THESIS FOR THE DEGREE OF LICENTIATE OF ENGINEERING

# On Securing Vehicular Communications

Methods and Recommendations for Secure In-vehicle and Car2X Communications

NASSER NOWDEHI

*Division of Networks and Systems*
*Department of Computer Science and Engineering*
CHALMERS UNIVERSITY OF TECHNOLOGY
Göteborg, Sweden 2017

**On Securing Vehicular Communications**

Methods and Recommendations for Secure In-vehicle and Car2X Communications

*Nasser Nowdehi*



Technical report 160L
ISSN 1652-876X
Department of Computer Science and Engineering
Division of Networks and Systems
Research group: Systems Security

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

Author e-mail: nasser.nowdehi@chalmers.se

Printed by Chalmers Reproservice
Göteborg, Sweden 2017

# On Securing Vehicular Communications

Methods and Recommendations for Secure In-vehicle and Car2X Communications

Nasser Nowdehi

*Division of Networks and Systems, Chalmers University of Technology*

Thesis for the degree of Licentiate of Engineering, an intermediate degree between M.Sc. and Ph.D.

## ABSTRACT

Today's vehicles contain approximately more than 100 interconnected computers (ECUs), several of which will be connected to the Internet or external devices and networks around the vehicle. In the near future vehicles will extensively communicate with their environment via Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) (together called V2X) communications. Such level of connectivity enables car manufacturers to implement new entertainment systems and to provide safety features to decrease the number of road accidents. Moreover, authorities can deploy the traffic information provided by vehicular communications to improve the traffic management. Despite the great benefits that comes with vehicular communications, there are also risks associated with exposing a safety-critical integrated system to external networks. It has already been proved that vehicles can be remotely hacked and the safety critical functions such as braking system and steering wheel can be compromised to endanger the safety of passengers. This puts high demands on IT security and car manufacturers to secure vehicular communications. In this thesis, we propose methods and recommendations for improving the security of internal and external vehicular communications.

The thesis is divided into two parts. In the first part, we identify weaknesses or deficiencies in the design of the ETSI V2X security standard and propose changes to fix the identified weaknesses or deficiencies. The second part of the thesis focuses on the security of the internal vehicular communications. First, in order to facilitate the implementation of security measures in in-vehicle networks, we propose an automated approach for grouping in-vehicle ECUs into domains based on different criteria. Then, we compare such an automatically generated in-vehicle network architecture with a reference architecture model to show that our approach is able to identify meaningful domains with better quality with respect to communication, safety and security. Finally, we seek to evaluate the applicability of existing CAN bus authentication solutions to a vehicular context. To this end, and in cooperation with industry, we have identified five critical requirements for an authentication solution to be used in such a context. We found that no authentication solution fulfilled all the requirements, something that indicates that the CAN bus may not be suitable for secure vehicular applications.

***Index terms—*** ETSI, V2X, in-vehicle network, security, vehicular communication

# THESIS

This thesis consists of an introductory summary and the following appended papers.

## Part I: Towards Securing the External Vehicular Communications

### ▷ Paper A

**Nasser Nowdehi**, Tomas Olovsson, "Experiences from implementing the ETSI ITS SecuredMessage service," in *IEEE Intelligent Vehicles Symposium Proceedings*, Dearborn, Michigan, USA, June 8-11, 2014, pp. 1055-1060.

## Part II: Towards Securing the Internal Vehicular Communications

### ▷ Paper B

Pierre Kleberger, **Nasser Nowdehi** and Tomas Olovsson, "Towards designing secure in-vehicle network architectures using community detection algorithms," in *IEEE Vehicular Networking Conference (VNC)*, Paderborn, Germany, December 3-5, 2014, pp. 69-76.

### ▷ Paper C

**Nasser Nowdehi**, Pierre Kleberger and Tomas Olovsson, "Improving in-vehicle network architectures using automated partitioning algorithms," in *IEEE Vehicular Networking Conference (VNC)*, Kyoto, Japan, December 16-18, 2015, pp. 259-266.

### ▷ Paper D

**Nasser Nowdehi**, Aljoscha Lautenbach and Tomas Olovsson, "In-vehicle CAN message authentication: An evaluation based on industrial criteria," submitted to *2017 IEEE Intelligent Vehicles Symposium*

# Acknowledgments

Firstly, I would like to express my sincere gratitude to my supervisor at Chalmers, Associate Professor Tomas Olovsson for the continuous support of my Ph.D study, for his patience, for his useful guidance and insightful comments. I would like to express my deep gratitude and appreciation to my industrial supervisor, Henrik Broberg for his generous support, his understanding, and especially for giving me the opportunity to study a PhD. I shall extend my thanks to my examiner Professor Erland Jonsson for his constructive feedback and kind assistance.
I also would like to thank current and former members of the security group at Chalmers for their support and of course their friendship. Thanks Aljoscha Lautenbach, Aras Atalar, Behrooz Sangchoolie, Boel Nelson, Elena Pagnin, Farnaz Moradi, Fatemeh Ayatolahi, Hamid Ebadi, Iosif Salem, Associate Professor Magnus Almgren, Pierre Kleberger, Thomas Rosenstatter and Valentin Tudor.

