THESIS FOR THE DEGREE OF LICENTIATE OF ENGINEERING

On Cyber-Security for In-Vehicle Software

ALJOSCHA LAUTENBACH

Department of Computer Science and Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY
Göteborg, Sweden 2017

On Cyber-Security for In-Vehicle Software

Aljoscha Lautenbach

Technical report 170L
ISSN 1652-876X
Department of Computer Science and Engineering

Chalmers University of Technology
SE-412 96 GÖTEBORG, Sweden
Phone: +46 (0)31-772 10 00

Author e-mail: aljoscha@chalmers.se

Printed by Chalmers Reproservice
Göteborg, Sweden 2017

On Cyber-Security for In-Vehicle Software

Aljoscha Lautenbach

Department of Computer Science and Engineering, Chalmers University of Technology

Thesis for the degree of Licentiate of Engineering

ABSTRACT

We live in a highly connected world, which brings many opportunities, but which also makes us vulnerable to attacks. Security in regular IT systems, such as desktop and server systems, has decades of active research behind it, whereas security in the automotive domain is still a relatively new topic. Vehicular systems are highly computerized: each vehicle, depending on type, brand and model, contains in the order of 100 electronic control units which govern most of the vehicle's functions. In order to maintain traffic safety, it is therefore paramount that these systems are protected from malicious manipulation, and a natural question is how and to what extent "IT security" can be applied to automotive systems.

This thesis covers two different aspects of automotive security, namely how to embed security engineering practices into the automotive development lifecycle, and how automotive characteristics influence the technical design and implementation of security measures. To this end, we develop a risk assessment framework which is well aligned with existing safety processes, since safety engineering is an integral part of automotive system design. We also investigate which typical pitfalls an automotive software developer has to be aware of to avoid the inadvertent creation of software vulnerabilities. We further identify five criteria that an in-vehicle network authentication solution needs to fulfill to be considered for practical use, and we evaluate authentication solutions for the most common automotive bus according to those criteria. Finally, we analyze the typical architecture of a resource constrained electronic control unit for possibilities of exploiting memory corruption bugs, and how techniques from desktop and server systems can mitigate the effects.

We can conclude that it is possible to use adaptations of existing security solutions in automotive systems. However, a fair amount of adaptation work is needed to account for the particular characteristics of the automotive domain.

Keywords: Automotive Security, Vehicular Security, Risk Assessment, Secure Software Development, In-Vehicle Network, CAN authentication, Memory Protection, Memory Exploitation

Acknowledgments

First of all, I would like to thank my supervisors Tomas Olovsson and Magnus Almgren for their advise, insights, support and patience. I would also like to thank my colleagues at our various industrial partners for interesting discussions and fruitful collaboration. I am also grateful to my current and former colleagues at Chalmers for making it a great place to work! Naturally, I am indebted to my friends who, even after years of neglect, are still my friends; and to my parents and my sister who always supported me and believed in me. This chapter would be incomplete without thanking my sambo Melisa for sharing her life with me, and for all the fun we have together: Thank you! Finally, I would like to express my gratitude to you, dear reader, for taking an interest in this thesis.

Aljoscha Lautenbach
Göteborg, November 6, 2017

List of Appended Papers

Paper A Mafijul Md. Islam, **Aljoscha Lautenbach**, Christian Sandberg and Tomas Olovsson, "A risk assessment framework for automotive embedded systems", in *2nd ACM Cyber-Physical System Security Workshop (CPSS 2016)*[1], Xi'an, China, May 30, 2016, pp. 3 - 14.

Paper B **Aljoscha Lautenbach**, Magnus Almgren and Tomas Olovsson, "Secure software development for automotive systems", Technical Report 2017:06, ISSN 1652-926X.

Paper C Nasser Nowdehi, **Aljoscha Lautenbach** and Tomas Olovsson, "In-vehicle CAN message authentication: An evaluation based on industrial criteria", in *2017 IEEE 86th Vehicular Technology Conference (VTC2017-Fall)*, Toronto, Canada, September 24 - 27, 2017.

Paper D **Aljoscha Lautenbach**, Magnus Almgren and Tomas Olovsson, "What the stack? On memory exploitation and protection in resource constrained automotive systems", in *the 12th International Conference on Critical Information Infrastructures Security (CRITIS '17)*, Lucca, Italy, October 9 - 11, 2017.

[1] This paper received the best-paper award at CPSS 2016

Contents

List of Figures

Part I

Introductory Summary

1

Introduction to automotive security

"If we're going to be connected, then we need to be protected"

- Barack Obama

(January 2015)

It is no secret that our world is increasingly connected. This connectivity brings many opportunities, but it also brings many threats. As we become more and more dependent on connected services, the need to protect them from malicious manipulation rises in lock-step. This is certainly true for connected vehicles.

1.1 Motivation

For decades, the automotive industry only considered security in a physical sense to ensure that a vehicle can not be stolen or broken into. However, in the last decade this has been rapidly changing: automotive security now also encompasses computer security, which is also known as cyber-security [35, 60]. It should also be noted that security is distinct from safety. While the overall goal of security and safety is the same, namely the protection of the system and the humans operating in the system's environment, their underlying fault model is different: security is generally concerned with protection against intentional malicious manipulation, whereas safety is concerned with protection against random faults [5, 21, 56].

Cyber-security has risen sharply in importance in the automotive industry in the last decade and this can be attributed to several factors. One of the factors is that many automotive systems that used to be mechanical or analog are now digital, including safety-critical functions such as steering and braking [19]. This digitalization lowers production costs, simplifies maintenance and enables advanced signal processing on relatively simple hardware. However, it also opens the door for malicious manipulation since most functions are configurable and controlled by software [9, 12, 40, 66]. Another factor for the increased security interest is that there is a larger trend in society and across all industries to interconnect all types of devices to facilitate new types of services. The automotive industry is no exception: vehicles connect to "cloud" services, for instance for remote diagnostics or remote software updates [36, 37, 38], and user expectations are that devices such as smartphones integrate seamlessly into the vehicle [64]. As a consequence, attackers have a significantly larger attack surface [12], and the need for security rises [14]. The final factor we will consider is the advent of so called intelligent transport systems (ITS). ITS are being developed in an effort to increase road safety and traffic flow and they introduce completely new communication channels such as vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication [16]. This in turn poses risks if the communication infrastructure and the participating systems are not sufficiently protected [54].

