Thesis for The Degree of Licentiate of Engineering

Towards a Standardised Framework for Securing Connected Vehicles

Thomas Rosenstatter

Division of Networks and Systems
Department of Computer Science & Engineering
Chalmers University of Technology
Gothenburg, Sweden, 2019

Towards a Standardised Framework for Securing Connected Vehicles

Thomas Rosenstatter

Technical Report No 198L
ISSN 1652-876X
Department of Computer Science & Engineering
Division of Networks and Systems
Chalmers University of Technology
Gothenburg, Sweden

Author e-mail: thomas.rosenstatter@chalmers.se

This thesis has been prepared using LaTeX.
Printed by Chalmers Reproservice,
Gothenburg, Sweden 2019.

Abstract

Vehicular security was long limited to physical security – to prevent theft. However, the trend of adding more comfort functions and delegating advanced driving tasks back to the vehicle increased the magnitude of attacks, making cybersecurity inevitable. Attackers only need to find one vulnerability in the myriad of electronic control units (ECUs) and communication technologies used in a vehicle to compromise its functions. Vehicles might also be attacked by the owners, who want to modify or even disable certain vehicle functions.

Many different parties are involved in the development of such a complex system as the functions are distributed over more than 100 ECUs, making it difficult to get an overall picture of the achieved security. Therefore, moving towards a standardised security framework tailored for the automotive domain is necessary.

In this thesis we study various safety and security standards and proposed frameworks from different industrial domains with respect to their way of classifying demands in the form of levels and their methods to derive requirements. In our proposed framework, we suggest security levels appropriate for automotive systems and continue with a mapping between these security levels and identified security mechanisms and design rules to provide basic security. We further study in detail a mechanism which provides freshness to authenticated messages, namely AUTOSAR SecOC Profile 3, and present a novel extension that offers a faster synchronisation between ECUs and reduces the number of required messages for synchronisation.

Keywords: Vehicular Security, In-Vehicle Network, Security Classification, Freshness

Acknowledgments

First, I would like to thank my supervisors Tomas Olovsson and Magnus Almgren for their advice and support. I would also like to thank the industrial partners involved in the HoliSec project – especially Volvo Trucks for having me in their office on Fridays. I am grateful to all current and former colleagues for making Chalmers a great place to work.

I want to express my deepest gratitude to my family, who supports me in any decision I made and will make even though it means to face hard times while being apart.

This research was supported by the HoliSec project (2015-06894), *HoliSec: Holistic Approach to Improve Data Security*, funded by VINNOVA, the Swedish Governmental Agency for Innovation Systems.

Contents

Part I

Thesis Summary

Introduction

1 Motivation

In the automotive domain, security was long limited to preventing unauthorised individuals from physically accessing vehicles. Media-players, navigation systems and functions that take over driving tasks, such as Cruise Control (CC) or Adaptive CC (ACC), have increased the comfort, extended the functionality of vehicles and provided a better driving experience. However, this still ongoing trend of adding advanced driving functionality requires more computing resources and more complex software – it marks the beginning of a new era of automotive security. The vehicle does not interact only with the driver anymore, interactions have become possible through the media player, mobile phones, other vehicles and infrastructure, e. g., traffic lights and road warnings. However, these new ways of interaction and control also cleared the way for attackers, making cybersecurity a necessity for vehicles.

Challenges and limitations specific to the automotive domain make it difficult to directly apply state-of-the-art security solutions designed for traditional IT systems. Moreover, the complexity of modern vehicles and the large number of components and developers as well as different parties involved make it increasingly difficult to get an overall picture of the achieved level of security in a vehicle. Therefore, it is necessary to work towards a security standard that is tailored for connected vehicles.

2 Background

Vehicles have evolved from being purely mechanical to becoming a network of Electrical and/or Electronic (E/E) systems. A reference architecture of such a connected vehicle is shown in Figure 1. Related functions, e. g., radar and cameras for perception, are grouped into separate network segments which are interconnected through gateways. The underlying network bus differs depending on the information the microcontrollers, so-called Electronic Control Units (ECUs), exchange. Controller Area Network (CAN) [1] is a relatively old network bus developed in 1983 and still in use in some segments, as it only requires a twisted pair cable and can offer real time guarantees. Ethernet on the other hand is mainly used for high bandwidth applications, such as streaming of video and sensor data.

