THESIS FOR THE DEGREE OF LICENTIATE OF ENGINEERING

A Structured Approach to Securing the Connected Car

PIERRE KLEBERGER

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

Göteborg, Sweden 2012

A Structured Approach to Securing the Connected Car
PIERRE KLEBERGER

Technical report no 99L
ISSN 1652-876X
Division of Networks and Systems
Department of Computer Science and Engineering
Chalmers University of Technology
SE-412 96 Göteborg
Sweden
Telephone: +46 (0)31-772 1000

Chalmers Reproservice
Göteborg, Sweden 2012

A Structured Approach to Securing the Connected Car

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

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

Abstract

Vehicles of today have become increasingly dependent on software to handle their functionalities. Updating and maintaining the software in vehicles has therefore become a costly process for the automotive industry. By introducing wireless communications to vehicles, vehicular maintenance can greatly be improved and many other new applications can also 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. Thus, this thesis presents a general approach to securing the connected car and the usefulness of the approach is demonstrated in a vehicular diagnostics scenario.

The thesis comes in two main parts. In the first part, we address security mechanisms for the connected car. First, a survey of current mechanisms to secure the in-vehicle networks is made. Then, a description of possible communication methods with vehicles is given and a taxonomy of current entities involved in such communication is presented. The taxonomy is organised in actors, vehicle-to-X communications, network paths, and dependability and security attributes. The usefulness of the taxonomy is demonstrated by two examples.

In the second part, we address security with respect to vehicular diagnostics. First, an overall security analysis of the interaction between the connected car and the repair shop is conducted. We find that the most imminent risk in the repair shop is the loss of authentication keys. The loss of such keys allows masquerading attacks against vehicles. To address this problem, we propose a Kerberos-inspired protocol for authentication and authorisation of the diagnostics equipment and a trusted third party is introduced.

To conclude, this thesis shows the value of adopting a structured approach to securing the connected car. The approach has been shown to be useful for identifying threats and countermeasures and thus help improving security.

Keywords: connected car; vehicular services; security mechanisms; remote diagnostics.

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 Asrin Javaheri, Farnaz Moradi, Laleh Pirzadeh, Magnus Almgren, and Vilhelm Verendel. I am also grateful to my friends, new and former colleagues I got to know during the way, especially Jochen Hollmann, Magnus Själander, Viacheslav Izosimov, and Wolfgang John.

Last, but not least, I would like to thank my family for all their support, and especially the support and encouragement I receive from my wonderful girlfriend Madelen.

Pierre Kleberger
Gothenburg, December 2012

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". *Proceedings of the 2011 IEEE Intelligent Vehicles Symposium (IV)*. Baden-Baden, Germany: IEEE, June 2011, pp. 528–533. DOI: IVS.2011.5940525

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

Part II: Securing Vehicular Diagnostics for Connected Cars

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

Paper D P. Kleberger and T. Olovsson. "Protecting Vehicles Against Unauthorised Remote Diagnostics". (Submitted)

Contents

Acronyms

ACL	Access Control List
AP	Access Point
ARP	Address Resolution Protocol
BS	Backend Server
C2C-CC	Car 2 Car Communication Consortium
CA	Certificate Authority
CAN	Controller Area Network
CBC-MAC	Cipher-Block Chaining Message Authentication Code
CCU	Communications Control Unit
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
ECM	Engine Control Module
ECU	Electronic Control Unit
ETSI	European Telecommunications Standards Institute
FOTA	Firmware Update Over The Air
GPS	Global Positioning System
HCI	Human Computer Interface
HMI	Human-Machine Interface
HSM	Hardware Security Module
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
ISO	International Standard Organisation
ISP	Internet Service Provider
ITS	Intelligent Transportation Systems
IVC	Inter-Vehicle Communication
KDC	Key Distribution Centre
KPS	Key Predistribution System
LAN	Local Area Network
LIN	Local Interconnect Network
MAC	Message Authentication Code
MITM	Man-in-the-Middle
MOST	Media Oriented Systems Transport

NDM	Network Device Monitor
NOC	Network Operation Centre
OBD-II	On-Board Diagnostics II
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
RDS	Radio Data System
RSU	Road-Side Unit
SIL	Safety Integrity Level
ToE	Target of Evaluation
TTP	Trusted Third Party
TVRA	Threat, Vulnerability, and Risk Analysis
V	Vehicle
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-X
VANET	Vehicle Ad-Hoc Network
VC	Vehicular Vommunication
VLAN	Virtual LAN
WLAN	Wireless LAN

Introductory Summary

1

Introduction

More and more functionality in today's vehicles are implemented in software. A modern car has somewhere between 50–100 embedded computers, i.e., electronic control units (ECUs). The 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 current way to update software is to bring the vehicle to the repair shop and physically connect a 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 (see [1, 2]).

