Identification of Automotive Digital Forensics Stakeholders

Kevin Gomez Buquerin
C-ECOS
Technical University Ingolstadt
Ingolstadt, Germany
e-mail: extern.kevinklaus.gomezbuquerin@thi.de

Hans-Joachim Hof
C-ECOS
Technical University Ingolstadt
Ingolstadt, Germany
e-mail: hof@thi.de

***Abstract*—New technologies and features emerging in modern vehicles are widening the attack surface for malicious tampering. As a result, security incidents including vehicles are on the rise. Automotive digital forensics investigations allow resolving such security incidents. This paper presents a stakeholder-based reference model for automotive digital forensics. It is essential to focus on stakeholders to provide the best possible automotive digital forensics investigation for them. We identified twelve distinct stakeholders relevant to automotive digital forensics and assigned them to the vehicle life-cycle's relevant phases. Furthermore, the stakeholders' questions for forensics investigations and their resources get analyzed. We created a Venn diagram to highlight differences and similarities between the stakeholders.**

***Keywords*—automotive; digital forensics; forensic; cyber security; embedded; vehicle; car; automobile; stakeholder**

I. Introduction

Features, such as car sharing or function-on-demand determine the design of modern vehicles. These use-cases are very attractive to customers. However, they allow cyber criminals to abuse novel use-cases for malicious purposes. Automotive Digital Forensics (ADF) must efficiently investigate and resolve resulting security incidents.

Vehicle manufacturer spend additional resources in security features and technologies. New security regulations such as the UNECE [12] or ISO-21434 [13] set new requirements for secure automotive systems and development of such. This change in the automotive domain, leads to additional stakeholders such as the UNECE approval authority. Also, the automotive industry sees a switch of focus from existing stakeholders in ADF. Addressing the needs and capabilities of stakeholders is important to ensure the best possible ADF investigation. This paper reports about our research on the questions: "*Which are ADF stakeholders?*" and " *What forensic questions are they interested in?*". The research on these questions contributes the following items:

- A list of twelve unique ADF stakeholders.
- Forensic questions asked by and relevant for ADF stakeholders.
- Forensic resources available to ADF stakeholders.
- Position of the ADF stakeholders in the vehicle life-cycle.
- A comparison between the ADF stakeholders based on defined close curves in a Venn diagram.

The paper is structured as follows: Section 2 presents related work on ADF and argues, why our work is unique. Section 3 provides a useful definition of ADF stakeholders. Section 4 summarizes methods to identify and describe ADF stakeholders. Section 5 presents the main contribution of our paper—the ADF stakeholders identified in our work. Section 6 elaborates differences in similarities of the identified stakeholders. Section 7 evaluates the quality of the identification of the stakeholders and shows, that indeed all relevant stakeholders were identified. Section 8 concludes the paper and gives an outlook on future work.

II. Related Work

Several scientists from academy and industry already published research on ADF. Only a minority of papers focus on stakeholders or interest groups of the technologies and methods.

Armstrong [5] defines stakeholder groups in Digital Forensics (DF) programs and evaluated a bias for each towards their aim for prosecution. The author presents the victim group and associates, law enforcement, forensic scientists and experts, witnesses, perpetrator group and associates of the perpetrator, judiciary, technology providers, media, and the public as relevant stakeholders. Based on these groups, requirements for the program are defined. Furthermore, the author captures differences and similar interests between the groups. As a result, the DF programs are implemented based on the input collected from the primary users.

Al Fahdi et al. [6] interviewed different stakeholders to determine future challenges in DF. Based on those, the most relevant areas of research are defined. The paper identifies two distinct stakeholder groups, forensic researchers and practitioners. The authors list three top challenges for these stakeholders: cloud computing, anti-forensics, and encryption.