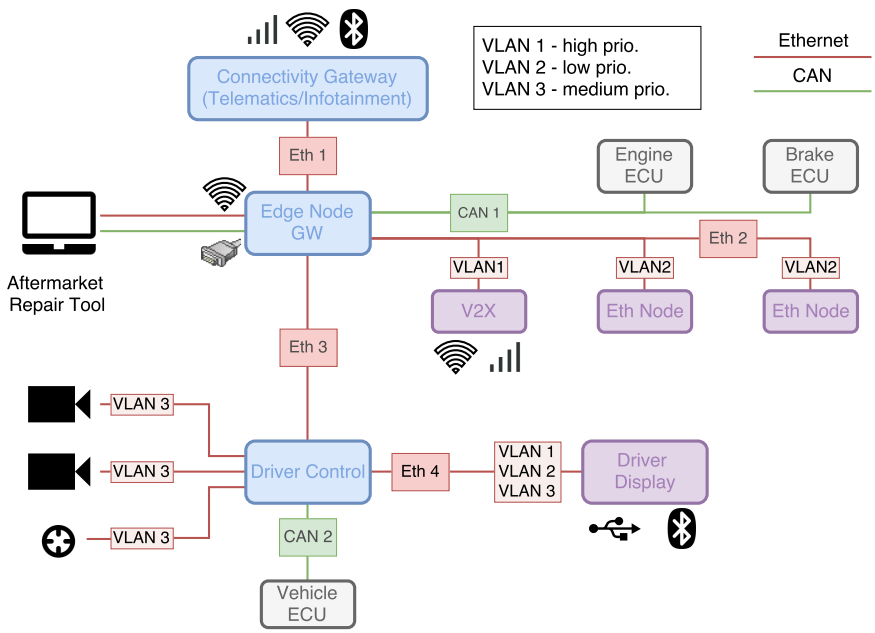

Figure 1: Reference architecture of a connected vehicle [2].

Securing such a system requires security by design, starting from considering an appropriate network architecture to hardware and software security measures to be implemented. The first attempt towards standardising best practices for the automotive domain is SAE J3061, *Cybersecurity Guidebook for Cyber-physical Vehicle Systems.* As a result, ISO/SAE 21434 [3], *Road vehicles – Cybersecurity Engineering*, has started in 2016 as a joint work between SAE and ISO. The standard is planned to be published in October 2019 and aims at

establishing a common base for the various stakeholders by specifying the requirements for cybersecurity risk management.

Safety and Security. The safety of individuals is of highest importance when developing automotive systems. ISO 26262 defines safety as the *"absence of unreasonable risk"* [4, p.14] and further specifies functional safety as the *"absence of unreasonable risk due to hazards caused by malfunctioning behaviour of E/E systems"* [4, p.8]. Cybersecurity on the other hand is concerned with individuals and organisations who want to gain unauthorised access to the system or even want to harm others [5]. The common goal of functional safety and cybersecurity is to protect individuals from harm, yet cybersecurity also aims to protect information. Reasons for protecting information may be safety-related, e. g., authenticating messages that contain the brake signal and availability measures, but are not limited to safety. Encrypting intellectual property, such as firmware, or encrypting personal information for maintaining privacy rights may be other rationales for protecting information.

The fundamental difference between safety and security is that security is about defending against attackers and organisations who are determined to find a vulnerability in order to achieve their goal which ultimately increases the complexity of necessary measures. Safety, on the other hand, deals with random faults.

The threat is real. Vehicles have not been targets of large-scale attacks yet, nevertheless, research by Checkoway et al. [6] dating back to 2011 already proved that attacks through the media player and the Tire-Pressure Monitoring System (TPMS) are possible. Over the years more and more reports about vulnerabilities concerning vehicles have been published [7–13]. Presumably, the most significant hack in the past is the "Jeep Cherokee Hack" [7] by Miller and Valasek which resulted in a recall of 1.4 million cars in the United States [14]. The disclosed vulnerabilities of connected vehicles range from cross-site scripting to exploiting vulnerabilities through WiFi and cellular networks.

Threats are not limited to attackers having the intent to steal information or harm other people. The attacker might be even the owner of the vehicle, who has complete physical access without time restrictions. Truck manufacturers, for instance, highlight the problem of illegal manipulation or modifications of heavy duty vehicles by the truck operators themselves. AdBlue, a diesel exhaust fluid, is used in heavy duty vehicles to reduce the nitrogen oxide (NOx) emissions. Some operators, however, consider purely the costs of AdBlue, regardless of the reduction in NOx emissions, and started to install "AdBlue emulators" to circumvent the AdBlue injection system [15].

The owners do not even need to be malicious in order to compromise the safety and security of the vehicle. A vulnerability published in April 2019 [16] showed that it is possible to locate and monitor tens of thousands of vehicles that use a specific GPS tracker which was installed by the owners. In certain cases it would have been even possible to turn off the engine in case this feature was enabled during the installation of the tracking device and the vehicle was driving at less than 20 km/h. This hack was possible due to the use of the same default password for all customers who signed up for the service.

