THESIS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

On Securing the Connected Car

Methods and Protocols for Secure Vehicle Diagnostics

PIERRE KLEBERGER

Department of Computer Science and Engineering
Division of Networks and Systems
CHALMERS UNIVERSITY OF TECHNOLOGY

Göteborg, Sweden 2015

On Securing the Connected Car
Methods and Protocols for Secure Vehicle Diagnostics
PIERRE KLEBERGER
ISBN 978-91-7597-241-1

Doktorsavhandlingar vid Chalmers tekniska högskola
Ny serie nr. 3922
ISSN 0346-718X

Technical report 120D
Department of Computer Science and Engineering

Research group: Computer Security

Department of Computer Science and Engineering
Division of Networks and Systems
Chalmers University of Technology
SE-412 96 Göteborg
Sweden
Telephone: +46 (0)31-772 1000

Chalmers Reproservice
Göteborg, Sweden 2015

On Securing the Connected Car

Methods and Protocols for Secure Vehicle Diagnostics

PIERRE KLEBERGER
Department of Computer Science and Engineering, Chalmers University of Technology

Thesis for the degree of Doctor of Philosophy

Abstract

Software has been the enabler for the last decades of innovation in new vehicle functions. It is now an integrated part of today's cars and the maintenance and update of this software have become a costly process for the automotive industry. As wireless communication to vehicles is being introduced, vehicular maintenance can greatly be improved and many other new applications can be brought to the vehicles. However, the vehicle was not designed with security in mind. Since the vehicle is safety-critical, it is vital that such new remote services do not violate the safety and security requirements of the vehicle and that appropriate security mechanisms are implemented in the vehicle to prevent malicious vehicle manipulations.

In this thesis, approaches to secure the connected car and in particular mechanisms and protocols to secure administrative services for vehicle diagnostics and software download are presented. First, the landscape of the connected car and its infrastructure is investigated. A survey of current mechanisms to secure the in-vehicle network is made and a description of possible communication methods with vehicles is given together with a taxonomy of current entities involved in such communication. The usefulness of the taxonomy is demonstrated by two examples. Then, security analyses of vehicle maintenance in repair shops are conducted. Generic mechanisms and protocols are proposed to secure vehicle diagnostics, which are independent of the diagnostics protocol being used. The proposed protocol prevents unauthorised access to vehicles and it has been formally verified to ensure its correctness. Finally, security mechanisms for in-vehicle communication is addressed, where analyses are performed to design better in-vehicle network architectures that support both safety and security.

To conclude, this thesis contributes with new approaches to perform secure maintenance of future connected cars using wireless communication and to prevent unauthorised manipulations of the vehicle.

Keywords: connected car; vehicular services; security mechanisms; remote diagnostics; in-vehicle networks.

Acknowledgements

First of all, I would like to give my most grateful thanks to Professor Erland Jonsson for giving me the opportunity to join the Computer Security group and conduct graduate studies. I would also like to thank Associate Professor Tomas Olovsson. I would like to express my gratitudes to both of you for your supervision, guidance, and support throughout my work leading to this thesis.

I would also like to thank Volvo Car Corporation and VINNOVA for funding my research within the two projects SIGYN II and Security Framework for Vehicle Communication. Special thanks go to Anna Sundalen, Henrik Broberg, and Kristina Bjelkstål.

I also would like to thank current and former members of the security group. Thanks Aljoscha Lautenbach, Asrin Javaheri, Elena Pagnin, Farnaz Moradi, Katerina Mitrokotsa, Laleh Pirzadeh, Magnus Almgren, Nasser Nowdehi, Valentin Tudor, and Vilhelm Verendel. I am also grateful to my friends, new and former colleagues I got to know during the way, especially Guilhem Moulin, Jochen Hollmann, Magnus Själander, Viacheslav Izosimov, and Wolfgang John.

Last, but not least, I would like to thank my family; my beloved Madelen and our newborn son, my father and mother, and my sister. Thanks for all your support and encouragement.

Pierre Kleberger
Gothenburg, August 2015

Thesis

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

Part I: A Survey and Taxonomy of the Connected Car Infrastructure

Paper A

P. Kleberger, T. Olovsson, and E. Jonsson. "Security Aspects of the In-Vehicle Network in the Connected Car". In *Proceedings of the 2011 IEEE Intelligent Vehicles Symposium (IV)*, Baden-Baden, Germany, Jun. 2011, pp. 528–533.

Paper B

P. Kleberger, A. Javaheri, T. Olovsson, and E. Jonsson. "A Framework for Assessing the Security of the Connected Car Infrastructure". In *Proceedings of the Sixth International Conference on Systems and Networks Communications (ICSNC)*, Barcelona, Spain, Oct. 2011, pp. 236–241.

Part II: Secure Vehicle Diagnostics

Paper C

P. Kleberger, T. Olovsson, and E. Jonsson. "An In-Depth Analysis of the Security of the Connected Repair Shop". In *Proceedings of the Seventh International Conference on Systems and Networks Communications (ICSNC)*, Lisbon, Portugal, Nov. 2012, pp. 99–107.

Paper D

P. Kleberger and T. Olovsson. "Protecting Vehicles Against Unauthorised Diagnostics Sessions Using Trusted Third Parties". In *Proceedings of the 32nd International Conference on Computer Safety, Reliability, and Security (SAFECOMP)*, Toulouse, France, Sep. 2013, pp. 70–81. Volume 8153 of Lecture Notes in Computer Science, Springer Berlin Heidelberg.

Paper E

P. Kleberger and G. Moulin. *Formal Verification of an Authorization Protocol for Remote Vehicle Diagnostics.* Technical Report 2013:09. Department of Computer Science and Engineering, Chalmers University of Technology, Nov. 2013.
(Short Paper. In *Proceedings of the 2013 IEEE Vehicular Networking Conference (VNC)*, Boston, USA, Dec. 2013, pp. 202–205)

Paper F

P. Kleberger and T. Olovsson. "Securing Vehicle Diagnostics in Repair Shops". In *Proceedings of the 33rd International Conference on Computer Safety, Reliability, and Security (SAFECOMP)*, Florence, Italy, Sep. 2014, pp. 93–108. Volume 8666 of Lecture Notes in Computer Science, Springer International Publishing.

Part III: Securing the In-Vehicle Network

Paper G **P. Kleberger**, N. Nowdehi, and T. Olovsson. "Towards Designing Secure In-Vehicle Network Architectures Using Community Detection Algorithms". In *Proceedings of the 2014 IEEE Vehicular Networking Conference (VNC)*, Paderborn, Germany, Dec. 2014, pp. 73–80.

Paper H N. Nowdehi, **P. Kleberger**, T. Olovsson. "Improving In-Vehicle Network Architectures Using Automated Partitioning Algorithms". (Submitted to conference).

Contents

Acronyms

ABS	Anti-lock Braking System
ACC	Adaptive Cruise Control
ACL	Access Control List
AP	Access Point
ARP	Address Resolution Protocol
ASIL	Automotive Safety Integrity Level
BAN	Burrows-Abadi-Needham
BS	Back-end System
C2C-CC	Car 2 Car Communication Consortium
CA	Certificate Authority
CAN	Controller Area Network
CBC-MAC	Cipher-Block Chaining Message Authentication Code
CC	Common Criteria
CCU	Communication Control Unit
CLL	Cryptographic Link Layer
CN	Common Name
CRC	Cyclic Redundancy Code
CRL	Certificate Revocation List
CU	Communication Unit
DE	Diagnostics Equipment
DHCP	Dynamic Host Configuration Protocol
DMS	Data Management System
DNS	Domain Name System
DoIP	Diagnostics over IP
DoS	Denial-of-Service
DSRC	Dedicated Short-Range Communication
DTLS	Datagram Transport Layer Security
ECM	Engine Control Module
ECU	Electronic Control Unit
ETSI	European Telecommunications Standards Institute
FOT	Field Operational Test
FOTA	Firmware update Over The Air
GPS	Global Positioning System
HCI	Human Computer Interface
HSM	Hardware Security Module
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IKE	Internet Key Exchange
IP	Internet Protocol
IPS	Intrusion Prevention System
ISO	International Standard Organisation
ISP	Internet Service Provider

ITS	Intelligent Transportation Systems
ITS-S	ITS-station
IVC	Inter-Vehicular Communication
KDC	Key Distribution Centre
KPS	Key Predistribution System
LAN	Local Area Network
LIN	Local Interconnect Network
MAC	Message Authentication Code
MIC	Message Integrity Code
MILP	Mixed Integer Linear Programming
MITM	Man-In-The-Middle
MOST	Media Oriented Systems Transport
NDM	Network Device Monitor
NOC	Network Operation Centre
OBD-II	On-Board Diagnostics II
PAD	Peer Authorisation Database
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
PP	Protected Profile
RDS	Radio Data System
RSU	Road-Side Unit
SA	Security Association
SIL	Safety-Integrity Level
TAL	Trust Assurance Level
ToE	Target of Evaluation
TTP	Trusted Third Party
TVRA	Threat, Vulnerability, and Risk Analysis
UDS	Unified Diagnostic Services
V	Vehicle
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-X
VANET	Vehicle Ad-hoc Network
VC	Vehicular Communication
VLAN	Virtual LAN
WLAN	Wireless LAN
WWH-OBD	World-Wide Harmonised On-Board Diagnostics

Introductory Summary

1

Introduction

More and more functions in today's vehicles are implemented in software. A modern car can have as many as a hundred or more embedded computers, i.e., electronic control units (ECUs), depending on brand and model. These ECUs handle different tasks, such as engine control, anti-spin system, and mirror adjustment. As vehicles have become so dependent on software, procedures to maintain and update the vehicles' software efficiently are crucial. The main way to update software is still to bring the vehicle to the repair shop and physically connect diagnostics equipment to the in-vehicle network. This is a costly process for the automotive company if cars need to be recalled due to bugs in their software. With the introduction of wireless vehicular communications, there is room for improvements [1, 2]: software can be distributed to vehicles without bringing them to a repair shop, and vehicles can be pre-diagnosed before a scheduled maintenance or before a mechanic is sent out to a vehicle that has broken down at the roadside, thus, enabling the mechanic to have the right replacement parts available or brought to the repair site.

Until recently, vehicles have been closed systems, but this is changing. Several projects have been conducted since the early 2000s to improve safety and efficiency on roads [3, 4]. An enabling factor for these projects has been wireless communication, but access to the vehicles' internal communication is also necessary to make these improvements work. For example has platooning been demonstrated where vehicles communicate with each other to establish a "train of vehicles" following a leader vehicle [5]. In the platoon, the vehicles exchange speed information and adjust their speeds to close the gap between them, which increases the capacity of roads.

Vehicle-to-Vehicle (V2V) communication, as utilised by platoons, is not the only type of communication to be introduced in the vehicles. Short-range communication inside the vehicle is already a fact in recent cars and used to connect mobile phones to the infotainment system through Bluetooth so that calls can be diverted to the vehicles sound system [6]. The result of this increased communication is that the previously closed in-vehicle network is now becoming more and more exposed to external traffic, traffic that is potentially dangerous with respect to the vehicle's safety requirements. Since vehicles were not exposed to such external threats before, they were not designed to have any security features, and the lack of security has already been shown by researches [7, 8]. Therefore, to be able to fruitfully benefit from wireless vehicular communications, the vehicle and its communication has to be secured. This thesis presents approaches to secure the connected car and in particular methods and protocols to secure the connected car for future secure maintenance — secure vehicle diagnostics and software download.

