Thesis for the Degree of Doctor of Philosophy

Automotive Communication Security

Methods and Recommendations for Securing In-vehicle and V2X Communications

Nasser Nowdehi

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

Automotive Communication Security
Methods and Recommendations for Securing In-vehicle and V2X Communications
Nasser Nowdehi
ISBN 978-91-7905-227-0

Doktorsavhandlingar vid Chalmers tekniska högskola
Ny serie nr 4694
Technical report 180D
ISSN 0346-718X
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, nasser.nowdehi@gmail.com`

Printed by Chalmers Reproservice
Göteborg, Sweden 2019

Automotive Communication Security

Methods and Recommendations for Securing In-vehicle and V2X Communications

Nasser Nowdehi
Department of Computer Science and Engineering
Chalmers University of Technology
Thesis for the degree of Doctor of Philosophy

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. This thesis proposes methods and recommendations for improving the security of internal and external vehicular communications.

The main contributions of this thesis are contained in six included papers, and cover the following research areas of automotive security: (i) *secure network architecture design*, (ii) *attack protection*, (iii) *attack detection*, and (iv) *V2X security*. The first two papers in the collection are on the topic of secure network architecture design and propose an automated approach for grouping in-vehicle ECUs into security domains which facilitate the implementation of security measures in in-vehicle networks. The third paper is on the topic of attack protection and evaluates the applicability of existing Controller Area Network (CAN) bus authentication solutions to a vehicular context. In particular, this paper identifies five critical requirements for an authentication solution to be used in such a context. The fourth paper deals with the issue of attack detection in in-vehicle networks and proposes a specification agnostic method for detecting intrusion in vehicles. The fifth paper identifies weaknesses or deficiencies in the design of the ETSI V2X security standard and proposes changes to fix the identified weaknesses or deficiencies. The last paper investigates the security implications of adopting 5G New Radio (NR) for V2X communications.

Keywords: V2X, automotive, security, in-vehicle network, vehicular communication

List of Publications

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

Part I: Towards Securing the Internal Vehicular Communications

▷ Paper A

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 B

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 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 (VTC-Fall)*, Toronto, ON, Canada, September 24-27, 2017, pp. 1-7

▷ Paper D

Nasser Nowdehi, Wissam Aoudi, Magnus Almgren and Tomas Olovsson,"CASAD: CAN-Aware Stealthy-Attack Detection for In-Vehicle Networks," submitted to *IEEE Transactions on Information Forensics & Security*

Part II: Towards Securing the External Vehicular Communications

▷ Paper E

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.

▷ Paper F

Aljoscha Lautenbach, **Nasser Nowdehi**, Tomas Olovsson and Romi Zaragatzky, "A Preliminary Security Assessment of 5G V2X," in *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, Kuala Lumpur, Malaysia, 28 April - 1 May, 2019, pp. 1-7.

Acknowledgments

Wear gratitude like a cloak
and it will feed every corner of your life.

Rumi

First and foremost, I wish to thank my supervisor at Chalmers, Associate Professor Tomas Olovsson for his constant support, personal and professional advice, and encouragement through the rough road to finish this thesis. You are an excellent example of a supportive and patient supervisor with positive attitude. I would like to express my gratitude and appreciation to my former examiner Professor Erland Jonsson for his constructive feedback and kind assistance. I shall extend my thanks to Professor Andrei Sabelfeld, who took over the examination of my Ph.D. studies. I am also grateful to my industrial advisor, Henrik Broberg for his generous support, his understanding, and especially for giving me the opportunity to study a PhD.

I am honored to have Professor Dieter Gollmann as the faculty opponent of my thesis defense. I also gratefully acknowledge the grading committee members: Professor Nahid Shahmehri, Dr. Hendrik Schweppe, and Professor Kurt Tutschku for taking the time to review my work.

I would like to thank current and former members of Chalmers' Department of Computer Science and Engineering, and in particular the members of the Security group for their support, friendship and making Chalmers a great place to work! I extend my thanks and appreciation to our fantastic administration team at Chalmers, with special thanks to Eva, Marianne, and Rebecca for all their support in the last five years.

Next, I would like to thank Volvo Car Corporation and VINNOVA for funding my research within the two projects SEFRAM and HoliSec. Special thanks go to my current and former colleagues at Volvo Car for all the knowledge they have shared with me, and for their support during my Ph.D. studies

Last, but by no means least, my heartfelt appreciation goes to my family: my beloved Nastaran, my parents, and my brothers for their constant love, encouragement, and moral support throughout my studies and my life in general. I have nothing but love for you, and I am eternally grateful for having you in my life!

Nasser Nowdehi
Göteborg, November 2019

Contents

I Thesis Summary

II Collection of Papers

Part I

Thesis Summary

Introduction

It takes 20 years to build a reputation
and few minutes of cyber-incident to ruin it.

Stephane Nappo

Modern vehicles are computers on wheels. The automotive industry has witnessed a shift in its manufacturing process over the past three decades with mechanic components being replaced with electronic devices controlled by software. Nowadays, the In-Vehicle Network (IVN) of a vehicle consists of more than 100 Electronic Control Units (ECUs) that communicate to each other via different bus technologies, and control almost every function of the vehicle, including the safety critical functions (see Figure 1). Modern IVNs are Internet enabled through their telecommunication ECU to provide in-vehicle entertainment, navigation information, semi autonomous driving features, and even Over The Air (OTA) updates to remotely perform software updates on the ECUs.

The increasing popularity of electric vehicles, autonomous driving, and mobility services such as car sharing means that more software, connectivity, and artificial intelligence is going to be added to vehicles. Moreover, the introduction of Cooperative Intelligent Transportation Systems (C-ITS) that enables vehicle to vehicle, vehicle to road side infrastructure, and vehicle to pedestrian communication (together called V2X) will increase the level of connectivity and intelligence in vehicles, and expose IVNs to the external world even more.

Although computerization of vehicles improves road safety, passenger comfort, and traffic management, 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 [33, 34, 44, 50, 72], mainly because IVNs were insecure. In most cases, the attackers managed to remotely exploit vulnerabilities found on Internet enabled ECUs such as the telecommunication unit or the Infotainment system, and from there laterally move through the IVN and take over safety critical components such as the brake, steering wheel and the engine control ECUs. Due to the criticality of such incidents and the increasing level of security threats against vehicles, there is an urgent need to address the security concerns of internal and external vehicular communications to protect the safety of passenger. To this aim, I collect in this thesis new proposals and recommendations for improving the security of in-vehicle networks and V2X communication. To put it more concretely, the present thesis contributes to the field of automotive security by *a*) proposing methods for designing secure IVN architectures and detecting attacks on IVN, and *b*) recommendations for improving V2X security protocols and state of the art IVN authentication solutions.

