Toward the Ontology-Based Security Verification and Validation Model for the Vehicular Domain

Abdelkader Magdy Shaaban[1], Christoph Schmittner[1], Gerald Quirchmayr[2], A. Baith Mohamed[2], Thomas Gruber[1], and Erich Schikuta[2]

[1] Center for Digital Safety & Security, Austrian Institute of Technology, Vienna, Austria {abdelkader.shaaban,christoph.schmittner,Thomas.Gruber}@ait.ac.at
https://www.ait.ac.at/en/

[2] Faculty of Computer Science, University of Vienna, Vienna, Austria
{gerald.quirchmayr,abdel.baes.mohamed,erich.schikuta}@univie.ac.at
https://www.univie.ac.at/en/

Abstract. Security verification and validation is an essential part of the development phase in current and future vehicles. It is essential to ensure that a sufficient level of security is achieved. This process determines whether or not all security issues are covered and confirms that security requirements and implemented measures meet the security needs. This work proposes a novel ontology-based security verification and validation model in the vehicular area. Ontologies allow creating a comprehensive view of threats and security requirements. The proposed model performs a series of queries and inference rules to the comprehensive view to ensure the compliance of vehicle components with security requirements.

Keywords: Ontology, Verification and Validation, Potential Threats, Security Requirements

1 Motivational Background

Modern vehicles are part of a substantial ecosystem, including communication with stakeholders, infrastructures, customers, and authorities. The increase of connected units in vehicles leads to a considerable number of attack surfaces, which possibly leads to an increasing amount of security incidents. A vehicle might perform correctly according to the functional requirements; however, it can make other unintended tasks in the process. Furthermore, verification and validation (V&V) procedures can miss simply some of the hidden security defects, which lead to threatening the whole vehicle. Accordingly, the vehicular security requirements must be fulfilled [7]. One way to manage the structure of security requirements is to define them in groups called protection profiles. A Protection Profile (PP) is a document that describes the security considerations and resulting requirements for a Target of Evaluation (ToE) according to Common Criteria (CC) [5]. The ToE is an abstract description of a system or a system unit for specific usage. Besides, the PP identifies Security Target (ST) or security properties of ToE(s). It is essential to ensure the compliance

of one or more PP(s) with identified ToE(s) to develop secure vehicles. This is especially important since systems designed for vehicular usage are often reused in a different context. Assuring that such a system complies with the PP for this context ensures that it is security needs are covered.

This work introduces a novel ontology-based security V&V model for the vehicular industry. The model creates a comprehensive ontological representation in terms of classes, subclasses, individuals, annotations, properties, and datatypes of vehicular ToE(s), threats, vulnerabilities, and security requirements (according to CC). A series of inference rules are applied to the ontology to determine whether or not the selected security requirements cover the security gaps, and confirms if security requirements meet the actual security condition. If this is not the case, it uses a Knowledge Base (KB) of several PPs to select additional security requirements. These additional requirements are applied to handle existing security weaknesses and assure the compliance with protection profiles to meet the ST of ToE. The ontologies assist in validating and verifying the operational and the performance of the security requirements against the vehicular security gaps. The paper is organized as follows; the related work on automotive cybersecurity is discussed in Sction 2. The main contribution of this work is presented in Section 3. A description of threats and relevant security requirements of some interconnected units in a modern vehicle is described in Section 4. Section 5 demonstrates that the importance of ontologies in the V&V process to manage a massive amount of security requirements. Then, the paper ends with a summary, conclusion, and presents future work.

2 Related Work

In 2010 cybersecurity began to take more attention in the automotive industry [11]. The vehicles could have physical changes if malicious messages could be injected into internal parts of a vehicle such as the Controller Area Network (CAN bus) [8]. Nevertheless, the attack surface against vehicles not only by physical access but also there are several remote approaches. Ref. [1] defines four different methods for remote vehicle attacks. In modern vehicles, the diversity in communication protocols and heterogeneity between connected units lead to a potential increase in the number of security vulnerabilities. Furthermore, cybersecurity requires to be considered in all of the vehicular development phases. The development of vehicles is a distributed effort, regarding different organizations which use various methods. The majority of current security requirements verification processes are performed in the late phase of the development process since it needs the System Under Test (SUT) to be implemented, where both budget and time are very limiting circumstances [7].

