Automotive Vehicle Security Metrics

Guillermo A. Francia, III

1 Introduction

Today's automobiles have more than 150 electronic control units (ECUs), which are embedded devices that control the actuators to ensure optimal engine performance. These vehicles have multiple wireless entry points, some connected to the Internet, that enable access convenience and online services [1].

A technical brief [2] by Trend Micro described the vulnerability found in modern vehicles' networks. This vulnerability enables a stealthy denial-of-service attack that practically works for every automotive vendor and had been disclosed and prompted an ICS-CERT alert: ICS-ALERT-17-209-01. Exploitable hardware design flaws in some capacitive micro-electromechanical system (MEMS) accelerometer sensors produced by prominent automobile parts manufacturers were reported in another ICS-CERT alert: ICS_ALERT-17-073-01A in early 2017.

Experience in securing traditional IT systems cannot simply be applied to vehicle systems due to their differing requirements and development; a special set of security metrics is needed for these systems. In this chapter, we present a literature review of various communication protocols, threats and vulnerability issues, and safety and security challenges on vehicle systems. We aggregate the information learned from the literature and devise a set of metrics for measuring the efficacy of security controls in vehicle systems.

The remainder of this chapter is organized as follows: Section 2 provides an overview of vehicle communication systems while Sect. 3 expounds on vehicle security and provides details on vehicle threats, vulnerabilities, and attacks. Section 4 presents automotive vehicle security metrics that were adapted from the Common

G. A. Francia, III (✉)
Center for Cybersecurity, University of West Florida, Pensacola, FL, USA
e-mail: gfranciaiii@uwf.edu

K. Daimi et al. (eds.), *Advances in Security, Networks, and Internet of Things*,
Transactions on Computational Science and Computational Intelligence,
https://doi.org/10.1007/978-3-030-71017-0_24

Vulnerability Scoring System (CVSS) and the Common Methodology for IT Security Evaluation. Finally, Sect. 5 provides concluding remarks and offers future research directions on automotive vehicle security metrics.

2 Vehicle Communication

The proliferation of electronic devices and the rapid advancement of communication technologies have ushered the steady progression of vehicular communication from an in-vehicle form to the far-reaching external variety.

Modern automotive vehicle communication can be classified into four main categories: in-vehicle communication, vehicle-to-device (V2D) communication, vehicle-to-vehicle communication (V2V), and vehicle-to-infrastructure (V2I) communication. An in-vehicle communication example could be a vehicle sensor transmitting operating signals to a controller connected to the vehicle network. The communication between the infotainment system and smart phone is an example of a V2D communication. An example of a V2V communication would be two or more vehicles connected through some form of ad hoc wireless network. This vehicular ad hoc network (VANET), first introduced at the turn of century, is an extension of the mobile ad hoc network (MANET). For the V2I communication category, a good example is the scenario wherein a vehicle captures and sends real-time data about the traffic conditions to the highway infrastructure management system through cellular communication. These captured data are then fed into an intelligent traffic system that manages and optimizes traffic control in that locality.

2.1 Intra-vehicle Communication Protocols

The intra-vehicle network communication protocol group consists of the three predominant communication protocols found in a modern automotive vehicle: Controller Area Network (CAN), Local Interconnect Network (LIN), and FlexRay. Recent advancements in in-vehicle protocol technology include the Automotive Ethernet.

The CAN [3] communication protocol works on a two-wired half-duplex high-speed serial network bus topology using the Carrier Sense Multiple Access (CSMA)/Collision Detection (CD) protocol. It implements most of the functions of the lower two layers of the International Standards Organization (ISO) Reference Model.

LIN [4] is an in-vehicle serial communication protocol that delivers a low-cost alternative to CAN and FlexRay [5] for vehicle network applications. However, it delivers a lower performance and less reliability. A LIN bus uses a single 12 V line and has a node that acts as a Master gateway for other LIN nodes. Up to 16 of these slave nodes can be connected to the LIN bus.

FlexRay [5] is an in-vehicle communication bus whose purpose is to meet the need for a fast, reliable, and greater bandwidth data communication system. National Instruments correctly pointed out that the optimization of cost and reduction of transition challenges can be accomplished by using FlexRay for high-end applications, CAN for powertrain communications, and LIN for low-cost body electronics .

