrate unexpected behavior. This constitutes a high risk for the passengers and the pedestrians.

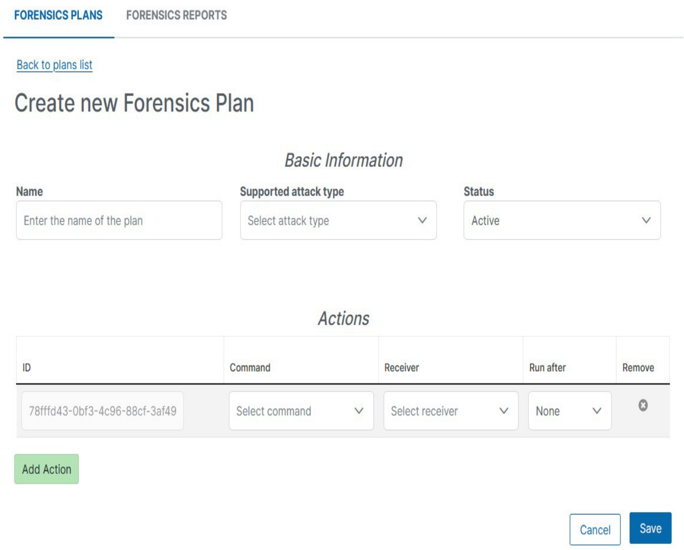

A1-2: GNSS signals spoofing
A3-2: CAN messages are altered
A3-3: CAN DoS attack
A3-4: Camera stream is altered
A3-11: False maneuvers

```
1654798955: [A1-2] Starting CARLA...
1654798955: [A1-2] Waiting for CARLA server...
1654798963: [A1-2] load map 'Town03'.
1654798963: [A1-2] Starting Carlaviz1...
1654798964: [A1-2] Carlaviz1 started.
1654799009: [A1-2] GNSS spoofing attack started...
```

Figure 1: The graphical user interface of the co-simulation tool used for the simulation of the DoS CAN bus attack.

Simulation environment

To simulate the attacks on CAVs, we used the co-simulation tool of the nIoVe framework (Figure 1). The co-simulation tool is based on the CARLA open-source simulator that supports the development, training, and validation of autonomous driving systems. The graphical user interface of the co-simulation tool i) enables the user (e.g., security expert) to execute a specific attack scenario, ii) provides a console with log to view the progress of the attack in real time, iii) provides a live video stream of the CAV moving in a metropolitan area.



Create new Forensics Plan

Basic Information

Name: Enter the name of the plan
Supported attack type: Select attack type
Status: Active

Actions

ID	Command	Receiver	Run after	Remove
78fffd43-0bf3-4c96-88cf-3af49	Select command	Select receiver	None	⊗

Figure 2: The graphical user interface of FoRePlan that enables forensic investigators to create digital forensic readiness plans.

Digital forensic readiness process

The digital forensic readiness process is divided into three main stages: i) pre-incident preparation, ii) during-incident forensics, and iii) post-incident investigation. We discuss them next.

Pre-incident preparation

Regarding the first stage, the nIoVe framework has integrated attack detection, response, and recovery processes for common attacks found in IoV and CAVs environments (e.g., GNSS-related attacks, CAN bus-related attacks, and V2X-related attacks). Moreover, forensic investigators must be able to adjust the behavior of the system dynamically, aiming to acquire and preserve forensic evidence. Such evidence could be used to perform a deep post-incident investigation and/or be presented during legal or law enforcement procedures (e.g., presented in court).

Towards this direction, the AAFRT component of the nIoVe framework provides the forensic investigators with a tool to manage digital forensic readiness plans for potential harmful incidents (e.g., IoV threats). The investigators are equipped with FoRe Plan [11] to create and configure such plans for common attacks found in IoV and supported by the nIoVe framework. Figure 2 depicts a screenshot of the graphical user interface of FoRe Plan used to create a new plan. FoRe Plan allows the forensic investigators to add actions and schedule them (e.g., in parallel, sequentially) for data acquisition, preservation, and further analysis. More information about FoRe Plan can be found in the work of Katsini et al. [11].