This introductory summary is organised as follows. After this section, an introduction to the connected car is given. The section serves as a background to the work presented in this thesis. The objective of this thesis is then given in Section 1.2. An overview of the research is then presented in Section 1.3, where a summary of the research is first given and then an overview of the appended papers. The contributions of the thesis is presented in Section 1.4. The thesis closes with an overview of the related work in Section 1.5, and the conclusion in Section 1.6.

1.1 The Connected Car

The connected car can be described as a vehicle with one or more external wireless communication possibilities, which connects the vehicle to an external network. These external links are used to supply the vehicle with different services, both administrative services such as remote diagnostics and software download, as well as other non-administrative services like platooning, eTolling, and media streaming. This section gives an introduction to the connect car and serves as a background to the work presented in this thesis.

1.1.1 The Vehicle

The vehicle consists of embedded computers, called electronic control units (ECUs), which are connected to each other in an in-vehicle network. ECUs are further connected to sensors and actuators, so that they can receive sensor information about the environment and send commands to actuators, to perform their tasks, e.g., send command to lift the windows as the driver presses the "lift window" button, or activate the airbag as the vehicle senses a collision.

The in-vehicle network is divided into sub-networks of different bus system technologies. Available technologies are: *Controller Area Network (CAN)*, *Local Interconnect Network (LIN)*, *Media Oriented Systems Transport (MOST)*, and *FlexRay*. An adapted version of Ethernet for vehicles is also expected to be deployed in vehicles in the near future. The choice of bus technology for the different sub-networks depends on the communication requirements of the tasks that run in the connected ECUs, e.g., if they are highly safety critical and requires a network with high reliability or if a low cost network with low

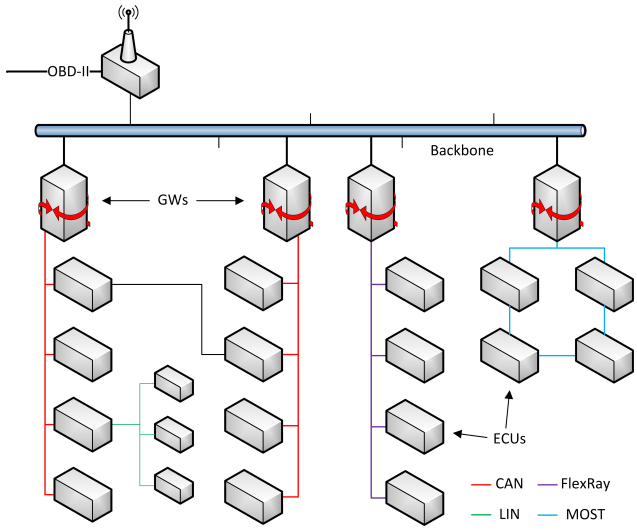

Figure 1.1: *Example of an in-vehicle network*

bit rate and less reliability is enough. The sub-networks are connected to each other through special *gateway ECUs* via a backbone network. Figure 1.1 shows an example of an in-vehicle network.

An On-Board Diagnostics II (OBD-II) interface enables diagnostics equipment to be physically connected to the in-vehicle network. This port is used to perform diagnostics of the vehicle, i.e., to communicate with ECUs by sending and receiving commands and status information and to update the firmware in the ECUs. Such communication is expected to be performed over a wireless link in future connected cars.

1.1.2 The Connected Car Infrastructure

The connected car have multiple communication possibilities to connect to external networks and services. A model that clarifies the details of the infrastructure of the connected car is shown in Figure 1.2. The model consists of two parts, the vehicle communication and the managed infrastructure. The details of the these are described in the following paragraphs.

Vehicle Communication

To enable vehicle communication, a wireless gateway, also known as the Communication Control Unit (CCU) [9], is introduced in the in-vehicle network. The gateway enables V2V and Vehicle-to-Infrastructure (V2I) communication, collectively known as Vehicle-to-X (V2X) communication.

A few different technologies exists for V2I communication. First, roads will be equipped with road-side units (RSUs) by means of which vehicles will establish communication to the infrastructure using the WAVE- or ETSI ITS-protocol stacks [10, 11]. These protocol

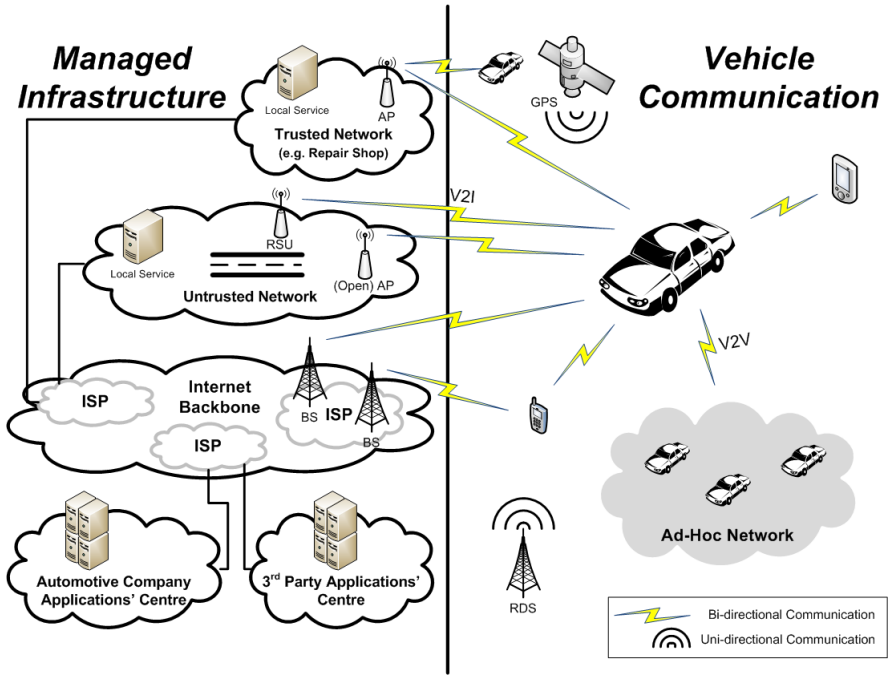

Figure 1.2: *Model of the connected car infrastructure*

stacks are also used for V2V communication. The second possibility is to use ordinary WiFi-technology where wireless access points (APs) are used, e.g., open APs in cities, or car owners' own APs at their parking lots, outside their homes. Finally, communication can be performed using cellular networks, such as 3G, HSDPA, and LTE.

It should also be noted that other communication means with the vehicle exists. For example, global positioning system (GPS) signals are received for positioning and navigation, and radio data system (RDS) signals are received for traffic information. Furthermore, Bluetooth is already available in recent cars to connect mobile phones and portable devices to the vehicle's infotainment system [6].

Managed Infrastructure

The managed infrastructure can be divided into five regions: automotive company applications' centre, third party applications' centre, trusted network, untrusted network, and Internet backbone.

The automotive company applications' centre consists of a set of servers that provides services to the automotive companies' vehicles. It holds necessary information about the vehicle, such as information from previous maintenance (e.g., diagnostics data), configuration data, cryptographic keys, as well as new software available for the ECUs. All other services delivered to the vehicle, but not provided by the automotive company, are provided by the third party applications' centre. It is not unrealistic to imagine that

large "application stores" will be implemented here by third parties.

Some networks can be considered to be trusted by the applications' centres and the vehicle. For example, a repair shop network may be considered trusted by the automotive company and the vehicle. For services delivered to this network, it may well be that some security requirements can be relaxed. Furthermore, other local services can be available in these networks to support the local infrastructure and provide services to the vehicle. Networks not considered to be trusted are regarded as untrusted, and in these networks, the services provided to the vehicle have to be adapted to the hostile environment of the Internet. In the same way as for the trusted networks, other local services may also be provided in these networks.

The Internet backbone, with its Internet Service Providers (ISPs), is the core network connecting the other four regions together. A backbone network is usually well protected and operated by network specialists in a Network Operation Centre (NOC). It is therefore reasonable to assume that intentional modification of data in these networks is rather unlikely.

1.1.3 Vehicular Services

Many services can be expected to be introduced in the connected car. As this thesis focus on secure vehicle maintenance, vehicular services are divided into administrative services, i.e., those that are used when maintaining the vehicle, and non-administrative services.

Administrative Services

Administrative services are those services that are used to maintain the connected car, i.e., to diagnose the vehicle and update its software. The services *remote diagnostics* [1] and *software download* [2] are generally referred to as two services, but depending on the remote diagnostics protocol used, software download can be incorporated as part of the diagnostics protocol as in ISO 14229 [12].

There are many expected benefits of introducing wireless remote diagnostics [2]. In the case of a repair shop, no cables are needed, which shortens the time for connecting the vehicle to the repair shop and also makes it possible to connect many vehicles at the same time. However, using wireless connections, where many vehicles can connect to the same wireless AP, also raises security related questions. How does the mechanic know that he/she is working with the right vehicle, and what support is implemented in the network to protect the vehicle against malicious network behaviour?

To conclude, since maintenance of the vehicle includes diagnostics and updates of the vehicle's ECUs, appropriate security mechanisms are needed for the entire vehicle.

Non-Administrative Services

Numerous non-administrative services using V2X communication have been discussed during the last decade [13, 14]. For example, platooning, pre-crash warning, virtual traffic lights, media streaming, etc. Even though these services may control the vehicle to some degree (e.g., adapting the vehicle's speed in platooning) they do not permanently change any software or issue any diagnostics commands. Nevertheless, these services need to

be developed in such a way that they do not affect the safety of the vehicle and the communication needs to be appropriately secured.

1.1.4 Security Considerations

This section gives a brief overview of the security problems faced by the car industry when introducing connectivity in their cars.

Terminology

First, we need to clarify some security terms that are important for the discussion in this thesis:

- **Authentication:** the process of establishing the identity of a subject.
- **Authorisation:** the permission a subject can exercise on an object.
- **Access Control:** the process to determine and enforce a subject's permission to an object in accordance to the authorisation.

Note that authentication is strictly limited to establishing the identity of a subject, it says nothing about what that subject is authorised to do once authenticated.

Adversaries

Automotive companies want to protect their investments in intellectual property, i.e., the software developed and installed in their vehicles. Anyone that wants to get hold of proprietary software or firmware can therefore create a potential loss in revenue (e.g., update software without paying) and appropriate security measures are needed to prevent such unauthorised access. There is therefore an interest in protecting the diagnostics communication with vehicles, especially the transfer of ECU firmware.

The integrity of vehicles must also be ensured. The vehicle has to be safe to drive, and an attacker might want to manipulate a vehicle just to cause harm to the driver or to the brand of the manufacturer. The possibility to disable the breaks while driving has already been demonstrated by researches [7], which leads to critical safety implications and must be prevented. As vehicles now are becoming connected and can be accessed through wireless communication, the likelihood of external attacks cannot be neglected.

Different objectives of an attacker to target vehicles overall are given by Brooks et al. [15], where the reason can be the challenge, status, thrill, financial gain, or damage, and the attacker may be hackers, corporate raiders, professional criminals, and terrorists.

1.1.5 Protocols and Standards

This section gives a short introduction to the protocols and standards used in vehicle diagnostics.