Automotive Ethernet is an adaptation of the standard ethernet but works on two-wire instead of the four-wire configuration. It implements a physical network that is used to connect components within a car using a wired network. It is designed to meet the needs of the automotive market, including meeting electrical requirements and emissions, bandwidth requirements, latency requirements, synchronization, and network management requirements.

2.2 Inter-vehicle Communication Protocols

The inter-vehicle network communication protocol group consists of several short- and long-range communication protocols and standards that enable services necessary for a robust, secure, and efficient transportation infrastructure.

Dedicated Short Range Communications (DSRC), a variation of the Institute of Electrical and Electronics Engineers (IEEE) 802.11 Wi-Fi standard, is primarily intended for the automotive environment. It uses the IEEE 802.11p standard in the 5.9 GHz band. Additionally, this standard is a companion for the proposed IEEE 1609 Family of Standards for Wireless access in Vehicular Environments (WAVE).

The 802.11a is one of the earliest wireless standards operating on both the 2.4 GHz and 5.2 GHz Industrial, Scientific, and Medical (ISM) bands. The data rate for this standard ranges from 6 to 54 Mbps with an operating bandwidth of 20 MHz. Compared to DSRC, this standard operates on a limited distance of approximately 100 meters.

Vehicular Ad Hoc Network (VANET) is a form of a Mobile Ad Hoc Network (MANET) that utilizes the Wi-Fi (802.11 a/b/g), the Worldwide Interoperability for Microwave Access (WiMAX), a family of wireless broadband communication standards based on IEEE 802.16, or the Wireless Access in Vehicular Environments (WAVE) based on the IEEE 1609–12 standards. WAVE is a layered protocol architecture that includes the security of message exchange and operates on the Dedicated Short-Range Communication (DSRC) band.

3 Automotive Vehicle Security

There have been several initiatives towards the protection of a vehicle's electronic control units. Notable examples are the E-safety Vehicle Intrusion Protected Application (EVITA) Project [6], the Preparing Secure Vehicle-to-X Communication

Systems (PRESERVE) Project [7], Secure Vehicular Communication (SeVeCom) Project [8], and the Society of Automotive Engineers (SAE) J3061 Guidebook [9]. In a very recent work by Bauer and Schartner [10], a table depicting attack surfaces and the classification of attack potential according to common criteria is presented. The table includes information on the difficulty and the impact of a certain exploit to an asset. Further, the work introduced a novel solution towards a realistic assessment of the integration of specialized countermeasures into the design of vehicular cybersecurity concepts.

3.1 Automotive Vehicle Threats and Vulnerabilities

Leopold postulates that "as cybersecurity risks are not covered by existing safety norms for surface vehicles, new guidelines and standards for automotive cybersecurity need to be established [11]." Acknowledging this urgent need, the automotive industry took the initiative to work on a cybersecurity standard: ISO/SAE 21434 "Road vehicles—Cybersecurity Engineering." The standard requires a security risk assessment that includes the identification of assets and the determination of potential damages resulting from the security breach. The first draft of this standard is scheduled to be released in early 2020. One major component of this standard is the determination of the security risk level of a vehicle and its components.

The ISO/SAE 21434 Joint Working Group (JWG) is divided into four part groups: PG1: Risk Management, PG2: Product Development, PG3: Operation, Maintenance and other Processes, and PG4: Process Overview and Interdependencies [12].

Keen Security Lab researchers uncovered the vulnerability of Tesla's touch screen infotainment system and used that as a gateway to manipulate the driver's seat motor, the windshield wipers, the turn indicators, and the sunroof from a distance of 12 miles while the car was in motion [13].

3.2 Automotive Vehicle Security Attacks

Petit, Feiri, and Kargl [14] described an abstract model of attack surfaces on the vehicular communication domain. The attack model considers the sensor data in various stages: acquisition, processing, storing, and transmission. The generic attack model appears to be adaptable to any communication protocol. This seminal work has been extended by Monteuuis et al. [15] with the notion of a secured automotive perception consisting of two main components: objects and data stages. Various attack surfaces on vehicles ranging from the OBD port to the infotainment system were examined by Koscher et al. [16]. One such surprising revelation is the ease of embedding CAN messages into an audio file and transforming the infotainment system as a gateway for attack vectors.