Over the last 15 years, attacks on automotive systems have been demonstrated in theory and practice. In 2004, Wolf et al. [70] were among the first to discuss the lack of security features in vehicular networks in a scientific context. Larson and Nilsson highlighted several security issues, such as threats emanating from wireless networks in cars [41], and they simulated attacks on the CAN bus [52]. Nilsson et al. [53] did the same on the FlexRay bus, and Larson et al. [42] also provided initial insights into the use of Intrusion Detection Systems (IDS) in vehicular networks. In 2010, Koscher et al. [40] provided an experimental analysis of a vehicular network, and demonstrated practically that once an attacker gains access to the in-vehicle network (for instance via the On-Board Diagnostics (OBD) port), it is very easy to disrupt and manipulate the vehicle's operations. However, the attacks demonstrated by Koscher et al. still required physical access, which is why Checkoway et al. [12] investigated a vehicle's external attack surfaces and found that many of the communication channels were unprotected. In 2013, Miller and Valasek [66] presented a media effective hack of a Ford Escape and a Toyota Prius via the OBD port. Since then, they have presented new vehicle related security issues every year: in 2015, they hacked a Jeep Cherokee remotely with a reporter in it [49]. As a result, there is a rising public awareness that security is

needed, and customers start to demand basic security and privacy features in vehicles [64]. At this point, it should be self-evident that security mechanisms are necessary to protect automotive systems from malicious manipulation.

Thesis objective: The goal of this thesis is to further the understanding of the specific characteristics of the automotive domain, and how these characteristics influence the potential for cyber attacks and corresponding defensive techniques.

In particular, we investigate how and to what extent well-known processes and mechanisms from IT security can be adapted to the automotive domain.

1.2 Challenges in automotive system development

Automotive systems are subject to certain conditions which are significantly different from regular IT systems [19, 39, 63]. Before we can discuss security, it is necessary to understand the setting in which it is to be applied. Automotive systems have

- **long product life-times** (10 - 20 years).
- **long development lead times** (~5 years), and thus slow technology adoption.
- **high cost pressure** to stay competitive: all possible cost-savings must be considered.
- **highly heterogeneous hardware** which is less powerful than in regular IT systems (slower processors, less memory, etc.).
- **legal, safety and real-time requirements** which must be fulfilled, and which may differ in different regions of the world.

The long life-time implies that chosen security mechanisms must function for up to 20 years. New vulnerabilities are regularly found in all kinds of systems, which makes secure software updates necessary [15, 18]. However, remote software updates are only slowly being introduced in vehicles, which is partly due to the long development lead time. Development times for new vehicles are long, and new technology is used sparingly [19].

Furthermore, market pressure introduces several more challenges. An obvious factor is cost: profit margins are small, and all possible cost-savings must be considered [7]. This often leads to very minimal and very efficient systems. The used microprocessors only have as much computing

power and memory as is absolutely necessary, and a similar point can be made for communication bandwidth. Additionally, energy consumption must be kept as low as possible to be competitive and to adhere to different laws [13]. The legal frameworks can differ greatly in different regions of the world, and vehicle manufacturers must be able to adapt to them to avoid losing access to those markets [18, 47, 58].

All of the above are reasons why many of the security solutions which work well on desktop computers and servers are not directly applicable in an automotive setting. It is necessary to first understand the automotive context in which the solutions are to be applied, and then to adapt the security solutions to that concrete context. A direct transference is usually not possible, as we will show in this thesis.

In addition to the security issues, the increased connectivity of vehicles also poses questions about privacy and the correct handling of collected data [62]. More and more data is being accumulated, and it must be handled properly in order to guarantee the privacy of the customers or drivers involved. For instance, Gao et al. [23] have shown that with only speed information (as a time series), positioning information can be deduced (even when GPS location information has been removed), so that it is possible to track the path of a particular driver. Furthermore, Enev et al. [17] highlighted how easy it is to fingerprint a particular vehicle with the right sensor data. Consequently, privacy issues and privacy legislation must be taken into account when designing new systems, as we discuss further in chapter 2.

1.3 Thesis scope and domain background

The security issues discussed in this thesis span roughly three different areas. The first is the automotive safety lifecycle, which covers processes, imperatives and recommendations for the different development phases, and how security engineering processes can be added. The second area is the in-vehicle network and security issues associated with a particular part of the network, the controller area network bus. Finally, the security issues on individual electronic control units which form the nodes in the in-vehicle network are investigated. The relationship of the three areas and how the papers in this thesis fit into them is depicted in figure 1.1. The necessary background for each of the three areas will be introduced in the following subsections.