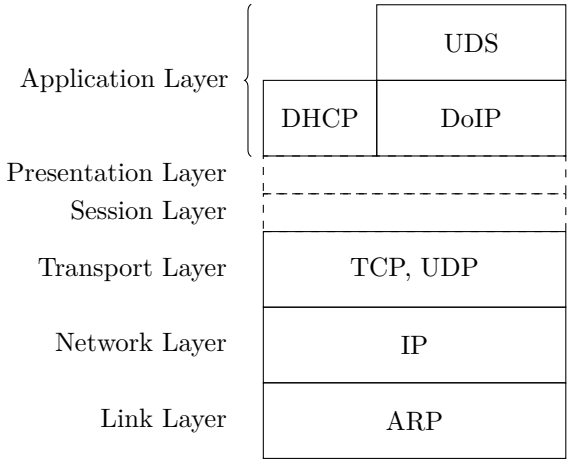

Figure 1.3: *The DoIP Stack*

ISO 13400 — Diagnostics over IP (DoIP)

Diagnostics over IP (DoIP) [16] is an ISO standard for conducting diagnostics over IP-based networks. The standard was approved in 2011/2012 and describes the required services from layer 2–4 and 7 (following the OSI layering model) for the diagnostics architecture. It defines an application protocol for exchanging management and diagnostics messages between DoIP-enabled devices. The diagnostics messages themselves are not specified by DoIP as the purpose of the standard only is to transmit these messages over IP-based networks. Instead, the diagnostics messages are described in other standards, such as ISO 14229 Unified Diagnostic Services (UDS) [12] and ISO 27145-3 World-Wide Harmonised On-Board Diagnostics (WWH-OBD) [17]. Figure 1.3 shows the DoIP stack with encapsulation of ISO 14229 diagnostics messages.

DoIP uses IP, TCP, and UDP, both in unicast and broadcast. Port 13400 is reserved for exchanging management communication over UDP and to establish diagnostics connections over TCP. However, no attention was given to security and no additional mechanisms were added to protect against threats and vulnerabilities available in today's Internet.

ISO 14229 — Unified Diagnostic Services (UDS)

ISO 14229 [12] defines an application layer protocol for diagnostics of vehicles. 26 services are provided and with these services, it is possible to read and write data to ECUs, reset ECUs, and upload firmware. Some support for secure communication is provided by the service `SecuredDataTransmission (0x84)`, but due to the request-response design of this service, services that do not obey such an approach cannot benefit from it and still have to be provided in an insecure way. The three services that cannot benefit from secure communication are: `ResponseOnEvent (0x86)`, `ReadDataByPeriodicIdentifier (0x2A)`, and `TesterPresent (0x3E)`. Furthermore, how the communication is protected during transmission by `SecuredDataTransmission (0x84)` is not described in this standard.

This is described in ISO 15764 [18].

1.1.6 Challenges

There are some general requirements that present special challenges for securing the connected car and its in-vehicle network:

(1) *resource constrains of the ECU.* The ECU has limited processing power and memory, which limits the possible security features that can be implemented on an ECU. Public-key cryptography is one example of a processing-intensive algorithm which currently takes long time to execute and therefore is not usable in verification of in-vehicle messages. Another example is firmware that is larger than the available internal memory in the ECU[1] and therefore creates implications for software download protocols and the ECU reprogramming process.

(2) *limited possibilities of extra cost for the connected devices.* The automotive industry is very cost sensitive and any new security solution must be cost efficient. Even small increases in cost of ECUs affect the revenue of the automotive company. For example, if the cost of an ECU is increased by just €1 and the vehicle has 10 ECUs of that kind, the total increase of cost for *one vehicle* will be €10. Even though €10 does not seem much, an automotive company selling 1 million vehicles a year will reduce its revenue by €10 million.

(3) *lifetime of the solution.* A vehicle of today may be used for as long as 10–15 years. This is quite an extensive period of time compared to ordinary desktop computers. One should note that this is only the time of usage and does not include the development time and that the architecture is used in production for several years. The overall lifecycle of a solution can therefore be as long as 20–25 years. How security features should be handled in the vehicle for such long timespans is yet an unsolved problem.

1.1.7 The Complexity of an In-Vehicle Network

There are many aspects to consider when developing an in-vehicle network, and these aspects can be divide into two major categories: the different *views* we can have of the in-vehicle network, and the *requirements* that are recognised and must be fulfilled by the engineers when designing the in-vehicle network architecture. The design aspects are shown in Figure 1.4 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.

[1] The flash memory holding the firmware may be larger than the available internal RAM.

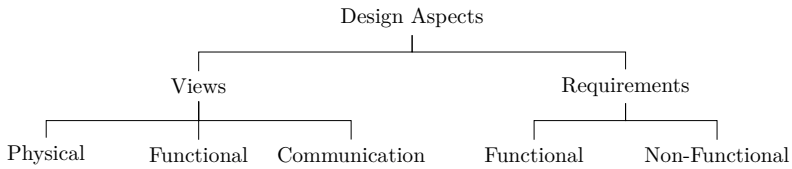

Figure 1.4: *Design aspects of an in-vehicle network architecture*

- **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. Examples of functions are the anti-lock braking system (ABS) and the adaptive cruise control (ACC).
- **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 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 behaviour, e.g., the maximum delay between the moment that driver hits the brake pedal till 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 behaviour, e.g., it should not be possible to activate the parking assistant while driving (safety), and updates of ECU firmware is only allowed by authorised personal (security).

The many aspects to consider makes the design of an in-vehicle network complex; all aspects have to be considered and compromises must be made.

1.2 Thesis Objective

The research presented in this thesis aims to provide approaches to secure the connected car, and in particular methods and protocols to support and provide secure diagnostics (maintenance) of vehicles. The following research questions are addressed:

1. Can a systematisation and categorisation of entities related to the connected car and its in-vehicle network help detecting security problems and finding security solutions?
2. How can the connected car be securely diagnosed (maintained) over an IP-based network?
3. How can the in-vehicle network be designed to facilitate the implementation of security controls? What methods and approaches exists?

The thesis is divided into three parts, where question 1, 2, and 3 are addressed in Part 1, 2, and 3, respectively.

1.3 On Securing the Connected Car

This section gives an overview of the work presented in the appended papers. First, a summary of this work is given, followed by an overview of each of the appended paper.

1.3.1 Research Summary

An important step to address security of the connected car is to have a good overview of the current state-of-art in the research community and what remains to be done. In addition, a clear model of the communication environment of the connected car is needed to be able to discuss and evaluate possible communication protocols and their requirements in the connected car domain. Consequently, a survey of current approaches to secure the in-vehicle network was conducted (Paper A) and a model that clarifies possible communication means with the connected car was proposed (Paper B). Additionally, a security assessment tree is presented that gives the possibility to analyse different security aspects when delivering services to the connected car.

One of the main purposes of this thesis is to identify security requirements and mechanisms to provide secure vehicle diagnostics. Several steps were taken to reach that goal. First, a security analysis of a limited vehicle diagnostics environment, that of a repair shop, is conducted (Paper C). Based on the model of the connected car infrastructure (Paper B), a model of the repair shop network was derived. A reduced version of the Threat, Vulnerability, and Risk Analysis (TVRA) method defined by the European Telecommunications Standards Institute (ETSI) for analysis of telecommunication networks was used to analyse the repair shop environment. Several security issues were identified when wireless communication is introduced in vehicle diagnostics and general countermeasures for these were suggested. However, the most critical security implication identified against vehicles was surprisingly not in the vehicle or in the repair shop themselves, rather in the lack of authorisation of diagnostics equipment. The reason is that, without authorisation, anyone that get hold of an authentic diagnostics equipment or its authentication keys (certificates), may connect and perform a diagnostics session with any vehicle that accepts these authentication keys. A protocol that prevents unauthorised diagnostics access to vehicles (Paper D) and a formal analysis that shows the correctness of the protocol (Paper E) is therefore provided. The protocol introduces a trusted third party (TTP) that governs the access to vehicles and issues a short-lived authorisation ticket to diagnostics equipment and vehicles. The ticket holds authorisation keys and information regarding what commands are allowed to be executed and for how long. Of course this does not *prevent* malicious activities within the scope of the authorised access, but it *eliminates large scale attacks to many vehicles*; attackers will not be able to use diagnostics equipment against arbitrary vehicles. A correct implementation of the protocol guarantees mutual authentication between the connecting diagnostics equipment and the vehicle, that the authorisation keys cannot be obtained by an attacker intercepting the communication, and that the information regarding the authorised commands are

fresh. Finally, to provide a secure vehicle diagnostics architecture, an analysis of possible approaches to secure diagnostics protocols in the repair shop is presented and the approach that is most suitable for this environment is identified (Paper F). The analysis is focused on the Diagnostics over IP (DoIP) protocol, ISO 13400, which can be expected to be used for future diagnostics communication, both in local networks as well as for remote diagnostics over the Internet. As already pointed out earlier, DoIP was not designed with security in mind and lacks fundamental security mechanisms to protect its diagnostics and management communication against threats and vulnerabilities in today's Internet communication. It was found that most of the requirements of a security architecture for the repair shop is best met by implementing security mechanisms as far down the network stack as possible, except for access control of diagnostics commands that needs to be handled at the application layer. Conclusively, even though it is a compromise, a security architecture based on IPsec seems to be the most desirable for the repair shop environment. A great benefit with IPsec is that it can be used to also secure remote diagnostics over the Internet. Moreover, the key agreement protocol, e.g., Internet Key Exchange (IKE), is decoupled from IPsec and can easily be replaced. Thus, by using the previously proposed authorisation protocol (Paper D), the session keys can be distributed to the diagnostics equipment and the vehicle and used by IPsec to secure the diagnostics communication. The combination of these, IPsec and the authorisation protocol, offers a secure diagnostics architecture for both local and remote diagnostics, and protects vehicles from unauthorised diagnostics access.

Given a secure diagnostics architecture between the diagnostics equipment and the vehicles, the in-vehicle network remains to be secured. Approaches to secure the in-vehicle network have been proposed (see Paper A), however, very little work has been conducted regarding the in-vehicle network architecture itself and how it should be designed to facilitate the implementation of security mechanisms. In the last part of the thesis, the problem of finding *automated* methods for, and their efficiency in, deriving in-vehicle network partitions (domains) is investigated. A reason for dividing a network into domains, from a security point of view, is to follow a well-known concept from traditional network security engineering: to protect the systems inside the domains from the outside, but also to isolate possible security problems and to retain them inside a domain. Security measures can then be placed at the borders of the domains to monitor and filter the communication to and from each domain, e.g., using Intrusion Detection Systems (IDSes) and firewalls. Four different community detection algorithms known from the area of social network analysis is therefore investigated (Paper G) to identify the algorithm that gives the "best" network partitions, i.e., the partitioning that keeps as much communication as possible inside the domains and as little communication as possible between the domains. The algorithms are applied to the in-vehicle network communication from a *real*, modern car and the partitioning results are compared using three commonly used quality measures for this class of algorithms, as well as plotting and ocular inspection. Among the compared algorithms, Louvain is found to give the best partitions of the in-vehicle network. To further analyse the usefulness and effectiveness of Louvain, the partitions gained by Louvain are compared to those defined by EVITA (Paper H). The Louvain algorithm improves (decreases) the inter-domain traffic for the analysis made on both message types and payload sizes. An architecture based on Louvain also successfully keeps

more messages that belong to safety critical ECUs inside the domains when compared to the EVITA architecture using Automotive Safety Integrity Levels (ASILs) as a safety criticality measure. Thus, for our dataset, an architecture based on Louvain simplifies the implementation of both security and safety measures as less inter-domain traffic need to be considered. Furthermore, the Louvain algorithm runs in the order of seconds on an in-vehicle network dataset. We therefore see great potential in introducing a tool that proposes an in-vehicle network architecture with domains to the vehicular engineer during the design phase. This architecture can then be used as a base for ECU allocation and be further refined when other design criteria are considered (see Section 1.1.7).