What is the problem?

The pace of introducing connectivity and the Internet to modern vehicles has not been met by making the necessary changes to the development process of vehicle systems to protect them against

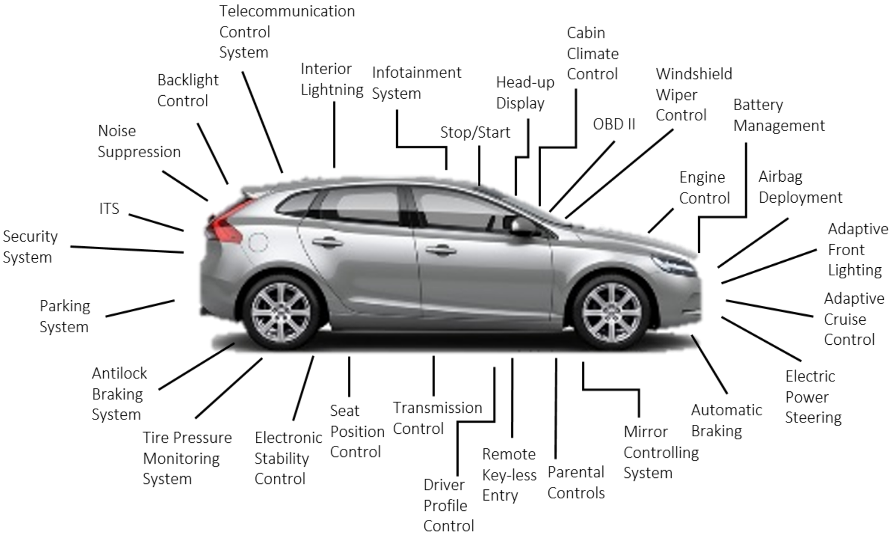


Figure 1: Examples of systems that are controlled by ECUs in a modern vehicle

cyber attacks. This is mainly on account of three major pitfalls. First, most of the technologies used in IVNs were mainly designed with safety and reliability in mind, but not security. The Controller Area Network (CAN), which is the most common bus technology used in vehicles for developing safety critical functions and the main target of most cyberattacks, is an example of such insecure designs. The CAN bus does not provide any mechanism to guarantee the confidentiality, integrity, authenticity, availability, and freshness of its messages [5, 23, 40, 44, 71].

Second, it is quite challenging to add established IT security solutions such as secure boot, secure software download, message authentication, firewall and Intrusion Detection System (IDS) to the already existing IVNs. This is largely due to strict resource constraints of automotive ECUs and other design criteria such as real-time requirements and backward compatibility. As shown in Table 1, most automotive ECUs have low-end hardware configuration which is primarily driven by cost requirements. Cost is one of the main restraining factors for implementing new security solutions in the automotive industry. This is mainly on account of market pressures that usually dictate prices, which means that vehicle manufacturers are bound to particular sales prices, independent of production costs. Low-cost solutions are needed to stay competitive. For example, requiring all ECUs to have hardware-supported cryptographic primitives to achieve the performance necessary for safety-critical real-time systems is not cost-effective. To illustrate this, consider a vehicle with just 25 ECUs. If an ECU with cryptographic hardware support requires an additional cost of €5, this translates to a revenue loss of €125 per sold vehicle. So for a manufacturer with yearly sales of 500,000 vehicles, this is a yearly revenue loss of €62,500,000. Obviously, very strong incentives must be in place for a company to choose such an investment.

Third, the lack of awareness about cybersecurity and a comprehensive and systematic approach to address all aspects of vehicle electrical systems' security throughout its lifecycle created a gap in the automotive cybersecurity engineering process. Unlike the widely accepted International Organization for Standardization (ISO) 26262 standard [25] that covers the functional safety aspects of the automotive Electric/Electronic (E/E) system, there is no single standard that addresses the cybersecurity aspects of the vehicle engineering process. In the absence of such a standard, most Original Equipment Manufacturer (OEMs) rely on security guidelines and best practices such as

ECU	**Flash**	**RAM**	**Processor**	Number of units
IHU[a]	2 GB	2 GB	600 MHz - 2.6 GHz	1
TCAM[b]	256 MB	512 MB	700 MHz - 1.2 GHZ	1
ECM[c]	1 - 8 MB	0.5 - 2 MB	Few Hundreds of MHz	1
Other[d]	<512 KB	64 KB	40-100 MHz	Dozens

[a] Infotainment Head Unit (IHU).
[b] Telecommunication Unit (TCAM).
[c] Central Electronic Module (CEM).
[d] For example Door Control Module (DCM).

Table 1: An approximation of ECU resources in a modern passenger vehicle.

the Society of Automotive Engineering (SAE) *J3061* [58] and the National Highway Traffic Safety Administration (NHTSA) *Automotive Security Best Practices* [8]. At the time of writing this thesis, the first automotive cybersecurity standard (ISO/SAE 21434) is under development by the ISO and SAE.

Lastly, is the issue of weaknesses in the newly developed security standards for V2X communication. Although much work has been done to enable C-ITS over the past decade, most of the conducted field tests neglect assessing the V2X security protocols in favor of evaluating the other parts of the technology such its basic operation, interoperability, and quality of services (QoS) metrics (e.g. communication range, throughput and packet loss rate). As a result, potential unidentified specification flaws, design flaws and ambiguities in the V2X security standards can lead to exploitable implementation defects that compromise the security of the communication.

Thesis objectives

The area of vehicle security is divided into two parts: The security of internal communications (in-vehicle security) and the security of external communications (V2X security). The problem that this thesis deals with is:

How to secure vehicular communications?

Thus, this thesis approaches the question from two directions: in-vehicle and V2X communication security. Given that the V2X standards were still in development during the period of my studies, most of my efforts were devoted to improve different aspects of the IVN security. As shown in Figure 2, my efforts in the area of IVN security are based on three topics, namely *secure network architecture design*, *attack protection* and *attack detection* mechanisms. Each of these topics represents an important aspect of the in-vehicle network security. The second perspective explores the security of V2X communication and it is based on two topics: the security of *802.11p based V2X* and the *Cellular V2X*.

More concretely, this thesis addresses the following research questions:

1. 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?

2. Why have proposed CAN message authentication solutions not yet been used in vehicles? What are the constraints and requirements from a practical perspective?

