Available online at www.sciencedirect.com

ScienceDirect

Transportation Research Procedia 52 (2021) 339–346

Transportation Research Procedia

www.elsevier.com/locate/procedia

23rd EURO Working Group on Transportation Meeting, EWGT 2020, 16-18 September 2020, Paphos, Cyprus

Enabling Digital Forensics Readiness for Internet of Vehicles

Alexakos C.[a,*], Katsini C.[a], Votis K.[b], Lalas A.[b], Tzovaras D.[b], Serpanos D.[a]

[a] *Industrial Systems Institute, ATHENA RC, Patras 26504, Greece*
[b] *Information Technologies Institute, CERTH, Thessaloniki 26504, Greece*

Abstract

Vehicles nowadays are equipped with a vast amount of sensors that collect data for the vehicle and its environment. This, combined with the acceleration of the automotive industry towards interconnected and autonomous cars, suggests that security and specifically the ability to detect compromised nodes, collect and preserve evidence of an attack or malicious activities emerge as a priority in successfully deploying the Internet of Vehicle ecosystem. Until today Digital Forensics attempts are concerned with in vehicle forensics. In this paper we present the challenges of integrating digital forensics in an IoV ecosystem and we introduce the Attack Attribution and Forensics Readiness Tool of the nIoVe system, an integrated holistic cybersecurity solution for IoV.

Keywords: IoV Cybersecurity; CAV Cybersecurity; Digital Forenscics; Forensics Readiness;

1. Introduction

Modern vehicles are empowered with cutting-edge technological achievements and are capable of exchanging data with other vehicles, the infrastructure, the pedestrians, and the network. In addition, Connected Autonomous Vehicle (CAV) technology is getting closer to maturity and CAVs are capable of sensing the environment and navigating with limited or no human intervention. The vast amount of the available data of the Internet-of-Vehicles (IoV) ecosystem makes it an important source of digital forensic evidence, since it can provide detailed digitally recorded facts such as recent destinations, favorite locations, routes, or even personal data (e.g., call logs, contact lists, SMS messages, pictures, and videos) (Le-Khac et al., 2018). The nature of incidents occurred in the transportation field (accidents where the human life is in danger) makes mandate for IoV systems to provide solid and reliable forensics mechanisms which record valuable information for the post-incident operations. Unfortunately, the Internet-of-Things (IoT) and vehicle forensics are relatively new (Conti et al., 2018; Jacobs et al., 2017), in comparison to the other branches of digital forensics. Nevertheless, many researchers suggest that new approaches must be supported by the forensic-by-design concept for the development of forensic capabilities to future driverless vehicles (De La Torre et al., 2020).

* Alexakos Christos. Tel.: +30-2610-901312 ; fax: +30-2610-901300.
E-mail address: alexakos@isi.gr

2352-1465
10.1016/j.trpro.2021.01.040

Digital Forensic Readiness (DFR) is the applied and research area around the planning of the digital forensic strategies. The DFR plans are created prior the occurrence of an attack or a criminal event in order to facilitate a cost-effective and efficient investigation (Rowlingson et al., 2004). For the implementation of DFR in an organization, a systematic and complex work must take place, including the incorporation of a range of operational and infrastructural readiness strategies, such as risk assessment, staff training, tool deployment, and evaluation metrics. A survey for security policies by Grispos et al. (2013), among other findings, reports that the criteria that directly impact digital forensic readiness are *access to security data* and *protecting digital evidence*. Theoretically, there are approaches which examine frameworks that comprise dimensions such as legal and judiciary matters, governance, policy, process, people, and technology to provide organizations with a state of forensic readiness. Furthermore, Elyas et al. (2014) proposed a DFR model based on two factors: a) forensic readiness capability, whose sub-components include organizational factors and forensic strategy; and b) forensic readiness objectives, whose sub-components include regulatory compliance, legal evidence management, forensic response, and business objectives.