1.3.2 Overview of Appended Papers

This section gives an overview of the appended papers.

Part I: A Survey and Taxonomy of the Connected Car Infrastructure

This part provides an overview of the security research within the in-vehicle network and a framework for addressing security in the connected car domain.

Paper A: Security Aspects of the In-Vehicle Network in the Connected Car. In this paper, a survey of the research within securing the in-vehicle network of the connected car was conducted. The survey was structured around the following five categories: problems in the in-vehicle network, architectural security features, IDSes, honeypots, and threats and attacks. There were several issues that lead to security problems. First, the communication buses were not developed to support security and therefore lacks sufficient protection mechanisms. However, this is not the only issue. Misuse of safety related protection mechanisms can cause denial-of-service (DoS) attacks by, for example, sending CAN-messages with the highest priority, and the Engine Control Module (ECM) could be put into programming mode while the vehicle was moving (because the protocol standard was not correctly followed). We found seven papers proposing approaches and protocols with various security, communication, and timing properties to secure the in-vehicle network. Furthermore, only a few papers addressed IDSes, honeypots, and threats and attacks. We note that both anomaly-based and specification-based IDSes have been considered and that work has already been conducted to adapt threat models to the vehicular domain. Conclusively, we found that most of the work published so far was towards identifying and demonstrating problems with security in the in-vehicle network and only to a lesser extent towards presenting solutions. Also, even though there are four major bus technologies used in in-vehicle networks (CAN, FlexRay, MOST, and LIN), almost all research has so far been focused on the CAN-bus. Thus, much research remains to be done.

Paper B: A Framework for Assessing the Security of the Connected Car Infrastructure. Vehicular services, which were developed for usage in closed networks, were not designed with security in mind and when remote and wireless connections are introduced, these services need to be adapted to the new hostile environment imposed

by open networks. However, to secure services for the connected car, a model of the infrastructure to analyse possible communication means and security threats is needed. In this paper, we present a framework for assessing the security of the connected car infrastructure. The framework consists of two parts, the model of the infrastructure and a security assessment tree. The model of the infrastructure is divided into two parts (as already shown in Figure 1.2), the managed infrastructure and the vehicle communication. The model clarifies possible communication means between the vehicle and services in the infrastructure. Furthermore, the assessment tree presents four categories of security related aspects that need to be considered when securing vehicular services: the actors, vehicle-to-X communication technologies, network paths, and the dependability and security attributes.

Using the framework, various security aspects and communication means can be analysed during design of vehicular services. For example, consider a remote diagnostics service where the vehicle is diagnosed from the automotive company, then multiple vehicle-to-X communication technologies and network paths are available and the different actors and security attributes that have to be considered for each of them. Thus, the assessment three helps us state requirements regarding the security of the services delivered to the vehicle, and the usefulness of the framework is demonstrated with the analysis of two services: a remote diagnostics service and a map service with GPS positioning.

Part II: Secure Vehicle Diagnostics

This part presents problems in securing vehicle diagnostics and an approach to define a secure vehicle diagnostics architecture that is general and independent of the diagnostics protocol being used.

Paper C: An In-Depth Analysis of the Security of the Connected Repair Shop. Using wireless networks for vehicle diagnostics in repair shops comes with many benefits, e.g, no cables are needed and many vehicles can be diagnosed at the same time. However, it also raises some security related questions, such as, how does the mechanic know that he/she connects to the right vehicle and how are vehicles protected against attacks from other connected vehicles? In this paper, we use a reduced version of the European Telecommunications Standards Institute's (ETSI) Threat, Vulnerability, and Risk Analysis (TVRA) method to analyse the security in future connected repair shops. The reason for using a reduced version of the method was that we wanted to find general security mechanisms and countermeasures for the repair shop and not identify countermeasures for a particular implementation. Fourteen vulnerabilities were identified and classified in accordance to the five categories defined by the TVRA method: eavesdropping, unauthorised access, masquerade, forgery, and information corruption. Countermeasures were identified to directly address twelve of the vulnerabilities. The remaining two were related to possible bugs in software, which may be exploited to install malware that may lead to unauthorised disclose of information or manipulation of data. A general countermeasure to reduce possible bugs is to limit the exposure of code, e.g., limit the exposure of the network stack in a device.

We also outline and discuss one approach to secure the repair shop. We found that,

for this environment, implementing security at link layer is beneficial, even though it is not supported in common protocols of today. Security mechanisms implemented at link layer can limit the possibility of unintended communication between devices, e.g., between vehicles in the repair shop, and reduce the exposure of software bugs in the devices, e.g., bugs in the network stack. We also found that, even though the repair shop can be secured, vehicles outside of the repair shop are still vulnerable. The authentication keys used in diagnostics equipment need to be handled carefully. If these keys are lost or stolen, they will give access to any vehicle that accepts these authentication keys, even outside of the repair shop.

Paper D: Protecting Vehicles Against Unauthorised Diagnostics Sessions Using Trusted Third Parties. As discovered in Paper C, the loss of diagnostics equipment or its authentication keys can have major security implications for vehicles. If an attacker manages to get hold of the authentication keys, the attacker may get access to any vehicle that accept these keys, even outside of the repair shop, until these keys are revoked or have expired. Hence, an attacker could possibly perform an attack with very high scalability, with rather little effort, e.g., manipulate all vehicles (of a specific brand) at a parking lot. In this paper, we address this security problem and propose an approach to prevent unauthorised access to vehicles. First, a trusted third party (TTP) is introduced to issue authorisation tickets. The TTP holds security policies for vehicles describing the time of access and type of diagnostics messages allowed to be processed by the vehicle. Then we propose an authorisation protocol to issue authorisation tickets to vehicles and diagnostics equipment. An informal security analysis of the protocol is also presented. Finally, we discuss how to enforce access control in vehicles, so that only authorised diagnostics commands can be executed.

Our approach is flexible and has a set of features that makes it suitable for large scale implementations and well adapted for different scenarios. First, the authorisation protocol is independent of the actual diagnostics protocol being used. Whether ISO 14229 or any other diagnostics protocol is being used does not change the *authorisation procedure*. Second, the protocol is scalable in the sense that it is not limited in number of TTPs nor tickets that can be issued. Hence, it can be used to issue a large set of tickets to, for example, authorise an update of firmware in a complete fleet of vehicles. Multiple TTPs can also be used to support different levels of trust, e.g., a TTP located at the vehicle inspection authority that only allows certain information to be accessed, while another TTP at the repair shop allows necessary access to maintain the vehicle. Third, no synchronised clocks are necessary, which otherwise could be problematic to maintain in a distributed environment.

To conclude, the proposed approach does not rely solely on proper identification and authentication of diagnostics equipment, but authorisation is also required to access a vehicle. However, even though authorisation does not offer complete protection, i.e., malicious activity can still be conducted by authorised users, it prevents large scale attacks and essentially eliminates the possibility to target an arbitrary vehicle.

Paper E: Formal Verification of an Authorization Protocol for Remote Vehicle Diagnostics. As always when introducing new security protocols, there are questions

regarding whether the protocol is correct or not. In Paper D, only an informal analysis of the protocol was presented. In this paper, we present a formal security analysis of the authorisation protocol using Burrows-Abadi-Needham (BAN) logic and the automated verification tool ProVerif. We show that the protocol provides mutual authentication between diagnostics equipment and the vehicle, and that it guarantees both secrecy of the distributed session key and freshness of the distributed authorisation information. Thus, a correct implementation of the authorisation protocol prevents unauthorised access to vehicles.

Paper F: Securing Vehicle Diagnostics in Repair Shops. A critical problem with Diagnostics over IP (DoIP) (ISO 13400) is the lack of security. No additional security was added on top of the ordinary Internet Protocol (IP) stack. The protocol is therefore subject to many of the attacks already known from ordinary IP-traffic in today's Internet, e.g., network spoofing and packet manipulations. If DoIP is ever going to be used for transmitting safety critical commands to vehicles, e.g., write configuration parameters or updated firmware in ECUs, it has to be secured. In this paper, we make a thorough analysis of possible approaches to implement secure vehicle diagnostics in repair shops using DoIP. We consider a set of possible security mechanisms to address security at different layers of the network stack: ISO 15764, SSL/TLS, IPsec, Virtual LAN (VLAN), and Cryptographic Link Layer (CLL). These are evaluated against the requirements identified for the repair shop environment.

Four security requirements were identified: data integrity, data authenticity, data freshness, and data confidentiality. Additionally, a set of desirable security requirements was identified. First, the diagnostics communication should be robust and not easily fail due to manipulations. Second, a fine-grained access control mechanisms is desirable to only let authorised diagnostics commands be handled by vehicles. Finally, communication between vehicles should be prevented, so that attacks from other vehicles are prevented. Furthermore, the security architecture must be attractive to the automotive industry to be implemented. Therefore, the final security architecture also has to be easy to deploy and maintain, not cost to much, and only allow authorised vehicles to connect to the repair shop.

To conclude, we find that most of the requirements are best met with security mechanisms implemented as far down in the network stack as possible, except for the fine-grained access control, which is best implemented at the application layer. Furthermore, we find two conflicting requirements that affect the choice of implementation: how easy the security architecture is to deploy and maintain vs. how robust the implementation is — an implementation based on IPsec vs. a complete link layer security architecture. We find that a security architecture based on IPsec is the most desirable one, even if it is a compromise. A complete link layer security architecture would prevent a man-in-the-middle attacker from gaining control of the delivery of diagnostics messages using Address Resolution Protocol (ARP) spoofing. However, there are no standard protocols available that are suitable for our environment for such link layer protection. IPsec, on the other hand, comes with great benefits; it can be used to protect remote diagnostics *over the Internet* and the key agreement protocol used to negotiate session keys, e.g., IKE, is decoupled from the IPsec standard and can be replaced. Thus, to further improve the protection of

the vehicle, we suggest that the previously proposed authorisation protocol (Paper D) should be used as a key exchange protocol replacing IKE. A complete security architecture for both local and remote diagnostics can now be implemented, which is independent of the diagnostics protocol being used, enables the authorisation of diagnostics equipment to vehicles and the distribution of session keys, and the enforcement of security policies in vehicles.

Part III: Securing the In-Vehicle Network

This part addresses issues in securing the in-vehicle network of the vehicle.

Paper G: Towards Designing Secure In-Vehicle Network Architectures Using Community Detection Algorithms. Efforts in securing the in-vehicle network have resulted in a number of proposed security mechanisms in recent years (see Paper A). However, little effort has been spent in analysing the in-vehicle network architecture itself and how it should be designed to facilitate the implementation of security mechanisms. Today's in-vehicle networks are divided into domains based on functions or bus technologies using a "best engineering practice" approach. The notion of (security) domains is also a well-known concept used in ordinary network security engineering, where the idea is to protect systems inside the domain from the outside and to also retain possible security problems within the domain. Security measures are then placed at the border of the domain to monitor traffic to and from the domain using, for example, IDSes and firewalls. In this paper, we investigate the possibility of using community detection algorithms known from the area of social network analysis to automatically partition the in-vehicle network into domains in an optimum way based on certain partitioning criteria. In this first attempt, we try to partition the in-vehicle network into domains based on message types (a.k.a. signals) and we use data from a *real* car. Four fundamentally different community detection algorithms are investigated: Louvain, Infomap, Eigenvector, and Edge betweenness. As there is no single quality measure to describe which algorithm that performs best, three different quality measures were used: Coverage, Modularity, and Conductance. As an in-vehicle network has only about 100 nodes, plotting and ocular inspection can also be used to identify the algorithm that performs well. We find that domains indeed could be identified and that Louvain was the algorithm that produced the best domains for our dataset and should be used in further analyses.