I would also like to thank Volvo Car Corporation and VINNOVA for funding my research within the two projects SEFRAM and HoliSec. Special thanks go to Stefan Andreasson, Kristian Calais, Mikel Nilsson, Jörgen Borg, Hans Alminger and Ubaid Khan.
Last, but not the least, I would like to thank my family: my parents, my brothers and my wife, for their constant love, encouragement, and moral support throughout my studies and my life in general.

Nasser Nowdehi
Göteborg, February 2017

# Contents

# Introductory Summary

# 1

# Introduction

The introduction of Electronic Control Units (ECUs) in vehicles was made decades ago, and the early versions of ECUs were used only for controlling engine fuel injection. Nowadays, a vehicle consists of more than hundred ECUs, sensors and actuators that control almost every function such as braking, steering, driving assistance, air conditioning, and in-car entertainment. Figure 1.1 shows a picture of functions and systems that are controlled by these small computers (ECUs). The in-vehicle networks are also able to communicate with the outside networks via Internet or Intelligent Transportation System (ITS) networks that enable Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I, together called V2X) communications. The ITS communications enable vehicles and roadside units to exchange traffic and safety related messages to improve the road safety and traffic management efficiency. The introduction of computers in vehicles has enabled car manufacturers to develop autonomous vehicles to, above all, eliminate the risk of human factors in road hazards. The computerization of vehicles improves road safety, passenger comfort, and traffic management, however, it also makes vehicles prone to cyber attacks that can endanger the safety of passengers. In recent years, security threats against vehicles' internal and external communications have proved to affect the safety of passengers [23, 33], mainly because the in-vehicle networks were insecure. Unfortunately, due to the constraints and requirements of the automotive life cycle, most traditional IT security solutions are not directly applicable to vehicles. This puts high demands on IT security and car manufacturers to ensure that it is not the communications that threaten the life of passengers by affecting the safety of the in-vehicle electrical systems. In this thesis, we aim to propose methods and recommendations for improving the security of the in-vehicle network and V2X communications.

This introductory summary is organized as follows. In Section 1.1 the in-vehicle network architecture and ITS communications are described. Then, the objective of this thesis is given in Section 1.2. The appended papers are summarized in Section 1.3 followed by a summary of the contributions of the thesis in Section 1.4. Finally, a conclusion is given in Section 1.5.

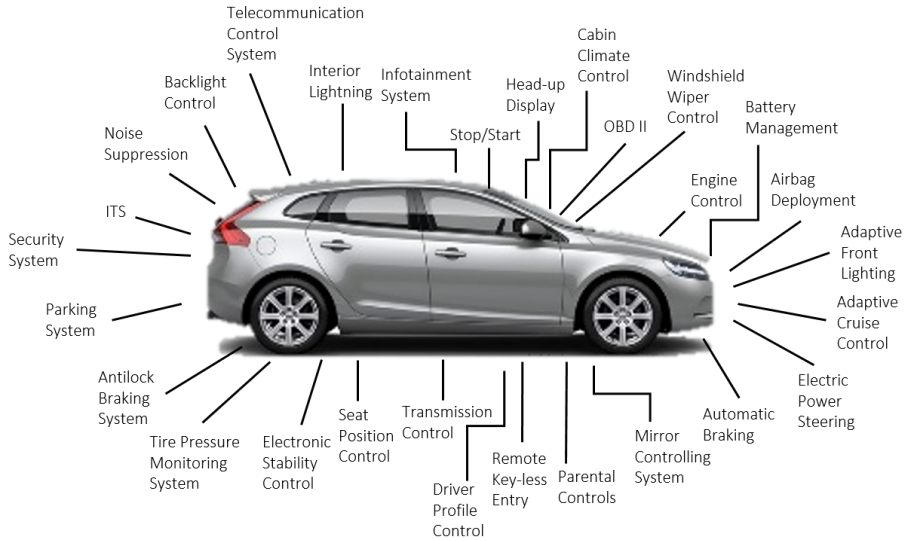


Figure 1.1: Examples of systems that are controlled by ECUs in a modern vehicle

## 1.1 Background

### 1.1.1 In-vehicle network

The in-vehicle network of a modern car consists of more than 100 ECUs which are connected to each other via different bus technologies such as Controller Area Network (CAN), Local Interconnect Network (LIN), Media Oriented Systems Transport (MOST), and FlexRay. As shown in Figure 1.2, In-vehicle networks are usually divided into several interconnected domains, and each domain has one or more buses depending on the cost, speed and timing requirements of the functions being implemented in the domain. These domains can communicate with each other through gateway ECUs that are connected to each other via a backbone. CAN and LIN are the most commonly used buses and many of the major functions of vehicles are implemented on CAN and LIN ECUs. In recent years, car manufacturers have shown interest in adapting Ethernet to vehicles and it is currently being standardized for use in automotive systems.