Mansor [4] presents automotive stakeholders in the area of security. The paper lists attack motivations, methods, and capabilities for each stakeholder. Based on this, a comprehensive understanding of each stakeholder is available. The authors define five stakeholder groups: Original Equipment Manufacturers (OEMs), users (e. g., car owner and drivers), service provides (e. g., dealers and workshops), insurance providers, and hackers (e. g., researchers, technical

 ISBN: 978-1-61208-919-5

enthusiasts, thieves, and OEM competitors).

All available research focuses on general and offensive automotive security. To the best of our knowledge, we are the first to present stakeholders in the automotive domain for ADF and general defense techniques. However, a solid understanding of stakeholders in the automotive domain is of uttermost importance for the design and development of sufficient technologies and methods for ADF investigations.

III. Definition of Automotive Digital Forensics Stakeholders

ADF utilizes DF techniques and methods within vehicular systems and the supporting infrastructure. It includes different data types and data sources. We define automotive systems as components installed in vehicles such as Electronic Control Units (ECUs) and modules connected to the vehicle such as manufacturer's backend, smartphones, or Vehicle to X (V2X) devices. X can be other vehicles, infrastructure components, smartphones, smart-home, backend-systems, and more. ADF includes many tasks, ranging from quickly collecting data from an in-vehicle black-box to in-depth analysis such as embedded forensics techniques. The general goal of ADF is answering questions asked by the entity that requests forensic investigation (vulgo stakeholder). The questions (6 WH's) include: *How*, *Why*, *Where*, *When*, *Who*, and *What*.

Freeman and Reed present two methods to define stakeholders. According to them, stakeholders are a "*group or [an] individual who can affect the achievement of an organization's objectives or who is affected by the achievement of an organization's objectives*" [1] or stakeholders are a "*group or [an] individual on which the organization is dependent for this continued survival*" [1]. Based on these definitions, the relevance for ADF stakeholders can be defined: "*ADF stakeholders are relevant if they have a significant negative or positive influence on digital forensics in the automotive sector. This includes in-vehicle systems and their supporting infrastructure.*".

IV. Identification and Description of Automotive Digital Forensics Stakeholders

Bryson [2] presents multiple methods to identify and analyze stakeholders. He introduces two identification methods. The first method is a brainstorming technique, having multiple people determine relevant stakeholders. Bryson suggests to involve people which have "*information that cannot be gained otherwise*" [2], to ensure that the determined stakeholders are the most relevant for the specific domain. The second method is a snow-ball technique that is based on King et al. [10]. Each identified stakeholder gets contacted and asked to lists other potential stakeholders. This method utilizes the experience and knowledge of existing stakeholders and allows the initial determination of stakeholders to be general and incomplete.

Bryson presents multiple analysis methods. It contains power-versus-interests grids that show the level of interest on the X-axis and the level of power on the Y-axis. The method allows to determine crowds, subjects, context setters, and players in the different quadrants. In addition, Bryson constitutes stakeholder influence diagrams that expand on power-versus-interests grids. Here, lines are drawn between identified stakeholders and interest flows as well as directions of interests are identified. Influence diagrams allow to determine the most important stakeholders of a group.

We decided to use the brainstorming technique. The snow-ball method is neglected as it is not feasible for groups such as criminals and government organizations. In addition, no stakeholder analysis is performed. This research does not focus on public value or business interest for an ADF company. Instead, this work focuses on identifying stakeholders, including their interests in, resources for, and potential impact on ADF.

Three different groups of attendees for the brainstorming session were selected. First, from academia with a focus on automotive security, second vehicle manufacturer staff working in automotive security, and third a mixed session including automotive security researchers, vehicle manufacturer staff, car owners, supplier staff, and insurer staff. As a result, the different groups consist of car owners, a professor, PhD students, OEM employees, tier one supplier employees, and insurer employees.

