Automotive Security Models

Subjects: Automotive Engineering

Submitted by: Jingjing Hao

Definition

As the intelligent car-networking represents the new direction of the future vehicular development, automotive security plays an increasingly important role in the whole car industry chain. On condition that the accompanying problems of security are proofed, vehicles will provide more convenience while ensuring safety. Security models can be utilized as tools to rationalize the security of the automotive system and represent it in a structured manner.

1. Introduction

As the intelligent car-networking represents the new generation of the vehicular trend, security plays a more and more important role in automotive industry. Unlike IT security, the security of the automotive system can have an effect on the physical environment directly. Therefore, several research projects for security in transport systems were funded and conducted over the last decade. The projects like PRESERVE (preparing secure vehicle-to-X Communication systems), EVITA (E-safety vehicle intrusion protected applications) and OVERSEE (open vehicular secure platform) were launched to study how to ensure the security of the intelligent transport system by European Commission. The objectives of PRESERVE is to design a scalable security subsystem for the communication of ITS. It aimed to secure the V2X (vehicle to everything) communication and protect the data being abused by malicious attackers. The performance and the cost are also considered for the product deployment in close-to-market implementation [1]. EVITA focused on the trustworthy intra-vehicular communication in order to protect the sensitive data, which are transferred inside a vehicle [2]. The goal of EVITA is to design a secure automotive on-board architecture. The security requirements are specified after analyzing the relevant use cases and the threat scenarios. EVITA proposed hardware security modules as trust anchors for automotive controllers to fulfill the security requirements. To meet the demand of information and communication management for vehicular applications, OVERSEE targeted to realize an open vehicular IT platform [3]. Based on the architecture of the platform, the applications are deployed in a secure and dependable way to avoid interfering with the functionality and safety of the vehicle.

Moreover, some standardization activities are carried out to address and enforce the security aspects for automotive industry [4]. Some security standards for vehicles have been developed such as SAE J3061[5] and ISO 20078 [6]. Some are still under development like ISO/SAE 21434 [7], whose progress is reported in[8]. In August of 2020, the UNECE WP.29 (the UN Economic Commission for Europe and the World Forum for Harmonization of Vehicle Regulations) released an exposure draft of uniform provisions. If it is passed, the member countries will be regulated to implement automotive cybersecurity practices and the cybersecurity management systems from January of 2021 [9].

The standards and the framework projects provide groundwork for in-depth study. They allow for supports for the applications in the field of automotive security. For the development of modern vehicles, rigorous security engineering is required as well as safety engineering [10]. An overview on how to apply security testing technologies to automotive engineering is conducted in [11]. Five techniques that are commonly used for automotive engineering are identified and classified according to the applications of different vehicle lifecycle phases and architecture layers. This paper addressed the need to develop testing methods to combine safety aspects for future work. As the security is brought up later than safety in automotive development, how to integrate them into the existing lifecycle is discussed in [12]. The SAE J3061 suggests some interaction points between safety and security engineering during development processes [13]. In [14], a process to integrate the properties of safety and security through automotive system development is proposed and illustrated with the use case of an electronic steering column lock system. Dürrwang et al. adapted the safety hazards analysis method with security guide-words in [15]. It is used to identify the threats and security requirements during the safety analysis. In addition, there are several researches performed to adapt the safety models with security characteristics for system analysis, such as the model of Failure Mode, Vulnerabilities and Effects Analysis (FMVEA) [16], and the model of Combined Harm Assessment of Safety and Security for Information Systems (CHASSIS) [17]. Unlike [18], this paper focuses on the perspectives of automotive security engineering—only the threat

models originally designed for automotive security with independent inputs and outputs are considered. Thus, the adapted safety models are out of the scope of the discussion.

2. Security Modeling Methods for Automotive Industry

Since the outputs of threat models identify the potential attacks and the corresponding mitigation, modeling and assessing the security risks are demanded at the first stage of the design [19]. Several automotive security modeling methods are proposed for automotive engineering [20]. The J3061 Appendix A specifies some methods and techniques including the approach that originated from the framework project such as EVITA [2] and standards such as European Telecommunications Standards Institute (ETSI) Threat Vulnerability, and implementation Risk Analysis (TVRA) standard [21]. In this section, we review the security risk analysis approaches, which are widely used by automotive industrial organizations and compare them from different aspects. It aims to provide hints for automotive engineer to better understand the security models.