Complexity of Automotive Systems. Vehicles differ in many ways from traditional computer systems. This distinctness, which is outlined below, makes it difficult for vehicle manufacturers to directly deploy well-established methods and security mechanisms, e. g., Common Criteria [17], NIST FIPS 199 [18] and the corresponding security and privacy controls [19], in their domain.

- **Lifetime.** The expected lifetime of a vehicle is 150,000 – 300,000 km [20], which corresponds to up to 20 – 25 years for a passenger car. Throughout this time, it is essential and necessary to keep the vehicle safe and secure.

- **Compliance to standards.** Some vehicle types may need to adhere to certain standards. SAE J1939 [21], for instance, is a standard for heavy duty vehicles that defines the content of specific frames sent on the vehicular network in order to provide interoperability between the truck and a variety of third-party equipment.

- **Alignment with safety.** Security mechanisms need to be implemented in compliance with the requirements of the functional safety standard for road vehicles, namely ISO 26262 [22]. Moreover, methods for designing secure vehicles should be aligned, where possible, with this standard as it found broad acceptance in industry.

- **Interplay between safety and security.** The passenger's safety has to be maintained in all situations. Therefore, it is of utmost importance that safety and security mechanisms do not counter their intended functionality.

- **Maintenance.** Authorised workshops need to be able to replace spare parts even in an offline environment.

- **Energy utilisation.** Power consumption is an important factor that needs to be considered as it affects the fuel consumption and may cause problems with heat dissipation.
- **Performance of ECUs.** Many ECUs deployed in today's vehicles do not have enough resources to implement new security functions to perform encryption or sign messages.
- **Costs.** Assuming that ECUs with hardware accelerated security features and secure storage cost 1 USD more than the version without, it is apparent that deploying them to a passenger vehicle comprising of more than 100 ECUs means a significant impact on revenue. For instance, a manufacturer producing 1,000,000 passenger cars a year with each including 100 ECUs would lose 100,000,000 USD in revenue per year. However, the necessity of securing connected vehicles should not only be considered as loss in revenue, as it contributes to maintaining the privacy and safety of the passengers and their surroundings.

3 State of the Art and Challenges

Threat Analysis and Risk Assessment (TARA) is an important step during the concept and development phases of a secure system. This analysis supports architects in identifying the assets and corresponding threats of a system, and provides classifiers for security demands in the form of security levels for further prioritisation and assignment of appropriate security measures. Furthermore, we focus on one specific security attribute, *freshness*, which prevents attackers from retransmitting old authenticated messages.

3.1 Threat Analysis

TARA is a technique to identify and rate the risk or security demands of a system. Figure 2 illustrates the steps when performing a TARA. First, the system is analysed and assets that need to be protected from certain threats are identified. An evaluation follows which results in a classification of the security demands and risks in form of levels. SAE J3061 [5] describes a lifecycle process framework including how to apply TARA in the concept phase.

Automotive specific TARA techniques referred to in the SAE J3061 guidebook include EVITA [23] and HEAVENS [24]. Examples of parameters considered in the HEAVENS TARA for evaluating the security demands are the knowledge of the attacker, window of opportunity, knowledge about the

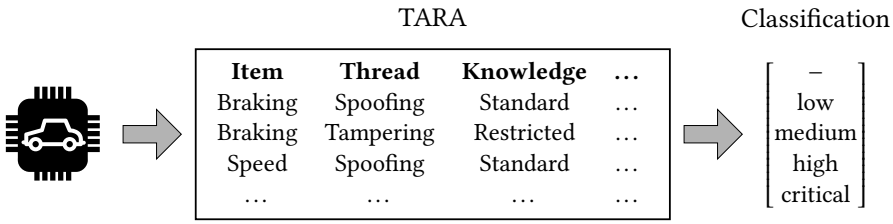

Figure 2: Overview of the steps from analysing the system, performing a TARA and getting a classification.

target, and financial and safety impact. These parameters are rated with numerical values for each asset/threat combination and consequently combined to a single value, the security level.

Microsoft STRIDE [25] is a technique to identify the assets and threats of a system. STRIDE classifies threats in six categories: spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. Its applicability in automotive systems has been discussed and shown [24, 26, 27].