3. What are the challenges for designing intrusion detection system for IVN? What type of attacks are possible on IVN traffic? Is there any method in the literature that can detect all

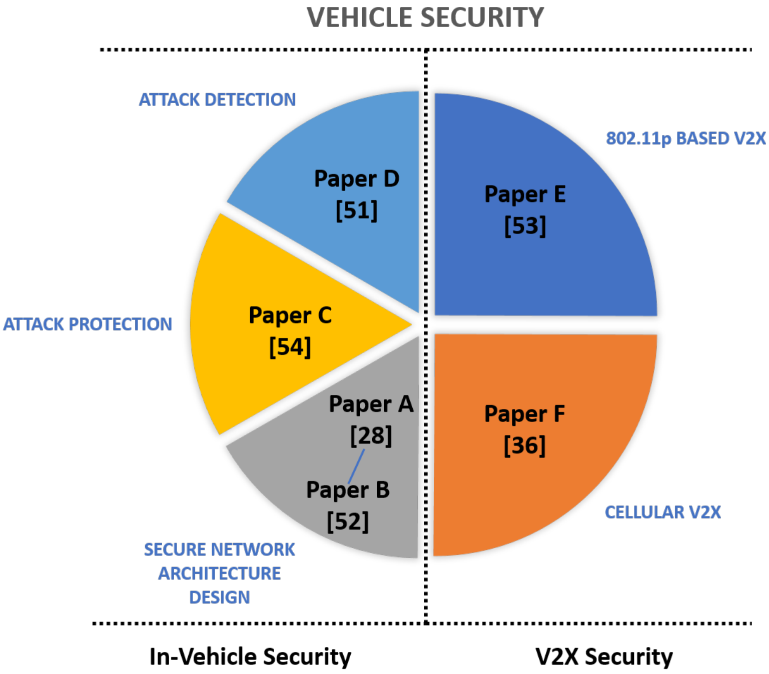


Figure 2: My publications [28, 36, 51–54] during the Ph.D.categorized based on their topic and the corresponding thesis objective. A line between papers shows logical connections between the results contained therein.

IVN attacks?

4. Is there any flaw or vulnerability in the design of the European Telecommunications Standards Institute (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?

5. What are the security requirements of ETSI ITS use cases? What are the security implications of replacing 802.11p with cellular V2X? Is it possible to facilitate security features at lower levels of the communication stack by relying on 5G New Radio features?

Thesis overview

This thesis collects together research results obtained during my doctoral studies related to vehicular communication security. The results can be used to improve the overall security of in-vehicle network and V2X communications. The thesis is organized in two parts. The first part consists of a brief introduction, a background that presents the basic concepts necessary to understand the included publications, and a brief summary of the results and contributions, followed by a conclusion. The second part of the thesis is a collection of six papers on variety of topics in the area of vehicle security. Figure 2 shows my publications during the course of my doctoral studies and groups them by topic and the corresponding thesis objective.

In summary, **Paper A** [28] and **Paper B** [52] contribute to the area of *secure network architecture design* by proposing a new method to identify in-vehicle network domains, which facilitate the implementation of security mechanisms. **Paper C** [54] addresses an issue in the area of *attack protection* by investigating why the proposed CAN bus message authentication solutions proposed in the literature have not yet been adopted by the industry. **Paper D** [51] makes several contributions to the field of IVN *attack detection*, including the introduction of a novel stealthy attack and proposing an efficient intrusion detection method. **Paper E** [53] identifies weaknesses in the ETSI V2X security standard for 802.11p and **Paper F** [36] investigates the security implications of replacing 802.11p with cellular V2X.

Background

If you think technology can solve your security problems,
then you don't understand the problems
and you don't understand the technology

Bruce Schneier

This section provides high-level and concise introductions to the five main areas of contributions of this thesis, namely: *secure network architecture design*, *attack protection*, *attack detection*, *802.11p based V2X* and *cellular V2X*. The reader is assumed to be familiar with basic concepts of security.

Secure network architecture design

The In-Vehicle Network (IVN) of a modern vehicle consists of more than 100 Electronic Control Units (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 3, IVNs 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 addition to these bus technologies, vehicle manufacturers have recently shown interest in adapting Ethernet to vehicles due to increase in bandwidth requirements of functions such as driving assistance and infotainment.

There are many aspects to consider when developing an IVN. These design aspects can be divided into two major categories: the *views* we can have of the IVN, and the *requirements* that are recognized and must be fulfilled by the engineers when designing the IVN architecture. The design aspects are shown in Figure 4 and explained below. The different *views* of the IVN can be divided into:

Physical. The physical view of the IVN is the collection of physical equipment needed to build the IVN 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 IVN.

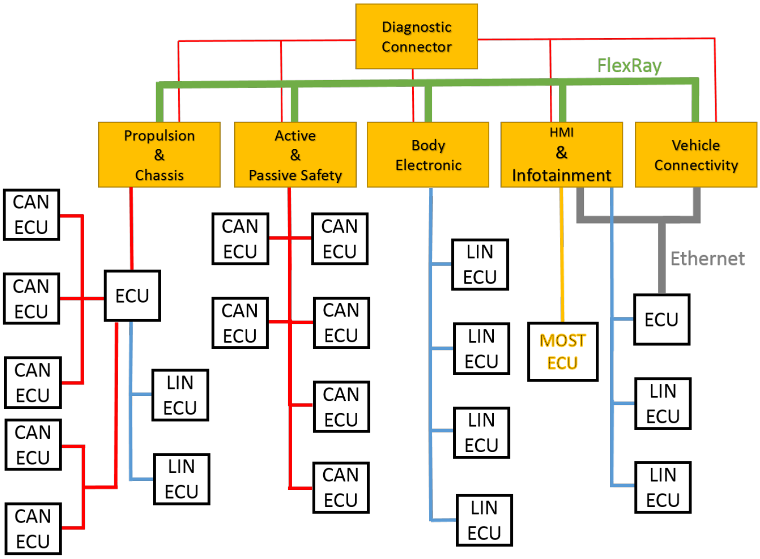


Figure 3: Typical IVN with a FlexRay backbone

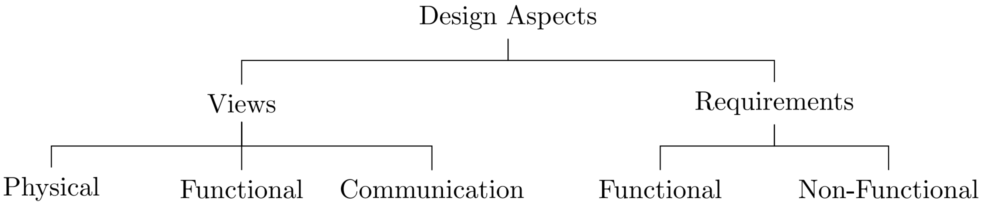


Figure 4: Design aspects of an IVN architecture

Communication. The communication view is the collection of issues related to communication in the IVN. For example, number of ECUs, gateways and domains, as 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 vehicle 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 has always been one of the most important criteria when designing IVNs. 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" [25], 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 IVNs 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 IVN [17, 29, 41, 51, 54, 63]. The EVITA project [15] 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 IVN architecture itself and how the IVN should be designed when security has the same criticality in the design process as safety and dependability [19].