In this article, we present the challenges of integrating digital forensics in an IoV ecosystem and we introduce the forensics readiness tool of the Novel Adaptive Cybersecurity Framework for the Internet of Vehicles (nIoVe), an integrated holistic cybersecurity solution for IoV. The Attack Attribution and Forensics Readiness Tool (AAFRT) of nIoVe aims to ensure that necessary forensic information can be collected and used as a knowledge base about the cyberattacks in CAVs and IoV ecosystem. nIoVe forensics readiness tool provides instant access to the forensically relevant data collected from networking endpoints through continuous monitoring and analysis of all network traffic (connected and autonomous vehicles, connected electronic control units, etc.,), including internal network traffic, internet-bound traffic and internal traffic between physical and virtual hosts including traffic between virtual workloads.

The rest of the paper is organized as follows. We first review the related work and identify the gap in the literature. Then, we discuss the challenges of integrating digital forensics in an IoV ecosystem, we introduce the nIoVe system, and present the architecture of the forensics readiness tool. Finally, we provide a discussion about our approach and conclude the paper.

2. Related Work

Digital forensics has received a lot of research attention in the past decade. Different approaches have been used for describing the Forensics Readiness (FR) processes. For example, Alharbi et al. (2011) categorized the FR processes in proactive and reactive through reviewing and mapping the processes that existed in digital FR at the time. Elyas et al. (2014) proposed a framework for organizing Digital Forensics Readiness (DFR) which consists of two components, namely the digital forensics factors and the capabilities, which include both technical and non-technical factors. Valjarevic and Venter (2013) proposed a harmonized model for implementing Digital Forensics Investigation Readiness processes (DFIRP), which was adopted by ISO/IEC 27043:2015. Their model consists of three component processes: planning, implementation, and assessment, which can be used for deploying DFR in organizations.

As cloud computing matured, the research attention focused on achieving DFR on the cloud. Thus, a number of frameworks were proposed mainly for Infrastructure-as-a-Service (IaaS) environments because they give the required control to the cloud users compared to Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) ones. De Marco et al. (2013) proposed Cloud Forensic Readiness System (CFRS) for implementing FR in the cloud. The system consists of three activities: the collection, the storage, and the management of the data. Data is collected from tools (e.g., file activity monitoring), artifacts (e.g., images of virtual machines) and logs (e.g., audit logs). The storage activity is responsible for preserving the data and management preform the forensics analysis and knowledge extraction for reconstructing the timeline of the incident. Dykstra and Sherman (2013) introduced FROST, a digital forensic tool for OpenStack cloud platform. The platform is suitable for IaaS environments. The advantage of FROST lies in that data is collected at the host operating system, thus data acquisition does not require the intervention of the cloud provider but they raise the challenge of preserving data in an investigation until that data can be identified and retrieved. They also emphasized the importance of trust in the cloud services. Kebande and Venter (2015) proposed Cloud Forensic Readiness Evidence Analysis System (CFREAS), which aims to reduce analysis time of large-scale evidence. Their approach is based on the MapReduce paradigm which enables processing of large sets of data without requiring the modification of the existing architecture. They acknowledge the challenges of the proposed approach

including the threat of preserving the chain of custody on the cloud and the lack a centralized legal authority. In 2017, the same team proposed an agent-based solution for digital forensics readiness in the cloud, which was aligned with ISO/IEC 27043:2015, and enabled conducting forensics investigation without disrupting cloud operations (Kebande and Venter, 2018).

In 2017, Alenezi et al. (2017) proposed a framework for cloud forensic readiness in organizations which included technical, legal, and organizational factors that affect digital forensic readiness. They also underpin the importance of proactively collecting data before the occurrence of the incident to save time, money, and effort. Park et al. (2018) proposed a readiness model for digital forensic readiness measurement in the cloud computing-based smart work environment, which consists of two components: the policy readiness component and the technical readiness component. The model offers flexibility as it can be adapted to any work environment and can be used in designing proactive counterstrategy before the occurrence of the incident. Sibiya et al. (2013) proposed a forensic readiness model that uses a forensic service hosted in the cloud, which aims to facilitate digital forensic readiness and minimize the cost of conducting forensics investigation in a distributed environment. Trenwith and Venter (2013) proposed a model that considered centralised logging of all activities within the cloud in as a method for proactive forensic readiness.