3.2 Security Classification and Requirements Engineering

As we mentioned, the result of the TARA is often referred to as risk or security level. These levels are further used to reflect the demands placed on functions, ECUs, and subnets. As an example, HEAVENS uses the outcome of the TARA for prioritisation and to guide engineers in manually deriving security requirements. The structure of these security levels differs between various presented models, for instance, HEAVENS uses a single value in the range of 0 to 4, whereas EVITA uses a vector of four elements to describe the risk with values ranging from 0 to 7. This variation of how security demands are expressed between different security models brings up the question: *What is the desired structure to classify security demands for the design and development of connected vehicles?*

Methods to classify security demands, respectively the risk of security threats, in form of levels have been proposed by various researchers. Much attention has been paid to investigate ways to combine safety and security in one framework [26–29]. A comparison of safety classifications throughout different domains has been carried out by Blanquart et al. [30]. Security frameworks developed for the automotive domain mainly focus on threat identification and risk assessment [23, 24]. The mapping from security levels directly to defined security requirements has been addressed in standards such as NIST SP 800-53 [19] and IEC 63442 [31]. *Connected Vehicles Pilot*

Development Phase 1 [32] applies NIST FIPS PUB 199 [18] and NIST SP 800-53 to vehicular systems. However, the resulting security requirements do not cover the needs of the automotive domain in depth, as the previously mentioned two NIST publications have been designed for security in federal information systems.

3.3 Freshness

The purpose of authenticating messages is (1) to ensure that the content has not been tampered with, and (2) to assure that the sender is indeed the correct source of the message. Message Authentication Codes (MACs) are commonly used for authenticating messages. They are similar to hash functions, but additionally require a secret key in order to fulfil the requirement of being resistant to manipulation. Freshness is a security property that provides additionally means to ensure that messages are fresh, i. e., they have not been replayed by an attacker. The simplest solution to provide freshness in authenticated messages is to include a freshness value in form of a counter or timestamp with each message when generating the MAC.

The receiver needs to know the MAC and freshness value of the message to correctly verify its authenticity and freshness. In networks with limited bandwidth and already high bus load, it may not be possible to send both the MAC and freshness value in full length with each message and thus, these values need to be truncated. The recommended minimum length by NIST SP 800-38B [33] for the truncated MAC is 64 bits, however, a shorter truncated MAC can be used when other measures, such as limiting the attempts for verifying an authenticated message, are in place. Sending a truncated freshness value requires additional mechanisms to synchronise this value between the different entities, as all entities need this information for generating and verifying messages.

The truncation of the freshness value is necessary in automotive networks as it has to be possible to deploy such solutions also on CAN [1]. The CAN bus has a maximum bit rate of 1 Mbit/s and is already highly utilised in vehicles. Given this requirement to not increase the bandwidth more than necessary, it is evident that the freshness value needs to be truncated and thus synchronised between senders and receivers. AUTOSAR, an open system platform for vehicles, describes [34] three security profiles for authenticating messages. One of these profiles, SecOC Profile 3, defines also a mechanism to synchronise the freshness value. Other solutions [35, 36] either require a modification of the CAN bus transceiver or require, as Profile 3 does, a periodic synchronisation of the freshness value.

4 Research Questions

This thesis contributes to the following research questions.

RQ1 How to express security demands for the design and development of connected vehicles?

RQ2 How to move forward from unique security requirements of individual systems to predefined security requirements?

RQ3 What are suitable security mechanisms for the automotive domain and how can they be used in a framework?

RQ4 What are the limitations and possible design considerations when implementing a freshness mechanism for authenticated messages in automotive systems?

5 Contributions

Previous research on security frameworks for connected vehicles has focussed on threat analysis, methods to combine safety and security, and techniques to manually derive security requirements.

In this work, we first study existing safety and security standards and frameworks from different domains in order to propose a suitable structure for security levels, e. g., a single value or a vector to express the security demands. With this classification of security demands in place, we continue to explore ways to directly move towards security requirements, respectively mandatory security mechanisms and design rules, without the need to manually derive security requirements by first defining high-level security requirements and dividing them in technical security requirements. Our proposed framework depends only on the resulting security levels from the conducted TARA and aims at providing basic security. Lastly, we study a solution for freshness in authenticated messages and present an extension which copes with the limitations we have identified when implementing such a method.