The ontology approach has been proposed in several works in the cybersecurity domain [9]. Ref. [13] proposed a reference ontology to help in finding security solutions to the Internet of Things (IoT) environment. The proposed reference ontology is based on the modeling process to unify concepts and explain relationships among the main components of risk analysis of information

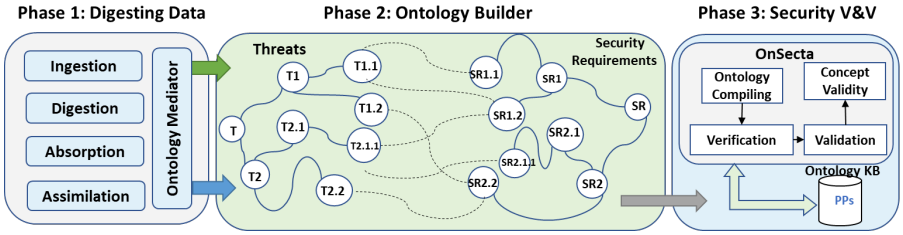

Fig. 1. The proposed ontology-based V&V model

security. Ref. [12] introduced a technical framework to monitor business process and technology assets using an ontology and knowledge reasoning for IoT security.

3 Ontology-Based Security V&V Model

The proposed model uses ontologies to describe a set of representational primitives of classes, individuals, and annotations of security properties of vehicles. The ontology generates new machine-processable meta-data for the vehicle security information, and then the model creates a domain knowledge. The domain knowledge is essential for identifying the relationships between threats and security requirements to verify and validate these security requirements according to CC in one or multiple PP(s). This Section describes the structure of the proposed model, as shown in Figure 1. The model consists of three main phases.

3.1 Phase One: Digesting Data

This phase receives data of ToE(s) with all related threats and security requirements. These data are processed by multiple sub-phases to extract the required information [6].

- **Ingestion:** collects the data are as follows:
  - list of identified assets with all related information,
  - all the detected threats with all related information details (i.e., name, id, type, description, and risk severity),
  - list of the security requirements according to the selected PP(s).
- **Digestion:** processes the raw data into a standard form that can facilitate to extract specific values from the original format.
- **Absorption:** extracts all data values which are needed to create an ontological representation from the input.
- **Assimilation:** acts as a filter to get rid of all unnecessary data. For example, the threats with low severity risk are not considered as significant security issues to threaten a vehicle.
- **Ontology Mediator:** this process propagates semantic annotations or statements (triples) in the form of the subject (threat) – predicate (property) – object(security requirements) which is defined the relationships between threats and the related security requirements.

3.2 Phase Two: Ontology Builder

This phase generates a comprehensive ontological overview of the threats and its relationships with security requirements. This overview has two main hierarchies:

- **Threats Hierarchy:** this is a hierarchical representation of a typical construction of vehicle threats.
- **Security Requirements Hierarchy:** it is a semantic representation of security requirements that are related to a specific PP for addressing potential vehicle threats.

Afterward, this phase creates an ontology linking between the threats hierarchical nodes and the security requirements nodes. This process defines links between these two hierarchical ontologies, which represent that the selected security requirements can handle one or more potential threat(s). The output of this phase is called "Ontology Outlook" as is illustrated in Figure 1 phase two. The left side of the ontology outlook represents the threats, whereas the security requirements are illustrated on the right side.

3.3 Phase Three: Security Verification and Validation

This phase is the core of the proposed model, which consists of two main parts:

Ontology Knowledge Base: this is a set of specific instances of PPs with all included security requirements and common criteria in an ontology representation format.

Ontology Security Testing Algorithm (OnSecta): is an ontology reasoner uses the Ontology Outlook to perform security V&V procedure:

- **Ontology Compiling:** this process compiles the contents of the Ontology Outlook (i.e., classes, subclasses, terms, annotations, and properties); this allows understanding the ontology linking between threats, and security requirements.
- **Verification:** performs a set of queries for ensuring that the vehicular ToEs are developed regarding CC according to specific PP.
- **Validation:** it assures the compliance of ToEs with PP to meet the actual ST. If that is not specified, OnSecta performs a series of inference rules to select new security requirements from other PPs in the KB to reach the actual ST.
- **Concept Validity:** this activity checks the content of the ontology KB to find new security requirements from other PPs.

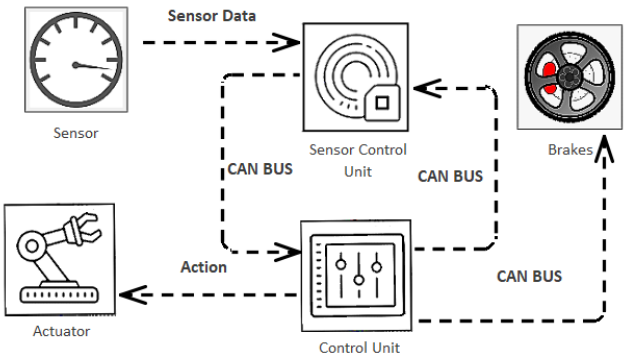

Fig. 2. Data flow between internal components in a modern vehicle

4 Case-Study: Modern Vehicles in Smart Farming

Future farming needs combination with innovative technologies to adapt and improve the production process. Smart farming applies and combines smart things with approaches from industry4.0 and intelligent mobility to address the challenges and improve a holistic system [9]. Integrating modern vehicles with current and future farming applications makes the farming process easier. The case-study shows a simple example of interconnected units in a modern vehicle as is depicted in Figure 2. The Figure contains a "Sensor" unit that collects data from the external environment. The sensor data are sent to "Sensor Control Unit" to process these inputs. Then the "Control Unit" manipulate the data to deliver the appropriate action to the "Actuator" unit for different action scenarios (i.e., drilling, fetching, cutting, etc.). Besides, the "Control Unit" controls the tracking of the vehicle according to different situations, such as controlling the vehicular "Brakes."