During-incident forensics

The nIoVe framework collects, analyzes, and temporarily stores a vast amount of data related to the overall behavior of the IoV system and the supported CAVs in real time. When an incident occurs, the framework detects anomalies which are then clustered into attacks. Focusing on our case study, when we simulate a DoS CAN bus attack using the co-simulation tool, the system detects various anomalies about the incident, which are classified as: i) DoS on the CAN bus, ii) camera stream alteration, and iii) GNSS spoofing.

spoofing. Moreover, when an incident occurs, the nIoVe framework collects additional data from the CAVs and the IoV ecosystem in real time.

Focusing on the forensic readiness process, AAFRT is activated for each detected attack. Given the type of the attack (e.g., DoS CAN bus attack), ForePlan [11] selects and executes the appropriate plan (e.g., plan for a DoS attack on the CAN bus). Regarding our scenario and the aforementioned detected attacks, the selected plans include the acquisition of the appropriate data which constitute the evidence for investigating the detected attacks, as presented in **Table 1**. As discussed, the nIoVe data collectors, which are deployed on the CAVs, collect data automatically and in real time. Next, they store the collected data at a secure repository for meta-analysis processes and/or post-incident investigation. The collected data and the data which results from any analysis processes form the forensic evidences. They are acquired and stored dynamically, and then, they are preserved by calculating their SHA hash values.

We observe that whilst the performed scenario simulated the DoS attack on the CAN bus, the nIoVe framework did not only detect this type of attack, but also other attacks (camera stream alteration and GNSS spoofing) were detected. This could mean either that the IoV system was under multiple attacks or that the simulated attack led to more anomalies, and thus, attacks of a different type. The latter is explained by the nature of the CAN bus, as it is responsible for communicating information critical to the CAV's proper and safe operation, and when an attacker floods the CAN bus, the CAV is unable to receive information from any device connected on the CAN. It starts demonstrating abnormal behavior, which explains why the aforementioned types of attacks are detected by the nIoVe framework. This requires further post-incident investigation, as discussed next.

Table 1: Collected data during the the DoS CAN bus attack.

Anomaly Type	Collected Data
DoS CAN bus	CAN bus traffic data CAN bus analyzer report
Camera stream alteration	Camera stream Sensor analyzer report Camera log file
GNSSspoofing	GNSS sensor raw data GNSS analyzer report Planned route GNSS log file

Post-incident investigation

After the detection and the mitigation of the DoS CAN bus attack, the stage of the post-incident investigation follows. As discussed, several anomalies have been reported, a number of attacks have been identified, and the related evidences have been collected through the nIoVe framework. AAFRT provides a graphical user interface to forensic investigators to perform a deep post-incident analysis. In the reported case study, three events of different attacks (i.e., threats) are detected and recorded: DoS attack on the CAN bus, camera stream alteration, and GNSS spoofing.

However, it is possible that they are interrelated as both the camera stream alteration and the GNSS spoofing could result from an attack on the CAN bus of the CAV, such as the DoS attack. When the CAN bus is attacked, the CAV is unable to receive important information coming from the devices connected on the CAN bus, thus it starts demonstrating abnormal behavior. For example, it may move differently than expected and the GNSS sensor will receive different data. As a result, the sensor analyzer will identify an anomaly in the GNSS data. In the case of this simulation this behavior was identified as a GNSS spoofing attack. The same could apply for the camera stream alteration that was detected by the nIoVe framework when simulating the DoS CAN bus attack.