Secure measures have been introduced to mitigate the vulnerabilities of the CAN protocol. An intrusion detection system based on the clock skew of the Electronic Control Unit (ECU) as a fingerprint to develop a reference behavior of legitimate devices was proposed by Cho and Shin [17]. Wang et al. [18] proposed a method wherein a CAN packet is augmented with an 8-byte message authentication code. In [19], the design, implementation, and evaluation of a hardware security module for a modern automotive vehicle is presented. Lokman et al. conducted a systematic review of Intrusion Detection Systems (IDS) for automotive CAN bus system based on detection approaches, deployment strategies, attacking techniques, and technical challenges [20]. The study categorized anomaly-based IDS into four methods, namely, frequency-based, machine learning-based, statistical-based, and hybrid-based. Kumar et al. focused on jamming signal-centric security issues for Internet of Vehicles (IoV) [21]. They proposed a machine learning-based protocol that focuses on jamming vehicle's discriminated signal detection and filtration for revealing precise location of jamming effected vehicles.

3.3 Industry and Government Initiatives

The U.S. Government Accountability Office (GAO) Report on Vehicle Cybersecurity [22] contains, among others, the key security vulnerabilities in modern vehicles, the key practices and technologies to mitigate vehicle cybersecurity vulnerabilities, the challenges facing stakeholders, and the Department of Transportation's (DOT) efforts in addressing the issues in vehicle cybersecurity.

The EVITA (E-Safety Vehicle Intrusion Protected Applications) project [6], which was co-funded by the European Commission and whose primary objectives are to design, verify, and prototype an architecture for automotive onboard networks to protect security-relevant components against tampering sensitive data against compromise when transferred inside a vehicle.

The Society of Automotive Engineers (SAE) Cybersecurity Guidebook for Cyber-Physical Vehicle Systems [23] provides and describes a cybersecurity process framework from which an organization can develop processes to design and build cybersecurity in vehicular systems. The process framework covers the entire product lifecycle, including postproduction aspects with respect to service, incident monitoring, incident response, etc.

The National Highway Traffic Safety Administration (NHTSA) Automotive Security Best Practices for Modern Vehicles [24] presents the results and analysis of a review of best practices and observations in the field of cybersecurity involving electronic control systems across a variety of industry segments where the safety of life is concerned.

The Intel® Automotive Security Research Workshops report [25] presents the findings that resulted from two automotive security workshops. The participants were afforded to perform hands-on work on a Linux®-based in-vehicle infotainment

(IVI) simulation platform to identify threats and vulnerabilities and to provide potential mitigation strategies.

4 Automotive Vehicle Security Metrics

A very well-known cliché states that "what cannot be measured cannot be improved." This is the motivation behind this research. To better develop security metrics, organizations must differentiate between measurement and metric [26]. Measurement represents raw data of a point in time while metric comes from the analysis of aggregate data overtime (e.g [27].). A good metric should measure the relevant data that satisfy the needs of decision makers and should be quantitatively measurable, accurate, validated on a solid base, inexpensive to execute, able to be verified independently, repeatable, and scalable to a larger scale [28]. By adapting security risk regression that is successful in predicting attacks from simple security threats, Schechter [29] concludes that security strength is a key indicator of security risks for more complex security threats in information systems. In congruence, Manadhata and Wing propose the attackability of a system as an indicator of security strength [30]. Their security metric is based on the notion of attack surface by comparing attackability of systems along three abstract dimensions: method, data, and channel. The attackability of a system is a cost-benefit ratio between efforts of gaining access and potential impacts of security failure among the three dimensions [31].