In [48], Müter and Freiling propose a model-based approach to analyze IVN 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 IVN architectures has also been conducted. In the EASIS project [35], 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, 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 [35, 42] has been to present different possible architectures in future vehicles where safety has been the main aspect. Methods for how to partition the IVN into domains were not presented nor was security considered.

Attack protection

The CAN bus has proved to be vulnerable to security attacks and has been the main target of most cyber attacks in the last decade [5, 22, 33, 44, 70]. CAN 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 5, a 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.

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 [70].

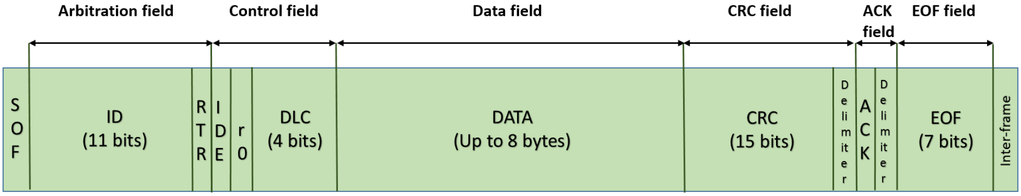


Figure 5: CAN frame format

- *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 [40].
- *Authenticity* can not be guaranteed, which implies that non-repudiation can not be guaranteed [5, 44]. 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 [23].

In recent years, researchers have shown an increasing interest in proposing security solutions for securing IVNs and particularly authenticating CAN communications [18, 21, 32, 56, 59, 66, 68, 72]. The maximum payload size of a CAN message being only 8 bytes makes appending a cryptographically secure Message Authentication Code (MAC) to the available space a challenge. Moreover, certain constraints and requirements of IVNs 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.

Attack detection

To combat the emerging security threats to IVNs, several defensive measures have been proposed in the literature, which can be broadly categorized as *message authentication schemes* and *intrusion detection systems*. Although several approaches have been proposed to authenticate the IVN communication and particularly the CAN bus messages [18, 55, 59, 66, 68, 69, 72], the proposed authentication schemes hardly make it to the industry due to the tight resource constraints in automotive systems, with backward compatibility and acceptable overhead expectations being the biggest adoption hurdles [54].

Intrusion detection systems, on the other hand, are designed to passively monitor IVN traffic for anomalies without imposing computational overhead on in-vehicle communication. As such, they meet the challenging resource constraints and strict real-time requirements of IVNs. In recent years, there have been several attempts to design and develop intrusion detection systems for IVNs [6, 26, 47, 49, 62]. Due to the long life-span (decades) of vehicles and the difficulty to maintain regular updates, anomaly-based detection has been considered to be more viable than signature-based approaches [49].

Most previous studies on anomaly-based attack detection leverage the high regularity of the timing behavior of IVN messages to detect malicious traffic by monitoring for unlikely changes in their periodicity. Other studies leverage the subtle, yet distinctive, differences in the physical properties of ECUs to detect intruders and identify compromised ECUs [6, 7, 30, 46]. Since a considerable portion of IVN messages are transmitted periodically, and CAN messages are inherently associated with unique low-level physical ECU properties, existing approaches are, by and large, capable of detecting attacks that cause such kinds of deviation. State-of-the-art solutions, however, fall short on two main fronts. First, there have been no noteworthy attempts to detect *stealthy attacks* that do not cause drastic changes in the IVN dynamics. Second, in most cases, prior knowledge about the underlying IVN traffic (frame ID, transmission frequency, etc.) and ECU configurations is needed. This makes the existing solutions *dependent on the underlying system specifications*, which are typically proprietary and may vary in vehicles of the same model and year produced by the same OEM, let alone in vehicles of different brands.

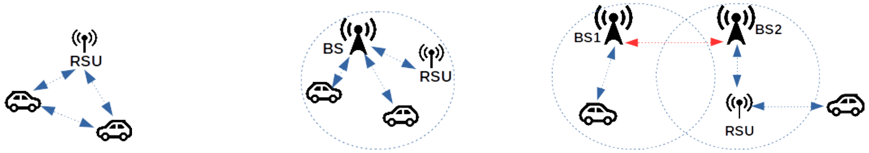
802.11p and cellular V2X

The vehicle to everything (V2X) communication technology 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), pedestrians and the infrastructure around the vehicles to communicate with each other. There are currently two types of communication technologies that can be used for enabling V2X: the Dedicated Short Range Communication (DSRC) that is based on the IEEE 802.11p protocol, and the cellular technology that is based on using Advanced Long Term Evolution (Advanced LTE) or 5G networks. V2X communication has several components including Vehicle-to-Vehicle (V2V), Vehicle-to-Roadside Unit (V2R) and Vehicle-to-Network (V2N) communications. Different communication scenarios exist for these components depending on the underlying V2X technology.

The 802.11p protocol enables vehicles to directly communicate via a Vehicular Ad Hoc Network (VANET) in which the participants are not required to authenticate and associate themselves to the network before sending data (Figure 6a). In Europe, the European Telecommunications Standards Institute (ETSI) has introduced the ETSI ITS G5 (ITSC) standard [12] to enable the implementation of V2X communication. The ITSC standard is based on IEEE 802.11p with some amendments towards European requirements. This standard enables dedicated short range communications between vehicles and RSUs (together called ITS stations), and its effective range of application is up to 500 meters [27]. Moreover, it defines a communication architecture and a standardized set of services and interfaces that enable secure V2X communications.