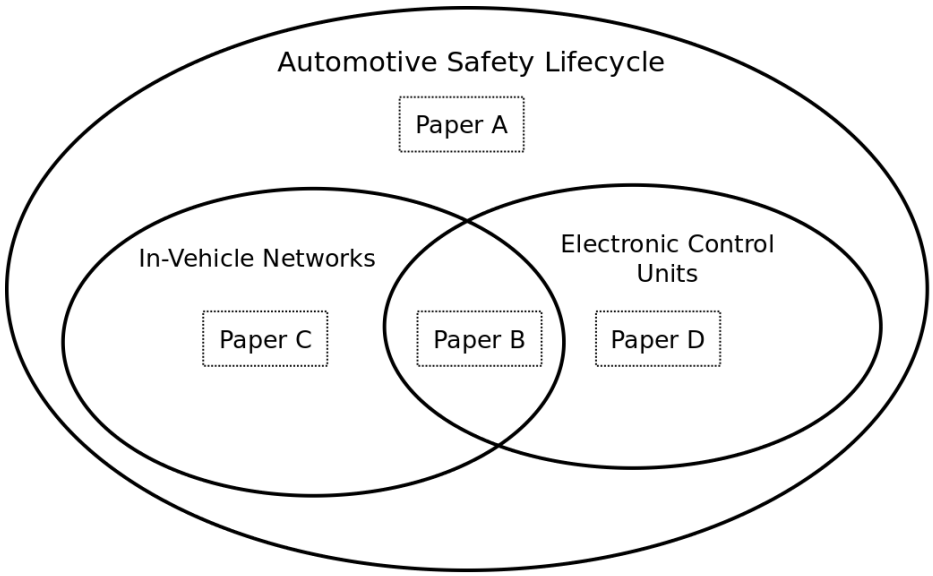

Figure 1.1: A visualization of the areas covered in this thesis

1.3.1 The automotive safety lifecycle

Due to the safety-critical nature of automotive systems, safety considerations are paramount and deeply entrenched in the development processes. Many companies follow the development model outlined in the functional safety standard for road vehicles ISO 26262 [27], which is an adaptation of the more general standard IEC 61508. In ISO 26262 a traditional V-model is assumed, which has three main phases: a concept phase, a product development phase and a production and operation phase. Note that the product development phase consists of several sub-phases. A typical example of a general V-model is depicted in figure 1.2, where the product development phase encompasses everything from “Requirements and Architecture” to “System Verification and Validation”.

The three main phases of the safety lifecycle can be summarized as follows. In the *concept phase* [28], an initial system design is developed, and the safety lifecycle is initiated. An important part of the concept phase is hazard analysis and risk assessment during which potential safety risks are assessed, and corresponding safety goals and automotive safety integrity levels (ASILs) are defined for each item in the system. Once the safety goals have been defined, the concept phase

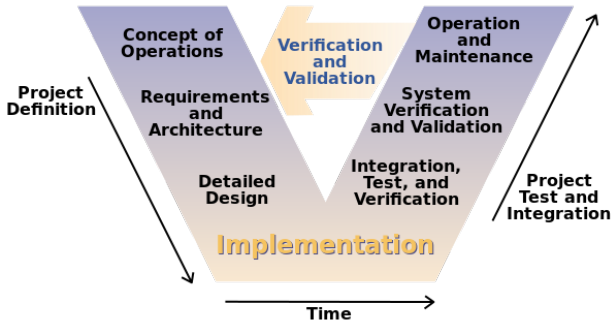

Figure 1.2: A typical V-model [55]

ends. The *product development phase* contains three additional nested V-models: "product development at the system level" [29], "product development at the hardware level" [30] and "product development at the software level" [31]. Each of them includes all the necessary development steps from requirements engineering to system integration and validation. The hardware and software development phases can be done in parallel. The product development phase ends with release for production. The final phase, *production and operation* [32], concerns the safe and correct production and operation of the product.

For both safety and security, risk assessment is an essential tool to guide and accompany the development process. An estimated risk rating for a potential negative event helps to determine for which events protection measures are needed, and to what degree. Risk is commonly estimated to be the product of the likelihood and the impact of the event. There are many risk assessment frameworks, but few were developed specifically for the automotive industry. In the HEAVENS project [1] we developed a security risk assessment framework which is closely aligned with the safety processes of ISO 26262. Standardization efforts for automotive security have started, but are far from completed, and the "HEAVENS model" for risk assessment was mentioned in the first security related automotive standard, the "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems", SAE J3061 [60]. Our risk assessment framework is presented in chapter 2.

1.3.2 The in-vehicle network

A modern vehicle has a long list of functions controlled by electronic control units (ECUs): adaptive cruise control, airbag deployment, anti-lock braking system, engine control, interior lighting, remote key-less entry, seat position control, telecommunication, etc. The ECUs which control these functions are interconnected, and in the following we introduce the technical background of vehicular networks.

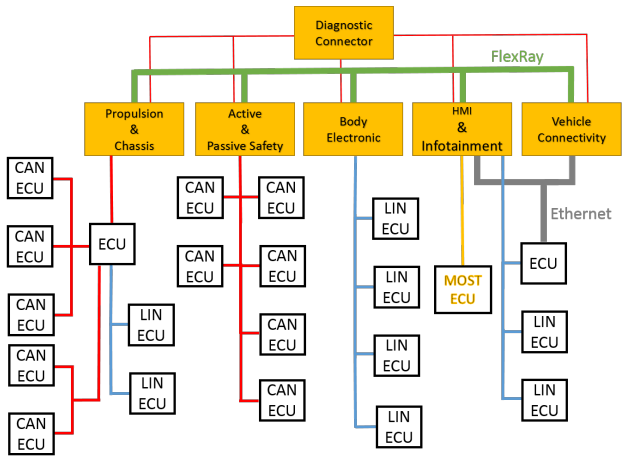

Figure 1.3: An example of an in-vehicle network with a FlexRay backbone

The communication infrastructure of a vehicle can be divided into its internal communication and its external communication. Internal communication includes signals, i.e., messages, between sensors, actuators and control units, for instance from the throttle sensor to the engine control unit to adjust the vehicle speed. External communication includes intelligent transport systems (ITS) related communication or communication to “cloud” services, such as remote music libraries or diagnostics servers. Most demonstrated attacks require a multi-layered approach: first the outer layers are compromised to serve as entry points to compromise the inner layers. In other words, a remote attacker needs to gain access to both the external and internal networks. Therefore, automotive security always needs to be holistic.

Depending on the type of vehicle, the brand and the precise model, modern vehicles typically contain somewhere around 30 - 150 electronic control units (ECUs). These ECUs form the internal,

or in-vehicle, network. This network consists of several different bus technologies. An example of such an in-vehicle network is depicted in figure 1.3, which is taken from chapter 4.