There exists notable works on automotive vehicle security metrics. In [32], a set of security metrics for the software system in a connected vehicle is proposed. The set of metrics provides a quantitative indicator of the security vulnerability of the following risks on the system software: ECU coupling, communication, complexity, input and output data, and past security issues. The ECU coupling metric is based on the connectivity of the ECUs. Simply put, the risk is proportional to the extent of the connectivity of the ECUs. This proposed metric failed to take into account the fact that most vehicle networks are using the bus topology for interconnection. The communication risk metric is based on the number of communication technologies that are enabled on-board the vehicle. These are further normalized by the level of risk assigned to each of those technologies. The issue with this metric is that the assignment of risk level is quite arbitrary. The metric on input and output data risk takes into account the number of input data, the fixed and fluctuating properties of the input data, and the sensitivity level of output data. The authors argue that fluctuating input data and sensitive output data are more significant and should be given more emphasis in the calculation of security vulnerability. This metric failed to account the level of security testing that was applied to the vehicle's embedded system before deployment. Finally, the metric on security history utilizes the number of past attacks that occurred on the vehicle. This metric appears to assume the recurrence of an attack and that the vulnerability was never fixed. With

system patches actively being carried out during vehicle recalls, this assumption is rather weak.

Use cases of automotive security threats are described in [33]. The use cases include, among others, brake disconnect, horn activation, engine halt air bag, portable device injection, key fob cloning, cellular attack, and malware download. The threat matrix on each of these use cases includes attributes such as exploitable vulnerability, difficulty of implementation, resources needed, attack scenario, and outcome.

A Bayesian Network (BN) for connected and autonomous vehicle cyber-risk classification was developed by Sheehan et al. [34]. The BN model uses the Common Vulnerability Scoring System (CVSS) software vulnerability risk-scoring framework for input parameters specifically on the Global Positioning System (GPS) jamming and spoofing.

In the following section, we present a collection of vehicle security metrics similar to those in an earlier work on critical infrastructure and industrial controls systems security [31, 35].

4.1 Common Vulnerability Scoring System

CVSS is an open framework for communicating the characteristics and severity of software vulnerabilities. It consists of three metric groups: Base, Temporal, and Environmental [36]. The Base group characterizes the static intrinsic qualities of vulnerability; the Temporal group represents the vulnerability as it evolves over time; and the Environmental group depicts the characteristics of the vulnerability that are endemic to the user's environment. The third group of metrics lends itself perfectly with that of an automotive vehicle system.

The Base group consists of two metrics: exploitability and impact. The Temporal group consists of the following metrics: Exploit Code Maturity, Remediation Level, and Report Confidence. The Environmental metrics include the following: Security Requirements and Modified Base.

To illustrate, we examined two published vulnerabilities: the Tesla Model S firmware vulnerability (CVE-2016-9337) [37] and the Mobile Devices OBD-II dongles firmware vulnerability (CVE-2015-2908) [38].

The Tesla Model S firmware vulnerability applies to versions below version 7.1 with web browser functionality enabled. The vehicle with this firmware is susceptible to commands that may allow an attacker to execute a Command Injection attack on the CAN bus [37]. It has the following CVSS v3.1 Base vector:

$$\text{AV} : \text{N}/\text{AC} : \text{H}/\text{PR} : \text{N}/\text{UI} : \text{R}/\text{S} : \text{U}/\text{C} : \text{N}/\text{I} : \text{H}/\text{A} : \text{H}$$

This translates to a Network for the Attack Vector (AV), High for Attack Complexity (AC), None for Privileges Required (PR), Required for User Interaction (UI), Unchanged for Scope, None for Confidentiality (C), High for Integrity (I), and

High for Availability. The CVSS score for this Base vector is 6.8. This CVSS Base Score is calculated based on a table of metric values and the following formulae found in CVSS v3.1 Specification Document [36]:

$$\text{BaseScore} = \begin{cases} 0 & \text{if Impact} \leq 0 \\ \left(\text{Min}\left[(\text{Impact} + \text{Exploitability}),\ 10\right]\right) & \text{if Scope is Unchanged} \\ \left(\text{Min}\left[\left(1.08 * \left(\text{Impact} + \text{Exploitability}\right),\ 10\right]\right)\right. & \text{if Scope is Changed} \end{cases}$$