Until recently, vehicles have been closed systems, but this is changing. As a consequence, the closed in-vehicle networks are now becoming exposed to external traffic, traffic that is potentially dangerous with respect to the vehicle's safety requirements. Since vehicles were not exposed to these threats before, they do not have any security features. The lack of security has already been shown by researches [3, 4]. Therefore, to be able to fruitfully benefit from wireless vehicular communications, the vehicle has to be secured. In this thesis, we adopt a structured approach to this task, i.e., to secure the connected car.

This introductory summary is organised as follows. After this section, the objective of the thesis is given in Section 1.1. Then, the connected car concept is presented in Section 1.2. The appended papers are summarised in Section 1.3 followed by the contributions of the thesis in Section 1.4. Related work is presented in Section 1.5. Finally, a conclusion is given in Section 1.6.

1.1 Thesis Objective

The research presented in this thesis aims to provide approaches to securing the connected car, and in particular the connected car's interaction with the repair shop. This goal is reached in several steps: First, a survey of existing research and security mechanisms is made. Second, an infrastructure for the connected car and its environment is presented and a taxonomy of relevant entities in the infrastructure is suggested. Third, a security analysis of the interaction between the connected car and the repair shop is made, thus providing an example of the use of the taxonomy. The security analysis points out a number of critical security problems. Finally, security solutions to the detected problems are suggested.

The following research questions are addressed:

1. Could 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. Which security problems could be derived by means of a structured security analysis of diagnostic services and repair shop interaction? Which corresponding countermeasures could be found?

3. How could the problem of lost authentication keys in connection with repair shop interaction be solved?

The thesis is divided into two main parts. Part I is a survey and taxonomy of the connected car infrastructure. It forms a scientific basis and provides a tool for the applied security analysis work to follow. Part II presents a security analysis of the connected repair shop using the tool proposed in Part I. Further, it suggests countermeasures for the detected security problems.

1.2 The Connected Car

1.2.1 Overview

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. The requirement of external wireless communication distinguishes the connected car from other vehicles where internal connections already exists, e.g., the On-Board Diagnostics II (OBD-II) interface used for wired vehicle diagnostics or the USB ports that are becoming more and more common. The external link is 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 eTolling and media streaming.

A simplified model of the connected car consists of three domains [5]:

(1) the *vehicle*, consisting of the in-vehicle network and ECUs,

(2) the *portal* at the automotive company, delivering services to the vehicle, and