There are many aspects to consider when developing an in-vehicle network. These design

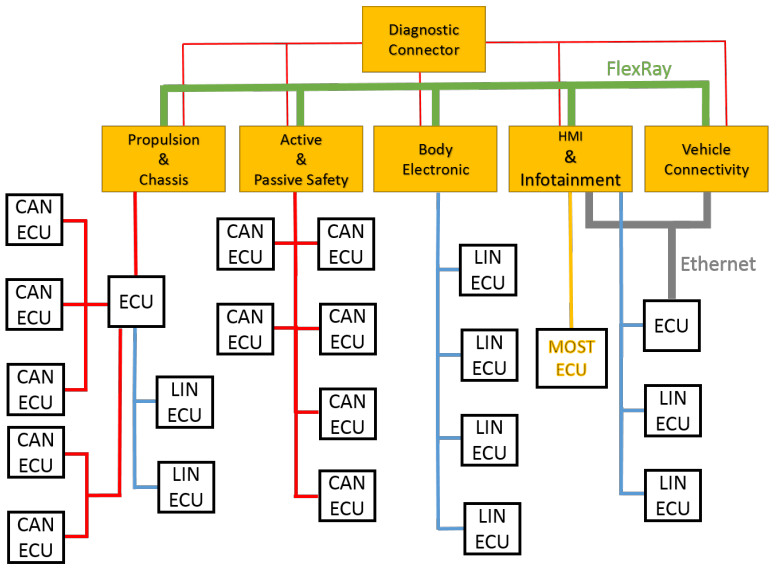


Figure 1.2: Typical in-vehicle network with a FlexRay backbone

aspects can be divided into two major categories: the *views* we can have of the in-vehicle network, and the *requirements* that are recognized and must be fulfilled by the engineers when designing the in-vehicle network architecture. The design aspects are shown in Figure 1.3 and explained below.

The different *views* of the in-vehicle network can be divided into:

- **Physical.** The physical view of the in-vehicle network is the collection of physical equipment needed to build the in-vehicle network and *their restrictions implied on the design*. For example, the engine control and its placement (most often in the front of the vehicle), turn indicators which normally have to be placed in the corners of the vehicle, and cameras for collision avoidance that have to be placed in the front of the vehicle. Thus, the physical view captures equipment, placement, and restrictions implied in the design of a function.

- **Functional.** The functional view is the collection of functional models that are implemented in the vehicle and their task allocation to the ECUs in the in-vehicle network.

- **Communication.** The communication view is the collection of issues related to communication in the in-vehicle network. For example, number of ECUs, gateways and domains, as

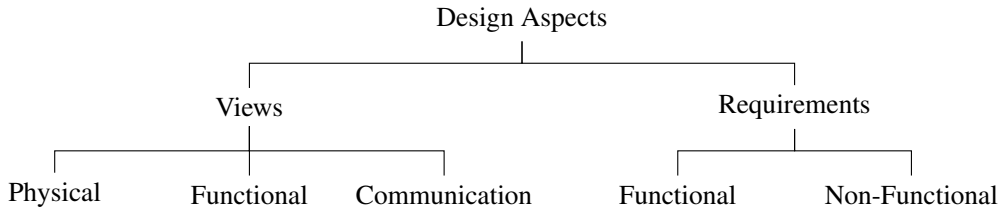


Figure 1.3: Design aspects of an in-vehicle network architecture

well as the communication patterns, network load, and the bus technology being used.

The *requirements* can be divided into:

- **Functional.** Functional requirements are those requirements that describe functional behavior, e.g., the maximum delay between the moment that driver hits the brake pedal until the moment that car starts to slow down, and the maximum delay-time allowed for an airbag to be released.
- **Non-Functional.** Non-functional requirements are those requirements that do not describe functional behavior, e.g., it should not be possible to activate the parking assistant while driving (safety), and updates of ECU firmware is only allowed by authorized personal (security).

### Safety and security aspects

Safety has always been one of the most important criteria when designing in-vehicle networks. Extensive work has been spent in automotive safety, most notable by the functional safety standard for road vehicles, ISO 26262. This standard provides an approach for determining the Automotive Safety Integrity Levels (ASILs) which specify the necessary safety requirements of automotive systems. Following ISO 26262, each item, i.e., "[a] system [...] or array of systems to implement a function at the vehicle level" [3], is described, developed, and initially evaluated independently of each others. During the process, ASILs are assigned to each component within a system depending on the impact to safety by the component. Necessary measures are then implemented to fulfill the safety requirements. Security, on the other hand, has not been regarded as an important requirement in the automotive industry until recently. In recent years, security issues of in-vehicle networks

have proved to affect safety of vehicles. Therefore, finding an approach to assign security levels to in-vehicle domains and apply appropriate security mechanisms should be attractive, but is currently missing. Quite some effort has been spent over the last years in proposing new security mechanisms to add security to the in-vehicle network [16, 29]. The EVITA project [1] has proposed security protocols and developed a Hardware Security Module (HSM) that is to be integrated into the ECUs. However, very little work has so far been conducted in the area of defining and evaluating the in-vehicle network architecture itself and how the in-vehicle network should be designed when security has the same criticality in the design process as safety and dependability [11].