The most prevalent bus is the controller area network (CAN) bus, which is favored because it is cheap and predictable. Even though the technology is quite old and slow (max. speed 1 Mbit/s), it is still the most used bus for safety-critical automotive applications [63, 70]. An alternative is the faster but more complex and more expensive FlexRay bus (max. speed 10 Mbit/s). An adaptation of Ethernet for automotive systems is also used in some newer vehicles, and "automotive Ethernet" is generally anticipated to be an important part of future automotive bus systems [24, 25, 43]. For infotainment systems the comparatively expensive media oriented system transport (MOST) bus is often used, whereas the very cheap local interconnect (LIN) bus is the typical bus of choice for body electronics [63]. In addition, every vehicle has a diagnostic connector.

A combination of the above buses can be found in every vehicle, and yet, none of them include any kind of security measures on the physical, link or network layer. In chapter 4 of this thesis, we have investigated proposed authentication mechanisms for the CAN bus, identified the criteria they would need to fulfill in order to be used in practice and evaluated the proposed solutions according to those criteria.

1.3.3 Electronic control units

Table 1.1: Typical ranges of resource constrained microcontroller configurations

Hardware	Specification	Most Common
RAM	4 KB - 500 KB	40 KB
Flash Memory	256 KB - 6 MB	1 MB
Processor Speed	16 - 150 MHz	80 MHz

The nodes in the in-vehicle networks are so called electronic control units (ECUs). They are typically 16-bit or 32-bit microcontrollers with a limited amount of permanent and volatile storage, and with one or more network interfaces. Table 1.1, taken from chapter 5, lists some typical hardware choices for microcontrollers. In addition to being networked, many ECUs are connected to actuators and sensors to collect, process and act on control information, which is the hallmark

of cyber-physical systems. A simplified representation of the hardware of an electronic control unit, which is sufficient for our purposes, is depicted in figure 1.4.

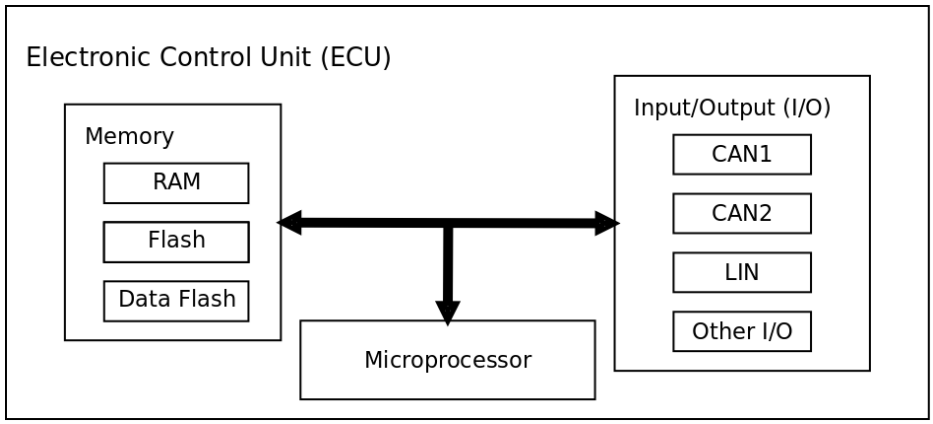

Figure 1.4: A simplified representation of an electronic control unit (ECU)

The architectures of those microcontrollers are highly heterogeneous. There are several different CPU architectures in common use, such as specific instruction sets from Renesas and Tricore, as well as ARM and PowerPC based architectures [4, 19, 22, 48, 50, 57]. Each of them have their own ways of interacting with and controlling their environment, and the corresponding memory architectures can vary widely. However, many of the underlying mechanisms are similar enough that their security properties can be analyzed, as we demonstrate in chapter 5.

The functions controlled by ECUs range from comfort functions over complex infotainment systems to safety-critical engine control systems. Even if a function is not safety-critical directly, it may still interact with safety-critical systems. That the integrity of safety-critical systems must be ensured should be self-evident, which is where security joins safety on stage.

Historically, embedded systems have had no or little need for security measures, because access to those systems often required physical access with specialized equipment. Since this is no longer the case, security mechanisms must be included in modern system designs.

Let us consider the case of memory management. On resource constrained ECUs memory is statically assigned, and the microcontrollers have a memory protection unit (MPU) which can segment the memory so that a task can not access the memory of another task. While this may be

sufficient from a safety point of view to guard against random faults, it does not protect against malicious manipulation, as we will discuss further in chapter 5.

There are several possibilities for an application to run on an electronic control unit. If the ECU is heavily resource constrained, the application may run directly on the processor, without any operating system. However, most ECUs have some form of real-time operating system which is responsible for scheduling and controlling the running applications. AUTOSAR is a platform which is being developed by a large consortium of automotive manufacturers and suppliers with the goal to increase software interoperability and to decrease development costs. It provides an interface standard and detailed development processes and guidelines. AUTOSAR is in widespread use in Europe, North-America and Japan, and it is likely that its adoption will continue to grow [33, 34].

There are several reasons why AUTOSAR is interesting from a security point of view. For one, the more ECUs run AUTOSAR, the more likely it is that hackers will target this platform for exploitation. This follows from the simple argument that platforms with more users are more popular targets for attackers: variations of Microsoft Windows are the most exploited desktop operating systems [51] and Android, as the most popular mobile operating system, has the largest share of mobile malware [71]. Another reason is that, since AUTOSAR offers an abstraction from the hardware and provides the same interface to all applications, it is possible to reason about the security on this platform without having to account for every possible hardware configuration. In chapter 3, we use an AUTOSAR case-study to highlight several of the typical security issues an automotive developer has to face.

1.4 Research questions

The research presented in this thesis aims to investigate and understand the specific security challenges in the automotive industry, and to adapt working security mechanisms and techniques from other domains to the automotive domain. The challenges identified in sections 1.2 and 1.3 lead us to the following research questions:

- **RQ1:** How can security engineering be integrated into automotive system development so that existing processes are impacted as little as possible?

- **RQ2:** How does the system architecture of automotive systems: (a) affect the creation and discovery of software vulnerabilities; and (b) influence the design of protective security mechanisms?
- **RQ3:** How do security mechanisms affect safety mechanisms in automotive systems, and vice versa?