There are multiple possibilities to describe ADF stakeholders. A bare listing of stakeholders is likely to be unclear and incomplete, and a reference to the automotive domain may not be evident. Hence, this work categorizes stakeholders based on the vehicle life-cycle that are *production*, *use*, and *end-of-life* [3]. The importance of ADF for a stakeholder is associated with the progression of the vehicle life-cycle. The advantage of such a categorization is the focus on ADF during specific steps of the manufacturing process. Our method is open to integration of additional stakeholders and to the adaption of existing collaborators in the future. To describe stakeholders, we use the following properties:

- The position in the vehicle life-cycle describes the stage in which the stakeholders has an impact on the vehicle or a focus on ADF.
- The stakeholders interests and exemplary forensic questions regarding the 6 WH's of DF.
- Resources available to the stakeholder. Capabilities of the stakeholder to perform or assist ADF investigations. Resources includes hardware, software, documentation, and experience.
- Examples for the stakeholder group.

We select a Venn diagram to visually present different stakeholders. Venn diagrams allow to easily recognize similarities as well as differences. Based on the brainstorming sessions, we identified different interests and focus areas of the stakeholder. Based on those, three closed curves are defined: *Trustworthiness, Functionality, and Law* as A. *Protection and Security* as B. *Misuse, Tampering, and Hacking* as C. Stakeholders in the closed curve A focus on trustworthiness and functionality of the vehicle systems. Furthermore, their interest is in fulfillment of regulations. Protection of the intellectual property as well

 ISBN: 978-1-61208-919-5

as ensuring security of the automotive systems do group stakeholders in B. Closed curve C comprises stakeholders that try to misuse, tamper with, and hack automotive systems.

V. Automotive Digital Forensics Stakeholder

Three brainstorming sessions were performed. All are based on Bryson's methodology presented in [2]. Within **session one**, one professor, four PhD students, and one master student were involved. The professor as well as all students are part of an automotive security research group at an university. Four PhD students with a focus on automotive security as well as two OEM employees and one tier one employee participated in the **second session**. **Session three** included one insurer employee, one tier one employee, two OEM employees, and two PhD students. All participants work in the area of automotive security and are car owners or business car users. We decided to have three brainstorming sessions in order to involve various relevant participants and stakeholders from different areas. All stated participants contribute to one session only. Further, PhD students as well as other contributors are not the same.

The following paragraphs present the identified stakeholders. Furthermore, forensic questions of the stakeholders, their position in the vehicle life-cycle and examples are presented. All results are from the brainstorming sessions.

a) OEM: OEMs are located in the *production* (vehicle development) as well as *use* (maintenance and sale of spare parts) phase of the vehicle life-cycle. OEMs are interested in identifying issues in their products. Forensic questions concern, among other things, the clarification of guilt questions such as "*Did a vehicle system cause the accident?*" or of legal questions such as "*Was there an inadequate handling of personal data in the vehicle?*". Due to the development background and the system knowledge, there are effects on vehicle development. In addition, OEMs have access to internal information of the vehicles that is valuable in digital forensic investigations (e. g., manufacturer-specific Unified Diagnostic Services (UDS) identifiers). Examples are Audi, BMW, Daimler, Tesla, and Toyota.

b) Business car owner: Business car owners own a fleet of vehicles. The position in the vehicle life-cycle lies in the *use* phase. They are interested in protecting employee data and in low insurance costs. Forensic questions include "*Was the driver or the vehicle to blame in the accident?*" or "*Who extracted the personal data from the vehicle?*". Business car owners have no system knowledge and sometimes use additional devices such as digital logbooks. Examples are companies such as Telekom or the police that own a vehicle fleet.

c) Private car owner: Private car owners have no additional resources to conduct ADF investigations. They *use* the car and are interested in the protection of personal data such as the travel route. Private car owners could also utilize ADF investigations to determine why their car is no longer reliable (e. g., a vulnerable device is installed and not properly patched). Examples are people who own a vehicle.