In [25], Müter and Freiling propose a model-based approach to analyze in-vehicle network architectures with respect to security aspects, such as integrity and confidentiality. An architecture is composed of ECUs, buses, interfaces, and gateways. The approach does not tell how secure a specific architecture is, rather it helps designers to evaluate different architectures against each other to identify the one that is more secure. Some general research regarding in-vehicle network architectures has also been conducted. In the EASIS project [2], a backbone network was considered to be the most suitable network architecture for the near future. Three architectures were suggested during their evaluation: (1) a *backbone architecture* where suitable sub-networks (domains) are defined and connected together via gateways over a backbone network, (2) a *multi-gateway architecture* where no backbone network is used, instead, each sub-network has a gateway and all gateways are chained together, and (3) a *central gateway architecture* where all sub-networks are connected to one single gateway that connects them together. Other variants have also been discussed by Mahmud and Alles [21], where different fault-tolerant architectures are presented. The fault-tolerance is achieved by duplicating parts of the network. A simulation model to evaluate the performance of different topologies were also introduced. Yet, the main goal in [2, 21] has been to present different possible architectures in future vehicles where safety has been the main aspect. Methods for how to partition the in-vehicle network into domains were not presented nor was security considered.

### CAN bus

CAN is the most widely used automotive bus. It is a relatively old bus technology developed by BOSCH in 1983. The CAN bus is used for implementation of many of the main operational functions of vehicles including safety-critical functions. The typical speed of a CAN bus is 500 kbit/s and a single CAN frame can carry a *maximum of 8 data bytes*. As shown in Figure 1.4, a

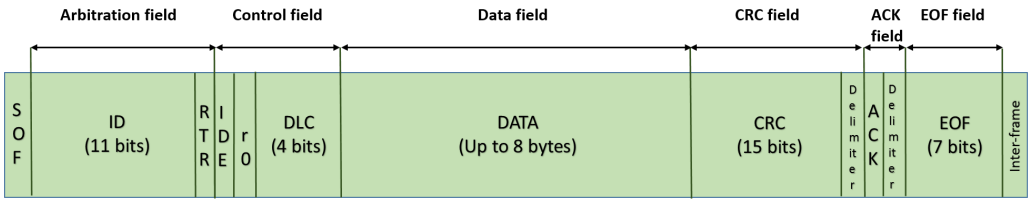


Figure 1.4: CAN frame format

CAN frame consists of multiple fields. The main fields of a CAN frame are the 11-bit ID (or 29-bit in extended format), a control field, a data field with a variable payload of 1 - 8 bytes, a Cyclic Redundancy Check (CRC) field and an acknowledgment field.

**Security threats against CAN bus**

Researchers have already shown that in-vehicle networks are vulnerable to cyber attacks. In recent years, attackers have managed to remotely take control of the engine system, braking system, the steering wheel and many other safety-critical functions. The CAN bus, in particular, has proved to be vulnerable to security attacks and has been the main target of most cyber attacks in the last decade [5, 14, 32]. Like most older technologies, CAN was not designed with security in mind, and the problems are many:

- *Confidentiality* can not be guaranteed, because all messages are broadcast and every node can read all messages.
- *Integrity* can not be guaranteed. CRCs guard only against random transmission errors, so stronger integrity measures like cryptographically secure hashes are required [32].
- *Availability* can not be guaranteed. By spoofing high priority messages on the bus, Denial of Service (DoS) attacks are easy to perform. Another DoS attack exploits CAN's rather complex error handling and fault containment functions, which ensure that faulty devices disconnect themselves if they cause too many errors [20].
- *Authenticity* can not be guaranteed, which implies that non-repudiation can not be guaranteed [5, 23]. CAN Message IDs only identify the content of a message, not the address of the sender or the receiver node, which exacerbates the problem.
- *Freshness* can not be guaranteed. Since no timestamps are included, replay attacks will work [13].

In recent years, researchers have shown an increasing interest in proposing security solutions for securing in-vehicle networks and particularly authenticating CAN communications [10, 12, 18, 26, 28, 30, 31, 34]. However, certain constraints and requirements of in-vehicle networks have made it difficult to propose applicable security solutions for vehicles. For instance, in-vehicle ECUs typically have very limited storage and computational power, which makes it difficult to use traditional IT security solutions. Another challenge is cost which is a driving factor in the automotive ecosystem and it is not easy to replace low-end ECUs with more powerful (more expensive) ECUs that are able to run cryptographic primitives. Since such challenges affect the applicability of the proposed solutions, they must be identified and addressed when designing in-vehicle security solutions. To the author's knowledge, so far little attention has been given to identifying the requirements that needs to be fulfilled by CAN authentication solutions.

### 1.1.2 ITS communications

The Intelligent Transportation System (ITS) is a set of applications that aim at improving road safety and traffic efficiency as well as providing environmental benefits by enabling vehicles, Roadside Units (RSUs) and the infrastructure around the vehicles to communicate with each other (V2X communications). ITS applications exchange messages containing information such as speed, direction and location via a Dedicated Short Range Communication (DSRC) network. Despite the benefits of ITS communications, there is a risk that the privacy of the users (e.g. location and identity of the driver) could be impaired by an adversary intercepting the communications. Also, ITS communication must be authenticated and authorized in order to keep unauthorized vehicles away from getting access to particular applications, services or privileges. For instance an adversary's vehicle could broadcast "Emergency vehicle approaching" messages to other neighboring vehicles to get ahead in a traffic jam. The possibility of performing typical network attacks against ITS communications, such as DoS attacks, man in the middle attacks, eavesdropping attacks and Sybil attacks have been investigated in several researches [4, 6, 7, 8, 17, 22].