Paper H: Improving In-Vehicle Network Architectures Using Automated Partitioning Algorithms. In the previous paper, Paper G, we concluded that domains indeed could be identified for in-vehicle network communication based on message types using Louvain, but we did not do any deeper analysis on how much improvement the new domain allocation resulted in. In this paper, we further analyse the improvements gained by Louvain by comparing it to the architecture proposed by EVITA. Thus, the in-vehicle network communication from the real car is mapped into the domains of the EVITA reference architecture and also partitioned using Louvain. We find that, when using message types as partitioning criterion, Louvain successfully identifies an architecture in which 55% of the messages are intra-domain messages. This is almost twice as much as in EVITA,

where 28% of the messages were intra-domain. Moreover, partitions identified based on message payload yields approximately 586 Kb/s (38 percent) less inter-domain communication 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. Furthermore, based on the ASIL levels associated with ECUs and their messages, our analysis concludes that safety also is improved as safety critical messages become more concentrated into fewer domains. This makes it easier for designers to provide safety measures for domains that have safety critical ECUs as they have to rely less on inter-domain traffic. Finally, the identified domains are also shown to be meaningful in the sense that the domains represent logical and meaningful functions. To conclude, for our dataset, we find that improvements to safety and security can be obtained at the same time and that safety and security requirements are not necessarily in conflict with each other when designing the architecture.

It should be emphasise that our analysis is based on only two criteria and many other aspects such as cost, reliability, and real-time requirements also need to be considered in a final in-vehicle network architecture. Yet, the method makes it possible to quickly analyse specific criteria during the design of in-vehicle networks. We therefore see great potential in introducing a tool that proposes an in-vehicle network architecture with domains to the vehicular engineer during the design phase. This architecture can then be used as a base for ECU allocation and be further refined when other design criteria are considered.

1.4 Thesis Contributions

The main contributions of this thesis are:

- I have surveyed current research on in-vehicle networks and identified open issues to secure the in-vehicle network. I have developed a general model of the connected car infrastructure and a taxonomy to facilitate the derivation of security mechanisms for the connected car's services. The survey and taxonomy addresses research question 1 and is a prerequisite for research question 2 and 3.

- I have evaluated the security of a diagnostics architecture for the connected car and proposed a general approach to secure diagnostics protocols, both for usage in local repair shops, as well as for remote diagnostics over the Internet. This work addresses research question 2.

- I have proposed a protocol to address the most severe security problem of remote vehicle diagnostics, that of loss of authentication keys. The protocol has also been formally verified. This protocol is necessary to address a secure vehicular diagnostics architecture. This work addresses research question 2.

- I have proposed and evaluated an approach to automatically identify partitions in an in-vehicle network to facilitate the implementation of security controls. This work addresses research question 3.

1.5 Related Work

This section presents related work in the area of the connected car. First, an overview of major surveys is given. Then, a short summary of V2X communication is presented. The work conducted in the main areas of the connected car is then presented, the work related to in-vehicle network architectures and remote diagnostics and software download. Finally, an overview of tools used in this thesis is given.

1.5.1 Overview

The research within the area of the connected car is just in its beginning and the field of securing the connected car roots from about a decade ago [19]. Since then, a lot of effort has been expended, especially during the last years. As the research area is young, only a few extensive surveys exists so far [4, 14, 20].

Brooks et al. [15] show with use-cases what needs to be protected in a vehicle and different scenarios of what operations may be conducted on the vehicle. The possible communication means to the vehicle were also classified. They further use an adapted version of the CERT Taxonomy to analyse attacks against services already implemented in the vehicle or that will come in the near future. Among the services analysed were the need for secure update of firmware in ECUs and attack risks when the vehicle becomes more and more integrated into the systems of the automotive company. One example of such an integration is remote diagnostics.

Othmane et al. [21] introduces a taxonomy of security and privacy aspects of connected vehicles. The taxonomy is divided into six classes: security of communication links, data validity, security of devices, identity and liability, access control, and privacy of drivers and vehicles. Numerous threats are presented to these classes and solutions are briefly surveyed to counter threats of each class. A summary of tools to formally verify security properties in different steps in the design of the connected car is also given.

Jenkins and Mahmud [22] discuss security problems and attacks against the vehicle. They look at inter-vehicle and in-vehicle communications, and also at software and hardware attacks. A further introduction to security for embedded systems is given by Kocher et al. [23].

1.5.2 Vehicle-to-X Communication

The research within Vehicle-to-X (V2X), i.e., Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V), are mainly performed in large collaboration projects or consortia.

Research in a security architecture for vehicular communication (VC) systems have been performed within the SeVeCOM project. In [24], Papadimitratos et al. present necessary security requirements to provide the services of secure beaconing, secure neighbour discovering, and secure geocasting in VC systems. Certificates are used for securing the communication between vehicles and pseudonyms for addressing the introduced privacy problem of using certificates; the certificate gives the vehicle a unique identity, which makes it possible to trace the vehicle and its driver. These privacy problems have further been addressed in the PRESERVE project [25]. In [26], Kargl et al. present implementation

details of the security architecture. Furthermore, the integration of mobile devices and different communication technologies into the VC system are briefly discussed.

The standardisation of inter-vehicular communication (IVC) has diverted into two different standards. In US, the communication is standardised by IEEE in the WAVE communication architecture [10, 27]. In Europe, ETSI was given the mandate to define the communication standard, known as ITS-G5, and the communication architecture [11, 28]. In an attempt to validate the correctness of the ETSI ITS-station (ITS-S) to be mounted on vehicles, Kiening et al. [29] propose to develop a new Protected Profile (PP) and to certify the ITS-S using Common Criteria (CC). Also, Trust Assurance Level (TAL) are introduced to describe the level of security implemented in the vehicle. The levels ranges from 0 to 4, where 0 means "no evaluated security mechanisms in place", and 4 means "all the components involved in the execution of the V2X application are protected against identified threats" [29].

Lately, the research has been focused on how to actually get V2X communication into practice. Field operational tests (FOTs) have been performed to analyse how the IVC behaves in reality and to identify problems that were not thought of [30]. One of the problems of these tests were that they often involve proprietary systems that could give results that was hard to evaluate and use in simulation models. Another major challenge is the integration and utilisation of different communication technologies for short- and long-range communication and the applications' requirements on low and high network bandwidth [30]. They emphasise the importance to use these technologies in the best way, both during the introduction of V2V communication when there are few vehicles with ITS-S, as well as later when the available bandwidth may become limited due to the number of ITS-S at the same place.

1.5.3 In-Vehicle Network Architecture

Most of the work in addressing security of the in-vehicle network has been about identifying and showing on the lack of security and less towards defining security measures. A few extensive investigations regarding the security of the vehicle has recently been conducted [7, 8, 31–33].

Some general research regarding in-vehicle network architectures have been conducted. In the EASIS project [34], a backbone network was considered to be the most suitable network architecture for the near future. Three architectures were considered during their evaluation: (1) a *backbone architecture* where suitable sub-networks are defined (domains) 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 [35], where different fault-tolerant architectures are presented. Fault-tolerance was achieved by duplicating parts of the network and a simulation model was introduced to evaluate the performance of different topologies. Yet, the main goal in [34, 35] has been to present different possible architectures in future vehicles where safety has been the main focus. Methods for how to partition the in-vehicle network into domains were not presented nor was security considered.

A few methods have been proposed where security is considered during the process of allocating tasks to in-vehicle network. A heuristic method to allocate the tasks of a functional block over the ECUs in the in-vehicle network is proposed by Je et al. [36]. The aim is to find allocations where important tasks are not allocated to the same bus as vulnerable tasks, e.g., safety-critical tasks are not allocated to the same sub-networks as tasks that may be more vulnerable (due to less extensive code review during development). An approach, where both security and safety is considered in a CAN-network, is proposed by Lin et al. [37]. By using Mixed Integer Linear Programming (MILP), they explore the possibility of mapping tasks to ECUs, when end-to-end deadlines (safety property) are considered and multiple signals are packed into CAN messages together with Message Authentication Codes (MACs) (security property). In addition to the MILP algorithm, a greedy heuristic algorithm is also proposed. In [38], Lin et al. also address mapping of tasks to time-triggered in-vehicle networks. The approaches mentioned above consider the allocation of tasks to ECUs and do not address architectural questions regarding the partitioning of in-vehicle networks into domains.

Wolf et al. [31] discuss the security within the vehicle. Possible attacks, protection mechanisms, and some security-critical applications are presented. Koscher et al. [7] have highlighted that there is a significant lack of necessary security mechanisms in in-vehicle networks. They conducted experiments on two vehicles and by using techniques such as packet sniffing, packet fuzzing, and reverse-engineering, they found a number of attacks that could be performed against the in-vehicle network. For example, among the attacks performed was the possibility to disable the brake while driving. Even though these attacks require physical access to the vehicle, it is not unrealistic to assume that such attacks also would be possible via a wireless connection to the vehicle. In [8], Checkoway et al. continue the work by analysing the attack surface of a vehicle and demonstrate a set of attacks against the vehicle. Among possible attacks were, for example, compromising the PassThru-device used for connecting the in-vehicle network to a WiFi-network. When the PassThru-device was compromised, malicious software was installed in the device, which attacked the connected vehicle. Another example is the possibility to send malicious messages onto the CAN-bus by playing a specially crafted WMA-file, thereby exploiting a buffer overflow in the decoder of the CD player. Woo et al. [39] demonstrate how malicious CAN-messages can be injected into the in-vehicle network using a smartphone with a self-diagnostics application for vehicles. The connection to the in-vehicle network is established over Bluetooth to an OBD-II scan tool connected to the vehicle. A malicious application was developed that could be controlled from a central server and this application was installed in the connected smartphone, thus, malicious CAN-messages could be injected into the in-vehicle network. In this way, they managed to, among other things, stop the engine by cutting the fuel. As there were more than 300 vehicle applications available in appstores for smartphones as of December 2013 [39], the possibility of an existing application with malicious intention should not be ignored. In addition to these attacks, Rouf et al. [32] have demonstrated security and privacy issues, where they performed an attack against the tire-pressure sensors in a vehicle. These sensors are mandatory in new vehicles so that drivers can be warned in case of a flat tire.

Simulations have been used for analysing the security in the in-vehicle network [40–42]. In [40], Hoppe and Dittmann investigate the possibility of performing sniffing and replay

attacks on the CAN-bus using simulations of an electronic window lift system. Attacks were also performed against the electronic window system using real hardware as well as attacks against the warning lights of the anti-theft system and the air-bag control system [43]. Nilsson and Larson [41] introduce the concept of a vehicle virus. The virus was listening for a message on the CAN-bus that locks the doors remotely, and when that message was captured, the virus executed malicious actions. A security evaluation has also been performed of the FlexRay-protocol [42]. However, security analysis of the MOST-bus has not been presented yet.

A model-based approach to evaluate different security architecture for the in-vehicle network is proposed by Müter and Freiling [44]. In their approach, blueprints of different in-vehicle networks can be described and *compared* with respect to security attributes, such as confidentiality and integrity, to identify the architecture that is the best one. Thus, the approach does not tell how secure a specific architecture is. In-vehicle networks are modelled by ECUs, buses, interfaces, and gateways.