Where

$$\text{Impact} = \begin{cases} 6.42 * \text{ISS} & \text{if Scope is Unchanged} \\ 7.52 * (\text{ISS} - 0.029) - 3.25 * (\text{ISS} - 0.02)^{15} & \text{if Scope is Changed} \end{cases}$$

$$\text{Exploitability} = 8.22 * \text{Attack Vector} * \text{Attack Complexity} * \text{Privileges Required} * \text{User Interaction}$$

$$\text{ISS} = 1 - \left[(1 - \text{Confidentiality}) * (1 - \text{Integrity}) * (1 - \text{Availability})\right]$$

Extending this to include the Temporal and Environmental metrics, we derive the following CVSS v3.1 vector:

AV : N/AC : H/PR : N/UI : R/S : U/C : N/I : H/A : H/E : X/RL : O/RC : C/CR : X/IR : X/AR : X/MAV : N/MAC : H/MPR : N/MUI : R/MS : U/MC : N/MI : H/MA : H

An explanation of the Temporal and Environmental metric notation is in order. The three metrics under the Temporal Score indicates E:X for undefined Exploitability, RL:O for Official fix on remediation, and RC:C for a confirmed Report Confidence. The eight metrics under the Environmental Score include MAV:N for a Modified Attack Vector on the Network, MAC:H for High on Modified Attack Complexity, MPR:N for none for Modified Privileges Required, MUI:R for required Modified User Interaction, MS:U for unchanged Modified Scope, MC:N for none on Modified Confidentiality, MI:H for high impact on Modified Integrity, and MA:H for high impact on Modified Availability. The overall CVSS score for the vector is 6.5. The Common Vulnerability Scoring System Calculator result is depicted in Fig. 1.

For the second illustration, we use the Mobile Devices OBD-II dongles firmware vulnerability (CVE-2015-2908). This disputed vulnerability does not validate firmware updates which enables the execution of arbitrary code remotely [38]. It has the following CVSS v3.1 Base vector:

AV : A/AC : H/PR : N/UI : R/S : U/C : H/I : N/A : H

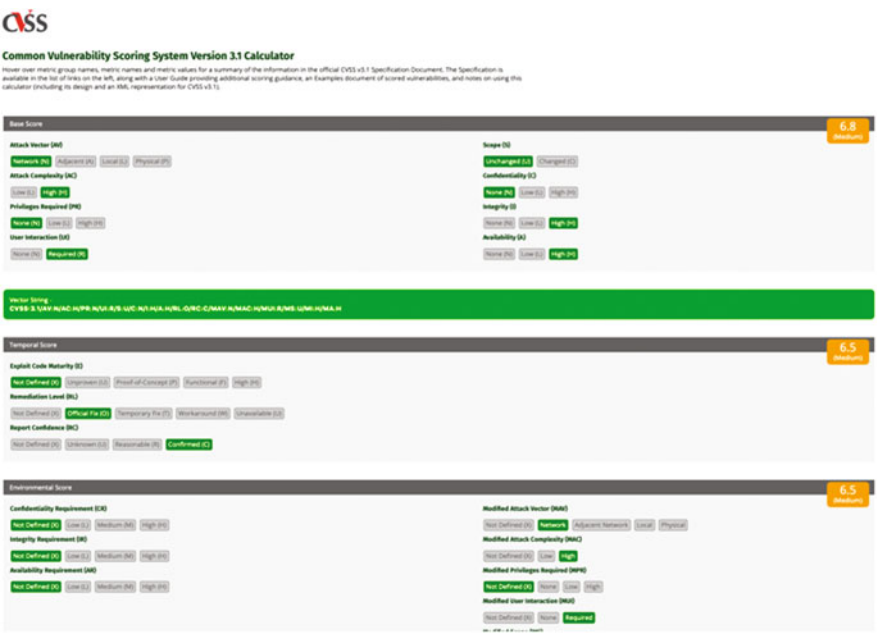

Fig. 1 CVSS calculator results

In this case, the Attack Vector (AV) is categorized as Adjacent Network (A) indicating that the vulnerable component is limited to the same physical network and cannot propagate beyond the layer 3 boundary of the network. The overall score for the Base metrics is 6.4.