The security and privacy requirements of ITS communications have been investigated in several European projects such as SEVECOM [19], and PRESERVE [27] and solutions have been proposed. In order to validate and authorize the ITS stations, the European Telecommunications Standards Institute (ETSI) has developed a security architecture that introduces privacy, confidentiality, authenticity and integrity to the ITS communications by using Certificate Authorities

(CAs) and identity management procedures. The ETSI ITS security architecture is described in a collection of standards, although the evaluation of most of these standards is still in progress. One of the most important parts of this security architecture is the ETSI TS 103 097 [15] standard, which describes the header, certificate formats and security services (e.g. message signing and verification) of ITS communications. As for any newly written security standard, the ETSI TS 103 097 should be evaluated to identify possible design flaws and vulnerabilities. However, to the best knowledge of the author, there have been very few works [24] that have attempted to evaluate the ETSI ITS security architecture.

## 1.2 Thesis objective

The research presented in this thesis aims to propose methods and recommendations for improving the security of vehicles. In order to achieve this, we have focused on both in-vehicle and V2X communications. The standardization of the V2X communications is an ongoing process and many of the security standards within this area are still being evaluated. So, in order to contribute in the process of developing secure V2X communications, we identify weaknesses or deficiencies in the design of the ETSI V2X security standard and we propose changes to fix the identified weaknesses.

Next, we focus on in-vehicle network security and in particular on two architectural problems, which have received little attention so far. First, we investigate the possibility of partitioning ECUs in a way that facilitates the implementation of security measures. In order to do that, we propose an automated approach for grouping in-vehicle ECUs into domains based on different criteria. Second, we compare our identified network architecture with a reference architecture model to show that our approach is very flexible and can identify meaningful in-vehicle network domains that are better with respect to communication, safety and security than those of the reference model.

Even though researchers have proposed many different message authentication solutions for securing in-vehicle networks over the last years, the translation of academic research into practice within this area has been very slow. This is mainly because they fail to meet the practical requirements. Thus, we analyze the authentication solutions proposed in literature and identify the criteria that they must fulfill in order to be applicable in practical contexts.

This thesis addresses the following research questions:

1. Is there any flaw or vulnerability in the design of the ETSI V2X security standard? Are there

parts of the standard which are open to misinterpretations leading to implementation errors? If so, what is the proposed solution to fix the flaw?

2. How can or should an in-vehicle network be partitioned to be optimized for security? Can community detection algorithms be used to identify such in-vehicle network domains? How meaningful and optimal are the identified domains with respect to communication, safety and security?
3. Why have proposed in-vehicle message authentication solutions not yet been used in vehicles? What are the constraints and requirements from a practical perspective?

The thesis is divided into two chapters. Chapter I presents our analysis of the ETSI ITS V2X security standard. Chapter II consists of three parts: the first two parts present our automated method for grouping in-vehicle ECUs into domains. The third part presents our review of some of the most prominent CAN message authentication protocols proposed in the literature, and the identified requirements that they need to fulfill in order to be applicable for use in vehicles.

## 1.3 On securing the vehicular communications

This section gives a summary of the papers presented in this thesis.

### 1.3.1 Towards Securing the external vehicular communications

**Paper A: Experiences from implementing the ETSI ITS SecuredMessage service**

Efforts for securing ITS communications are currently going on, and IEEE and ETSI have separately introduced protocols to secure this type of communication. In Europe ETSI has published a collection of documents describing the security architecture of the ETSI ITS communications. ETSI TS 103 097 describes the header, certificate formats and security services of the ITS communications. At the time of writing this paper, there were only a few implementation of the ETSI TS 103 097 V1.1.1 standard. An accepted method of identifying the flaws, complexities and weaknesses of a newly introduced standard is to implement and test it. This enables the researcher to gain empirical knowledge about the standard based on the experience and observations. Paper A presents our experience from implementing the ETSI TS 103 097 V1.1.1. SecuredMessage, certificate format and sign/verify services on an existing ETSI ITS communication stack. We tested our

implementation against a list of potentially vulnerable fields identified during the implementation phase.

We found a major flaw in our implementation of the SecuredMessage and signature verification service. Surprisingly, we also found another implementation of the standard, provided by the Fraunhofer FOKUS institute, showing unexpected behavior due to the same flaw. The identified flaw is related to the specification of the payload structure of a SecuredMessage which allows having unsigned (i.e. *unsecured*) payloads in an otherwise signed secured message. We demonstrate how to exploit the identified flaw to force an actual implementation of the ITS communication stack to crash by having it parsing unexpected field values. SecuredMessage uses a dynamic structure with different rules for the encoding and decoding of each type of message. This means that the type of the header and trailer fields in different SecuredMessages varies depending on the rules specified in the security profile for each message. The second identified problem originates from the specification of the security profiles which only defines what fields must be included in the encoding of a SecuredMessage, and therefore allows additional *HeaderFieldTypes* that are not specified in the security profile. This makes it very difficult to test that a given implementation of the SecuredMessage behaves correctly on all possible inputs. Finally, we show that these problems are the result of weaknesses and complexities in the design of the standard and we also propose solutions to mitigate the identified problems.