Ab Rahman et al. (2016) proposed a forensic-by-design model for cyber-physical systems which includes six factors: risk management principles and practices, forensic readiness principles and practices, incident handling principles and practices, laws and regulation, cyber-physical cloud systems (CPCS) hardware and software requirements, and industry-specific requirements.

The discussed models are concerned with achieving digital forensics readiness mainly for organizations in the cloud. IoV is an emerging ecosystem where data is collected and shared within the vehicle, vehicle-to-vehicle, vehicle-to-infrastructure, and vehicle-to-everything. The heterogeneity of the available stand-alone computing devices (different electronic modules, configurations, and interactions) which work together in a network, constitutes essential the development of a digital forensics readiness model. The model will enable the collection of the necessary forensic information which can be used both for providing forensic reports, but also for building a knowledge base about cyber-attacks in CAVs and the IoV ecosystem.

3. Forensics Readiness Architecture for IoV

3.1. Challenges of integrating digital forensics in IoV

IoV is a dynamic ecosystem which includes Vehicle-to-Vehicle (V2V) communication, Vehicle-to-Infrastructure (V2I) communication, Vehicle-to-Network (V2N) communication and Vehicle-to-Pedestrian (V2P) communication. Compared to other IoT systems, it is a more challenging environment, since it features dynamic topological structures, a huge network scale, non-uniform distribution of nodes, complex granularities, and mobile limitation (Sun et al., 2017) . If an intrusion happens in IoV, attackers may take control of vehicles which could lead to accidents and even loss of human lives. Therefore, forensics readiness is necessary not only for presenting evidence to court but also for ensuring IoV is capable of handling attacks and developing mitigation strategies. In this section, we identify and present the challenges of integrating digital forensics in an IoV ecosystem:

- *Heterogeneity of data*: In an IoV ecosystem, there is a vast amount of data sources, both in-vehicle and infrastructure. This suggests that there is no standard and the data must be modelled in a manner that they are forensically sound. In addition, there is huge amount of the available data, and it is therefore of major importance to identify, collect, analyze, and preserve only those essential for digital forensics.
- *Chain of custody*: Another major challenge of the IoV ecosystem is that the network changes dynamically and the nodes are not uniformly distributed. In such a dynamic network, maintaining the chain of custody is challenging, given that the majority of the nodes are not storing any metadata, especially temporal information.
- *Forensically sound evidence*: Most often, manufacturers are not willing to provide open access to the in-vehicle collected data (e.g., due to intellectual property or competition concerns), which introduces a major concern in regards to collecting, analyzing, and preserving forensically sound evidence. The vehicles are constructed in different countries which are governed by different laws which introduces the challenge of acquiring in-vehicle data.

- *Privacy*: In the IoV ecosystem, privacy is key in terms of what types of data are collected and who has access to this data, given that most of the data contains personal information.

3.2. The nIoVe framework

nIoVe is a cybersecurity framework for the IoV ecosystem and enables the identification of risks associated with the IoV networks, the recognition of suspicious threat patterns, and the appropriate coordinated mitigation actions in order to pertain vehicle safety and security. In addition, it offers real time anomaly detection in the data fusion and analysis tool along with response against cyberattacks and recover strategies. AAFRT lies between the data fusion and analysis tool and the response and recover tools and it is responsible for collecting, analyzing, and preserving evidence and for enabling event reconstruction.