To classify attacks against the vehicle, both the CERT Taxonomy by Howard and Longstaff [45] and the taxonomy by Hamle and Bauer [46] have been used or adapted [15, 41, 43, 47, 48]. A defence-in-depth approach based on [46] for securing the vehicle is discussed by Larson and Nilsson [47]. The five layers they look at are: prevention, detection, deflection, countermeasures, and recovery. In [48], Nilsson and Larson present their approaches for the different layers. With respect to prevention, quite some proposals have now been suggested regarding protection of the communication in the in-vehicle network [19, 39, 49–65]. Among these do Matsumoto et al. [60] present an interestingly simple approach to prevent unauthorised transmission of messages on a CAN-bus. By letting each ECU monitor the network for their own message-IDs (i.e., the message-IDs suppose to be sent by themselves) and if such IDs are seen on the network, thus, another ECU is maliciously injecting unauthorised messages, the ECU issues a CAN Error Frame to discard the message. Furthermore, a few approaches to introduce specification-based [66] and anomaly-based [67–70] IDSes (hence detection) into the vehicle have been suggested. An initial implementation of a security gateway that monitors the frequency and order (but not payload) of communication between in-vehicle networks using automata has been presented by Seifert and Obermaisser [71]. The security gateway considers event-triggered, time-triggered, and streams of communication for both CAN and FlexRay. Lastly, for deflection and countermeasures, an attempt to deflect attacks using honeypots has been described by Verendel et al. [72]. The implementation of an in-vehicle Intrusion Prevention System (IPS) as a countermeasure is simulated, evaluated, and compared with [57, 60, 69] by Otsuka et al. [73]. In [73], their approach is based on the expected frequency of cyclic CAN messages. If a message arrives too frequently to the gateway implementing the IPS, the message is held by the IPS and depending on the frequency of previous messages, either discarded or delayed, i.e., forwarded later.

Lang et al. [74] provide an interesting discussion of the security implications when the vehicle is connected using an IP-based network. Nine ”hypothetical attack scenarios” were suggested based on attacks known from ”ordinary IT systems”, i.e. attacks on the communication protocols, malicious code, and social engineering. Each scenario was analysed with respect to confidentiality, integrity, availability, authenticity, and non-repudiation. Also, an attempt to quantitatively estimate the impact on safety was

made. Thus, for each of the scenarios a safety-integrity level (SIL) value was proposed.

Finally, a hardware security module (HSM) has been developed by the EVITA Project [75]. The HSM comes with three security levels: high, medium, and light. Depending on the requirement of the different vehicle ECUs, one of these HSMs can be integrated into the ECU. The HSM enables hardware-accelerated cryptographic operations, so that in-vehicle network traffic can be protected by use of encryption.

1.5.4 Remote Diagnostics and Software Download

Most of the work within securing remote diagnostics and software download has been directed towards the software download process and very little towards remote diagnostics.

Both unicast and multicast approaches have been proposed for secure remote software download. In [76], Mahmud et al. describe a protocol by means of which software download is performed using an Intelligent Transportation Systems (ITS) infrastructure. The automotive company issues symmetric keys to encrypt the software transmitted between the software supplier and the vehicle. To increase the security in the transmission, they propose that the software should be sent twice and possibly also in random order to avoid attackers from predicting the message order. To authenticate the vehicle, a set of authentication keys are installed in the vehicle and also stored in a central server and transmitted to the appropriate AP within the ITS during authentication. The protocol was analysed in [77].

In the multicast approach proposed by Hossain and Mahmud [78], a special device denoted Network Device Monitor (NDM) is installed in the AP within an ITS infrastructure. The purpose of the NDM is to authenticate vehicles, manage the session keys for the multicast group, and to send software to the vehicles therein. For distribution of software, digital certificates are used for authentication between the automotive company, the software supplier, and the NDMs. Furthermore, a set of authentication keys are installed in the vehicle and also stored in a central server. These keys are used to authenticate the vehicle to the NDMs.

In [79], Nilsson and Larson propose a firmware update process where the firmware is split into smaller fragments and transmitted to the vehicle. Each fragment is hashed and the hash is concatenated to the previous fragment. Thus, all fragments needs to be hashed, in reverse order, before any of them can be transmitted. An initial fragment is then created containing the hash of the first fragment and a digital signature of that hash together with the number of frames in the hash-chain, thereby ensuring that all following hashes cannot be modified without detection. Encryption is also applied to the transmission. This protocol ensures data integrity, data authentication, data confidentiality, and data freshness.

Idrees et al. [80] give a detailed presentation of a remote software download procedure including some remote diagnostics, which utilises the HSM designed within the EVITA project. Mechanisms for exchanging necessary keys between EVITA-enabled devices and for protection of transmitted data are described.

Efforts are also made by ISO to create a standardised diagnostics protocol, DoIP [16], and some initial tests have been performed by Johanson et al. [81]. However, appropriate security mechanisms are still missing in the DoIP-protocol.

Finally, as the firmware has reached the ECU, reprogramming of the ECU needs to be performed securely. Methods for ensuring that the firmware is flashed correctly have also been proposed in [82–84].

To conclude, we find that very little has been done regarding secure remote diagnostics. Instead, a majority of the proposals address software download as a single service. Since there are great benefits of a remote diagnostics service, an architecture for secure remote diagnostics, including software download, should be defined.

1.5.5 Tools and Standards Used

This section introduces some of the tools and standards used in this work.

ETSI Thread Vulnerability Risk Assessment (TVRA)

The European Telecommunications Standards Institute (ETSI) have defined a Threat, Vulnerability, and Risk Analysis (TVRA) method for use by their standards developers to analyse telecommunication systems [85]. The method has been used to evaluate the emerging ITS architecture [86].

The TVRA method is divided into ten steps and can briefly be summarised as follows: The *target of evaluation (ToE)* is identified and the assets within are described together with the goals of the evaluation. *Security objectives* are then identified and classified based on the five security attributes: confidentiality, integrity, availability, authenticity, and accountability (CIAAA). These security objectives are then used to derive the *functional security requirements*. Then, an *inventory of assets* is done. Possible *vulnerabilities* are then identified and classified together with their *corresponding threats* and their unwanted outcome. These threats are classified based on the following four categories: interception, manipulation, denial of service, and repudiation. *Risks* are then calculated depending on the *likelihood* of these threats and their unwanted outcome. Finally, a set of *countermeasures* are derived and a *cost-benefit analysis* is performed to select the most suitable ones to *reduce the risks* of the identified threats. These results are then used to design the *security services*.

ProVerif

ProVerif is an automated protocol verification tool by Bruno Blanchet based on a subset of the π-calculus [87, 88]. The tool is used to formally verify security protocols and can handle security primitives such as symmetric and asymmetric key encryptions, signatures, and hash functions. The attacker is assumed to have access to all communication on the public channel between the communicating entities (Dolev-Yao capabilities), thus, the attacker may read, modify, delete, and inject messages into the communication. The reachability of secret data for an attacker can be evaluated and if secret data is leaked, a trace of the attack is provided as a counterexample. Protocol synchronisation can also be expressed, so that a certain event must have happened before another event, e.g., to verify the non-existence of replay attacks. Formal verification using the ProVerif tool has been used to analyse security properties in different vehicular protocols [89–91].

Community Detection Algorithms

Community detection algorithms is a group of algorithms with the purpose of identifying communities (partitions/clusters) in a graph, where a community is represented by a set of nodes that share many edges between each other and few edges with others outside the community [92]. There are different community detection algorithms that use different approaches to identify communities. Which one that will be successful in identifying communities depends on the graph itself (structure, density, connectivity, number of edges connected to each node, etc.). Moreover, since different algorithms behave differently depending on the data being analysed, there is a need to describe how well the algorithms perform, hence, a measure of the quality of their results (i.e., the identified communities) is needed.

The most widely used quality measures in the community detection domain are Coverage, Modularity, and Conductance [93]. These quality measures describe the following properties:

- **Coverage.** Coverage tells the percentage of edges covered by the partitioning. A coverage of 0 means there are no communities, whereas a coverage of 1 means that there are no inter-connected edges between communities (ideal communities) [92]. Thus, the higher the coverage is, the better. However, coverage is biased to favour coarse-grained clustering.

- **Modularity.** A negative modularity value means that there are no communities. Zero modularity means there is a single community containing all the nodes. A positive and rather large modularity value indicates the presence of communities [94]. Therefore, the higher the modularity is, the better.

- **Conductance.** The conductance tries to capture how well connected the internal nodes of a community are compared to the rest of the graph. A low conductance value means a more well-defined community.

To conclude, an algorithm that performs well, thus gives the best partitioning of a dataset, should result in a high coverage, high modularity, and a low conductance with respect to these quality measures.

1.6 Conclusion

Opening the in-vehicle network for communication to the outside world has many benefits, but also comes with many security challenges. In this thesis, these security challenges have been tackled in three ways: by presenting an approach to analyse the delivery of new services to future connected cars, by proposing a security architecture for vehicle diagnostics, and by proposing and analysing an automated approach to divide in-vehicle networks into domains. The goal of these are to secure the service delivery and the maintenance of the connected car from attacks from both external and internal sources.

For automotive companies, the need for secure and efficient methods for diagnosing vehicles and updating their software are becoming more and more important as more

functions are implemented in software. The benefits of wireless diagnostics and software updates are many, but such communication must be secured and standard protocols for diagnostics communication over IP have not considered this enough. The security architecture for vehicle diagnostics presented in this thesis is general, i.e., it does not depend on a specific diagnostics protocol, supports remote diagnostics, and prevents unauthorised access to vehicles.

With respect to designing in-vehicle networks, little effort has previously been spent in identifying methods for designing in-vehicle networks that facilitates the implementation of security mechanisms. Dividing the in-vehicle network into domains and following a well-known strategy from ordinary network security engineering is one approach. However, finding the optimal allocations of ECUs to domains is infeasible even for as few as 100 nodes. Instead, community detection algorithm can be used to identify such domains in an optimum way. The benefits of this approach is that it is fast (in the order of seconds), gives meaningful partitions, supports different criteria, and has given good results for our in-vehicle network communication where both safety and security has been improved.

References

[1] S. You, M. Krage, and L. Jalics. *Overview of Remote Diagnosis and Maintenance for Automotive Systems*. Tech. rep. 2005-01-1428. Warrendale, PA: SAE International, Apr. 2005.

[2] M. Shavit, A. Gryc, and R. Miucic. *Firmware Update Over The Air (FOTA) for Automotive Industry*. Tech. rep. 2007-01-3523. Warrendale, PA: SAE International, Aug. 2007.

[3] P. Papadimitratos, A. d. La Fortelle, K. Evenssen, R. Brignolo, and S. Cosenza. Vehicular Communication Systems: Enabling Technologies, Applications, and Future Outlook on Intelligent Transportation. *IEEE Communications Magazine* **47**.11 (2009), 84–95. DOI: 10.1109/MCOM.2009.5307471.

[4] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil. Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions. *IEEE Communications Surveys & Tutorials* **13**.4 (2011), 584–616. DOI: 10.1109/SURV.2011.061411.00019.

[5] C. Bergenhem, S. Shladover, E. Coelingh, C. Englund, and S. Tsugawa. "Overview of platooning systems". *Proceedings of the 19th ITS World Congress, Oct 22-26, Vienna, Austria (2012)*. 2012.