### 1.3.2 Towards Securing the internal vehicular communications

**Paper B: Towards designing secure in-vehicle network architectures using community detection algorithms**

In recent years, In the recent years, quite some effort has been spent in proposing new security mechanisms for the in-vehicle network, however, little attention has been paid to the architecture and especially on how to group ECUs for good security performance. This is important because the identification of good domains can facilitate the implementation of security measures. The current approach in industry for grouping ECUs into domains is based on “best engineering practice’ and the division criteria are mainly functions or bus technologies. The notion of security domains is a well-recognized concept used in traditional network security engineering, where the idea is to protect systems inside a domain from the outside, but also to isolate possible security problems and to retain them inside a domain. Security measures such as Intrusion Detection Systems (IDSs)

or firewalls are then placed at the borders of the domains to monitor and filter the communication to and from each domain. In paper B, we analyze the in-vehicle network communication from a real, modern vehicle using four community detection algorithms, namely Louvain, Infomap, Eigenvector and Edge Betweenness, to find the optimum grouping in an automated way. We limit our analysis to focus on only one particular criterion: the message types (a.k.a. signals). As there is no common agreement of what is the best measure to decide which algorithm performs best, we use three different quality measures: Coverage, Modularity, and Conductance. We use plotting and ocular inspection of the domains as another approach for identifying the algorithm that performs better than the others. Our analysis shows that Louvain is the best community detection algorithm to use on our dataset and should be used in our further analysis (see Paper C).

**Paper C: Improving in-vehicle network architectures using automated partitioning algorithms**

In Paper B we showed that automated partitioning algorithms are suitable to identify good security domains in an in-vehicle network. However, two questions were left to be answered: 1. How is the quality of the identified domains with respect to communication, safety and security? 2. How meaningful are the identified domains with respect to functionality? In this paper, we answer the above questions by comparing our identified architecture with the EVITA reference architecture [9]. In order to do that, the in-vehicle network communication is mapped into the domains defined in EVITA, and also partitioned using the Louvain algorithm. We find that, when using message type as partitioning criterion, Louvain identifies an architecture in which $55\%$ of the messages are intra-domain which is almost twice as much as the $28\%$ in the EVITA architecture. When the amount of traffic (payload) is used as partitioning criterion, the Louvain architecture has approximately 586 Kb/s (38 percent) less inter-domain traffic than EVITA. These improvements mean that the Louvain architecture is much more suitable for an implementation of security measures (e.g. firewall functionality) as it has significantly less inter-domain and more intra-domain communication. With respect to safety, we find that the Louvain architecture performs better than the EVITA architecture, as the Louvain architecture successfully keeps more messages that belong to safety-critical ECUs inside the domains. This makes it easier for designers to provide safety measures for domains that have safety critical ECUs and they have to rely less on inter-domain communications. Furthermore, we find that the identified domains are both intuitive and meaningful with respect to functionality.

Our results show that safety and security improvements can be obtained at the same time, and that safety and security requirements are not necessarily in conflict with each other. We believe that our approach has great potential to help engineers in deriving secure in-vehicle network architectures during the design of a vehicle. It should be emphasized that many other aspects such as cost, reliability, bandwidth, and real-time requirements also need to be considered when designing an in-vehicle network. Even though the work presented here will not be the final design of the in-vehicle network architecture, we believe that the architecture identified in our work can be used as a base model or reference architecture for further in-vehicle network development.

**Paper D: In-vehicle CAN message authentication: A perspective from the industry**

In-vehicle networks still suffer from a lack of agreed and applicable security solutions. Researchers have proposed several solutions for securing in-vehicle networks in recent years, but few, if any, have been adopted in practice. The introduction of message authentication on CAN buses would have a large positive impact on security, but it also poses the biggest practical challenges. In paper D, we identify five industrial requirements which a solution must fulfill in order to be considered for implementation in a vehicle. The identified requirements are: cost-effectiveness, backward compatibility, repair and maintenance, prototype implementation and acceptable overhead. We then performed a literature review on some of the most promising CAN bus message authentication solutions proposed in literature, and analyzed them according to the identified requirements. The evaluation shows that none of the proposed CAN authentication solutions meet all of the criteria, with backward compatibility and acceptable overhead being the biggest adoption hurdles. We find that Most solutions are cost-effective, if we assume that we only implement them on a small subset of safety-critical ECUs. On the other hand, only three of the solutions can meet our rather strict interpretation of backward compatibility. For a less strict interpretation, several more could be deemed backward compatible. While support for repair and maintenance is rarely considered explicitly, in most cases it can be addressed without undue effort. Regarding sufficient implementation details, slightly more than half of the solutions provide enough details to properly evaluate their performance and to be able to implement the solution in real life. Finally, about half of the solutions have an unacceptable overhead, and for the other half it is not possible to judge because the evaluation environment is not well explained, with the notable exception of one solution. We conclude that the CAN bus might be fundamentally unsuitable for secure communication, and that a gradual shift towards more modern bus technologies with higher

bandwidth is needed, in order to secure in-vehicle communications.