Security Classification and Requirements Engineering [37,38]. In Paper 1 [37], we address research questions *RQ1* and *RQ2*. We propose a structure for security levels for the automotive domain based on an analysis of various standards and frameworks across different industrial domains, focussing on the way security or safety demands are expressed. The result of this analysis of security standards and frameworks showed that the classification of security differs significantly, whereas all studied safety standards use the same

structure. In addition, we also investigate how the studied standards and frameworks move from safety or security levels to requirements: *Do they provide guidance or processes to define security requirements/goals? Do they offer a direct transition from the resulting levels to specific requirements?*

Continuing at the point of having a structure to describe security demands, we contribute in Paper 2 [38] to research questions *RQ2* and *RQ3*. We propose a framework that supports architects and engineers in obtaining basic security requirements that only depend on the result of TARA. This way, developers are able to discover at an early stage if there are any conflicts between basic security requirements and safety measures. Moreover, this standardised method provides consistency of security requirements throughout an organisation and its suppliers, increases traceability of the security demands and required security mechanisms, and enables developers to focus on formulating additional application-specific security requirements that need special attention.

Freshness [39]. We contribute to research question *RQ4*, by studying AUTOSAR SecOC Profile 3 and providing details about the situations in which Profile 3 is not able to correctly verify authenticated messages when truncated freshness values are transmitted. Based on this analysis we also identify design consideration and limitations, and further propose a novel extension of Profile 3 that addresses them. Our suggested improvements have been implemented on a test bed consisting of three ECUs and evaluated in terms of flexibility, time to resynchronise the freshness value and control messages needed for synchronisation.

6 Conclusion and Outlook

Securing modern vehicles has become more important as vehicles are not only connected to the Internet. Vehicles are also going to be interconnected with each other and with the road infrastructure, such as traffic lights. In addition, the increased capabilities of vehicles, e. g., automated driving assistance, magnifies the extent to which an attacker will be able to control the vehicle.

The research presented in this thesis starts with investigating how security demands in the form of security levels should be expressed for further use in product development. By providing a framework that directly assigns security requirements, i. e., security mechanisms and design rules, to these security levels, it is possible to extract the requirements needed to be implemented and possible conflicts with the safety requirements in an early stage of development. Next, we focussed on one specific security mechanism that

provides freshness for authenticated messages, namely AUTOSAR SecOC Profile 3. Based on an analysis of the method which synchronises the freshness value and a discussion on the limitations and design considerations of such a method, we propose an extension of this mechanism that allows a faster synchronisation and requires less bandwidth in terms of synchronisation messages that need to be sent.

Figure 3 provides an overview of current research publications and their directions, including future work. Paper 1 and Paper 2 are focussing on the use of security levels and how to further continue with a framework that directly assigns security mechanisms to be implemented to a function, ECU or network segment. Paper 3 concentrates on one specific mechanism identified in Paper 2.

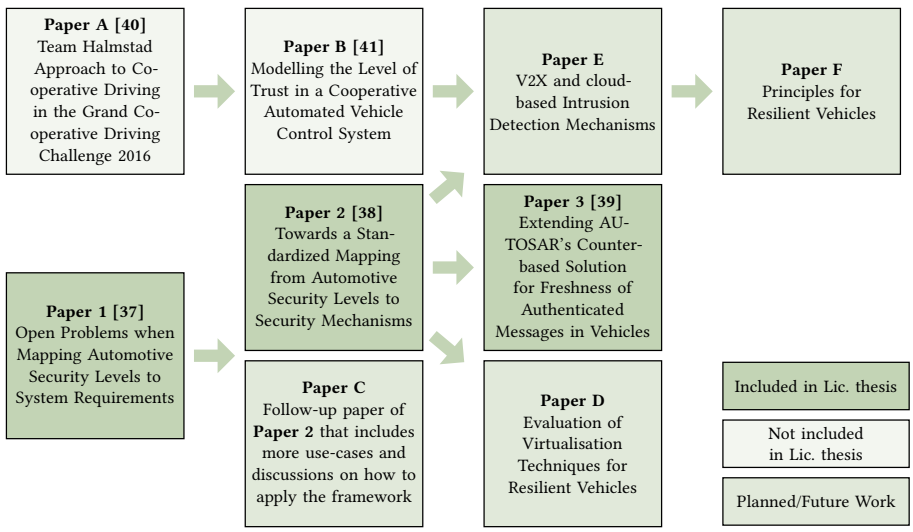

Figure 3: Research publications and planned future work.

As Paper 2 is currently only validated by an industrial partner given a simple use case, a follow-up is planned on this framework to apply more (complex) use cases to verify the usability of the proposed framework, as well as the assignment of security mechanisms to security levels (Paper C). Paper D plans to explore another security mechanism, namely virtualisation. The main idea is to set up a test bed using open source software solutions and to evaluate different techniques, i. e., container-based and hypervisor-based virtualisation, in regard to security and resiliency of vehicles.