[6] *Cars | Bluetooth Technology Website*. URL: http://www.bluetooth.com/Pages/Cars.aspx (visited on 02/17/2015).

[7] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, et al. "Experimental Security Analysis of a Modern Automobile". *2010 IEEE Symposium on Security and Privacy (SP)*. 2010, pp. 447–462. DOI: 10.1109/SP.2010.34.

[8] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno. "Comprehensive Experimental Analyses of Automotive Attack Surfaces". *Proceedings of the 20th USENIX Security Symposium*. San Francisco, CA, USA, Aug. 2011, pp. 77–92.

[9] O. Henniger, L. Apvrille, A. Fuchs, Y. Roudier, A. Ruddle, and B. Weyl. "Security requirements for automotive on-board networks". *2009 9th International Conference on Intelligent Transport Systems Telecommunications,(ITST)*. Oct. 2009, pp. 641–646. DOI: 10.1109/ITST.2009.5399279.

[10] R. Uzcategui and G. Acosta-Marum. Wave: A tutorial. *Communications Magazine, IEEE* **47**.5 (May 2009), 126–133. DOI: 10.1109/MCOM.2009.4939288.

[11] *Intelligent Transport Systems (ITS); Communications Architecture*. European Standard EN 302 665, v1.1.1. 650 Route des Lucioles, F-06921 Sophia Antipolis Cedex, France: ETSI, Sept. 2010.

[12] *ISO 14229-1:2013: Road vehicles — Unified diagnostic services (UDS) — Part 1: Specification and requirements*. ISO, 2013.

[13] *C2C-CC Manifesto*. v1.1. Aug. 2007. URL: http://www.car-to-car.org/ (visited on 06/23/2015).

[14] T. L. Willke, P. Tientrakool, and N. F. Maxemchuk. A Survey of Inter-Vehicle Communication Protocols and Their Applications. *IEEE Communications Surveys & Tutorials* **11**.2 (2009), 3–20. DOI: 10.1109/SURV.2009.090202.

[15] R. Brooks, S. Sander, J. Deng, and J. Taiber. Automobile Security Concerns. *Vehicular Technology Magazine, IEEE* **4**.2 (June 2009), 52–64. DOI: 10.1109/MVT.2009.932539.

[16] *ISO 13400-1:2011: Road vehicles — Diagnostic communication over Internet Protocol (DoIP) — Part 1: General information and use case definition*. ISO, 2011.

[17] *ISO 27145-3:2012: Road vehicles — Implementation of World-Wide Harmonized On-Board Diagnostics (WWH-OBD) communication requirements — Part 3: Common message dictionary*. ISO, 2012.

[18] *ISO 15764:2004: Road vehicles — Extended data link security*. ISO, 2004.

[19] M. Wolf, A. Weimerskirch, and C. Paar. "Security in Automotive Bus Systems". *Workshop on Embedded IT-Security in Cars*. Bochum, Germany, Nov. 2004.

[20] M. L. Sichitiu and M. Kihl. Inter-Vehicle Communication Systems: A Survey. *IEEE Communications Surveys & Tutorials* **10**.2 (2008), 88–105. DOI: 10.1109/COMST.2008.4564481.

[21] L. Othmane, H. Weffers, M. Mohamad, and M. Wolf. "A Survey of Security and Privacy in Connected Vehicles". *Wireless Sensor and Mobile Ad-Hoc Networks*. 2015, pp. 217–247. DOI: 10.1007/978-1-4939-2468-4_10.

[22] M. Jenkins and S. M. Mahmud. "Security Needs for the Future Intelligent Vehicles". *2006 SAE World Congress*. Detroit, Michigan, USA, Apr. 2006.

[23] P. Kocher, R. Lee, G. McGraw, and A. Raghunathan. "Security as a New Dimension in Embedded System Design". *Proceedings of the 41st annual Design Automation Conference*. DAC '04. Moderator-Ravi, Srivaths. San Diego, CA, USA, 2004, pp. 753–760. DOI: http://doi.acm.org/10.1145/996566.996771.

[24] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux. Secure Vehicular Communication Systems: Design and Architecture. *IEEE Communications Magazine* **46**.11 (Nov. 2008), 100–109. DOI: 10.1109/MCOM.2008.4689252.

[25] *PRESERVE — Preparing Secure Vehicle-to-X Communication Systems*. URL: https://www.preserve-project.eu/ (visited on 04/04/2015).

[26] F. Kargl, P. Papadimitratos, L. Buttyan, M. Muter, E. Schoch, B. Wiedersheim, et al. Secure Vehicular Communication Systems: Implementation, Performance, and Research Challenges. *IEEE Communications Magazine* **46**.11 (Nov. 2008), 110–118. DOI: 10.1109/MCOM.2008.4689253.

[27] D. Jiang and L. Delgrossi. "IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments". *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*. May 2008, pp. 2036–2040. DOI: 10.1109/VETECS.2008.458.

[28] E. Strom. On Medium Access and Physical Layer Standards for Cooperative Intelligent Transport Systems in Europe. *Proceedings of the IEEE* **99**.7 (July 2011), 1183–1188. DOI: 10.1109/JPROC.2011.2136310.

[29] A. Kiening, D. Angermeier, H. Seudie, T. Stodart, and M. Wolf. "Trust Assurance Levels of Cybercars in V2x Communication". *Proceedings of the 2013 ACM Workshop on Security, Privacy & Dependability for Cyber Vehicles*. CyCAR '13. New York, NY, USA, 2013, pp. 49–60. DOI: 10.1145/2517968.2517974.

[30] F. Dressler, H. Hartenstein, O. Altintas, and O. Tonguz. Inter-vehicle communication: Quo vadis. *Communications Magazine, IEEE* **52**.6 (June 2014), 170–177. DOI: 10.1109/MCOM.2014.6829960.

[31] M. Wolf, A. Weimerskirch, and T. Wollinger. State of the Art: Embedding Security in Vehicles. *EURASIP Journal on Embedded Systems* **2007** (2007). Article ID 74706, 16 pages. DOI: 10.1155/2007/74706.

[32] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar. "Security and Privacy Vulnerabilities of In-car Wireless Networks: A Tire Pressure Monitoring System Case Study". *Proceedings of the 19th USENIX Conference on Security*. USENIX Security'10. Berkeley, CA, USA, 2010, pp. 21–21.

[33] I. Studnia, V. Nicomette, E. Alata, Y. Deswarte, M. Kaaniche, and Y. Laarouchi. "Survey on security threats and protection mechanisms in embedded automotive networks". *2013 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W)*. 2013, pp. 1–12. DOI: 10.1109/DSNW.2013.6615528.

[34] *EASIS — General Architecture Framework*. Deliverable D0.2.4. Aug. 2004.

[35] S. M. Mahmud and S. Alles. *In-Vehicle Network Architecture for the Next-Generation Vehicles*. SAE Technical Paper 2005-01-1531. SAE International, Apr. 2005.

[36] D.-H. Je, Y.-H. Choi, and S.-W. Seo. "A heuristic task allocation methodology for designing the secure in-vehicle network". *2012 IEEE 1st International Workshop on Vehicular Communications, Sensing, and Computing (VCSC)*. June 2012, pp. 25–30. DOI: 10.1109/VCSC.2012.6281238.

[37] C.-W. Lin, Q. Zhu, C. Phung, and A. Sangiovanni-Vincentelli. "Security-aware mapping for CAN-based real-time distributed automotive systems". *2013 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. Nov. 2013, pp. 115–121. DOI: 10.1109/ICCAD.2013.6691106.

[38] C.-W. Lin, Q. Zhu, and A. Sangiovanni-Vincentelli. Security-Aware Modeling and Efficient Mapping for CAN-Based Real-Time Distributed Automotive Systems. *IEEE Embedded Systems Letters* **Early Access Online** (2014). DOI: 10.1109/LES.2014.2354011.

[39] S. Woo, H. Jo, and D. Lee. A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN. *Intelligent Transportation Systems, IEEE Transactions on* **16**.2 (Apr. 2015), 993–1006. DOI: 10.1109/TITS.2014.2351612.

[40] T. Hoppe and J. Dittmann. "Sniffing/Replay Attacks on CAN Buses: A simulated attack on the electric window lift classified using an adapted CERT taxonomy". *Proceedings of the 2nd Workshop on Embedded Systems Security (WESS)*. Salzburg, Austria, 2007.

[41] D. K. Nilsson and U. E. Larson. "Simulated Attacks on CAN Buses: Vehicle Virus". *Proceedings of the 5th IASTED International Conference on Communication Systems and Networks*. AsiaCSN '08. Anaheim, CA, USA. Palma de Mallorca, Spain, 2008, pp. 66–72.

[42] D. K. Nilsson, U. E. Larson, F. Picasso, and E. Jonsson. "A First Simulation of Attacks in the Automotive Network Communications Protocol FlexRay". *Proceedings of the International Workshop on Computational Intelligence in Security for Information Systems (CISIS'08)*. Vol. 53. Advances in Intelligent and Soft Computing. 10.1007/978-3-540-88181-0_11. 2009, pp. 84–91.

[43] T. Hoppe, S. Kiltz, and J. Dittmann. "Security Threats to Automotive CAN Networks - Practical Examples and Selected Short-Term Countermeasures". *Computer Safety, Reliability, and Security*. LNCS 5219. Sept. 2008, pp. 235–248.

[44] M. Müter and F. Freiling. "Model-Based Security Evaluation of Vehicular Networking Architectures". *2010 Ninth International Conference on Networks (ICN)*. 2010, pp. 185–193. DOI: 10.1109/ICN.2010.38.

[45] J. D. Howard and T. A. Longstaff. A Common Language for Computer Security Incidents. Sandia Report: SAND98-8667 (1998).

[46] L. R. Hamle and R. K. Bauer. "AINT Misbehaving — A Taxonomy of anti-intrusion techniques". *Proceedings of the 18th National Information Systems Security Conference*. Oct. 1995, pp. 163–172.

[47] U. E. Larson and D. K. Nilsson. "Securing Vehicles against Cyber Attacks". *CSIIRW '08: Proceedings of the 4th annual workshop on Cyber security and information intelligence research*. CSIIRW '08. Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead. New York, NY, USA, 2008, 30:1–30:3. DOI: 10.1145/1413140.1413174.

[48] D. K. Nilsson and U. E. Larson. A Defense-in-Depth Approach to Securing the Wireless Vehicle Infrastructure. *Journal of Networks* **4**.7 (Sept. 2009), 552–564. DOI: 10.4304/jnw.4.7.552-564.

[49] M. L. Chávez, C. H. Rosete, and F. R. Henríguez. "Achieving Confidentiality Security Service for CAN". *Proceedings of the 15th International Conference on Electronics, Communications and Computers, 2005. CONIELECOMP 2005.* Feb. 2005, pp. 166–170. DOI: 10.1109/CONIEL.2005.13.

[50] H. Oguma, A. Yoshioka, M. Nishikawa, R. Shigetomi, A. Otsuka, and H. Imai. "New Attestation-Based Security Architecture for In-Vehicle Communication". *IEEE Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008*. New Orleans, Louisiana, 2008, pp. 1–6. DOI: 10.1109/GLOCOM.2008.ECP.369.

[51] A. Groll and C. Ruland. "Secure and Authentic Communication on Existing In-Vehicle Networks". *2009 IEEE Intelligent Vehicles Symposium*. 2009, pp. 1093–1097. DOI: 10.1109/IVS.2009.5164434.