Listing 1: Sample of CAN bus raw data (JSON format).

```
{
   "_id":{
      " $oid" : " 60 edba0 ce 62 b 1c 00130c 74 bd"
   },
   "vehicle_id":"ff630e31-50a8-4b0d-9810-eca76e1a997
   a",
   "entity_id":"53ac163d-34ef-415c-943b-1853d923b2e
   0", "entity_type":"can",
   "message_timestamp":162619239608
   9, "message_id":1626192395502,
"  source":"data_collector",
   "data":{
     "raw_data":{
      "  header":{
            " seq " : 1 ,
            " stamp" : {
               " secs " : 1626192396 ,
               " nsecs " : 78843593
            },
            " frame_id " : " vcan0 "
         },
         " id " : 501 ,
  "is_rtr":false,
      "is_extended":true,
      "is_error":false,
      "dlc":5,
      "data":[0,150,0,180,0,0,0,0]
    }
  },
  "metadata":{
    "sensor_description":"CAN BUS data from
                simulation environment
                Belle Idee Site",
    "issues":" "
  }
}
```

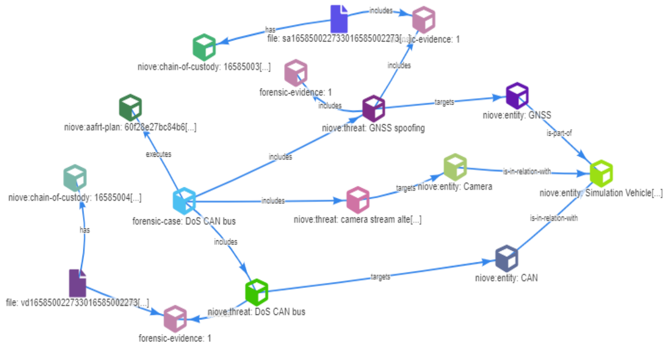

includes
has
file: sa165850022733016585002273[...]ic-evidence: 1
niove:chain-of-custody: 16585003[...]
forensic-evidence: 1
includes
includes
targets
niove:entity: GNSS
niove:aafrt-plan: 60f28e27bc84b6[...]
niove:threat: GNSS spoofing
is-part-of
executes
includes
niove:chain-of-custody: 16585004[...]
targets niove:entity: Camera
is-in-relation-with
niove:entity: Simulation Vehicle[...]
forensic-case: DoS CAN bus
includes
niove:threat: camera stream alte[...]
is-in-relation-with
has
includes
targets
niove:entity: CAN
file: vd165850022733016585002273[...]
niove:threat: DoS CAN bus
forensic-evidence: 1

Figure 3: A graph displaying information about the clustered attacks of the DoS CAN bus case study. The graph is provided by the MISP-based threat intelligence repository of AAFRT.

Therefore, the forensic investigator of the case uses the threat intelligence repository of AAFRT, based on MISP [12], to further explore and cluster the detected attacks into one major forensic case. As depicted in **Figure 3**, the forensic case includes the different attacks (DoS on the CAN bus, camera stream alteration, and GNSS spoofing). Each attack targets a specific component of the CAV: CAN bus for the DoS attack, camera device for the camera stream alteration, and GNSS sensor for the GNSS spoofing). As expected, the reported targeted components are all parts of the same CAV (i.e., the simulated vehicle of the co-simulation tool).

Moreover, the forensic case is associated with several items of forensic evidence, as presented in **Table 1**. The collected evidence is typically raw data stored in files, typically starting a few seconds before the attack happened. A sample of the raw data stored for the DoS attack on the CAN bus is provided in **Listing 1**. Apart from raw data, AAFRT also stores the analysis reports produced by the analyzers of the nIoVe framework. A sample of a CAN bus analysis report where a DoS attack has been detected is provided in Listing 2. The stored file includes all the reports that were produced since the attack started. As discussed, the forensic evidence stored for each type of attack are defined in the pre-incident stage, through the creation of the appropriate forensic readiness plans.

When these files are collected (e.g., through the automatic process supported by AAFRT), the platform generates the corresponding entry. The files are stored in a persistent volume within the nIoVe platform along with several metadata (e.g., size in bytes, checksum, encoding, compilation timestamp). Hence, the continuous availability of the collected files and data is ensured either for further analysis or for law enforcement procedures (e.g., presentation in court). Furthermore, for each file, a chain of custody is created and stored, which identifies when (i.e., timestamp) the file was changed, what was the reason of the change (e.g., updated with analysis results), what was the collection method (e.g., via network, external analysis, person), which component or who released the file (e.g., data storage), and which component or who received the file (e.g., AAFRT). As a result, AAFRT ensures not only the availability but also the integrity and the soundness of the collected forensic evidence.