4.2 Common Methodology for IT Security Evaluation (CEM) [39]

The CEM is a companion document to the Common Criteria for Information Technology Security Evaluation (CC) [40]. It defines the minimum actions to be taken by an evaluator conducting a CC evaluation utilizing the criteria and evidence as stated in the CC.

In this chapter, we specifically examine the attack potential on an automotive vehicle. The following factors need to be considered when performing an analysis of an attack potential:

- Elapsed time: Time taken by an attacker to identify a potential vulnerability, to develop an attack method, and to sustain effort required to execute the attack. Value ranges from 1 day to more than 6 months.

Table 1 Attack Potential calculation

Asset	Time	Expertise	Knowledge	Opportunity	Equipment	Total
False data from ECU	10	6	3	1	4	24
Blocking bus	4	3	3	0	4	14
Malicious software	10	6	3	1	4	24
Unauthorized access	1	3	3	1	2	10
Masquerading	4	3	5	5	5	22
Data tampering	1	2	4	1	2	10

- Specialist expertise: Describes the level of sophistication of the attacker. Levels include laymen, proficient personnel, expert and multiple experts.
- Knowledge of the target: Refers to the familiarity of the attacker on the target. Levels include public knowledge availability, restricted information, sensitive information, and critical information.
- Window of opportunity: This refers to the duration of time in which the vulnerability is exploitable. Window of opportunity includes unlimited, easy, moderate, difficult, and none.
- IT hardware/software or other equipment. This refers to the availability and the level of complexity of equipment/software needed to identify or exploit a vulnerability. Classes of equipment/software include standard, specialized, highly specialized, and multi-specialized.

Levels in each factor are assigned corresponding numeric values and illustrated in [39]. Bauer and Schartner demonstrate sample calculations of attack potential [10] on generic threat assets in an automotive vehicle. An excerpt of those calculations is shown on the first three rows of Table 1. The table is augmented by our own analysis of threats that are prevalent on connected automotive vehicles. Those last three rows represent unauthorized access, identity masquerading, and unauthorized data tampering.

An unauthorized access may originate locally, such as a cloning of key fob, or remotely through an internetwork communication channel. Time factor could be between 1 day and 1 week (1); expertise factor requires at least at the proficient level; knowledge of the vehicle assets will be most likely at the restricted level; the window of opportunity is unlimited; and the attack may not need specialized equipment.

The time to accomplish identity masquerading in connected vehicles may take a bit longer compared to unauthorized access; expertise factor requires at least at the proficient level; knowledge of the vehicle assets will be most likely at the sensitive level; the window of opportunity is very limited; and the attack may need some specialized equipment.

Data tampering can be accomplished by the widespread Man-In-The-Middle (MITM) attack tools. The time to accomplish such attack can take place very quickly; expertise factor requires at least at the semi-proficient level; knowledge

of the vehicle assets will be most likely at the familiarity level; the window of opportunity is somehow large; and the attack may not need specialized equipment.

5 Conclusion and Future Research Directions

The recent developments in connected vehicle technology ushered newly found vulnerabilities in automotive vehicle systems. These vulnerabilities underscore the need to look closely at the state of automotive vehicle security. In conjunction with this effort, it is paramount that we investigate the metrics with which security can be measured. As a major component of continuous improvement, quantitative and qualitative measures must be devised to be able to make a full appreciation.

This chapter presents a comprehensive review of communication technologies found in modern vehicles. It covers the threats, vulnerabilities and attacks that are prevalent in modern automotive vehicles and the transportation infrastructure system. Further, widely recognized security metrics are adapted to automotive vehicle security. Sample metric calculations are illustrated to belabor the significance of the adaptations.

With the preceding discussions in mind, we offer the following future research directions:

- The development of a unified automotive vehicle security metrics framework that incorporates both the CVSS framework and the Common Criteria for Information Security Evaluation.
- The utilization of machine-learning techniques to predict the status of automotive vehicle security based on known vulnerability attributes. An ongoing research by the author in this area of applied ML appears to reveal promising results.

Acknowledgments This work is partially supported by the Florida Center for Cybersecurity, under grant # 3901-1009-00-A (2019 Collaborative SEED Program) and the National Security Agency under Grant Number H98230-19-1-0333. The U.S Government is authorized to reproduce and distribute reprints notwithstanding any copyright notation herein.