Paper A [40] and Paper B [41] focus on vehicles cooperating with each other in order to perform a certain action, such as efficiently crossing an intersection. Paper A gives an overview of an implemented software architecture

of a cooperative vehicle designed and developed for the Grand Cooperative Driving Challenge (GCDC) in 2016. Paper B [41] focusses on one specific module, the trust system, which verifies information received from other vehicles at system level and associates a so-called trust index with each vehicle which is further used for decision making of cooperative actions. A verification on system level is necessary as securely transmitted information might still contain incorrect or faulty information as a result of, for instance, malfunctioning sensors. A planned continuation of Paper B is to investigate cloud-based mechanisms to verify information received from other entities and extend the proposed trust index accordingly (Paper E). When having an intrusion detection system in place it is also necessary to decide on the actions when an intrusion or corruption of information is detected (Paper F).

Papers Overview

Paper 1: Open Problems when Mapping Automotive Security Levels to System Requirements [37]

T. Rosenstatter, T. Olovsson

This paper provides an analysis of standards and frameworks for the automotive and other industrial domains in respect to their methodology on how they classify security, respectively safety. A classification of security is necessary in order to indicate the security demands of a certain function or ECU. We first highlight the challenges that the automotive domain faces when designing and developing secure systems. Second, we study how selected standards and frameworks structure the classifier for their corresponding domain. Lastly, we propose a structure for automotive security levels that considers the identified challenges which are specific to the automotive domain. In this paper, we

- provide a study of safety and security standards, along with proposed security models and frameworks for the automotive domain.
- propose methods for how to move forward from unique requirements of individual systems and identified security levels to a set of mandatory requirements, design rules and security mechanisms.
- show that such requirements should be based on the security level of the function to be implemented.
- describe the benefits with having such a framework in place when dealing with third-party developed functionality.

Appeared in: *Proceedings of the 4th International Conference on Vehicle Technology and Intelligent Transport Systems, VEHITS 2018, Funchal, Madeira, Portugal, March 16-18, 2018*

Paper 2: Towards a Standardized Mapping from Automotive Security Levels to Security Mechanisms [38]

T. Rosenstatter, T. Olovsson

We continue at the point of having performed a TARA resulting in a set of Security Levels for each identified asset, which can be a function, a vehicle ECU, or even a network segment. The proposed framework guides designers and engineers in identifying necessary security mechanisms to be implemented based on a mapping from Security Levels (SLs) to a list of security mechanisms. In this paper, we have identified appropriate security mechanisms suitable for automotive systems and assigned them to particular SLs. We additionally show how to apply our proposed framework to an automotive use case, which has been verified by a vehicle manufacturer. By applying this framework, we

- provide a strict rule-set which fulfils basic security demands to allow designers to focus on application specific requirements that are not covered,
- allow designers to identify conflicts and dependencies between safety and security requirements in an early stage of development, and
- provide a common ground for required security mechanisms to be implemented between vehicle manufacturers and their suppliers.

Appeared in: *21st International Conference on Intelligent Transportation Systems, ITSC 2018, Maui, HI, USA, November 4-7, 2018*

Paper 3: Extending AUTOSAR's Counter-based Solution for Freshness of Authenticated Messages in Vehicles [39]

T. Rosenstatter, C. Sandberg, T. Olovsson

Freshness is a security property that protects against replay attacks of authenticated messages. AUTOSAR, an open system platform for vehicles, describes three so-called SecOC Profiles for authenticating messages sent over vehicular networks. Two of the described security profiles also provide freshness; one profile is using a single counter, the other one, namely SecOC Profile 3, uses a counter that is divided into several sub-counters and additionally provides a method for synchronising it. Synchronisation of this counter or Freshness Value (FV) needs to be in place as it is not feasible to send the complete FV on a highly utilised network.

In this paper, we analyse Profile 3 while focussing on usability and its ability to synchronise the counter value, discuss design considerations and limitations of such a mechanism that provides freshness using a counter, and lastly, we propose improvements on Profile 3 that address the identified shortcomings. Our novel approach has been implemented on test bed consisting of three vehicle ECUs and has been further validated in regard to its flexibility for synchronisation, faster resynchronisation when a receiving ECU is out of sync, and the reduction of necessary control messages that need to be sent on the bus. In this paper, we

- discuss design considerations and limitations when implementing a freshness mechanism in vehicles.
- identify the situations in which it is not possible to recover the correct freshness value when only a truncated freshness value is transmitted with every message.
- propose an extension of AUTOSAR SecOC Profile 3 which allows faster resynchronisation and requires less synchronisation messages to be transmitted.

In submission, 2019

Bibliography

[1] "ISO 11898-1:2015 Road vehicles – Controller area network (CAN) – Part 1: Data link layer and physical signalling," International Organization for Standardization (ISO), Standard, 2015.