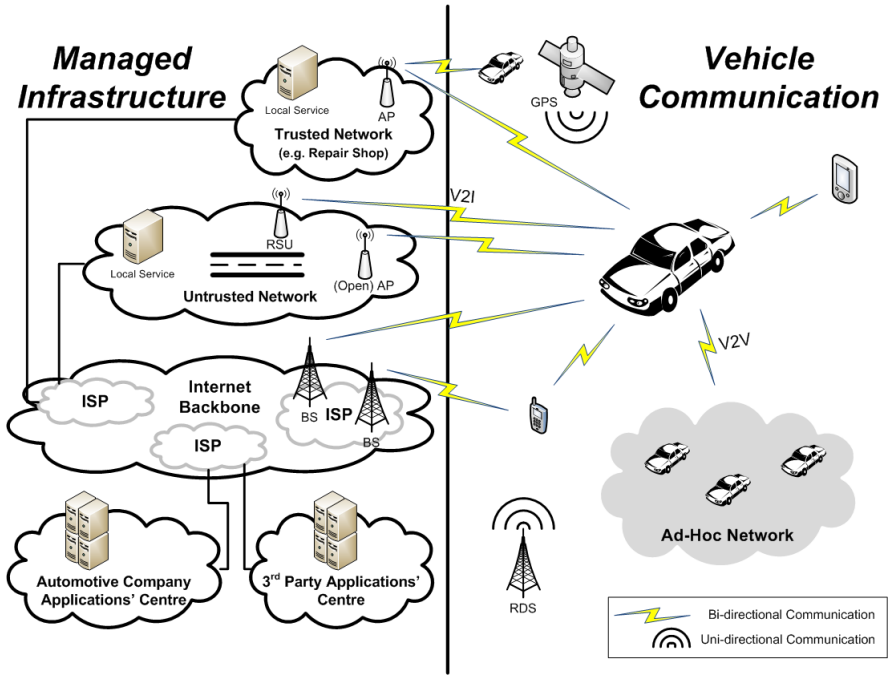

Figure 1.1: *Model of the connected car infrastructure*

(3) the *communication link* between the vehicle and the portal.

The model shows the concept of the connected car by the vehicle utilising an external communication link to the portal, which can supply the vehicle with services from the automotive company.

Another model that clarifies the details of the connected car and its infrastructure is shown in Figure 1.1. This model consists of two domains, the managed infrastructure and the vehicle communication. Details of the vehicle, the managed infrastructure, and the vehicle communication are described in the following paragraphs.

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 information from sensors 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*. The choice of bus technology used in different sub-networks depends on the communication requirements of

the tasks that are run in the connected ECUs. The sub-networks are connected to each other through special *gateway ECUs*.

An OBD-II interface enables a 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.

Managed Infrastructure

The managed infrastructure is divided into five parts. These parts are: 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, which provides services to the automotive companies' vehicles. It holds necessary information about the vehicle, such as information from previous services (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 may be considered to be a trusted network by the automotive company and the vehicle. In delivering a service to this network, it may well be that some requirements in an implementation can be relaxed. Furthermore, other local services can be available in these networks for running the local infrastructure and providing service to the vehicle. Networks not considered to be trusted are regarded as untrusted. 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 for 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 very unlikely.

Vehicle Communication

To enable vehicle communication, a wireless gateway, also known as the Communication Unit (CU) [6], is introduced in the in-vehicle network. The gateway enables Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) 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 unit (RSU) by means of which vehicles will establish communication to the infrastructure using the WAVE-protocol [7]. These RSUs provide services to the vehicles, including general Internet access. 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 and HSDPA.

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.

1.2.2 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, for example, verification of in-vehicle messages. Another example is firmware that is larger than the available internal memory in the ECU 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 therefore be very cost efficient. Even very 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 developed 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.

1.2.3 Vehicular Services

Many services can be expected to be introduced to the connected car. These services can be divided into administrative services 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 is incorporated within the diagnostics protocol as, e.g., in the `programmingSession` in ISO 14229 [8].

There are many expected benefits of introducing wireless remote diagnostics [2]. In the case of a repair shop, no cables are needed, something that 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 she is working with the right vehicle, and what support is implemented in the network to protect the vehicle against malicious network behaviour?

In an effort to create a common diagnostics protocol for vehicles connected over IP-based networks, ISO has introduced the protocol Diagnostics over IP (DoIP) [9]. This protocol enables the transmission of other diagnostics protocols as application data, such as ISO 14229 [8]. Unfortunately, there are no security mechanisms in this protocol.

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 [10, 11]. For example, platooning (trains of vehicles), 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.

1.3 A Structured Approach to Securing the Connected Car

This section gives a summary of the appended papers.

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

Paper A: Security Aspects of the In-Vehicle Network in the Connected Car

In Paper A, a survey of the research within securing the in-vehicle network of the connected car was performed. 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 bus technologies used within the in-vehicle network (CAN, FlexRay, MOST, and LIN), almost all of the research has 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 a wireless connection is introduced, these services need to be adapted to the new hostile environment provided by the wireless connection. However, to secure services for the connected car, a model of the infrastructure to analyse possible communication means and security threats is needed. In Paper B, 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 helps us to map possible communication means between the vehicle and various services in the infrastructure. The assessment tree assesses different security aspects of the service delivery.