3.3. Architecture of forensic readiness for IoV

The architecture of the AAFRT tool for IoV follows a harmonized process model for digital forensic investigation readiness proposed by Valjarevic and Venter (2013) and has been adapted by ISO/IEC 27043:2015 encompassing three processes groups for DFR:

- *Identify potential evidence sources*: The identified evidence sources could include application and systems logs, and events derived from physical system sensors.
- *Plan pre-incident collection*: Definition of strategies for collecting raw evidence data. This strategy is implemented by sub-systems which apart from data collection, they can automatically send event metadata to a forensic database, such as risk assessment evaluation, attack attribution, etc.
- *Define storage and evidence handling*: A centralized and securely configured forensic database can store collected evidential data.
- *Plan pre-incident analysis*: Definition of strategies and tools to detect incidents by analyzing data, such as intrusion detection systems, log monitoring, and security information and event management systems.
- *Plan incident detection*: This activity, typically part of the digital investigation procedure, involves identifying actions to be undertaken after the incident has occurred or has been detected. Important factor in this procedure is the forensic responsibility boundary, that must be studied and defined carefully.

The forensic readiness process is initiated after detecting an anomaly, performing risk assessment analysis and classifying the anomaly as high-risk in the IoV system. The forensic readiness in the IoV system serves a dual purpose:

1. It is responsible to identify the characteristics of the attack for gaining useful insights of the attack. This knowledge contributes to the classification of attack's attributes to known vulnerabilities, which permits the appropriate engagement of response activities that lead to the successful mitigation of the attack.
2. It implements the basic DFR mechanism of the nIoVe security framework. This mechanism aims to ensure that necessary forensic information can be collected and used as knowledge base about the cyber-attacks in CAVs and the IoV ecosystem. Attack attribution provides the necessary information for the selection of the appropriate DFR plans that must be executed in order to facilitate a cost-effective and efficient investigation.

3.3.1. DFR modules

The forensic readiness physically is implemented through a software application installed inside the nIoVe framework. It mainly interacts with the other components of the nIoVe framework. Furthermore, there are two human-computer interfaces for the administrators and cybersecurity personnel. Their purpose is for the editing of forensics readiness plans, the assessment of a selected forensics strategy. The physical view of the forensic readiness architecture is depicted in Fig. 1.

From the view of system architecture, the AAFRT tool is an integrated systems consisting of functional modules/blocks and interfaces with the other systems of nIoVe framework. The main components of the AAFRT architecture, as depicted in Fig. 2, are the following:

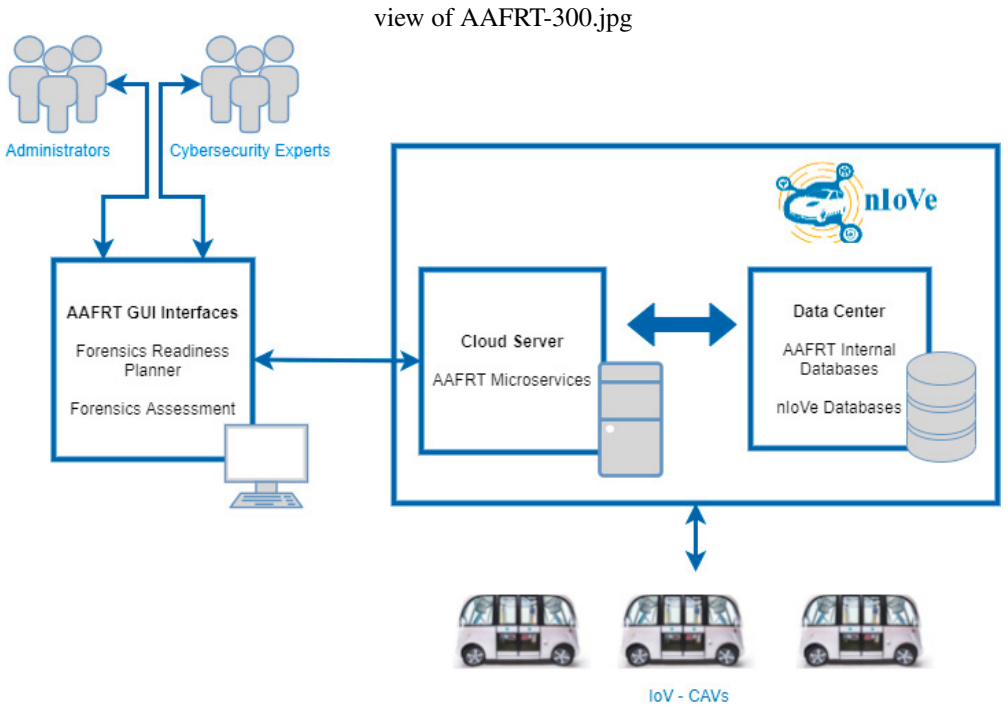

Fig. 1. Physical view of forensics readiness architecture of the IoV ecosystem.

- *Attack Attribution Module*: This module is responsible for attributing the attack. It receives an event after an anomaly detection in the IoV system followed by its risk assessment. Afterwards, it initiates the attack attribution procedure. The module acquires additional information from the Threat Intelligence Repository and from the rest of the IoV system. It is responsible for processing the information, identifying specific characteristics of the attack, such as type of known attack, IoV components that are affected, possible attack propagation, etc. The outcome of the attack attribution is forwarded to the Forensic Readiness Planning component and the Response Toolkit for the selection of the appropriate digital forensics plan and the suitable response strategy.
- *Forensic Readiness Planning*: This module is responsible to decide the most suitable digital forensics plan for the collection of evidence-related data, after an incident has been detected and the attack has been attributed. The plan is composed as a set of activities called digital forensic activities, the description of these activities is stored in the Forensic Readiness Plans Repository, an internal database of the system. The goal of this module is to prepare for an event whose occurrence cannot be predicted, and ensure the minimization of the cost of response, recovery, and investigation without interrupting the IoV ecosystem.
- *Forensics Strategy Orchestrator*: This module is responsible to execute the activities of the forensics plan, which was composed in the Forensic Readiness Planning component. It consists of two major sub-modules: a) the Data Acquisition, which is an interface with the rest of IoV infrastructure and it executes the collection of the incident's data according to the forensics plan's activities; and b) the Digital Preservation, where the collected data is timestamped for safe storage to the Forensics Database. The Data Acquisition sub-module collects both network data and host data. The Digital Preservation module is responsible for preserving the chain of custody and the integrity of the evidence.
- *Forensic Readiness Planner*: This module provides a graphical user interface to the administrators in order to manage the forensics plans and activities. Through a usable and secure interface, it enables the administrators to view, create, alter, or delete plans and activities.
- *Forensics Assessment*: This module consists of a graphical user interface providing two services: a) The reconstruction of the event, based on the collected data related to the evidence for investigation purposes; and b) the assessment of the selected forensics strategy from experts. This assessment will provide points of failure or lack