d) Supplier: Suppliers support the OEM in the development of vehicle components and functions during the *production* phase. This gives them partial system knowledge. However, this knowledge is very deep because a supplier implements certain subsystems. ADF supports suppliers in troubleshooting and resolving issues during investigations. In addition, suppliers have manufacturer-specific information (e. g., manufacturer-specific UDS identifiers). Examples are Continental, Bosch, and Faurecia.

e) Mobility provider: Mobility providers are in the *use* phase of the vehicle life-cycle. They protect their intellectual property and the personal data of their customers. Forensic questions are similar to those of the business car owner, such as "*Was the accident caused by the customer or the vehicle?*" or "*Who extracted the personal data from the vehicle?*". Due to additional components such as tracking devices or tachographs, mobility providers sometimes have system knowledge. Examples are SIXT, Hertz, and DriveNow.

f) Legal institution: Legal institutions own official testers, maintenance equipment, and contracts with the manufacturer to carry out tests on vehicles. They use these resources to determine whether laws and regulations are being followed, which can lead to ADF investigations. They also offer services such as the extraction of Diagnostic Trouble Codes (DTCs). Legal institutions are located in the *production* and *end of life* phase of the vehicle life-cycle. Examples are the German TÜV, independent workshops, and the Federal Motor Transport Authority.

g) Government organization: Government organizations have an influence on ADF in the *use* and *end of life* phase. They protect vehicles with a sovereign role (e. g., the government fleet). ADF questions include "*Has the vehicle been compromised?*" and "*What data was collected by vehicle systems?*". System knowledge is available by requesting necessary information from the manufacturer. In addition, there are special agreements on compliance with laws when the safety of vehicles with sovereign issues is affected. Examples are BND, NSA, CIA, MI5, and Mossad.

h) Insurer: Insurers affects ADF in the *use* phase of the vehicle life-cycle. They tend to determine whether the status of the vehicle permits registration and assess the insurance coverage. ADF questions are but are not limited to "*Has the vehicle accelerated by itself?*" and "*Has the vehicle been manipulated (tuned)?*". System knowledge is partly given through the cooperation with manufacturers. Examples are DEKRA or Allianz.

i) Criminal: Criminals concentrate on ADF in the *production* and *use* phases of the vehicle life-cycle. They aim to activate chargeable services and products. In addition, criminals disable immobilizers and steal intellectual property or personal data. ADF questions include "*What personal information can be stolen*" and "*What intellectual property can be collected?*". Their system knowledge varies between threat actors. Advanced attackers can be very skilled.

j) Tuner: Tuners are in the *use* phase of the vehicle life-cycle. Their goal is to achieve increases in performance and

 ISBN: 978-1-61208-919-5

to carry out vehicle configurations. Therefore, ADF questions could be "*Where can you find specific information about a functionality in the vehicle?*" and "*Where is the configuration of the engine stored?*". Their system knowledge is high and there is networking as well as cooperation between the tuners. Hardware for communication with the vehicle is also available. Examples are Brabus, MTM, and MHD.

k) Researcher: Researchers are in the *use* phase of the vehicle life-cycle. Their aim is to carry out scientific research on vehicles and, for example, to identify problems within vehicle components. ADF questions include "*Which personal data are stored by modern vehicles*" and "*Which components contain forensically relevant data?*". System knowledge may be available. It is determined by open source resources and reverse engineering of components. The researchers are networked through conferences and publications. Examples are academic researchers, private researchers, and penetration testers.

l) Approval authority: Approval authorities position themselves in all three phases of the vehicle life-cycle. They determine the fulfillment of legal requirements. New regulations such as UNECE place demands on automotive security, security development, and forensics. An example for a model based security framework is presented by Volkersdorfer and Hof in [11]. Such research directly addresses challenges in security development and testing for modern automotive systems. ADF questions include "*Is personal data stored and protected in the vehicle?*" and "*What information is stored in vehicle systems?*". Approval authorities have no system knowledge. However, there is close cooperation with the manufacturers and they can collect documentation for components. One example is the approval authority for the UNECE standard.