Listing 2: Sample of CAN bus analysis report (JSON format).

```
{
 "_id": {
  "$oid": "62d516b6d1f40a00146571c7"
 },
 "vehicle_id": "3fa25bcb-4f96-48eb-97b4-bc9f3b1e63ba",
 "entity_id": "sensor_id",
 "entity_type": "can",
 "message_timestamp": 1658132073398,
 "message_id": 1658132073398,
 "source": "vad",
 "data": {
  "raw_data": {
   "id": "001",
   "secs": "1658132073",
   "nsecs": 398405,
   "data": "B5CF6E60AA1FFEC7",
   "bus": "vcan0"
  },
  "prediction": "0",
  "anomaly_type": "dos_CANbus",
  "f1_score": 0.99,
  "recall": 0.99
 },
 "metadata": {
  "sensor_description": "",
  "issues": "",
  "algorithm_info": "Analysed with ML algorithms."
 }
}
```

We should note that during the post-incident investigation, the AAFRT tool allows the forensic investigators to create their own file entries (e.g., files that have been acquired physically from the CAVs, files that resulted from external analysis tools) and upload them as forensic evidences in the system. The uploaded forensic evidences have the same structure and metadata as the ones that were automatically preserved. However, there is a clear distinction between these two types (i.e., automatically and manually collected/uploaded evidence) in the system.

The forensic investigator analyzes the evidence using the virtual machine provided by AAFRT, where several evidence analysis tools (e.g., Volatility, Wireshark, Sleuth Kit) are installed and available for use. After analyzing the forensic evidence, the investigator documents a full narration of the evidence gathered, the findings of the investigation, a detailed analysis supporting the findings and formulates a conclusion about the case. AAFRT supports the creation and editing of one or more investigation reports. These include the title of the report, the report, the name of the investigator, the date of the creation of the report.

Discussion

In this paper, we presented the use of the AAFRT tool for the post incident investigation of a DoS attack on the CAN bus of a simulated IoV environment. AAFRT is part of the nIoVe framework and provides a holistic approach for forensic investigation in IoV ecosystems by supporting the forensic readiness process in three stages: i) prior to the incident (by enabling the creation of forensic readiness plans for attacks, the occurrence of which cannot be predicted), ii) during the incident (for collecting and preserving volatile and non-volatile evidence when an attack is detected), and iii) after the incident (for supporting the in-depth analysis in the post-incident investigation process).

As shown in the case study of a DoS attack on the CAN bus, AAFRT leverages the ability of the IoV ecosystem to collect and preserve forensic evidence related to an attack with no human intervention. When an attack is detected, the appropriate forensic readiness policy is implemented through the proper execution of well-defined and established forensic plans. Forensic evidence is transparently collected and properly preserved. Considering the dynamic and transparent nature of the process, the forensic investigator does not need to identify when (e.g., timestamp) the attack happened, what components were targeted, or to physically access the IoV components to collect the evidence. Therefore, AAFRT makes the forensic readiness process and the collection of the evidence an effortless and automatic procedure. Apart from that, the nIoVe framework ensures that the volatile data are collected and stored, with minimal cost for the IoV ecosystem and offers the capability to conduct forensic investigations with minimal impact on the CAV and the IoV ecosystem. Finally, the forensic investigation report can be exported and used as a response to requests for digital evidence, from the internal security team of the IoV or from law enforcement agencies.

Focusing on the DoS attack on the CAN bus, we presented the ways that the forensic investigator interacted with AAFRT to draw conclusions about the attack. Despite the fact that the system detected other types of attacks, due to the collected evidence and the analysis reports provided by other nIoVe components, the investigator concluded that this was related to the DoS attack on the CAN, which requires physical access to the vehicle. Therefore, the attack could be attributed to the fact that the attacker must have gained access when the vehicle was not in service. Therefore, further investigation should be conducted to find out who had access to the vehicle when it was located at the parking lot, and thus, identify the threat actor. In case that the parking lot features CCTV, then the camera stream could also be uploaded to the forensic case as evidence through the aforementioned process.