In addition to the 802.11p based V2X standard, the 3rd Generation Partnership Project (3GPP) has investigated the possibility of using the Advanced LTE cellular network for V2X communications. 3GPP and ETSI collaborated to develop standards to enhance LTE communications for V2X applications [13, 14]. The cellular V2X has two types of working modes, namely the cellular communication (Uu) and direct communication (PC5). The Uu mode allows vehicles to communicate using the existing cellular network (see Figure 6b), while the PC5 mode is similar to the DSRC, enabling direct communications between vehicles. Moreover, vehicles and RSUs can use a combination of Uu and PC5 communication to discover and communicate to each other (see Figure 6c). The new telecommunication standard under development, 5G, and the related new radio technology "New Radio (NR)" promise significant improvements w.r.t network latency, throughput and reliability in V2X communications. The development and standardization of 5G for V2X communications is ongoing and the 5G Automotive Associations (5GAA) is developing 5G enabled solutions for V2X applications [64].

V2X applications exchange messages containing information such as speed, direction and location. Despite the benefits of V2X 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 commu-



(a) 802.11p or PC5 (b) Uu (c) Uu + PC5

Figure 6: Different scenarios for V2V and V2R communications

nications. Moreover, V2X 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 V2X communications, such as DoS attacks, man in the middle attacks, eavesdropping attacks and Sybil attacks have been investigated in several researches [3, 9–11, 31, 43]. The security and privacy requirements of V2X communications have been investigated in several European projects such as SEVECOM [37], and PRESERVE [57] and solutions have been proposed.

In order to validate and authorize the ITS stations, 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 [24] 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 [45] that have attempted to evaluate the ETSI ITS security architecture.

Since the 802.11p protocol itself does not provide any mechanisms for authenticating ITS users for performance reasons, ETSI ITSC addresses security and privacy concerns with services in the higher layers of the communication stack (see paper E [53]). Therefore, an interesting question to ask is whether 5G New Radio can facilitate security features at lower levels, and what the security impact of replacing 802.11p with 5G NR in the ETSI stack would be.

Summary of Papers and Contributions

If you can't explain it simply,
you don't understand it well enough.

Albert Einstein

This section gives a summary of the papers presented in Section II of this thesis and my contributions to each work.

Towards Designing Secure In-Vehicle Network Architectures Using Community Detection Algorithms

Problem statement and related work. In the recent years, quite some effort has been spent in proposing new security mechanisms for the IVN, 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 meaningful 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 IDS or firewalls are then placed at the borders of the domains to monitor and filter the communication to and from each domain. Previous works in this area can be classified as general research about IVN architecture and its performance where safety has been the main criteria [35, 42], model-based approaches to compare different architectures against each other with respect to security aspects without stating how secure a specific architecture is [48], and approaches to perform task allocation where both security and safety are considered, without addressing the architectural questions regarding partitioning of the in-vehicle network into domains [38, 39].

Contributions and their implications. In this paper, we analyze the IVN 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 [52]).

Statement of contributions. This paper is the result of a collaboration started within the objective of the SeFram [60] project funded by VINNOVA. The original idea of the paper was proposed by my co-author Tomas Olovsson and later refined together with me and the other co-author of this paper Pierre Kleberger. I facilitated obtaining the data from Volvo Cars, Pierre Kleberger implemented the code, and the analysis of the results was performed by me and my co-authors. Pierre Kleberger and I were the main contributors to the writing of the paper.

Improving In-Vehicle network Architectures Using Automated Partitioning Algorithms

Problem statement and related work. This paper is a follow-up of our work on using community detection algorithms for automating the process of identifying security domain in IVN [28]. In [28] we showed that automated partitioning algorithms are suitable to identify good security domains in an IVN. 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?

Contributions and their implications. In this paper, we answer the above questions by comparing our identified architecture with the EVITA reference architecture [15]. In order to do that, the IVN 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 IVN 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 IVN. Even though the work presented here will not be the final design of the IVN architecture, we believe that the architecture identified in our work can be used as a base model or reference architecture for further IVN development.

Statement of contributions. This paper is a natural follow-up to our earlier paper on using community detection algorithms for automating the process of identifying security domain in IVN [28]. I am the first author. Pierre Kleberger further developed the code, and the analysis of the result was performed by me, Pierre Kleberger and Tomas Olovsson. Pierre Kleberger and I were the main contributors to the writing of the paper.

In-vehicle CAN Message Authentication: A Perspective from the Industry

Problem statement and related work. In-vehicle networks still suffer from a lack of agreed and applicable security solutions. Researchers have proposed several solutions for securing s in recent years [18, 21, 32, 56, 59, 66, 68, 72], 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.

Contributions and their implications. In this paper, 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.

Statement of contributions. This paper is the result of a joint work between Aljoscha Lautenbach, Tomas Olovsson and myself, started within the objective of the HoliSec [65] project funded by VINNOVA. I proposed the original idea of the paper and I am the first author. Aljoscha Lautenbach and I contributed equally to the technical material and the writing of this paper.

CASAD: CAN-Aware Stealthy-Attack Detection for In-Vehicle Networks

Problem statement and related work. Over the past decade there has been a rapid increase in the number of attacks on in-vehicle networks where CAN bus has been the primary target of the attacks. With CAN being the most prevalent protocol used for safety critical applications in vehicles, designing intrusion detection systems for CAN communications has become a major area of interest within the field of automotive security. A large number of studies are centered around the idea of monitoring CAN traffic for unlikely deviations in the periodicity of messages [26, 47, 49, 62], while others focus on measuring and utilizing deviations in low-level physical properties of ECUs to identify the attacker [6, 7, 30, 46]. Despite being capable of detecting attacks that cause obvious deviations in the highly regular properties of IVN communications, the proposed methods in literature suffer from two major limitations: they are dependent on the underlying system specifications and they fail to detect critical stealthy attacks.

Contributions and their implications. In this paper we propose a new method that addresses the above mentioned limitations for detecting IVN attacks. Our fast, lightweight, and system-agnostic approach learns the normal behavior of IVN dynamics from historical data and detects deviations by continuously monitoring IVN traffic. We demonstrate the effectiveness of our approach by conducting various experiments on a CAN bus prototype, a 2018 Volvo XC60, and publicly available data from two real vehicles. This paper makes several noteworthy contributions to the field of automotive security. First, we introduce the conquest attack, which is stealthy, feasible, and has potential to cause serious impact on IVNs. Second, we present CASAD, an efficient **C**AN-**A**ware **S**tealthy-**A**ttack **D**etection mechanism that is particularly suitable for the IVN domain. Third, we demonstrate through extensive experiments, how CASAD overcomes the limitations of existing work by being capable of detecting stealthy attacks on IVNs in addition to the classical attacks that exist in the literature, while not abiding by the strict specifications predefined for every vehicle model.