VI. Comparison of the Automotive Digital Forensics Stakeholder

To visualize all presented ADF stakeholders, a Venn diagram is created and presented in Figure 1. This research focuses on the main interests and areas of focus in ADF of the shown stakeholders. The results come from the brainstorming sessions. The authors are aware that multiple stakeholders do have interest in all areas. However, we categorized stakeholders based on *strong* interest in one of the closed curves: *Trustworthiness, Functionality, and Law* as A. *Protection and Security* as B. *Misuse, Tampering, and Hacking* as C. Various key interests were identified during the brainstorming sessions. The closed curves result from these.

Table I presents the results of the comparison. Set A holds the insurer and approval authority. The business car owner is included in B, while the criminal is in Set C. Set $A \cap B$ contains the OEM, legal institution, researcher, and supplier. The tuner is located in Set $A \cap C$. Government organizations in Set $B \cap C$. Finally, Set $A \cap B \cap C$ contains the private car owner and mobility provider.

The Venn diagram visualizes similarities and differences. Similarities are shared between stakeholders in the same or adjoining sets. Differences are represented by closed curves in which there is a symmetrical difference. The symmetric difference is compared for all pairs of close curves, that is $A \triangle B$, $A \triangle C$, and $B \triangle C$.

TABLE I
Comparison of Automotive Digital Forensics Stakeholder based on a Venn Diagram

Set	Stakeholder
A	Insurer, approval authority
B	Business car owner
C	Criminal
$A \cap B$	OEM, legal institution, researchers, supplier
$A \cap C$	Tuner
$B \cap C$	Government organization
$A \cap B \cap C$	Private car owner, mobility provider

One example for the symmetric difference $A \triangle C$ is the insurer and the criminal. The insurer tends to not change automotive components and ensure their safety, while the criminal tampers with devices while not properly testing the safety of performance increases. Another example of the symmetrical difference $A \triangle B$ is the licensing authority and the government organization. Differences are represented by closed curves in which there is a symmetrical difference.

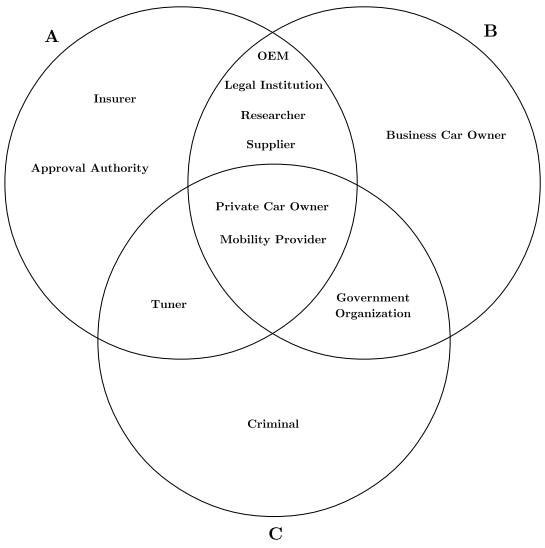

Figure 1. Automotive Digital Forensics Stakeholders in a Venn Diagram

VII. Evaluation

The next step is to evaluated the shown results. It includes a validation for the methodology and the presented stakeholder table.

A. Completeness of the Automotive Digital Forensics Stakeholder Table

To evaluate completeness of the stakeholder tables, we assessed them using the following list. The list is created based

on prior research in stakeholder identification and analysis work:

- *A*: Used identification techniques are in the context of identification and analysis [7].
- *B*: Involved phases are included in the stakeholder identification process [7].
- *C*: Accessible resources are utilized [7].
- *D*: A suitable identification method is used [2] [10].
- *E*: Suitable factors to identify stakeholders are used [8].
- *F*: Legitimacy, urgency, and proximity of stakeholders are considered [9].