[2] A. Yadav and C. Sandberg. (2018) Holisec reference architecture. (Accessed: 2018-04-10). [Online]. Available: http://autosec.se/wp-content/uploads/2018/04/HOLISEC_D4.1.3_v1.0.pdf

[3] International Organization for Standardization (ISO), "ISO/SAE AWI 21434 - Road Vehicles - Cybersecurity Engineering," (Accessed: 2019-04-16). [Online]. Available: https://www.iso.org/standard/70918.html

[4] "ISO 26262-1:2011 Road Vehicles – Functional Safety – Part 1: Vocabulary," International Organization for Standardization (ISO), Standard, 2011.

[5] "SAE J3061: SURFACE VEHICLE RECOMMENDED PRACTICE - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems," SAE International, Standard, 2016.

[6] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher *et al.*, "Comprehensive experimental analyses of automotive attack surfaces." in *USENIX Security Symposium*. San Francisco, 2011.

[7] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," *Black Hat USA*, vol. 2015, 2015.

[8] T. Fox-Brewster and Forbes, "BMW Update Kills Bug In 2.2 Million Cars That Left Doors Wide Open To Hackers," Feb 2015, (Accessed: 2016-12-12). [Online]. Available: http://www.forbes.com/sites/thomasbrewster/2015/02/02/bmw-door-hacking/

[9] Vulnerability Lab, "BMW ConnectedDrive - (Update) VIN Session Vulnerability," July 2016, (Accessed: 2016-11-17). [Online]. Available: https://www.vulnerability-lab.com/get_content.php?id=1736

[10] ——, "BMW - (Token) Client Side Cross Site Scripting Vulnerability," July 2016, (Accessed: 2016-11-17). [Online]. Available: https://www.vulnerability-lab.com/get_content.php?id=1737

[11] Keen Security Lab of Tencent, "Car Hacking Research: Remote Attack Tesla Motors," September 2016, (Accessed: 2016-11-17). [Online]. Available: http://keenlab.tencent.com/en/2016/09/19/Keen-Security-Lab-of-Tencent-Car-Hacking-Research-Remote-Attack-to-Tesla-Cars/

[12] Promon AS, "Updates and precisions on the Tesla hack," November 2016, (Accessed: 2016-11-25). [Online]. Available: https://promon.co/blog/updates-precisions-tesla-hack/

[13] Dustin Childs, "Pwn2Own Vancouver 2019: Wrapping Up and Rolling Out," March 2019, (Accessed: 2019-04-11). [Online]. Available: https://www.zerodayinitiative.com/blog/2019/3/22/pwn2own-vancouver-2019-wrapping-up-and-rolling-out

[14] BBC, "Fiat Chrysler recalls 1.4 million cars after Jeep hack," July 2015, (Accessed: 2019-04-11). [Online]. Available: https://www.bbc.com/news/technology-33650491

[15] ACEA European Automobile Manufacturers' Association, "Truck manufacturers call for action to prevent aftermarket manipulation of emissions controls," February 2017, (Accessed: 2019-04-16). [Online]. Available: https://www.acea.be/press-releases/article/truck-manufacturers-call-for-action-to-prevent-aftermarket-manipulation-of

[16] Lorenzo Franceschi-Bicchierai, "Hacker Finds He Can Remotely Kill Car Engines After Breaking Into GPS Tracking Apps," April 2019, (Accessed: 2019-04-28). [Online]. Available: https://motherboard.vice.com/en_us/article/zmpx4x/hacker-monitor-cars-kill-engine-gps-tracking-apps

[17] "ISO/IEC 15408:2009 Information technology – Security techniques – Evaluation criteria for IT security," International Organization for Standardization (ISO), Standard, 2009.

[18] "NIST FIPS PUB 199 – Standards for Security Categorization of Federal Information and Information Systems," National Institute of Standards and Technology, Standard, 2004. [Online]. Available: https://doi.org/10.6028/NIST.FIPS.199

[19] "NIST Special Publication 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations," National Institute

of Standards and Technology, Standard, 2013. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-53r4

[20] T. R. Hawkins, O. M. Gausen, and A. H. Strømman, "Environmental impacts of hybrid and electric vehicles—a review," *The International Journal of Life Cycle Assessment*, vol. 17, no. 8, pp. 997–1014, may 2012.

[21] "Serial Control and Communications Heavy Duty Vehicle Network - Top Level Document," SAE International, Tech. Rep., 08 2013. [Online]. Available: http://doi.org/10.4271/J1939_201308

[22] "ISO 26262:2011 Road Vehicles – Functional Safety," International Organization for Standardization (ISO), Standard, 2011.