RQ1: Security engineering encompasses all aspects of security: identifying threats, assessing the threats, implementing mitigating security measures, and adding forensic and recovery mechanisms [3]. However, due to the safety-critical nature of vehicular systems, automotive companies have strict development processes which must be observed, and changing these processes is not easy. Therefore, it is important to investigate how security engineering mechanisms and processes can be added to and integrated with existing automotive development processes.

RQ2: As outlined in section 1.2, the automotive industry has some unique challenges in system design. The results are highly customized systems which need to be analyzed from a security point of view: are there systematic vulnerabilities, and if so, can they be exploited? How does the specific architecture influence the design of protection mechanisms? Is it possible to use security mechanisms known from desktops and servers? If they can be used, do they need to be adapted, or can they be re-used as is? These are all questions which follow from RQ2, and which need to be investigated.

RQ3: Safety engineering has a long tradition in automotive systems, but the emergence of security engineering poses the interesting question how they affect each other. It is easy to imagine that some safety mechanisms such as redundancy can create security vulnerabilities which can be exploited. On the other hand, security mechanisms such as authentication could lead to safety issues: if for instance all breaking messages fail to authenticate and the breaks stop working completely. This interplay of safety and security in real automotive systems has seen relatively little research and is worth investigating further.

1.5 Paper summaries and contributions

In the following we summarize the papers included in this thesis. We put the papers into context, describe their contributions, and discuss to what degree they address the research questions presented above.

1.5.1 Paper A - A risk assessment framework for automotive embedded systems (chapter 2)

Problem statement. Risk assessment is an integral part of safety and security engineering to guide the implementation of safety and security measures. The automotive safety standard ISO 26262 [27] outlines procedures for the entire safety lifecycle, which includes hazard analysis and risk assessment (HARA). The outcome of the hazard analysis and risk assessment are high-level safety goals and an assignment of "automotive safety integrity levels (ASILs)". ASILs provide an indication of the level of safety needed. To date, no similar standard exists for automotive security. Since ISO 26262 has already been adopted by many automotive companies, it is logical that new security processes should be well aligned with the ISO standard. To that end, we propose a risk assessment framework to derive "security levels" to provide an indication of the level of security a particular system should have, similar to ASILs.

Related work. The pioneering risk rating methodology for automotive electrical and/or electronic (E/E) systems stems from the EVITA project [59]. In the EVITA approach [26, 59], the estimation of threat level and attack potential is inspired by Common Criteria [11] (a well known standard for security evaluations). Wolf and Scheibel [69] further refined the ideas by Henniger et al. [26], and also combine existing techniques into a risk rating framework for automotive systems. Several other security risk assessment approaches have been proposed which integrate directly into existing safety processes [8, 45, 46, 61]. In contrast, we propose an independent risk assessment for security purposes which run in parallel with the safety processes, because it requires a different set of expertise.

Contributions. The design of our risk assessment framework, specifically tailored towards the automotive industry, was heavily influenced by RQ1, i.e., how to add security engineering practices to automotive development processes with minimal changes to existing processes. In order to achieve that goal, our risk assessment framework is closely aligned with the processes of the widely used safety standard ISO 26262. Moreover, to further facilitate its practical adoption, it combines elements from several additional standards such as Common Criteria [10] and BSI 100-4 [20]. The first international standard which addresses automotive cyber-security, SAE standard "J3061 - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems" [60], includes the "HEAVENS" model which paper A is based on as one of several possible risk assessment frameworks.

1.5.2 Paper B - Secure software development for automotive systems (chapter 3)

Problem statement. Secure software development is hard: it requires some training to identify the patterns which constitute code vulnerabilities. Moreover, until recently security was of little concern in vehicular software. Most automotive software developers are well trained in writing software that adheres to safety regulations, but they often lack similar training for security. In paper B we develop a simple AUTOSAR application to demonstrate the various security issues and pitfalls one encounters during the implementation. This paper has tutorial character and is aimed at automotive software developers.

Related work. The difficulties of implementing cryptographic software or even using cryptographic libraries correctly are well documented [2, 44]. Murvay et al. [50] evaluated state-of-the-art automotive microcontrollers for their ability to process cryptographic primitives and they found that the results varied largely. Bernardeschi et al. [6] propose an integration of security requirements into the specification of AUTOSAR application components.

Contributions. We demonstrate that security is a pervasive design issue by identifying various pitfalls in securing a simple AUTOSAR application on several conceptual levels: Organizational, Architectural and Implementation. We also give recommendations for each identified security issue. We partly address both RQ1 and RQ2 by show-casing that some of the responsibility for implementing security measures can be put on the software developers without affecting existing processes much, if the developers receive security training. RQ3 is also partially addressed by highlighting how some of the AUTOSAR safety features are beneficial for security.

1.5.3 Paper C - In-vehicle CAN message authentication: An evaluation based on industrial criteria (chapter 4)

Problem statement. The controller area network (CAN) bus is still the most prevalent bus in in-vehicle networks. The underlying technology and protocols are over 30 years old, and, as can be expected, include no security features. Many solutions have been proposed to add authentication to the CAN bus, but few, if any, of them have been implemented in practice. In an effort to identify the cause, we, with help from industry experts, identified five requirements that such an authentication solution would have to fulfill in order to be a viable option for practical use. We then evaluated the most promising authentication solutions according to those industrial criteria.

Related work. The security problems of the CAN bus have been highlighted in many publications, for instance in [9, 40, 63, 70] to name but a few. Vasile et al. [68] evaluated the performance of several proposed CAN message authentication solutions on CAN-FD and FlexRay. We are not aware of any other work which compares or evaluates the various CAN message authentication solutions.

Contributions. We provide a comprehensive overview of the most promising CAN authentication solutions, and compare them according to five industrial criteria: "cost-effectiveness", "backward compatibility", "support for vehicle repair and maintenance", "sufficient implementation details" and "acceptable overhead". We find that no solution meets all five criteria, with backward compatibility and acceptable overhead being the biggest adoption hurdles for CAN authentication. We further find that a partial answer to RQ1 is to demand backward compatibility from security mechanisms. RQ2 is also partially answered: the wide-spread use of CAN is questionable from a security point of view, and despite efforts to strengthen the provided security by adding authentication, no solution to this difficult problem has been found yet. RQ3 on the other hand is only lightly touched upon to the extend that one of the solutions uses an existing safety mechanism to add a security mechanism on top of it.