A secure vehicle can be developed only if the exact security requirements are fulfilled against potential threats. In the course of the authors' research, they developed the Threat Management Tool (ThreatGet). ThreatGet identifies, detects, and understands potential threats in the vehicular sector. It integrates the initial steps of the developing vehicular process to guarantee the security-by-design [3]. In addition, the authors created a security requirement tool is called Model-Based Security Requirement Management Tool (MORETO) [16]. MORETO aims to manage a vast number of PPs with all related security requirements according to CC. The ThreatGet and the MORETO tools are applied to this example to define potential threats, manage, and select security requirements. Afterward, the ontology-based model is applied to validate and verify the selected security requirements. The model generates multiple classes, subclasses, individuals, properties, and annotations of all detected potential threats and selected security requirements. Then it generates the Ontology Outlook to depict a comprehensive overview of all threats and security requirements as discussed in Section 3.2. Figure 3 shows the structure of the Ontology Outlook; this structure consists of three main parts:

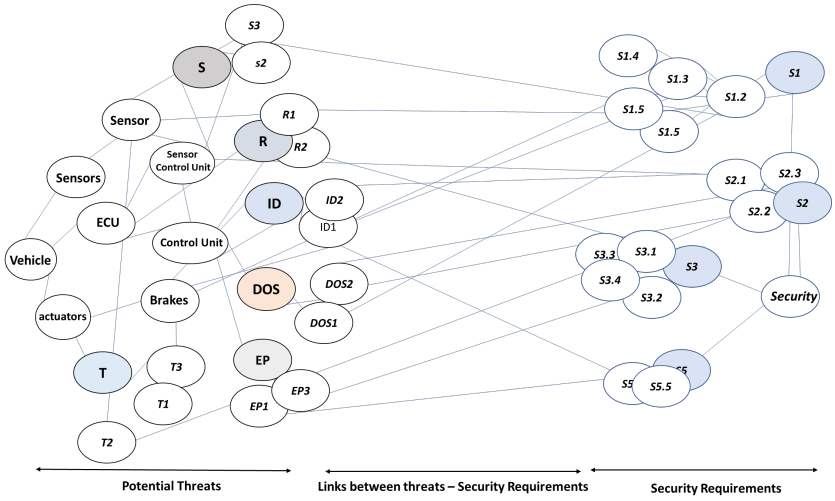

Fig. 3. Ontology outlook: ontology hierarchy between threats (left) and security requirements (right)

- **Potential Threats (left-side):** this hierarchy has all the vehicular units, which are defined in this case study. The colored nodes define the threat categories regarding the STRIDE model (i.e., Spoofing (S), Tampering (T), Repudiation (R), Information Disclosure (ID), Denial of Service (DoS), and Elevation of Privilege (EP)) [17]. The leaf nodes represent the actual detected potential threats.
- **The Security-Requirements (right-side):** this hierarchy represents CC are used to handle the potential threats. The colored nodes represent the category of security requirements (i.e., access control, communication port access, use control, data confidentiality, and so on). The leaf units represent the exact security requirements.
- **The Links Between the Two Ontologies:** the links between these two hierarchies can be defined not only between leaves of the hierarchies but also between internal nodes. Accordingly, a node specifying a more general threat type in the threat ontology can link to a subtree in the security requirements hierarchy identifying a set of similar security requirements can fit for handling related security issues [15].

OnSecta uses SPARQL language to perform queries across diverse data sources (threats and security requirements). These queries are applied to ensure that a vehicle is being developed based on standard security requirements, according to CC. Besides, to assures, the compliance of ToEs with PP meet the actual ST. OnSecta applies a series of rules to specify new PPs and selects additional security requirements. The rules are based on Semantic Web Rule Engine (SWRL), SWRL builds up a Horn clause representing the simple if-then conditional statement likewise formally from the Ontology KB to select proper security requirements [4].