of AAFRT-300.jpg

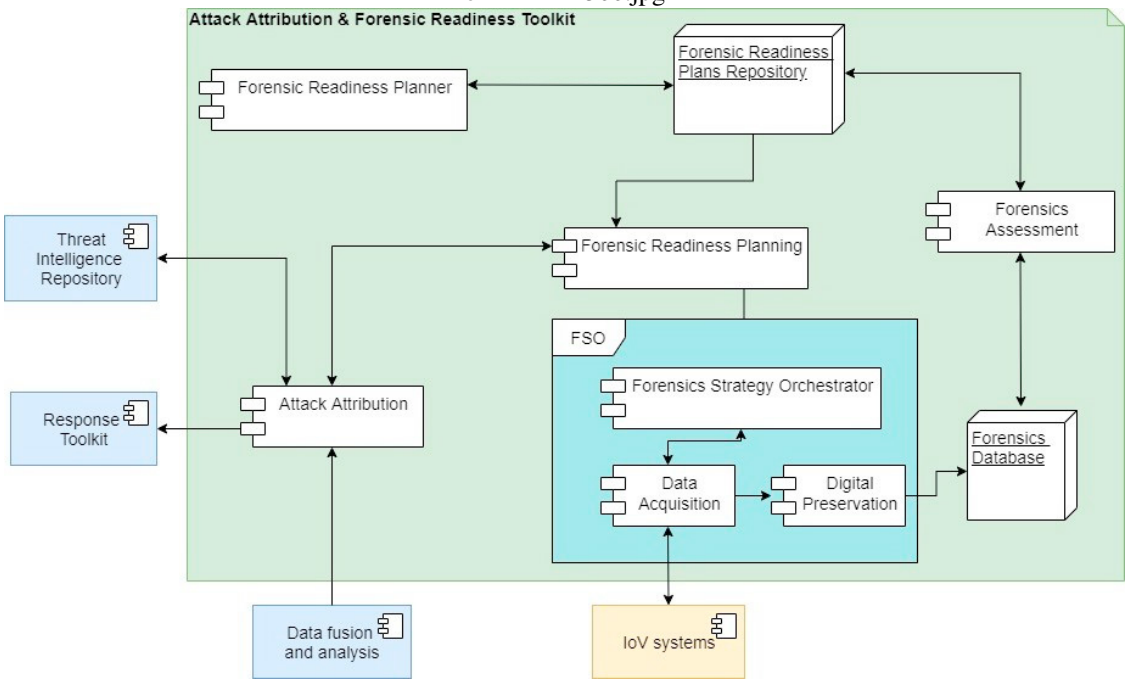

Fig. 2. Architecture of forensics readiness for the IoV ecosystem.

of valuable information, which will lead to the improvements of the forensics readiness plans. The assessment results are sent to the Threat Intelligence Repository for update.

3.3.2. DFR process

The described modules are connected by the DFR process presented in Fig. 3. The Attack Attribution module gets the detected anomaly along with the outcome of the risk assessment from the data fusion and analysis subsystem of the IoV ecosystem. The module requests threat related data from the Threat Intelligent Repository in order to analyze the data and attribute the attack. The result of the analysis is provided to the another subsystem of the IoV ecosystem, the Response Toolkit and to the Forensics Readiness Planning (FRP) module. The FRP module retrieves the plans for the Forensics Readiness Plans repository and composes a DFR plan appropriate for the attributed attack. The DFR plan is then passed to the Forensics Strategy Orchestrator, which is responsible for executing the DFR plan. The Data Acquisition sub-module is triggered to request the related incident data from the IoV ecosystem. The IoV ecosystem provides the data to the Data Acquisition sub-module which in turn provides the data to the Digital Preservation sub-module. In the Digital Preservation sub-module the data are processed for preservation and then saved to the Forensics Database. The Forensics Assessment module can trigger two actions. The event reconstruction and the forensics assessment. The results of the Forensics Assessment module are fed in to the Threat Intelligent repository.

4. Discussion

The forensics readiness architecture we propose in this paper is part of a larger cybersecurity solution of the nIoVe Framework. Its purpose is twofold: From a legal point of view, it provides forensically sound data and enables the preservation and reconstruction of an event so that it can be presented at court. Apart from that, from a technological point of view, the outcome of the forensic readiness process is stored in the Threat Intelligent repository, and can be used not only for identifying future attacks, but also for adopting appropriate intrusion avoidance strategies. Therefore, it is of paramount importance, once an anomaly is detected to be able to attribute the attack, compose, and execute a