1.5.4 Paper D - What the stack? On memory exploitation and protection in resource constrained automotive systems (chapter 5)

Problem statement. Memory corruption bugs are arguably among the most dangerous kinds of software bugs, since their exploitation can grant the attacker a large degree of control over the attacked system. On regular IT systems, such as desktops and servers, a figurative war has been and is being fought for control of system memory. More advanced protection mechanisms regularly elicit even more advanced attacks. For resource constrained embedded automotive systems, however, this development has been without consequence so far. Nevertheless, the increased connectivity of vehicles necessitates that the possibilities for exploiting memory corruption bugs are investigated. This paper does just that.

Related work. Van der Veen et al. [67] and Szekeres et al. [65] independently provided a historic overview and a classification of different types of memory corruption bugs. We are not aware of any work that specifically discusses memory corruption bugs in the context of constrained automotive systems.

Contributions. In chapter 5, we discuss and analyze the typical hardware architecture of an electrical control unit, and how the architecture affects memory exploitation and protection techniques. We discuss that currently deployed systems have little to no memory protection, and that stack-based memory corruption bugs can be exploited. However, well-known techniques such as stack canaries and non-executable RAM can considerably decrease the risk of successful exploitation. This work directly addresses RQ2, and slightly addresses RQ3 by once again pointing out some safety procedures which have a positive impact on security.

1.6 Concluding remarks

This thesis covers two different aspects of automotive security, namely how to embed security engineering practices into the automotive development lifecycle, and how automotive characteristics influence the technical design and implementation of security measures.

We make several contributions to improve the state of automotive security. In chapter 2, we propose a risk assessment framework to identify and rate threats to automotive systems with a "security level". The security levels can then guide the further development process of security-relevant functions in a similar fashion that ASILs guide the development process for safety-critical functions. In chapter 3, we demonstrate that developer training is necessary in order to avoid the inadvertent creation of software vulnerabilities. In chapter 4, we discuss various authentication solutions for the most prevalent automotive bus, the CAN bus. We evaluate several CAN authentication solutions according to five industrial criteria we identified, and we find that none of the solutions fulfill all criteria. Finally, in chapter 5, we analyze the architecture of a resource constrained electronic control unit for its vulnerability of exploiting memory corruption bugs for attacks. We find that stack-based buffer overflow attacks work as expected, but that the protection mechanisms of stack canaries and non-executable RAM, which are commonplace in desktop and server systems, should mitigate the problem.

Automotive security has become a very active research field, and vehicle manufacturers and suppliers have understood that this topic requires attention. Despite these recent advances, a lot of open questions remain and they need to be answered soon: the first steps to realize intelligent transport systems and self-driving cars have already been taken.

References

[1] HEAVENS: HEAling Vulnerabilities to ENhance Software Security and Safety – Project Proposal, December 2012.

[2] R. Anderson. Why cryptosystems fail. In *Proceedings of the 1st ACM Conference on Computer and Communications Security*, CCS '93, pages 215–227, New York, NY, USA, 1993. ACM.

[3] R. J. Anderson. *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons, 2010.

[4] ARM. *ARMv7-M Architecture Reference Manual*, December 2014. `https://developer.arm.com/docs/ddi0403/e/armv7-m-architecture-reference-manual`.

[5] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, 1(1):11–33, 2004.

[6] C. Bernardeschi, G. Del Vigna, M. Di Natale, G. Dini, and D. Varano. Using autosar high-level specifications for the synthesis of security components in automotive systems. In J. Hodicky, editor, *Modelling and Simulation for Autonomous Systems: Third International Workshop, MESAS 2016, Rome, Italy, June 15-16, 2016, Revised Selected Papers*, pages 101–117. Springer International Publishing, 2016.

[7] S. Biller, L. M. A. Chan, D. Simchi-Levi, and J. Swann. Dynamic pricing and the direct-to-customer model in the automotive industry. *Electronic Commerce Research*, 5(2):309–334, 2005.

[8] 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, pages 150–159, New York, NY, USA, 2012. ACM.

[9] P. Carsten, T. R. Andel, M. Yampolskiy, and J. T. McDonald. In-vehicle networks: Attacks, vulnerabilities, and proposed solutions. In *Proceedings of the 10th Annual Cyber and Information Security Research Conference*, pages 1–8. ACM, 2015.

[10] CCRA Members. *Common Criteria for Information Technology Security Evaluation*. CCMB-2012-09-00X, Version 3.1, Revision 4.

[11] CCRA Members. *Common Methodology for Information Technology Security Evaluation – Evaluation Methodology*, chapter Vulnerability Assessment (AVA), pages 404 – 433. September 2012. CCMB-2012-09-004, Version 3.1, Revision 4.

[12] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno. Comprehensive experimental analyses of automotive attack surfaces. In *Proceedings of the 20th USENIX Security Symposium*, pages 77–92, San Francisco, CA, USA, Aug. 2011.

[13] F. Chiara and M. Canova. A review of energy consumption, management, and recovery in automotive systems, with considerations of future trends. *Proceedings of the Institution of Mechanical Engineers, Part D: Journal of Automobile Engineering*, 227(6):914–936, 2013.

[14] I. G. Cohen, S. Hoffman, and E. Y. Adashi. Your money or your patient's life? Ransomware and electronic health records. *Annals of Internal Medicine*, 167(8):587–588, 2017.

[15] A. Costin, J. Zaddach, A. Francillon, D. Balzarotti, and S. Antipolis. A large-scale analysis of the security of embedded firmwares. In *USENIX Security Symposium*, pages 95–110, 2014.

[16] G. Dimitrakopoulos and P. Demestichas. Intelligent transportation systems. *IEEE Vehicular Technology Magazine*, 5(1):77–84, March 2010.