References

1. A. Karahasanovic, *Automotive Cyber Security* (Chalmers University of Technology University of Gothenburg, Gotehnburg, Sweden, 2016)
2. T. Micro, A Vulnerability in Modern Automotive Standards and How We Exploited It. (July 2017). [Online]. Available: https://documents.trendmicro.com/assets/A-Vulnerability-In-Modern-Automotive-Standards-and-How-We-Exploited-It.pdf. Accessed Nov 2018
3. SAE International, CAN Specification 2.0: Protocol and Implementations. (01 August 1998). [Online]. Available: https://www.sae.org/publications/technical-papers/content/921603/ . Accessed 13 Oct 2019

4. CSS Electronics, A Simple Intro to LIN bus. (2019). [Online]. Available: https://www.csselectronics.com/screen/page/lin-bus-protocol-intro-basics/language/en. Accessed Oct 2019
5. National Instruments, FlexRay Automotive Communication Bus Overview. (28 May 2019). [Online]. Available: https://www.ni.com/en-us/innovations/white-papers/06/flexray-automotive-communication-bus-overview.html. Accessed 13 Oct 2019
6. EVITA Project, EVITA E-Safety Vehicle Intrusion Protected Applications. (01 December 2011). [Online]. Available: https://www.evita-project.org/. Accessed 13 Nov 2018
7. PRESERVE, About the Project. (June 2015). [Online]. Available: https://preserve-project.eu/about. Accessed 12 Oct 2019
8. SeVeCom, Security on the Road. (2008). [Online]. Available: https://www.sevecom.eu/. Accessed 13 Oct 2019
9. Society of Automotive Engineers (SAE), Cybersecurity Guidebook for Cyber-Physical Vehicle Systems J3061. (12 January 2012). [Online]. Available: https://www.sae.org/standards/content/j3061/. Accessed 13 Oct 2019
10. S. Bauer, P. Schartner, Reducing risk potential by evaluating specialized countermeasures for electronic control units, in *17th Escar Europe Conference 2019*, (Stuttgart, Germany, 2019)
11. D. Leopold, Relevance of ISO 21434 for the Automotive Development Process, ITEMIS. (20 December 2019). [Online]. Available: https://blogs.itemis.com/en/relevance-of-iso-21434-for-the-automotive-development-process. Accessed 12 Feb 2020
12. C. Schmittner, G. Griessnig, Z. Ma, Status of the Development of ISO/SAE 21434, in *Proceedings of the 25th European Conference, EuroSPI 2018*, (Bilbao, Spain, 2018)
13. D. Pauli, Hackers Hijack Tesla Model S from Afar, While the Cars are Moving. (16 September 2016). [Online]. Available: https://www.theregister.co.uk/2016/09/20/tesla_model_s_hijacked_remotely/. Accessed Oct 2019
14. J. Petit, M. Feiri, F. Kargl, Revisiting attacker model for smart vehicles, in *2014 IEEE 6th International Symposium on Wireless Vehicular Communications, WiVec 2014 Proceedings*, (2014)
15. J.-P. Monteuuis, J. Petit, J. Zhang, H. Labiod, S. Mafrica, A. Servel, Attacker model for connected and automated vehicles, in *ACM Computer Science in Cars Symposium (CSCS'18)*, (Berlin, Germany, 2018)
16. K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, Experimental security analysis of a modern automobile, in *2010 IEEE Symposium on Security and Privacy*, (Berkeley/Oakland, CA, 2010)
17. K.-T. Cho, K.G. Shin, Fingerprinting electronic control units for vehicle intrusion detection, in *Proceedings of the 25th USENIX Security Symposium (USENIX Security 16)*, (2016)
18. Q. Wang, S. Sawhney, VeCure: A practical security framework to protect the CAN bus of vehicles, in *International Conference on the Internet of Things (IOT)*, (Cambridge, MA, 2014)
19. M. Wolf, T. Gendrullis, Design, implementation, and evaluation of a vehicular hardware security module, in *14th International Conference on Information Security and Cryptology*, (Seoul, South Korea, 2011)
20. S. Lokman, T. Othman, M. Abu-Bakar, Intrusion detection system for automotive Controller Area Network (CAN) bus system: A review. EURASIP J. Wirel. Commun. Netw. **184** (2019)
21. S. Kumar, K. Singh, S. Kumar, O. Kaiwartya, Y. Cao, H. Zhao, Delimitated anti jammer scheme for internet of vehicle: Machine learning based security approach. IEEE Access **7**, 113311–113323 (2019)
22. Government Accountability Office (GAO), United States, Vehicle Cybersecurity: DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack. GAO Report 16-350. (2016). [Online]. Available: https://www.gao.gov/assets/680/676064.pdf. Accessed 14 Nov 2018
23. Society of American Engineers (SAE), Cybersecurity Guidebook for Cyber-Physical Vehicle Systems J3061. (17 January 2012). [Online]. Available: https://www.sae.org/standards/content/j3061/. Accessed 13 Nov 2018