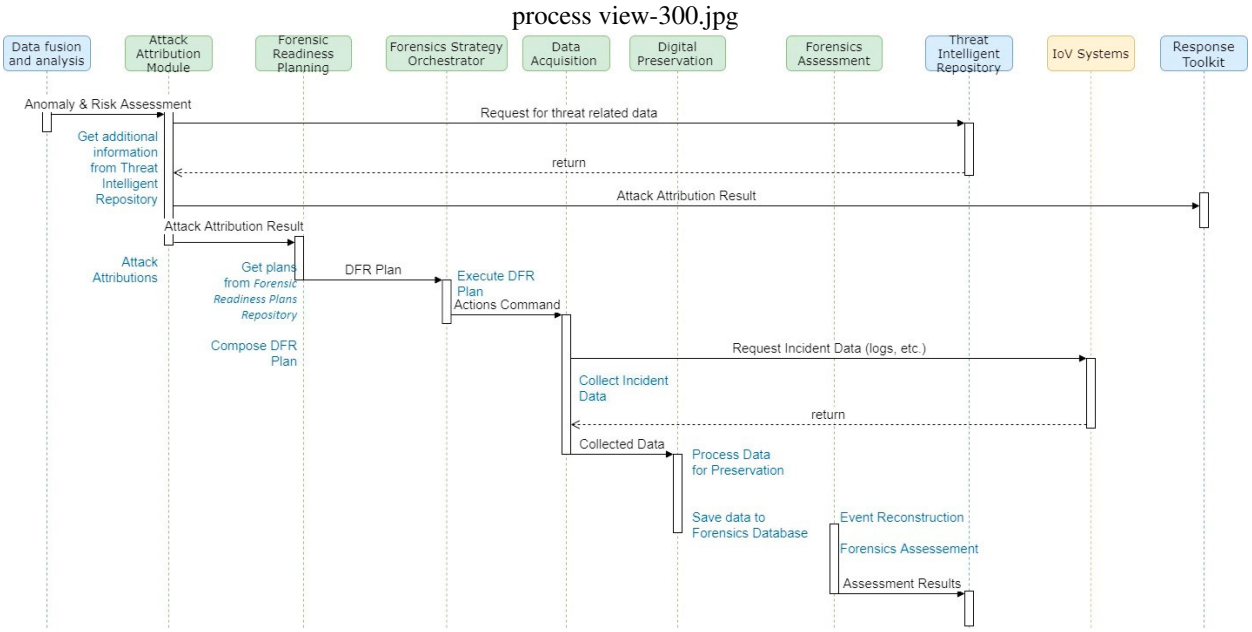

Fig. 3. Process view of forensics readiness for the IoV ecosystem.

forensics readiness plan and assess the outcome. The timing is a very crucial parameter and what should be considered is whether the necessary data is available after an anomaly is detected so that it can be collected by a forensics readiness tool and whether it is possible to go back to a previous safe state in an IoV ecosystem.

5. Conclusion

The main aim of this paper was to provide the basis for a DFR architecture in CAVs and IoV ecosystem. We discussed the challenges of integrating digital forensics in such systems including the heterogeneity of the data, the difficulties associated with maintaining the chain of custody, collecting forensically sound evidence, and the privacy issues raised. We introduced the architecture of the AAFRT tool for the nIoVe system which consists of five modules and we provided a process view of the architecture. AAFRT is under continuous development, upgrading its modules with additional capabilities. The current prototype is tested in simple network attacks, such as denial of service (DoS) in the Vehicle-to-Infrastructure communications. The next steps include the adaptation of malware detection platform for the identification of attacks in the software components and interfaces with other tools, such as visual analytics tools that can assist both the attack attribution and the investigation of an event. Finally, the overall nIoVe framework will be validated under physical and virtual pilot scenarios.

The network analysis showed that the proposed approach is feasible and applicable, but more challenges are expected in the next versions (i.e. malware analysis) where the implementation limits will be tested. As we move inside the CAV systems, we will find embedded proprietary systems and sensors. The challenge there will be the in depth collection of data, such as memory dumps, file system history, and access logs, which is difficult to be obtained, especially by closed proprietary systems. In this case, the analysis must be based on the available data, and the attack investigation and assessment must be provide a holistic presentation of system's behaviour during an incident.

Another issue that considers the applicability of the proposed approach is the data privacy and the related regulations. nIoVe project will follow an integrated approach for the alignment of the operation of all the components to national and international laws, with focus on the EU's General Personal Data Protect Regulation (GPDR). This is an undergoing work and its results will be integrated in the AAFRT.