Conclusion

In this paper, we presented a case study of using our tool for post-incident investigation of a DoS CAN bus attack. We discussed how our tool supports the steps prior, during, and after the attack, and we have shown how our tool can be used for reaching to conclusions about the incident. It is evident that our tool can be used for supporting the post-incident investigation and its major advantage is the automatic collection and preservation of the forensic evidence, as it saves a lot of time and effort during the investigation process. In addition, the related reports and the pre-processing of the evidence contributes to drawing conclusions faster following a sound procedure. Our immediate future plans include studying more attacks and drawing holistic conclusions about the utility of our tool for the post-incident investigation in IoV.

Acknowledgements

We acknowledge support of this work by the European Union (EU) Horizon 2020 research and innovation programme nIoVe: A Novel Adaptive Cybersecurity Framework for the Internet-of-Vehicles under grant agreement No 833742.

References

1. Zacharaki A, Paliokas I, Votis K, Alexakos C, Serpanos D. Complex engineering systems as an enabler for security in internet of vehicles: The nIoVe approach, in: 2019 First International Conference on Societal Automation (SA), IEEE, Danvers, MA, 2019; 1-8.

2. Alexakos C, Katsini C, Votis K, Lalas A, Tzovaras D, et al. Enabling digital forensics readiness for internet of vehicles, Transportation Research Procedia.2021; 52: 339-346.

3. Raptis GE, Katsini, C. Alexakos C. Towards automated matching of cyber threat intelligence reports based on cluster analysis in an internet of-vehicles environment. in: 2021 IEEE International Conference on Cyber Security and Resilience (CSR), IEEE, Danvers, MA, 2021; 366-371.

4. Serketzis N, Katos V, Ilioudis C, Baltatzis D, Pangalos GJ. Actionable threat intelligence for digital forensics readiness. Information and Computer Security. 2019; 27: 273-291.

5. Shalaginov A, Iqbal A, Olegård J. Iot digital forensics readiness in the edge: A roadmap for acquiring digital evidences from intelligent smart applications, in: A. Katangur, S.-C. Lin, J. Wei, S. Yang, L.-J. Zhang (Eds.), Edge Computing – EDGE 2020, Springer International Publishing, Cham, 2020; 1-17.

6. Le-Khac NA, Jacobs D, Nijhoff J, Bertens K, Choo KKR. Smart vehicle forensics: Challenges and case study. Future Generation Computer Systems. 2020; 109: 500–510.

7. Nilsson DK, Larson UE. Conducting forensic investigations of cyber attacks on automobile in-vehicle networks. International Journal of Digital Crime and Forensics (IJDCF). 2009; 1: 28-41.

8. Hossain M, Hasan R, Zawoad S, Trust-IoV: A trustworthy forensic investigation framework for the internet of vehicles (iov), in: 2017 IEEE International Congress on Internet of Things (ICIOT), IEEE, Danvers, MA, USA. 2017; 25-32.

9. Lacroix J, El-Khatib K, Akalu R. Vehicular digital forensics: What does my vehicle know about me?, in: Proceedings of the 6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications, DIVANet ’16, Association for Computing Machinery, New York, NY, USA. 2016; 59-66.

10. Feng X, Dawam E, Amin S. A new digital forensics model of smart city automated vehicles, in: 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, Danvers, MA, USA. 2017; 274-279.

11. Katsini C, Raptis GE, Alexakos C, Serpanos D. FoRePlan: Supporting digital forensics readiness planning for internet of vehicles, in: 25th Pan-Hellenic Conference on Informatics, PCI 2021, Association for Computing Machinery, New York, NY, USA. 2021; 369-374.

12. Wagner C, Dulaunoy A, Wagener G, Iklody, Misp: The design and implementation of a collaborative threat intelligence sharing platform, in: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, WISCS ’16, Association for Computing Machinery, New York, NY, USA. 2016; 49-56.