Statement of contributions. This paper is the result of a joint work between Wissam Aoudi, Magnus Almgren, Tomas Olovsson and myself, started within the objective of the HoliSec project funded by VINNOVA. I am the first author. The original idea of the paper was inspired by a recently proposed specification-agnostic method (PASAD) for detecting attacks on industrial control systems [4]. My contribution in terms of technical material was implementing and performing the attacks. Wissam Aoudi developed the detection engine and the analysis of the results was performed by me and Wissam Aoudi. I and Wissam Aoudi were the main contributors to the writing of the paper.

Experiences from Implementing the ETSI ITS SecuredMessage Service

Problem statement and related work. 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 implementations 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.

Contributions and their implications. This paper presents our experience from implementing the ETSI TS 103 097 V1.1.1. SecuredMessage, certificate format and sign/verify services on an existing ETSI Intelligent Transportation System (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.

Statement of contributions. This paper is the outcome of my master thesis project under the supervision of Tomas Olovsson. I am the main author of the paper and developed all the results. Tomas Olovsson is the corresponding author.

A Preliminary Security Assessment of 5G V2X

Problem statement and related work. Although V2X communications offer a wide range of safety and environmental benefits, there are also security and privacy concerns. The V2X messages exchanged between ITS users often contain data such as speed, direction and GPS coordinates. Therefore, it must be ensured that malicious attackers cannot violate the privacy of ITS users by intercepting V2X messages and obtaining the vehicle owner's identity information, vehicle location information or direction. Furthermore, attackers may broadcast false messages to mislead the drivers and cause serious road accidents or redirect the traffic flow. Since the 802.11p protocol itself does not provide any mechanisms for authenticating V2X users for performance reasons, ETSI ITSC addresses security and privacy concerns with services in the higher layers of the communication stack. Due to its technological advantages such as higher speeds and reliability, the new 5G telecommunication standard is being considered to be used for V2X services. The new radio technology "New Radio (NR)", which is being developed as part of 5G, can complement or replace 802.11p in V2X applications. While there has been some work to compare 802.11p and 5G New Radio in terms of performance and applicability for safety-critical use cases [1, 2, 16, 20, 61, 67], little work has been done to investigate the implications for security.

Contributions and their implications. In this paper, we investigate whether 5G New Radio can facilitate security features at lower levels of the communication stack, and what the security impact of replacing 802.11p with 5G NR in the ETSI stack would be. In order to understand the security implications of using cellular V2X and 5G NR for V2X communications, we detail the security requirements for known ITS applications, motivate these requirements and provide an in-depth analysis of different application use cases. For each use case, we study the requirements w.r.t security attributes identified by ETSI, which are *confidentiality*, *integrity*, *availability*, *privacy* and *authentication*. We find that use cases with safety impacts require *integrity*, *availability*, *authentication* and *privacy*, while *confidentiality* do not seem to be a major concern. On the other hand, use cases that rely on communications with external entities on the Internet have high *confidentiality* requirements. Next, we explore the new physical layer of 5G, a technology simply called New Radio, and investigate to which degree V2X security mechanisms can be simplified or removed from higher layers when cellular V2X and 5G are used. We find that due to the use of millimeter waves, beamforming and massive MIMO, there will be an implicit improvement for confidentiality and privacy, and it may also be possible to shorten authentication procedures in certain cases. When a fully network-assisted cellular V2X mode (Uu) is chosen, all messages are signed and encrypted by the 5G network, therefore it is possible to outsource several of the ITS security requirements to the cellular network.

Statement of contributions. This paper is the outcome of Romi Zaragatzky's successful master thesis project [73] under the supervision of Erland Jonsson and the examination of Tomas Olovsson. Aljoscha Lautenbach and I contributed with constant support for technical matters during the development of the master thesis and shaped up the results into a publishable paper. Aljoscha Lautenbach is the first author, I am the corresponding author. I and Aljoscha Lautenbach were the main contributors to the writing of the paper.

Conclusion

One person's "paranoia"
is another person's engineering redundancy.

Marcus J. Ranum

Cyber attacks on connected vehicles have already made the headlines and increased the awareness of the importance of security in modern vehicles. This thesis contributes to the growing field of automotive security research. It provides a high-level overview of the security concerns in IVN and V2X communications, and a collection of 6 papers that investigate secure IVN architecture design, attack protection, attack detection, and V2X security. The following are the highlights of the contributions of this thesis.

Paper A and **Paper B** propose an automated method for grouping in-vehicle ECUs into domains based on different criteria, and show that the proposed approach is able to identify meaningful domains with good quality with respect to communication, safety and security. The proposed method has been further developed by Volvo Cars for industrial use. **Paper C** makes two contributions to the area of attack protection in in-vehicle networks. First, it identifies five general requirements which a security solution needs to fulfill in order to be considered for adoption in vehicles. Secondly, it evaluates the applicability of several in-vehicle message authentication protocols based on the identified requirements, and shows that none of the solutions meet all of the criteria. **Paper D** makes several noteworthy contributions to the area of attack detection in IVNs. First, it introduces the conquest attack, which is novel, stealthy, and has potential to cause serious impact on vehicles. Secondly, it presents CASAD,,a specification agnostic and efficient attack-detection mechanism that is particularly suitable for the IVN domain and applicable to a wide range of vehicles. Thirdly, it demonstrates how unlike existing methods, CASAD is capable of detecting stealthy attacks on IVNs in addition to the classical attacks that exist in the literature. **Paper E** identifies a rather serious flaw in the design of the ETSI V2X security standard and demonstrates how to exploit the flaw to attack an ITSC stack. Moreover, it identifies potential problems in the description of the standard that are open to misinterpretation and potentially can lead to vulnerable implementations. It also proposes changes to fix the identified weaknesses. **Paper F** finds that due to the use of millimeter waves, beamforming and massive MIMO in 5G NR, there will be an implicit improvement for confidentiality and privacy of V2X communications. Moreover, it suggests that the authentication procedures that are currently handled by services in the higher layers of the communication stack can be shortened by using physical layer security in some cases.

Bibliography

[1] Mamta Agiwal, Abhishek Roy, and Navrati Saxena. "Next generation 5G wireless networks: A comprehensive survey". In: *IEEE Communications Surveys & Tutorials* 18.3 (2016), pp. 1617–1655.

[2] Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, and Andrei Gurtov. "5G security: Analysis of threats and solutions". In: *2017 IEEE Conference on Standards for Communications and Networking, CSCN 2017* (2017), pp. 193–199.