[17] M. Enev, A. Takakuwa, K. Koscher, and T. Kohno. Automobile driver fingerprinting. *Proceedings on Privacy Enhancing Technologies*, 2016(1):34–50, 2016.

[18] ENISA. Cyber security and resilience of smart cars, January 2017. https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars.

[19] J. Erjavec and R. Thompson. *Automotive technology: a systems approach*. Cengage Learning, 2014.

[20] Federal Office for Information Security (BSI), Germany. *BSI-Standard 100-4 – Business Continuity Management*. 2009.

[21] D. G. Firesmith. Common concepts underlying safety security and survivability engineering. Technical Report CMU/SEI-2003-TN-033, Software Engineering Institute - Carnegie Mellon University, Dec 2003.

[22] P. Gai and M. Violante. Automotive embedded software architecture in the multi-core age. In *2016 21st IEEE European Test Symposium (ETS)*, pages 1–8, May 2016.

[23] X. Gao, B. Firner, S. Sugrim, V. Kaiser-Pendergrast, Y. Yang, and J. Lindqvist. Elastic pathing: Your speed is enough to track you. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, UbiComp '14, pages 975–986, New York, NY, USA, 2014. ACM.

[24] P. Hank, S. Müller, O. Vermesan, and J. Van Den Keybus. Automotive ethernet: In-vehicle networking and smart mobility. In *Proceedings of the Conference on Design, Automation and Test in Europe*, DATE '13, pages 1735–1739, San Jose, CA, USA, 2013. EDA Consortium.

[25] P. Hank, T. Suermann, and S. Müller. Automotive ethernet, a holistic approach for a next generation in-vehicle networking standard. In G. Meyer, editor, *Advanced Microsystems for Automotive Applications 2012: Smart Systems for Safe, Sustainable and Networked Vehicles*, pages 79–89, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[26] O. Henniger, L. Apvrille, A. Fuchs, Y. Roudier, A. Ruddle, and B. Weyl. Security requirements for automotive on-board networks. In *Proceedings of the 9th International Conference on Intelligent Transport System Telecommunications (ITST)*, 2009.

[27] ISO. Road vehicles — Functional safety, 2011. ISO 26262:2011.

[28] ISO. Road vehicles — Functional safety — Part 3: Concept phase , 2011. ISO 26262-3:2011.

[29] ISO. Road vehicles — Functional safety — Part 4: Product development at the system level, 2011. ISO 26262-4:2011.

[30] ISO. Road vehicles — Functional safety — Part 5: Product development at the hardware level, 2011. ISO 26262-5:2011.

[31] ISO. Road vehicles — Functional safety — Part 6: Product development at the software level, 2011. ISO 26262-6:2011.

[32] ISO. Road vehicles — Functional safety — Part 7: Production and operation, 2011. ISO 26262-7:2011.

[33] E. Juliussen. Automotive Software: Trends, Importance and Opportunities, 2017. https://at.projects.genivi.org/wiki/download/attachments/14549424/GENIVI%20May%202017-Egil.pdf?version=1&modificationDate=1495125475000&api=v2.

[34] E. Juliussen and R. Robinson. Is europe in the driver's seat? the competitiveness of the european automotive embedded systems industry. *Institute for Prospective Technological Studies, European Comission, Londres*, 2010. https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/europe-drivers-seat-competitiveness-european-automotive-embedded-systems-industry.

[35] R. A. Kemmerer. Cybersecurity. In *25th International Conference on Software Engineering, 2003. Proceedings.*, pages 705–715, May 2003.

[36] P. Kleberger and T. Olovsson. Protecting vehicles against unauthorised diagnostics sessions using trusted third parties. In F. Bitsch, J. Guiochet, and M. Kaâniche, editors, *Computer Safety, Reliability, and Security: 32nd International Conference, SAFECOMP 2013, Toulouse, France, September 24-27, 2013. Proceedings*, pages 70–81, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[37] P. Kleberger and T. Olovsson. Securing vehicle diagnostics in repair shops. In A. Bondavalli and F. Di Giandomenico, editors, *Computer Safety, Reliability, and Security: 33rd International Conference, SAFECOMP 2014, Florence, Italy, September 10-12, 2014. Proceedings*, pages 93–108. Springer International Publishing, 2014.

[38] P. Kleberger, T. Olovsson, and E. Jonsson. An in-depth analysis of the security of the connected repair shop. In *The Seventh International Conference on Systems and Networks Communications (ICSNC), Proceedings. Lisbon, 18-23 November, 2012. IARIA.*, page 99, 2012.

[39] P. Koopman. Embedded system security. *Computer*, 37(7):95–97, July 2004.

[40] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage. Experimental security analysis of a modern automobile. In *Security and Privacy (SP), 2010 IEEE Symposium on*, pages 447–462, May 2010.

[41] U. E. Larson and D. K. Nilsson. Securing vehicles against cyber attacks. In *Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead*, CSIIRW '08, pages 30:1–30:3, New York, NY, USA, 2008. ACM.

[42] U. E. Larson, D. K. Nilsson, and E. Jonsson. An approach to specification-based attack detection for in-vehicle networks. In *Intelligent Vehicles Symposium, 2008 IEEE*, pages 220–225. IEEE, 2008.

[43] J. Lastinec and L. Hudec. Approach to securing in-vehicle communication using ethernet/IP. Dec 2014.

[44] D. Lazar, H. Chen, X. Wang, and N. Zeldovich. Why does cryptographic software fail?: A case study and open problems. In *Proceedings of 5th Asia-Pacific Workshop on Systems*, APSys'14, pages 7:1–7:7, New York, NY, USA, 2014. ACM.

[45] G. Macher, A. Höller, H. Sporer, E. Armengaud, and C. Kreiner. A combined safety-hazards and security-threat analysis method for automotive systems. In *Computer Safety, Reliability, and Security*, pages 237–250. Springer, 2015.