[52] D. K. Nilsson, U. E. Larson, and E. Jonsson. "Efficient In-Vehicle Delayed Data Authentication Based on Compound Message Authentication Codes". *Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th.* 2008, pp. 1–5. DOI: 10.1109/VETECF.2008.259.

[53] C. Szilagyi and P. Koopman. "A Flexible Approach to Embedded Network Multicast Authentication". *2nd Workshop on Embedded Systems Security (WESS)*. 2008.

[54] C. Szilagyi and P. Koopman. "Flexible multicast authentication for time-triggered embedded control network applications". *IEEE/IFIP International Conference on Dependable Systems Networks, 2009. DSN '09.* 2009, pp. 165–174. DOI: 10.1109/DSN.2009.5270342.

[55] C. Szilagyi and P. Koopman. "Low Cost Multicast Authentication via Validity Voting in Time-triggered Embedded Control Networks". *Proceedings of the 5th Workshop on Embedded Systems Security*. WESS '10. Scottsdale, Arizona, 2010, 10:1–10:10. DOI: 10.1145/1873548.1873558.

[56] 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". *2011 IEEE Vehicular Technology Conference (VTC Fall)*. 2011, pp. 1–5. DOI: 10.1109/VETECF.2011.6093081.

[57] A. Van Herrewege, D. Singelee, and I. Verbauwhede. "CANAuth — A Simple, Backward Compatible Broadcast Authentication Protocol for CAN bus". *9th Embedded Security in Cars Conference (escar)*. Dresden, Germany, 2011.

[58] B. Groza and S. Murvay. "Secure Broadcast with One-Time Signatures in Controller Area Networks". *Availability, Reliability and Security (ARES), 2011 Sixth International Conference on*. Aug. 2011, pp. 371–376. DOI: 10.1109/ARES.2011.62.

[59] C.-W. Lin and A. Sangiovanni-Vincentelli. "Cyber-Security for the Controller Area Network (CAN) Communication Protocol". *2012 International Conference on Cyber Security (CyberSecurity)*. 2012, pp. 1–7. DOI: 10.1109/CyberSecurity.2012.7.

[60] T. Matsumoto, M. Hata, M. Tanabe, K. Yoshioka, and K. Oishi. "A Method of Preventing Unauthorized Data Transmission in Controller Area Network". *Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th.* 2012, pp. 1–5. DOI: 10.1109/VETECS.2012.6240294.

[61] A. Hazem and H. A. Fahmy. "LCAP — A Lightweight CAN Authentication Protocol for Securing In-Vehicle Networks". *10th Embedded Security in Cars Conference (escar)*. Berlin, Germany, 2012.

[62] B. Groza, S. Murvay, A. van Herrewege, and I. Verbauwhede. "LiBrA-CAN: A Lightweight Broadcast Authentication Protocol for Controller Area Networks". *Cryptology and Network Security*. Vol. 7712. LNCS. 2012, pp. 185–200. DOI: 10.1007/978-3-642-35404-5_15.

[63] B. Groza and S. Murvay. Efficient Protocols for Secure Broadcast in Controller Area Networks. *Industrial Informatics, IEEE Transactions on* **9**.4 (Nov. 2013), 2034–2042. DOI: 10.1109/TII.2013.2239301.

[64] Q. Wang and S. Sawhney. "VeCure: A practical security framework to protect the CAN bus of vehicles". *Internet of Things (IOT), 2014 International Conference on the*. Oct. 2014, pp. 13–18. DOI: 10.1109/IOT.2014.7030108.

[65] P. Mundhenk, S. Steinhorst, M. Lukasiewycz, S. A. Fahmy, and S. Chakraborty. "Lightweight Authentication for Secure Automotive Networks". *Proceedings of the Conference on Design, Automation and Test in Europe (DATE 2015)*. France, 2015, pp. 285–288. DOI: 10.7873/DATE.2015.0174.

[66] U. E. Larson, D. K. Nilsson, and E. Jonsson. "An Approach to Specification-based Attack Detection for In-Vehicle Networks". *Proceedings of the IEEE Intelligent Vehicles Symposium*. June 2008, pp. 220–225.

[67] T. Hoppe, S. Kiltz, and J. Dittmann. "Adaptive Dynamic Reaction to Automotive IT Security Incidents Using Multimedia Car Environment". *Proceedings of the 4th International Conference on Information Assurance and Security (ISIAS '08)*. Sept. 2008, pp. 295–298. DOI: 10.1109/IAS.2008.45.

[68] T. Hoppe, S. Kiltz, and J. Dittmann. Applying Intrusion Detection to Automotive IT — Early Insights and Remaining Challenges. *Journal of Information Assurance and Security* **4**.3 (2009), 226–235.

[69] M. Müter, A. Groll, and F. C. Freiling. "A Structured Approach to Anomaly Detection for In-Vehicle Networks". *2010 Sixth International Conference on Information Assurance and Security (IAS)*. Atlanta, GA, Aug. 2010, pp. 92–98. DOI: 10.1109/ISIAS.2010.5604050.

[70] M. Müter and N. Asaj. "Entropy-Based Anomaly Detection for In-Vehicle Networks". *2011 IEEE Intelligent Vehicles Symposium (IV)*. Baden-Baden, Germany, June 2011, pp. 1110–1115. DOI: 10.1109/IVS.2011.5940552.

[71] S. Seifert and R. Obermaisser. "Secure automotive gateway — Secure communication for future cars". *Industrial Informatics (INDIN), 2014 12th IEEE International Conference on*. July 2014, pp. 213–220. DOI: 10.1109/INDIN.2014.6945510.

[72] V. Verendel, D. K. Nilsson, U. E. Larson, and E. Jonsson. "An Approach to using Honeypots in In-Vehicle Networks". *Proceedings of the 68th IEEE Vehicular Technology Conference (VTC)*. Sept. 2008, pp. 1–5.

[73] S. Otsuka, T. Ishigooka, Y. Oishi, and K. Sasazawa. "CAN Security: Cost-Effective Intrusion Detection for Real-Time Control Systems". *SAE Technical Paper*. 2014-01-0340. Apr. 2014. DOI: 10.4271/2014-01-0340.

[74] A. Lang, J. Dittmann, S. Kiltz, and T. Hoppe. "Future Perspectives: The Car and Its IP-Address — A Potential Safety and Security Risk Assessment". *Proceedings of the 26th International Conference on Computer Safety, Reliability, and Security (SAFECOMP '07)*. SAFECOMP '07. Nuremberg, Germany, Sept. 2007, pp. 40–53.

[75] M. Wolf and T. Gendrullis. "Design, Implementation, and Evaluation of a Vehicular Hardware Security Module". *Information Security and Cryptology - ICISC 2011*. LNCS 7259. Jan. 2012, pp. 302–318.

[76] S. M. Mahmud, S. Shanker, and I. Hossain. "Secure Software Upload in an Intelligent Vehicle via Wireless Communication Links". *IEEE Intelligent Vehicles Symposium, 2005. Proceedings*. 2005, pp. 588–593. DOI: 10.1109/IVS.2005.1505167.

[77] I. Hossain and S. M. Mahmud. "Analysis of a Secure Software Upload Technique in Advanced Vehicles using Wireless Links". *Proceedings of the IEEE Intelligent Transportation Systems Conference (ITSC 2007)*. 2007, pp. 1010–1015. DOI: 10.1109/ITSC.2007.4357797.

[78] I. Hossain and S. M. Mahmud. "Secure Multicast Protocol for Remote Software Upload in Intelligent Vehicles". *Proc. of the 5th Ann. Intel. Vehicle Systems Symp. of National Defense Industries Association (NDIA)*. Traverse City, Michigan, June 2005, pp. 145–155.

[79] D. K. Nilsson and U. E. Larson. "Secure Firmware Updates over the Air in Intelligent Vehicles". *IEEE International Conference on Communications Workshops, 2008. ICC Workshops '08*. May 2008, pp. 380–384. DOI: 10.1109/ICCW.2008.78.

[80] M. S. Idrees, H. Schweppe, Y. Roudier, M. Wolf, D. Scheuermann, and O. Henniger. "Secure Automotive On-Board Protocols: A Case of Over-the-Air Firmware Updates". *Communication Technologies for Vehicles*. LNCS 6596. Mar. 2011, pp. 224–238.

[81] M. Johanson, P. Dahle, and A. Söderberg. "Remote Vehicle Diagnostics over the Internet using the DoIP Protocol". *Proceedings of the Sixth International Conference on Systems and Networks Communications (ICSNC 2011)*. Barcelona, Spain, Oct. 2011, pp. 226–231.

[82] D. Nilsson, L. Sun, and T. Nakajima. "A Framework for Self-Verification of Firmware Updates over the Air in Vehicle ECUs". *2008 IEEE GLOBECOM Workshops*. Nov. 2008, pp. 1–5. DOI: 10.1109/GLOCOMW.2008.ECP.56.

[83] A. Weimerskirch. "Secure Software Flashing". *SAE Int. J. Passeng. Cars - Electron. Electr. Syst.* Vol. 2. 2009, pp. 83–86.

[84] A. Adelsbach, U. Huber, and A.-R. Sadeghi. "Secure Software Delivery and Installation in Embedded Systems". *Embedded Security in Cars*. 10.1007/3-540-28428-1_3. 2006, pp. 27–49.

[85] *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis*. Technical Specification TS 102 165-1, v4.2.3. 650 Route des Lucioles, F-06921 Sophia Antipolis Cedex, France: ETSI, Mar. 2011.

[86] *Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)*. Technical Report TR 102 893, v1.1.1. 650 Route des Lucioles, F-06921 Sophia Antipolis Cedex, France: ETSI, Mar. 2010.

[87] B. Blanchet. Automatic verification of correspondences for security protocols. *Journal of Computer Security* **17**.4 (Jan. 2009), 363–434. DOI: 10.3233/JCS-2009-0339.

[88] B. Blanchet, B. Smyth, and V. Cheval. *ProVerif 1.87: Automatic Cryptographic Protocol Verifier, User Manual and Tutorial*. 2013.

[89] D. K. Nilsson, U. E. Larson, and E. Jonsson. "Low-Cost Key Management in Hierarchical Wireless Vehicle Networks". *Proc. IEEE Intelligent Vehicles Symposium*. June 2008. DOI: 10.1109/IVS.2008.4621299.

[90] G. Lee, H. Oguma, A. Yoshioka, R. Shigetomi, A. Otsuka, and H. Imai. "Formally Verifiable Features in Embedded Vehicular Security Systems". *2009 IEEE Vehicular Networking Conference (VNC)*. Oct. 2009, pp. 1–7. DOI: 10.1109/VNC.2009.5416378.

[91] G. Pedroza, M. Idrees, L. Apvrille, and Y. Roudier. "A Formal Methodology Applied to Secure Over-the-Air Automotive Applications". *2011 IEEE Vehicular Technology Conference (VTC Fall)*. 2011, pp. 1–5. DOI: 10.1109/VETECF.2011.6093061.

[92] S. Fortunato. Community detection in graphs. *Physics Reports* **486**.3–5 (Feb. 2010), 75–174. DOI: 10.1016/j.physrep.2009.11.002.

[93] F. Moradi, T. Olovsson, and P. Tsigas. "An Evaluation of Community Detection Algorithms on Large-Scale Email Traffic". *Experimental Algorithms*. LNCS 7276. 2012, pp. 283–294.

[94] M. E. J. Newman. Modularity and community structure in networks. *Proceedings of the National Academy of Sciences* **103**.23 (June 2006). PMID: 16723398, 8577–8582. DOI: 10.1073/pnas.0601602103.