The literature survey of the references on automotive security modeling was conducted and five representative methods for the subject were found. A comparison is made with respect to the reviewed methods and the results are showed in Table 1.

Table 1. Comparison of the automotive security models.

Factors Methods	Application Context	Security Attributes	Reference Methods	Safety-Related	Risk Impact	Inputs & Outputs
EVITA	Vehicular IT systems	Authenticity, Integrity, Authorization, Freshness, Non-repudiation, Privacy, Confidentiality, Availability	Attack tree	YES	Safety, Finance, Privacy, Operation	Input: system use cases and assets Output: attack scenarios, risk levels and security requirements
HEAVENS	Automotive electrical and/or electronic systems	Confidentiality, Availability, Integrity, Authenticity, Authorization, Non-repudiation, Privacy, Freshness	STRIDE	YES	Safety, Finance, Privacy & legislation, Operation	Input: functional use cases Output: risk matrix with threat level and impact level, high-level security requirements
SINA	Connected vehicle systems	Authenticity, Availability, Integrity, Confidentiality, Authorization	STRIDE (with different threat types), Attack tree	YES	Safety	Input: system use cases Output: the list of threats, failure mode, potential effects and severity
SAHARA	Automotive embedded systems	Confidentiality, Availability, Integrity	STRIDE	YES	Safety	Input: the outcomes of safety analysis Output: threat level and security level
TVRA	Communications and services in ITS	confidentiality, integrity, availability, authenticity, accountability	TVRA for Telecommunications	NO	Availability of the network, Customer confidence	Input: ITS target of evaluation Output: risk determination and possible countermeasures

- Application context: The five modeling methods for automotive security reviewed in the last section are exploited for different usage scope. Some methods targeted on the systems on the vehicle and others took the V2X scenarios into

account. For example, the method of the TVRA is designed to evaluate the communications and services of network infrastructure in the ITS.

- Security attributes: The security attributes are the protected targets of the valuable asset. Ordinarily, security is composed of the attributes of confidentiality, integrity and availability. The attributes and security objectives in the context of the automotive systems are extended by adding authenticity, accountability, authorization, privacy, non-repudiation, and freshness. The explanation of the attributes can be referred to in [21][22]. Each method specifies different security attributes as objectives.
- Reference methods: Since automotive security is developed based on the traditional IT security modeling methods, the approaches to build a threat model used either the quantitative or the qualitative methods.
- Safety related: The safety has always been regarded as a critical engineering concern for the automotive industry. Unlike IT security, the safety process is essential for automotive design.
- Risk impacts: Risk assessment is employed to rank the threat with impact level parameters. It aids to analyze the potential impacts of threats on the stakeholders like user, dealer or manufacturer of the vehicles. The impact factors can be considered such as the safety of the car occupants and road users, the direct and indirect financial cost for the stakeholders, the operational incidents, and the violation of privacy and regulations. These factors assist to derive the security objectives.
- Inputs and outputs: These factors can be used to better understand the models especially from the engineering point of view. The perspectives of analysis are different from the methods, and thus, the required and start point are different. Since the objectives of each method are various, the outcomes are diverse accordingly.