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 and also the European Union (EU) Horizon 2020 research and innovation programme CONCORDIA: Cyber security cOmpeteNce fOr Research anD Innovation under grant agreement No 830927.

References

Ab Rahman, N.H., Glisson, W.B., Yang, Y., Choo, K.K.R., 2016. Forensic-by-design framework for cyber-physical cloud systems. IEEE Cloud Computing 3, 50–59.

Alenezi, A., Hussein, R.K., Walters, R.J., Wills, G.B., 2017. A framework for cloud forensic readiness in organizations, in: 2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), IEEE. pp. 199–204.

Alharbi, S., Weber-Jahnke, J., Traore, I., 2011. The proactive and reactive digital forensics investigation process: A systematic literature review, in: International Conference on Information Security and Assurance, Springer. pp. 87–100.

Conti, M., Dehghantanha, A., Franke, K., Watson, S., 2018. Internet of things security and forensics: Challenges and opportunities.

De La Torre, G., Rad, P., Choo, K.K.R., 2020. Driverless vehicle security: Challenges and future research opportunities. Future Generation Computer Systems 108, 1092–1111.

De Marco, L., Kechadi, M.T., Ferrucci, F., 2013. Cloud forensic readiness: Foundations, in: International Conference on Digital Forensics and Cyber Crime, Springer. pp. 237–244.

Dykstra, J., Sherman, A.T., 2013. Design and implementation of frost: Digital forensic tools for the openstack cloud computing platform. Digital Investigation 10, S87–S95.

Elyas, M., Maynard, S.B., Ahmad, A., Lonie, A., 2014. Towards a systemic framework for digital forensic readiness. Journal of Computer Information Systems 54, 97–105.

Grispos, G., Glisson, W.B., Storer, T., 2013. Cloud security challenges: Investigating policies, standards, and guidelines in a fortune 500 organization. arXiv preprint arXiv:1306.2477 .

Jacobs, D., Choo, K.K.R., Kechadi, M.T., Le-Khac, N.A., 2017. Volkswagen car entertainment system forensics, in: 2017 IEEE Trustcom/BigDataSE/ICESS, IEEE. pp. 699–705.

Kebande, V., Venter, H., 2015. A functional architecture for cloud forensic readiness large-scale potential digital evidence analysis, in: European Conference on Cyber Warfare and Security, Academic Conferences International Limited. p. 373.

Kebande, V.R., Venter, H.S., 2018. Novel digital forensic readiness technique in the cloud environment. Australian Journal of Forensic Sciences 50, 552–591.

Le-Khac, N.A., Jacobs, D., Nijhoff, J., Bertens, K., Choo, K.K.R., 2018. Smart vehicle forensics: Challenges and case study. Future Generation Computer Systems .

Park, S., Kim, Y., Park, G., Na, O., Chang, H., 2018. Research on digital forensic readiness design in a cloud computing-based smart work environment. Sustainability 10, 1203.

Rowlingson, R., et al., 2004. A ten step process for forensic readiness. International Journal of Digital Evidence 2, 1–28.

Sibiya, G., Fogwill, T., Venter, H.S., Ngobeni, S., 2013. Digital forensic readiness in a cloud environment, in: 2013 Africon, IEEE. pp. 1–5.

Sun, Y., Wu, L., Wu, S., Li, S., Zhang, T., Zhang, L., Xu, J., Xiong, Y., Cui, X., 2017. Attacks and countermeasures in the internet of vehicles. Annals of Telecommunications 72, 283–295.

Trenwith, P.M., Venter, H.S., 2013. Digital forensic readiness in the cloud, in: 2013 Information Security for South Africa, IEEE. pp. 1–5.

Valjarevic, A., Venter, H., 2013. A harmonized process model for digital forensic investigation readiness, in: IFIP International Conference on Digital Forensics, Springer. pp. 67–82.