[3] 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.* IEEE. 2012, pp. 1–9.

[4] Wissam Aoudi, Mikel Iturbe, and Magnus Almgren. "Truth Will Out: Departure-Based Process-Level Detection of Stealthy Attacks on Control Systems". In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security.* CCS '18. Toronto, Canada: ACM, 2018, pp. 817–831.

[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.* ACM. 2015, pp. 1–8.

[6] Kyong-Tak Cho and Kang G. Shin. "Fingerprinting Electronic Control Units for Vehicle Intrusion Detection". In: *25th USENIX Security Symposium (USENIX Security 16).* Austin, TX: USENIX Association, 2016, pp. 911–927.

[7] Wonsuk Choi, Hyo Jin Jo, Samuel Woo, Ji Young Chun, Jooyoung Park, and Dong Hoon Lee. "Identifying ECUs Using Inimitable Characteristics of Signals in Controller Area Networks". In: *IEEE Transactions on Vehicular Technology* 67.6 (June 2018), pp. 4757–4770.

[8] *Cybersecurity Best Practices for Modern Vehicles Systems.* NHTSA, 2016. URL: `{https://bit.ly/33e9RYB}` (visited on Nov. 1, 2019).

[9] Anup Dhamgaye and Nekita Chavhan. *Survey on security challenges in VANET 1.* 2013. URL: `{http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.300.3967}` (visited on Nov. 1, 2019).

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

[11] Richard Gilles Engoulou, Martine Bellaïche, Samuel Pierre, and Alejandro Quintero. "VANET security surveys". In: *Computer Communications* 44 (2014), pp. 1–13.

[12] ETSI. *Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band.* European Standard for Intelligent Transport Systems (ITS) TS 302 663 - V1.2.0. 2012.

[13] ETSI. *Architecture enhancements for V2X services.* Technical specification on Universal Mobile Telecommunications System (UMTS); LTE TS 123 285 - V14.3.0. 2017.

[14] ETSI. *Service requirements for V2X services.* Technical specification on LTE TS 122 185 - V14.3.0 Release 14. 2017.

[15] EVITA. *E-safety vehicle intrusion protected applications (EVITA).* 2016. URL: `{http://www.evita-project.org/}` (visited on Nov. 18, 2016).

[16] Alessio Filippi, Kees Moerman, Vincent Martinez, Andrew Turley, Onn Haran, and Ron Toledano. *IEEE802.11p ahead of LTE-V2V for safety applications.* Tech. rep. 2017.

[17] B. Groza and P. Murvay. "Security Solutions for the Controller Area Network: Bringing Authentication to In-Vehicle Networks". In: *IEEE Vehicular Technology Magazine* 13.1 (Mar. 2018), pp. 40–47.

[18] 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.* Springer, 2012, pp. 185–200.

[19] Milena Guessi, Elisa Yumi Nakagawa, Flavio Oquendo, and José 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. New York, NY, USA: ACM, 2012, 31–40.

[20] Akhil Gupta and Rakesh Kumar Jha. "A survey of 5G network: Architecture and emerging technologies". In: *IEEE Access* 3 (2015), pp. 1206–1232.

[21] Oliver Hartkopp, Cornel Reuber, and Roland SCHILLING. "MaCAN - Message Authenticated CAN". In: *Escar Conference, Berlin, Germany.* 2012.

[22] 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. Hamburg, Germany: Springer-Verlag, 2009, pp. 145–158.

[23] Tobias Hoppe, Stefan Kiltz, and Jana Dittmann. "Computer Safety, Reliability, and Security: 27th International Conference". In: ed. by Michael D. Harrison and Mark-Alexander Sujan. Berlin, Heidelberg: Springer, 2008. Chap. Security Threats to Automotive CAN Networks – Practical Examples and Selected Short-Term Countermeasures, pp. 235–248.

[24] European Telecommunications Standards Institute. *ETSI TS 103 097 V1.1.1, Intelligent Transport Systems (ITS); Security; Security header and certificate formats.* 2013.

[25] *ISO 26262-1:2011: Road vehicles — Functional safety — Part 1: Vocabulary.* ISO, 2011.

[26] Min-Joo Kang and Je-Won Kang. "Intrusion Detection System Using Deep Neural Network for In-Vehicle Network Security". In: *PLOS ONE* 11.6 (June 2016), pp. 1–17.

[27] Vaishali D Khairnar and Ketan Kotecha. "Performance of vehicle-to-vehicle communication using IEEE 802.11 p in vehicular ad-hoc network environment". In: *arXiv preprint arXiv:1304.3357* (2013).

[28] P. Kleberger, N. Nowdehi, and T. Olovsson. "Towards designing secure in-vehicle network architectures using community detection algorithms". In: *2014 IEEE Vehicular Networking Conference (VNC).* Dec. 2014, pp. 69–76.

[29] 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).* Baden-Baden, Germany, June 2011, pp. 528–533.

[30] Marcel Kneib and Christopher Huth. "Scission: Signal Characteristic-Based Sender Identification and Intrusion Detection in Automotive Networks". In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security.* CCS '18. Toronto, Canada: ACM, 2018, pp. 787–800.

[31] 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*. IEEE. 2014, pp. 1–5.

[32] 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.

[33] Keen Security Lab. *Experimental Security Assessment of BMW Cars: A Summary Report*. Tech. rep. 2018. URL: {https://keenlab.tencent.com/en/Experimental_Security_Assessment_of_BMW_Cars_by_KeenLab.pdf} (visited on Nov. 15, 2018).

[34] Fred Lambert. *Keen Lab Hackers Managed to Take Control of Tesla Vehicles Again*. 2017. URL: {https://electrek.co/2017/07/28/tesla-hack-keen-lab/} (visited on Nov. 15, 2018).

[35] Vera Lauer, Martin Hiller, Massimo Osella, Marko Auerswald, and Jürgen Lucas. "Easis-electronic architecture and system engineering for integrated safety systems". In: *TRA-Transport Research Arena Europe 2006: Goeteborg, Sweden, June 12th-15th 2006: Greener, Safer and Smarter Road Transport for Europe. Proceedings* Deliverable D0.2.4 (2006).

[36] A. Lautenbach, N. Nowdehi, T. Olovsson, and R. Zaragatzky. "A Preliminary Security Assessment of 5G V2X". In: *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*. Apr. 2019, pp. 1–7.

[37] Tim Leinmueller, Levente Buttyan, Jean-Pierre Hubaux, Frank Kargl, Rainer Kroh, Panagiotis Papadimitratos, Maxim Raya, and Elmar Schoch. "SEVECOM - Secure Vehicle Communication". 2006. URL: {http://infoscience.epfl.ch/record/124920} (visited on Nov. 1, 2019).