24. C. McCarty, K. Harnett, A. Carter, *A Summary of Cybersecurity Best Practices* (National Highway Traffic Safety Administration, Washington, DC, 2014)
25. Intel Corporation, Intel Automotive Security Research Workshops. (2016). [Online]. Available: https://www.intel.com/content/www/us/en/automotive/automotive-security-research-workshops-summary.html?wapkw=automotive+security. Accessed 13 Nov 2018
26. S. Payne, A Guide to Security Metrics, SANS Institute. (19 June 2006). [Online]. Available: http://www.sans.org/readingroom/papers/5/55.pdf
27. K. Kark, P. Stamp, J. Penn, S. Bernhardt, A. Dill, Defining An Effective Security Metrics Program. (16 May 2007). [Online]. Available: https://www.forrester.com/report/Defining+An+Effective+Security+Metrics+Program/-/E-RES42354#. Accessed Feb 2020
28. S. Saydjari, Is risk a good security metric? in *Proceedings of the 2nd ACM Workshop on Quality of Protection*, (2006)
29. S. Schechter, Toward econometric models of security risk from remote attack. IEEE Secur. Priv., 40–44 (2005)
30. P. Manadhata, J. Wing, *An Attack Surface Metric–CMU-CS-05-155* (Carnegie Mellon University, Pittsburgh, PA, 2005)
31. G.A. Francia, Baseline operational security metrics for industrial control systems, in *International Conference on Security and Management*, (Las Vegas, NV, 2016)
32. L. Moukahal, M. Zulkernine, Security vulnerability metrics for connected vehicles, in *2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, (Sofia, Bulgaria, 2019)
33. C. McCarthy, K. Harnett, A. Carter, Characterization of Potential Security Threats in Modern Automobiles: A Composite Modeling Approach. (October 2014). [Online]. Available: https://rosap.ntl.bts.gov/view/dot/12119. Accessed 25 Feb 2020
34. B. Sheehan, F. Murphy, M. Mullins, C. Ryan, Connected and autonomous vehicles: A cyber-risk classification framework. Transp. Res. A **124**, 523–536 (2019)
35. G.A. Francia, X.P. Francia, Critical Infrastructure Protection and Security Benchmarks, in *Encyclopedia of Information Science and Technology*, 3rd edn., (IGI Global, Hershey, PA, 2014), pp. 4267–4278
36. Forum of Incident Response and Security Teams (FIRST), Common Vulnerability Scoring System version 3.1: Specification Document. (June 2019). [Online]. Available: https://www.first.org/cvss/specification-document. Accessed 13 Feb 2020
37. National Institute of Standards and Technology, CVE-2016-9337 Details. (14 March 2017). [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2016-9337. Accessed 13 Feb 2020
38. Common Vulnerabilities and Exposure, CVE-2015-2908. (3 April 2015). [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2908. Accessed 13 Feb 2020
39. Common Criteria Portal, Common Methodology for Information Technology Security Evaluation. (July 2017). [Online]. Available: https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R5.pdf. Accessed 24 Feb 2020
40. Common Criteria Portal, Common Criteria for Information Technology Security Evalaution. (April 2017). [Online]. Available: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf. Accessed 24 Feb 2020