## 1.4 Contributions

The main contributions of this thesis are as follows.

- I have implemented and evaluated the upcoming ETSI standard TS 103 097 for V2X communications and identified vulnerabilities in it. I have been able to influence the next version of the standard with respect to security functionality through our participation in the Car-to-Car Consortium (C2C). This work addresses the research question 1.
- I have implemented a tool for identifying potential security domains of the in-vehicle network. My tool is able to group ECUs into domains with respect to different criteria where the identified partitions are meaningful with respect to functionality. I have shown that my identified architecture has higher quality with respect to communication, safety and security than the EVITA reference architecture. This work addresses the research question 2.
- I have identified five industrial requirements that a message authentication protocol needs to fulfill in order to be considered for adoption in a vehicle. I have also evaluated some of the most promising CAN message authentication protocols proposed in literature with respect to the identified requirements. This work addresses the research question 3.

## 1.5 Conclusion

In this thesis, we propose methods for designing secure in-vehicle architectures and for improving the security of the ETSI V2X communications. We have identified weaknesses in the design of the ETSI V2X security standard and we have proposed changes to fix the identified weaknesses. We have proposed an automated approach for grouping in-vehicle ECUs into domains based on different criteria and we have shown that our approach is able to identify meaningful domains with good quality with respect to communication, safety and security. Finally, we have evaluated the applicability of several in-vehicle message authentication protocols based on our five identified requirements, and shown that none of the solutions meet all of the criteria.

# References


[1] E-safety vehicle intrusion protected applications (EVITA). URL http://www.evita-project.org/.

[2] EASIS — general architecture framework. Deliverable D0.2.4, August 2004.

[3] Iso 26262-1:2011: Road vehicles — functional safety — part 1: Vocabulary, 2011.

[4] Mohammed Saeed Al-Kahtani. Survey on security attacks in vehicular ad hoc networks (vanets). In *Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference on*, pages 1–9. IEEE, 2012.

[5] Paul Carsten, Todd R Andel, Mark Yampolskiy, and Jeffrey 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. ISBN 978-1-4503-3345-0. doi: 10.1145/2746266.2746267.

[6] Anup Dhamgaye and Nekita Chavhan. Survey on security challenges in vanet 1. 2013.

[7] Roberto Di Pietro, Stefano Guarino, Nino Vincenzo Verde, and Josep Domingo-Ferrer. Security in wireless ad-hoc networks–a survey. *Computer Communications*, 51:1–20, 2014.

[8] Richard Gilles Engoulou, Martine Bellaïche, Samuel Pierre, and Alejandro Quintero. Vanet security surveys. *Computer Communications*, 44:1–13, 2014.

[9] EVITA. *E-safety vehicle intrusion protected applications (EVITA)*, 2016 (Accessed: 18-Nov-2016). http://www.evita-project.org/.

[10] Bogdan Groza, Stefan Murvay, Anthony Van Herrewege, and Ingrid Verbauwhede. LiBrA-CAN: a lightweight broadcast authentication protocol for controller area networks. In *Cryptology and Network Security*, pages 185–200. Springer, 2012.

[11] Milena Guessi, Elisa Yumi Nakagawa, Flavio Oquendo, and JosÃl' Carlos Maldonado. Architectural description of embedded systems: A systematic review. In *Proceedings of the 3rd International ACM SIGSOFT Symposium on Architecting Critical Systems*, ISARCS '12, page 31âĂŞ40, New York, NY, USA, 2012. ACM. ISBN 978-1-4503-1347-6. doi: 10.1145/2304656.2304661. URL http://doi.acm.org/10.1145/2304656.2304661.

[12] Oliver Hartkopp, Cornel Reuber, and Roland SCHILLING. Macan - message authenticated can. In *Escar Conference, Berlin, Germany*, 2012.

[13] Tobias Hoppe, Stefan Kiltz, and Jana Dittmann. *Computer Safety, Reliability, and Security: 27th International Conference*, chapter Security Threats to Automotive CAN Networks – Practical Examples and Selected Short-Term Countermeasures, pages 235–248. Springer, Berlin, Heidelberg, 2008. ISBN 978-3-540-87698-4. doi: 10.1007/978-3-540-87698-4_21. URL http://dx.doi.org/10.1007/978-3-540-87698-4_21.

[14] Tobias Hoppe, Stefan Kiltz, and Jana Dittmann. Automotive it-security as a challenge: Basic attacks from the black box perspective on the example of privacy threats. In *Proceedings of the 28th International Conference on Computer Safety, Reliability, and Security*, SAFECOMP '09, pages 145–158, Berlin, Heidelberg, 2009. Springer-Verlag. ISBN 978-3-642-04467-0. doi: 10.1007/978-3-642-04468-7_13. URL http://dx.doi.org/10.1007/978-3-642-04468-7_13.