[38] C. W. Lin, Q. Zhu, C. Phung, and A. Sangiovanni-Vincentelli. "Security-aware mapping for CAN-based real-time distributed automotive systems". In: *2013 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. Nov. 2013, pp. 115–121.

[39] Chung-Wei Lin, Qi Zhu, and Alberto Sangiovanni-Vincentelli. "Security-aware mapping for TDMA-based real-time distributed systems". In: *Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design*. IEEE Press, 2014, pp. 24–31.

[40] 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.

[41] J. Liu, S. Zhang, W. Sun, and Y. Shi. "In-Vehicle Network Attacks and Countermeasures: Challenges and Future Directions". In: *IEEE Network* 31.5 (2017), pp. 50–58.

[42] Syed Masud Mahmud and Sheran Alles. *In-Vehicle Network Architecture for the Next-Generation Vehicles*. SAE Technical Paper 2005-01-1531. SAE International, Apr. 2005.

[43] Mohamed Nidhal Mejri, Jalel Ben-Othman, and Mohamed Hamdi. "Survey on VANET security challenges and possible cryptographic solutions". In: *Vehicular Communications* 1.2 (2014), pp. 53–66.

[44] Charlie Miller and Chris Valasek. "Remote exploitation of an unaltered passenger vehicle". In: *Black Hat USA* (2015), p. 91.

[45] 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*. Vol. 1417. 2014.

[46] Pal-Stefan Murvay and Bogdan Groza. "Source Identification Using Signal Characteristics in Controller Area Networks". In: *IEEE Signal Processing Letters* 21.4 (2014), pp. 395–399.

[47] M. Müter and N. Asaj. “Entropy-Based Anomaly Detection for In-Vehicle Networks”. In: *2011 IEEE Intelligent Vehicles Symposium (IV)*. IEEE, 2011, pp. 1110–1115.

[48] M. Müter and F.C. Freiling. “Model-Based Security Evaluation of Vehicular Networking Architectures”. In: *2010 Ninth International Conference on Networks (ICN)*. 2010, pp. 185–193.

[49] M. Müter, A. Groll, and F. C. Freiling. “A Structured Approach to Anomaly Detection for In-Vehicle Networks”. In: *2010 Sixth International Conference on Information Assurance and Security (IAS)*. IEEE, Aug. 2010, pp. 92–98.

[50] Sen Nie, Ling Liu, and Yuefeng Du. *Free-Fall: Hacking Tesla from Wireless to Can Bus.* 2017. URL: {https://ubm.io/2NhSMrb} (visited on Nov. 1, 2019).

[51] N. Nowdehi, W. Aoudi, M. Almgren, and T. Olovsson. “CASAD: CAN-Aware Stealthy-Atack Detection for In-Vehicle Netwoks”. In: *Submitted to IEEE Transactions on Information Forensics & Security*. 2019.

[52] N. Nowdehi, P. Kleberger, and T. Olovsson. “Improving in-vehicle network architectures using automated partitioning algorithms”. In: *2015 IEEE Vehicular Networking Conference (VNC)*. Dec. 2015, pp. 259–266.

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

[54] 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 (VTC-Fall)*. IEEE, Sept. 2017, pp. 1–7.

[55] Stefan Nürnberger and Christian Rossow. “– vatiCAN – Vetted, Authenticated CAN Bus”. In: *Cryptographic Hardware and Embedded Systems – CHES 2016: 18th International Conference, Santa Barbara, CA, USA, August 17-19, 2016, Proceedings*. Ed. by Benedikt Gierlichs and Axel Y. Poschmann. Springer Berlin Heidelberg, 2016, pp. 106–124.

[56] 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. IEEE. 2008, pp. 1–6.

[57] PRESERVE. *Preparing Secure Vehicle-to-X Communication Systems (PRESERVE)*. 2016. URL: {https://www.preserve-project.eu/} (visited on Nov. 18, 2016).

[58] *SAE International: J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*. 2016.

[59] 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*. Sept. 2011, pp. 1–5.

[60] *Security framework for vehicle communication (SeFram)*. URL: {https://www.vinnova.se/p/sakerhetsramverk-for-fordonskommunikation/} (visited on Nov. 1, 2019).

[61] S. A. A. Shah, E. Ahmed, M. Imran, and S. Zeadally. “5G for Vehicular Communications”. In: *IEEE Communications Magazine* 56.1 (Jan. 2018), pp. 111–117.

[62] Hyun Min Song, Ha Rang Kim, and Huy Kang Kim. “Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network”. In: *2016 international conference on information networking (ICOIN)*. IEEE, 2016, pp. 63–68.

[63] 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)*. 2013, pp. 1–12.

[64] *The Case for Cellular V2X for Safety and Cooperative Driving*. Tech. rep. 23-Nov-2016. 5G Automotive Association, 2016, pp. 1–8.

[65] *The Vinnova/FFI HoliSec project*. URL: {https://www.vinnova.se/p/holisec-holistiskt-angreppssatt-att-forbattra-datasakerhet/} (visited on Apr. 25, 2018).

[66] 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*. 2011, pp. 229–235.

[67] Vladimir Vukadinovic, Krzysztof Bakowski, Patrick Marsch, Ian Dexter Garcia, Hua Xu, Michal Sybis, Pawel Sroka, Krzysztof Wesolowski, David Lister, and Ilaria Thibault. “3GPP C-V2X and IEEE 802.11p for Vehicle-to-Vehicle communications in highway platooning scenarios”. In: *Ad Hoc Networks* 74 (2018), pp. 17–29.

[68] 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*. Oct. 2014, pp. 13–18.

[69] Yuval Weisglass and Yoram Oren. “Authentication Method for CAN Messages”. In: ESCAR Europe, 2016.

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

[71] Marko Wolf, André Weimerskirch, and Christof Paar. “Security in Automotive Bus Systems”. In: *Workshop on Embedded IT-Security in Cars*. Bochum, Germany, Nov. 2004.

[72] Samuel Woo, Hyo Jin Jo, and Dong Hoon Lee. “A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN”. In: *IEEE Transactions on Intelligent Transportation Systems* (2014), pp. 1–14.

[73] Romi Zaragatzky. “Security analysis of introducing 5G in V2X communications”. eng. In: (2018). URL: {https://odr.chalmers.se/handle/20.500.12380/255942} (visited on Nov. 1, 2019).