a) A, B, C: In [7], Luyet et al. stated that stakeholder identification techniques depend on the context of the identification and analysis, the phase involved, and the accessible resources. In case of this research, context and phase is "stakeholder identification". Accessible resources depend on the identification technique. As a result, evaluation is performed on techniques that focus on identification and not on stakeholder analysis. Furthermore, required resources are included in the evaluation criteria that comprises access to stakeholder groups (OEM employees, supplier employees, PhD students, master students, professors, insurer employees, and car owners), number of interviews (3), and interview type (physical and online).

b) D: In [2], Bryson presented 15 stakeholder identification and analysis techniques. To evaluate completeness of the automotive stakeholder tables we determine which identification method is used in all 15 techniques. In 12 of 15 techniques, brainstorming is mentioned for stakeholder identification. 3 of 15 techniques do not mention a stakeholder identification technique. Prior the stakeholder analysis, the method assumes that stakeholders have been identified. Furthermore, snow-ball technique by King et al. [10] is not feasible for ADF stakeholders, because no interviews are viable with government institutions or criminals.

c) E: Creighton implemented different factors to identify stakeholders [8]. Those include proximity, economy, and social values. Those characteristics are relevant for stakeholder identification in specific geographical areas. It is not feasible for ADF stakeholders because this topic of DF is not dependent on geographical areas. Hence, we did not include factors presented by the author.

d) F: In [9], Mitchell et al. identified stakeholders based on legitimacy, urgency, and proximity. These characteristics are covered by their position in the vehicle life-cycle. Legitimacy is covered because each stakeholder is part of the life-cycle—otherwise there would not be any impact from the stakeholder. Due to the different life-cycle phases, urgency and proximity is given for each stakeholder.

B. Validation of Stakeholder List

We performed multiple interviews with identified stakeholders to validate the stakeholder list. To achieve sufficient coverage we aimed to interview at least one representative for each identified stakeholder group. During each interview, we described the aim of this research. Each representative was able to comment on the table and the shown results. Furthermore, they were instructed to specifically look into interests and resources for their associated stakeholder group. We were not able to contact a representative for government organizations, criminals, approval authority, or tuners. The following results were collected:

- 2 *OEM* representatives: Missed offensive stakeholders. The aim of this thesis is to identify automotive forensics stakeholders and not offensive security stakeholders.
- 2 *business car owner* representatives: No comments.
- 6 *private car owner* representatives: Missed *reliability of the car* as one of their interests. Added this interest to the table.
- 1 *supplier* representative: No comments.
- 1 *mobility provider* representative: No comments
- 1 *legal institution* representative: Missed *fulfillment of safety requirements* as one of their interests. We include those into *laws* since fulfillment of safety requirements is mandatory for a vehicle registration.
- 1 *insurer* representative: Missed *fulfillment of safety requirements* as one of their interests. We include those into *laws* since fulfillment of safety requirements is mandatory for a vehicle registration.
- 2 *researcher* representative: No comments
- 0 *government organization* representative: No interview performed.
- 0 *criminal* representative: No interview performed.
- 0 *tuner* representative: No interview performed.
- 0 *approval authority* representative: No interview performed.

We showed validity for 8 out of 12 presented stakeholders based on the stated interviews. Furthermore, we added missing interests mentioned by the stakeholders. However, additional interviews and surveys with stakeholder group would be beneficial.

C. Limitations of the Presented List of Automotive Digital Forensics Stakeholder

The presented list of ADF stakeholders is a snapshot. The automotive industry is changing frequently. As a result, the list of stakeholders can change in the course of time. However, our method of adding new stakeholders or adapting interests and resources of existing stakeholders is independent of changes in the industry. New technologies and opportunities lead to adjustments of the stakeholders interests and resources. New regulations can add additional stakeholders—similar to the introduction of UNECE and the approval authority as a new stakeholder in automotive security.

We further emphasize that this research and the resulting stakeholder list is focusing on ADF only. We are aware that stakeholders as well as their interests and resources are similar to general and offensive automotive stakeholders. However, differences between the areas of research are present.