[46] G. Macher, H. Sporer, R. Berlach, E. Armengaud, and C. Kreiner. Sahara: a security-aware hazard and risk analysis method. In *Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition*, pages 621–624. EDA Consortium, 2015.

[47] S. E. Markey. Security and privacy in your (spy) car act of 2017. Technical report, March 2017. `https://www.congress.gov/bill/115th-congress/senate-bill/680`.

[48] A. Mayer and F. Hellwig. System performance optimization methodology for Infineon's 32-bit automotive microcontroller architecture. In *Proceedings of the Conference on Design, Automation and Test in Europe*, DATE '08, pages 962–966, New York, NY, USA, 2008. ACM.

[49] C. Miller and C. Valasek. Remote Exploitation of an Unaltered Passenger Vehicle. Technical report, Defcon 23, August 2015. `http://illmatics.com/Remote%20Car%20Hacking.pdf`.

[50] P. S. Murvay, A. Matei, C. Solomon, and B. Groza. Development of an autosar compliant cryptographic library on state-of-the-art automotive grade controllers. In *2016 11th International Conference on Availability, Reliability and Security (ARES)*, pages 117–126, Aug 2016.

[51] K. Nayak, D. Marino, P. Efstathopoulos, and T. Dumitraş. Some vulnerabilities are different than others. In *International Workshop on Recent Advances in Intrusion Detection*, pages 426–446. Springer, 2014.

[52] D. K. Nilsson and U. E. Larson. Simulated attacks on can buses: vehicle virus. In *IASTED International conference on communication systems and networks (AsiaCSN)*, pages 66–72, 2008.

[53] D. K. Nilsson, U. E. Larson, F. Picasso, and E. Jonsson. A first simulation of attacks in the automotive network communications protocol flexray. In *Proceedings of the International Workshop on Computational Intelligence in Security for Information Systems CISIS'08*, pages 84–91. Springer, 2009.

[54] N. Nowdehi and T. Olovsson. Experiences from implementing the ETSI ITS SecuredMessage service. In *2014 IEEE Intelligent Vehicles Symposium Proceedings*, pages 1055–1060, June 2014.

[55] L. Osborne, J. Brummond, R. D. Hart, M. Zarean, and S. M. Conger. Clarus: Concept of operations. Technical Report FHWA-JPO-05-072, United States. Federal Highway Administration, 2005.

[56] L. Piètre-Cambacédès and M. Bouissou. Cross-fertilization between safety and security engineering. *Reliability Engineering & System Safety*, 110:110–126, 2013.

[57] C. P. Quigley, R. McMurran, R. P. Jones, and P. T. Faithfull. An investigation into cost modelling for design of distributed automotive electrical architectures. In *2007 3rd Institution of Engineering and Technology Conference on Automotive Electronics*, pages 1–9, June 2007.

[58] C. Ratcliff. *Fact Sheets of the European Union - Road traffic and safety provisions*, March 2017. `http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_5.6.5.html`.

[59] A. Ruddle, D. Ward, B. Weyl, S. Idrees, Y. Roudier, M. Friedewald, T. Leimbach, A. Fuchs, S. Gürgens, O. Henniger, R. Rieke, M. Ritscher, H. Broberg, L. Apvrille, R. Pacalet, and G. Pedroza. Security requirements for automotive on-board networks based on dark-side scenarios. EVITA Project, Deliverable D2.3, v1.1., Dec. 2009.

[60] SAE International. SAE J3061_201601 - Cybersecurity guidebook for cyber-physical vehicle systems, Jan. 2016.

[61] C. Schmittner, T. Gruber, P. Puschner, and E. Schoitsch. Security application of failure mode and effect analysis (FMEA). In *Computer Safety, Reliability, and Security*, pages 310–325. Springer, 2014.

[62] D. J. Solove. I've got nothing to hide and other misunderstandings of privacy. *San Diego L. Rev.*, 44:745, 2007.

[63] I. Studnia, V. Nicomette, E. Alata, Y. Deswarte, M. Kaaniche, and Y. Laarouchi. Survey on security threats and protection mechanisms in embedded automotive networks. In *2013 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W)*, pages 1–12, 2013.

[64] M. K. Svangren, M. B. Skov, and J. Kjeldskov. The connected car: An empirical study of electric cars as mobile digital devices. In *Proceedings of the 19th International Conference on Human-Computer Interaction with Mobile Devices and Services*, MobileHCI '17, pages 6:1–6:12, New York, NY, USA, 2017. ACM.

[65] L. Szekeres, M. Payer, T. Wei, and D. Song. SoK: Eternal War in Memory. In *2013 IEEE Symposium on Security and Privacy (SP)*, pages 48–62, May 2013.

[66] C. Valasek and C. Miller. Adventures in Automotive Networks and Control Units. Technical report, Defcon 21, August 2013. `http://www.ioactive.com/pdfs/~IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf`.

[67] V. Van der Veen, N. dutt-Sharma, L. Cavallaro, and H. Bos. Memory errors: the past, the present, and the future. In *Proceedings of the 15th International Symposium on Research in Attacks, Intrusions, and Defenses*, pages 86–106. Springer, 2012.

[68] P. Vasile, B. Groza, and S. Murvay. Performance analysis of broadcast authentication protocols on CAN-FD and FlexRay. In *Proceedings of the WESS'15: Workshop on Embedded Systems Security*, WESS'15, pages 7:1–7:8, New York, NY, USA, 2015. ACM.

[69] M. Wolf and M. Scheibel. A systematic approach to a qualified security risk analysis for vehicular IT systems. In E. Plödereder, P. Dencker, H. Klenk, H. B. Keller, and S. Spitzer, editors, *Automotive - Safety & Security 2012*, Lecture Notes in Informatics, pages 195–210. Gesellschaft für Informatik, Bonn, 2012.

[70] M. Wolf, A. Weimerskirch, and C. Paar. Security in automotive bus systems. In *Workshop on Embedded Security in Cars*, 2004.

[71] Y. Zhou and X. Jiang. Dissecting Android malware: Characterization and evolution. In *2012 IEEE Symposium on Security and Privacy*, pages 95–109, May 2012.