[23] O. Henniger, L. Apvrille, A. Fuchs, Y. Roudier, A. Ruddle, and B. Weylr, "Security requirements for automotive on-board networks," in *2009 9th International Conference on Intelligent Transport Systems Telecommunications, (ITST)*. Institute of Electrical and Electronics Engineers (IEEE), oct 2009.

[24] M. M. Islam, A. Lautenbach, C. Sandberg, and T. Olovsson, "A risk assessment framework for automotive embedded systems," in *Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security - CPSS 16*. Association for Computing Machinery (ACM), 2016.

[25] Microsoft Corporation, "The stride threat model," 2005, (Accessed: 2017-02-23). [Online]. Available: https://msdn.microsoft.com/en-us/library/ee823878.aspx

[26] G. Macher, H. Sporer, R. Berlach, E. Armengaud, and C. Kreiner, "SAHARA: A security-aware hazard and risk analysis method," in *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2015*. EDAA, 2015.

[27] C. Schmittner, Z. Ma, and E. Schoitsch, "Combined safety and security development lifecylce," in *2015 IEEE 13th International Conference on Industrial Informatics (INDIN)*. Institute of Electrical and Electronics Engineers (IEEE), jul 2015.

[28] S. Burton, J. Likkei, P. Vembar, and M. Wolf, "Automotive functional safety = safety + security," in *Proceedings of the First International Conference on Security of Internet of Things - SecurIT 12*. Association for Computing Machinery (ACM), 2012.

[29] C. Schmittner and Z. Ma, "Towards a framework for alignment between automotive safety and security standards," in *Lecture Notes in Computer Science*. Springer Nature, 2015, pp. 133–143.

[30] J.-P. Blanquart, J.-M. Astruc, P. Baufreton, J.-L. Boulanger, H. Delseny, J. Gassino, G. Ladier *et al.*, "Criticality categories across safety standards in different domains," *ERTS-2012, Toulouse*, pp. 1–3, 2012.

[31] "IEC 62443 – Industrial communication networks - Network and system security," International Electrotechnical Comission, Standard, 2013.

[32] S. Galgano, M. Talas, W. Whyte, J. Petit, D. Benevelli, R. Rausch, and S. Sim, "Connected Vehicles Pilot Deployment Phase 1 – Security Management Operating Concept – New York City," 2016.

[33] "NIST Special Publication 800-38B – Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication," National Institute of Standards and Technology, Standard, 2005. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-38B

[34] AUTOSAR 4.4.0, *Specification of Secure Onboard Communication*, 2018, (Accessed: 2018-10-31). [Online]. Available: https://www.autosar.org/fileadmin/Releases_TEMP/Classic_Platform_4.4.0/Communication.zip

[35] S. Gürgens and D. Zelle, "A hardware based solution for freshness of secure onboard communication in vehicles," in *Computer Security*, S. K. Katsikas, F. Cuppens, N. Cuppens, C. Lambrinoudakis, A. Antón, S. Gritzalis, J. Mylopoulos, and C. Kalloniatis, Eds. Cham: Springer International Publishing, 2019, pp. 53–68.

[36] S. Nürnberger and C. Rossow, "vatiCAN - Vetted, Authenticated CAN Bus," in *Cryptographic Hardware and Embedded Systems – CHES 2016*, B. Gierlichs and A. Y. Poschmann, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 106–124.

[37] T. Rosenstatter and T. Olovsson., "Open problems when mapping automotive security levels to system requirements," in *Proceedings of the 4th International Conference on Vehicle Technology and Intelligent Transport Systems - Volume 1: VEHITS*, INSTICC. SciTePress, Mar 2018, pp. 251–260.

[38] T. Rosenstatter and T. Olovsson, "Towards a standardized mapping from automotive security levels to security mechanisms," in *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, Nov 2018, pp. 1501–1507.

[39] T. Rosenstatter, C. Sandberg, and T. Olovsson, "Extending AUTOSAR's Counter-based Solution for Freshness of Authenticated Messages in Vehicles," in *under submission*, 2019.

[40] M. Aramrattana, J. Detournay, C. Englund, V. Frimodig, O. U. Jansson, T. Larsson, W. Mostowski, V. D. Rodríguez, T. Rosenstatter, and G. Shahanoor, "Team Halmstad Approach to Cooperative Driving in the Grand Cooperative Driving Challenge 2016," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 4, pp. 1248–1261, April 2018.

[41] T. Rosenstatter and C. Englund, "Modelling the Level of Trust in a Cooperative Automated Vehicle Control System," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 4, pp. 1237–1247, April 2018.

Part II

Appended Papers