5 Model Evaluation

Ontologies are considered a powerful method that uses regular specifications for knowledge representation such as vocabularies, taxonomies, classes, individuals, and annotations. Ontologies function acts like the human brain. They work and reason with concepts and relationships among multiple entities. That is considered the same way as humans perceive interlinked thoughts [14]. Furthermore, ontologies are integrated with this proposed model to perform security verification and validation in the vehicular domain. The vehicle development process requires to merge a significant number of security requirements according to multiple PPs. For instance, the requirements that relate to the Security Development Lifecycle (SDL) are appropriate to all industrial application such as vehicle development [10]. Managing hundreds or thousands of security requirements is considered a challenging task because it is time-consuming and complex work. The structure of the ontologies has a significant role in reducing the query complexity [2]. Furthermore, OnSecta manages ontologies by applying queries and rules over a massive number of ontology entities and define relationships and concept matching new security requirements to achieve a particular ST. Especially in the automotive domain the basic hardware of ECUs is often used for multiple vehicle types and even roles in the same vehicle where an adaption to new roles is done only by software and configuration. Giving guidance on the necessary security requirements for a specific role will ease the re-usability and adaptability of ECUs.

6 Conclusion and Future Work

To conclude this contribution, security verification and validation in the vehicular domain is one of the most critical challenges in the vehicular industry. On the first hand, it is quite a time, and effort consuming process to manage hundreds of interconnected units with thousands of threats. On the second hand, multiples of security requirements address potential threats according to CC. This work introduced an ontology-based security V&V model for current and modern vehicles. Ontologies are used to define domain knowledge representation of potential threats in vehicles and security requirements in multiples of PPs. The core of this model is OnSecta, which applies queries and a series of inference rules to perform verification and validation process to ensure the compliance of vehicle components with PP to meet a required ST. Future work will include the following points:

- **Protection Profiles:** create ontological representations of the most common security requirements in the vehicular domain.
- **OnSecta Implementation:** OnSecta is still in the developing stage; the authors work on developing the different building blocks of OnSecta.
- **Comparative Study:** the future work will include a comparative study between the proposed method with other kinds of typical techniques in the related domain to validate the superiority of the proposed method.

Acknowledgment

This work has received funding from the "AFarCloud" project, under grant agreement #783221. The project is partially funded by the EC Horizon 2020 Programme, ECSEL JU, and the partner National Funding Authorities (for Austria these are bmvit and FFG).

References

1. Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., Kohno, T., et al.: Comprehensive experimental analyses of automotive attack surfaces. San Francisco (2011)
2. Choksuchat, C., Chantrapornchai, C.: Benchmarking query complexity between rdb and owl. In: International Conference on Future Generation Information Technology (2010)
3. El Sadany, M., Schmittner, C., Kastner, W.: Assuring compliance with protection profiles with threatget. In: International Conference on Computer Safety, Reliability, and Security (2019)
4. Hebeler, J., Fisher, M., Blace, R., Perez-Lopez, A.: Semantic web programming. John Wiley & Sons (2011)
5. IEC: Iso/iec 15408-1:2009-information technology–security techniques–evaluation criteria for it security–part 1: Introduction and general model. standard (2009)
6. Josverwoerd: Digesting big data. https://blog.bigml.com/2012/11/12/digesting-big-data/, accessed: 24.09.2019
7. KASTEBO, M., NORDH, V.: Model-based Security Testing in Automotive Industry. Master's thesis, Department of Computer Science and Engineering - UNIVERSITY OF GOTHENBURG, Gothenburg, Sweden (2017)
8. Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., et al.: Experimental security analysis of a modern automobile. In: 2010 IEEE Symposium on Security and Privacy (2010)
9. Magdy, A., Schmittner, C., Gruber, T., Mohamed, A.B., Quirchmayr, G., Schikuta, E.: Cloudwot-a reference model for knowledge-based iot solutions (iiwas, 2018)
10. McAfee: Automotive security best practices. Tech. rep., McAfee (2016)
11. Miller, C., Valasek, C.: Remote exploitation of an unaltered passenger vehicle. Black Hat USA (2015)
12. Mozzaquatro, B., Agostinho, C., Goncalves, D., Martins, J., Jardim-Goncalves, R.: An ontology-based cybersecurity framework for the internet of things (2018)
13. Mozzaquatro, B.A., Jardim-Goncalves, R., Agostinho, C.: Towards a reference ontology for security in the internet of things. In: IEEE International Workshop on Measurements & Networking (M&N) (2015)
14. Ontotext: What are ontologies? https://ontotext.com/knowledgehub/fundamentals/what-are-ontologies/, accessed: 22.09.2019
15. Schikuta, E., Magdy, A., Mohamed, A.B.: A framework for ontology based management of neural network as a service. In: International Conference on Neural Information Processing (2016)
16. Shaaban, A.M., Kristen, E., Schmittner, C.: Application of iec 62443 for iot components. Springer (2018)
17. Shostack, A.: Experiences threat modeling at microsoft. vol. 413 (2008)