As mentioned in Section VII-B, we were not able to interview representatives for the stakeholder groups government organizations, criminals, approval authority, or tuners. Hence,

 ISBN: 978-1-61208-919-5

results for these stakeholders are not sufficiently validated. In addition, more brainstorming sessions including relevant participates could result in more detailed results.

VIII. Conclusion and Future Work

One challenge in automotive digital forensics is the amount of research questions and forensic problems. Knowing stakeholders relevant in this domain allows researchers to identify problems and ask valuable research questions. Furthermore, vehicles and their components are expensive. Extensive research with multiple evidence items is difficult to achieve. Hence, researchers must fall back to experience and questions asked by practitioners (i. e. stakeholders).

In this work, we determined twelve unique stakeholders relevant in the area of ADF. We were able to identity those, by adapting three brainstorming sessions with relevant participants from academia, the automotive industry, and insurance domain. To present the relevance and impact on each stakeholder, we determined their position on the vehicle life-cycle, their main interest in ADF, as well as their resources and capabilities in performing and assisting ADF investigations. To identify differences and similarities between all stakeholders, we created a Venn diagram with three closed curves.

Future work will focus on interviews of different stakeholders. Based on those, requirements for forensics investigations and DF questions can be determined. This opens new research areas in the field of ADF. Furthermore, constant refinement of the list of relevant stakeholders is required to work on a roster that is up to date. We will identify relevant research questions for the shown stakeholders. These research questions will allow us to create a more fundamental understanding of ADF.

References

[1] R. Freeman and D. L. Reed, “Stockholders and Stakeholders: A New Perspective on Corporate Governance”, California Management Review, vol. 25, pp. 88-106, April 1983.

[2] J. M. Bryson, “What to do when Stakeholders matter”, Public Management Review, num. 1, vol. 6, pp. 21-53, March 2004.

[3] T. R. Hawkins, B. Singh, G. Majeau-Bettez, and A. Hammer Strømman, “Comparative Environmental Life Cycle Assessment of Conventional and Electric Vehicles”, Journal of Industrial Ecology, num. 1, vol. 17, pp. 53-64, October 2012.

[4] H. Mansor, “Security and Privacy Aspects of Automotive Systems”, Royal Holloway, University of London, July 2017.

[5] C. Armstrong, “Including Stakeholder Perspectives in Digital Forensic Programs”, 45th Hawaii International Conference on System Sciences, January 2012.

[6] M. Al Fahdi, N. L. Clarke, and S.M. Furnell, “Challenges to digital forensics: A survey of researchers, practitioners attitudes and opinions”, Information Security for South Africa, IEEE, August 2013.

[7] V. Luyet, R. Schlaepfer, M. B. Parlange, A. and Buttler, “A framework to implement Stakeholder participation in environmental projects”, Journal of Environmental Management, Elsevier BV, pp. 213-219, November 2012.

[8] J. L. Creighton, “Managing Conflict in Public Involvement Settings: Training Manual for Bonneville Power Administration”, Creighton and Creighton, 1986.

[9] R. K. Mitchell, B. R. Agle, and D. J. Wood, “Toward a theory of stakeholder identification and salience: the principle of who and what really count” Academy of Management Review 22, 1997.

[10] C. S. King, K. M. Feltey, and B. O. Sused, “The question of participation: toward authentic public participation in public administration” Public Administration Review 58 (4), 1998.

[11] T. Volkersdorfer and H. J. Hof, “A Concept of an Attack Model for a Model-Based Security Testing Framework”, SECURWARE 2020, The Fourteenth International Conference on Emerging Security Information, Systems and Technologies, 2020.

[12] Economic and Social Council, “Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system”, UNECE WP.29 Standard, June 2020.

[13] ISO/SAE, “ISO/SAE 21434:2021: Road vehicles — Cybersecurity engineering”, edition: 1, August 2021.

 ISBN: 978-1-61208-919-5