[15] European Telecommunications Standards Institute. Etsi ts 103 097 v1.1.1, intelligent transport systems (its); security; security header and certificate formats, 2013.

[16] Pierre Kleberger, Tomas Olovsson, and Erland Jonsson. Security aspects of the in-vehicle network in the connected car. In *2011 IEEE Intelligent Vehicles Symposium (IV)*, pages 528–533, Baden-Baden, Germany, June 2011. doi: 10.1109/IVS.2011.5940525.

[17] P Vinoth Kumar and M Maheshwari. Prevention of sybil attack and priority batch verification in vanets. In *Information Communication and Embedded Systems (ICICES), 2014 International Conference on*, pages 1–5. IEEE, 2014.

[18] R Kurachi, Y Matsubara, H Takada, N Adachi, Y Miyashita, and S Horihata. Cacan-centralized authentication system in can (controller area network). In *14th Int. Conf. on Embedded Security in Cars (ESCAR 2014)*, 2014.

[19] Tim Leinmueller, Levente Buttyan, Jean-Pierre Hubaux, Frank Kargl, Rainer Kroh, Panagiotis Papadimitratos, Maxim Raya, and Elmar Schoch. SEVECOM - Secure Vehicle Communication. 2006.

[20] Congli Ling and Dongqin Feng. An algorithm for detection of malicious messages on can buses. In *2012 National Conference on Information Technology and Computer Science. Atlantis Press*, 2012.

[21] Syed Masud Mahmud and Sheran Alles. In-vehicle network architecture for the next-generation vehicles. SAE Technical Paper 2005-01-1531, SAE International, April 2005. URL `http://dx.doi.org/10.4271/2005-01-1531`.

[22] Mohamed Nidhal Mejri, Jalel Ben-Othman, and Mohamed Hamdi. Survey on vanet security challenges and possible cryptographic solutions. *Vehicular Communications*, 1(2):53–66, 2014.

[23] Charlie Miller and Chris Valasek. Remote exploitation of an unaltered passenger vehicle. *Black Hat USA*, 2015.

[24] Rim Moalla, Brigitte Lonc, Gerard Segarra, Marcello Laguna, Panagiotis Papadimitratos, Jonathan Petit, and Houda Labiod. Experimentation with the preserve vss and the score@ f system. In *Proceedings of the 5th Conference on Transport Research Arena (TRA), Paris, France*, volume 1417, 2014.

[25] M. Müter and F.C. Freiling. Model-based security evaluation of vehicular networking architectures. In *2010 Ninth International Conference on Networks (ICN)*, pages 185–193, 2010. doi: 10.1109/ICN.2010.38.

[26] Hisashi Oguma, XAkira Yoshioka, Makoto Nishikawa, Rie Shigetomi, Akira Otsuka, and Hideki Imai. New attestation based security architecture for in-vehicle communication. In *2008 IEEE Global Telecommunications Conference*, IEEE GLOBECOM 2008, pages 1–6. IEEE, 2008.

[27] PRESERVE. *Preparing Secure Vehicle-to-X Communication Systems (PRESERVE)*, 2016 (Accessed: 18-Nov-2016). `https://www.preserve-project.eu/`.

[28] H. Schweppe, Y. Roudier, B. Weyl, L. Apvrille, and D. Scheuermann. Car2x communication: Securing the last meter - a cost-effective approach for ensuring trust in car2x applications using in-vehicle symmetric cryptography. In *Vehicular Technology Conference (VTC Fall), 2011 IEEE*, pages 1–5, Sept 2011. doi: 10.1109/VETECF.2011.6093081.

[29] Ivan Studnia, Vincent Nicomette, Eric Alata, Yves Deswarte, Mohamed Kaaniche, and Youssef 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. doi: 10.1109/DSNW.2013.6615528.

[30] Anthony Van Herrewege, Dave Singelee, and Ingrid Verbauwhede. Canauth-a simple, backward compatible broadcast authentication protocol for can bus. In *ECRYPT Workshop on Lightweight Cryptography*, pages 229–235, 2011.

[31] Q. Wang and S. Sawhney. Vecure: A practical security framework to protect the can bus of vehicles. In *Internet of Things (IOT), 2014 International Conference on the*, pages 13–18, Oct 2014. doi: 10.1109/IOT.2014.7030108.

[32] Marko Wolf, André Weimerskirch, and Christof Paar. Security in automotive bus systems. In *Workshop on Embedded Security in Cars*, 2004.

[33] S. Woo, H. J. Jo, and D. H. Lee. A practical wireless attack on the connected car and security protocol for in-vehicle can. *IEEE Transactions on Intelligent Transportation Systems*, 16(2):993–1006, April 2015. ISSN 1524-9050. doi: 10.1109/TITS.2014.2351612.

[34] Samuel Woo, Hyo Jin Jo, and Dong Hoon Lee. A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN. *IEEE Transactions on Intelligent Transportation Systems*, pages 1–14, 2014. ISSN 1524-9050, 1558-0016. doi: 10.1109/TITS.2014.2351612. URL http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6894181.