References

1. PRESERVE Project. Preparing Secure V2X Communication Systems (PRESERVE). Available online: http://www.preserveproject.eu/ (accessed on 5 October 2020).
2. EVITA Project. E-safety Vehicle Intrusion Protected Applications (EVITA). Available online: http://www.evitaproject.org/ (accessed on 5 October 2020).
3. OVERSEE Project. Open Vehicular Secure Platform (OVERSEE). Available online: https://www.oversee-project.com/ (accessed on 5 October 2020).
4. Ur-Rehman, O.; Zivic, N.; Ruland, C. An Overview of Automotive Security Standards. Available online: http://docs.mipro-proceedings.com/iss/03_iss_5618.pdf (accessed on 5 October 2020).
5. SAE J3061. Cybersecurity Guidebook for Cyber-Physical Vehicle Systems; SAE International: Warrendale, PA, USA, 2016.
6. ISO/TR 20078-4. Road Vehicles—Extended Vehicle (ExVe) 'Web Services'; ISO/TC 22/SC 31 Data Communication; Technical Committee: Geneva, Switzerland, 2019.
7. ISO/SAE DIS 21434. Road Vehicles—Cybersecurity Engineering; ISO/TC 22/SC 32 Electrical and Electronic Components and General System Aspects; Technical Committee: Geneva, Switzerland, 2020.
8. Schmittner, C.; Ma, Z. Status of the Development of ISO/SAE 21434. In Proceedings of the 25th European Conference, EuroSPI 2018, Bilbao, Spain, 5–7 September 2018.
9. Burkacky, O.; Deichmann, J.; Klein, B.; Pototzky, K.; Scherf, G. Cybersecurity in Automotive, Mastering the Challenge; McKinsey & Company: New York, NY, USA, 2020.
10. Schmittner, C.; Ma, Z. Towards a framework for alignment between automotive safety and security standards. In Proceedings of the 34th International Conference on Computer Safety, Reliability, and Security, Delft, The Netherlands, 23–25 September 2015; pp. 133–143.
11. Pekaric, I.; Sauerwein, C.; Felderer, M. Applying Security Testing Techniques to Automotive Engineering. In Proceedings of the ARES'19: 14th International Conference on Availability, Reliability and Security, Canterbury, UK, 26–29 August 2019; pp. 1–10.
12. Schoitsch, E.; Schmittner, C.; Ma, Z.; Gruber, T. The need for safety and cybersecurity co-engineering and standardization for highly automated automotive vehicles. In Advanced Microsystems for Automotive Applications 2015; Schulze, T., Müller, B., Meyer, G., Eds.; Springer: Berlin/Heidelberg, Germany, 2016; pp. 251–261.
13. Schmittner, C.; Ma, Z.; Reyes, C.; Dillinger, O.; Puschner, P. Using SAE J3061 for Automotive Security Requirement Engineering. In Proceedings of the 35th International Conference on Computer Safety, Reliability, and Security, Trondheim, Norway, 20–23 September 2016.
14. Macher, G.; Messnarz, R.; Armengaud, E.; Riel, A.; Brenner, E.; Kreiner, C. Integrated Safety and Security Development in the Automotive Domain. In Proceedings of the SAE International WCX™ 17: SAE World Congress Experience, Detroit, MI, USA, 4–6 April 2017.
15. Dürrwang, J.; Beckers, K.; Kriesten, R. A Lightweight Threat Analysis Approach Intertwining Safety and Security for the Automotive Domain. In Proceedings of the SAFECOMP 2017: 36th International Conference on Computer Safety, Reliability, and Security, Trento, Italy, 12–15 September 2017; pp. 305–319.

16. Schmittner, C.; Gruber, T.; Puschner, P.; Schoitsch, E. Security Application of Failure Mode and Effect Analysis (FMEA). In Proceedings of the SAFECOMP 2014: 33rd International Conference on Computer Safety, Reliability, and Security, Florence, Italy, 10–12 September 2014; Volume 8666, pp. 310–325.
17. Raspotnig, C.; Karpati, P.; Katta, V. A Combined Process for Elicitation and Analysis of Safety and Security Requirements. In Enterprise, Business-Process and Information System; Bider, I., Halpin, T.A., Krogstie, J., Nurcan, S., Ukor, R., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; Volume 113, pp. 347–361.
18. Macher, G.; Armengaud, E.; Brenner, E.; Kreiner, C. A Review of Threat Analysis and Risk Assessment Methods in the Automotive Context. In Computer Safety, Reliability, and Security; Skavhaug, A., Guiochet, J., Bitsch, F., Eds.; Springer: Berlin/Heidelberg, Germany, 2016; Volume 9922, pp. 130–141.
19. Eichler, J.; Angermeier, D. Modular risk assessment for the development of secure automotive systems. In Proceedings of the 31st VDI/VW joint conference Automotive Security, Wolfsburg, Germany, 21–22 October 2015.
20. Alberts, C.J.; Behrens, S.G.; Pethia, R.D.; Wilson, W.R. Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVESM) Framework, Version 1.0; Carnegie Mellon University: Pittsburgh, PA, USA, 1999.
21. European Telecommunication Standards Institute (ETSI). Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA); ETSI: Sophia Antipolis Cedex, France, 2017.
22. Islam, M.; Sandberg, C.; Bokesand, A.; Olovsson, T.; Brober, H.; Kleberger, P.; Lautenbach, A.; Hansson, A.; Soderberg-Rivkin, A. P.Kadhirvelan, S. Deliverable D2: Security Models (Version 2.0); Vinnova/FFI (Fordonsutveckling/Vehicle Development): Göteborg, Sweden, 2016.

Keywords

Automotive Security Models;intelligent car-networking;PRESERVE