1.3.2 Part II: Securing Vehicular Diagnostics for Connected Cars

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 are vehicles protected towards 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. Threats, vulnerabilities, and general countermeasures were derived for this environment. We found that, for this environment, implementing security at link layer is beneficial, even though it is not supported in common protocols of today. 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 Remote Diagnostics

As discovered in Paper C, the loss of authentication keys to diagnostics equipment can have major security implications on vehicles. If an attacker manages to get hold of a pair of authentication keys, the attacker may get access to all vehicles that accept these keys, even outside of the repair shop. In this paper, we address this security problem and propose an authorisation protocol. In this, a trusted third party (TTP) is used to issue authorisation tickets, so that access control can be enforced in the vehicle. The TTP holds the security policies for vehicles describing the time of access and type of diagnostics messages allowed to be processed by the vehicle. The authorisation protocol is independent of the diagnostics protocol used.

1.4 Thesis Contributions

The main contributions of this thesis are:

- We have surveyed current research on in-vehicle network and identified open issues to secure the in-vehicle network. Thus, research question 1 is addressed.
- We 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 taxonomy addresses research question 1 and is a prerequisite for research question 2.
- We have made a security analysis of the interaction between the connected car and the repair shop. Thus, we have shown that our structured approach to assess the security is valuable. The approach helped us identify threats and countermeasures, as well as critical security issues that might not have been found otherwise. The security analysis addresses research question 2.
- We have proposed a protocol to address the most severe security problem of remote vehicular diagnostics, that of loss of authentication keys. Thus, research question 3 is addressed.

1.5 Related Work

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 [12]. Since then, lots of effort has been spent, especially during the last years. As the research area is young, only a few extensive surveys exists so far [13–15].

Brooks et al. [16] 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 towards 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 a system is remote diagnostics.

Jenkins and Mahmud [17] discuss security problems and attacks towards 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. [18].

1.5.1 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 [19]. In [20], 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. In [21], 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.

1.5.2 In-Vehicle Network

Most of the work in addressing security of the in-vehicle network has been towards 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 [3, 4, 22, 23].

Wolf et al. [22] discuss the security within the vehicle. Possible attacks, protection mechanisms, and some security-critical applications are presented. Koscher et al. [3] have recently highlighted that there is a significant lack of necessary security mechanisms in in-vehicle networks. They conducted experiments on two vehicles. Using techniques such as packet sniffing, packet fuzzing, and reverse-engineering, they found a number of attacks that could be performed towards the in-vehicle network. For example, among the attacks performed were 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 [4], Checkoway et al. continues the work by analysing the attack surface of a vehicle and demonstrated a set of attacks towards the vehicle. Among possible attacks were, for example, compromising the PassThru-device used for connecting the in-vehicle network to the 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 CD, thereby launching a buffer overflow in the decoder of the CD player. In addition to these attacks are the security and privacy issues demonstrated by Rouf et al. [23], where they performed an attack against the tire-pressure sensors in the vehicle. These sensors are mandatory in new vehicles so that drivers can be warned in case of flat tires.

Simulations have extensively been used for analysing the security in the in-vehicle network [24–26]. In [24], 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 [27]. Nilsson and Larson [25] 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 on the FlexRay-protocol [26]. However, analysis of the MOST-bus has not, to our knowledge, been conducted yet.

To classify attacks against the vehicle, both the CERT Taxonomy by Howard and Longstaff [28] and the taxonomy by Hamle and Bauer [29] have been used or adapted [16, 25, 27, 30, 31]. A defence-in-depth approach based on [29] for securing the vehicle is discussed by Larson and Nilsson [30]. The five layers they look at are: prevention, detection, deflection, countermeasures, and recovery. In [31], Nilsson and Larson present their approaches for the different layers. In general, not so many proposals have been suggested regarding protection (hence prevention) of the communication in the in-vehicle network [12, 32–38]. Furthermore, a few approaches to introducing Intrusion Detection System (IDS) into the vehicle have been suggested. Both specification-based [39] and anomaly-based approaches [40–43] have been investigated. An attempt to deflect attacks using honeypots has been described in [44].

Lang et al. [45] 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 [46]. The HSM comes with three security levels: high, medium, and low. Depending on the requirement of the different vehicle ECUs, one of these HSMs should be integrated into each ECU. The HSM enables hardware-accelerated cryptographic operations, so that in-vehicle network traffic can be protected by use of encryption.

1.5.3 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 [47], 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 [48].

In the multicast approach proposed by Hossain and Mahmud [49], 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. A set of authentication keys are installed in the vehicle and also stored in a central server. These keys are transmitted and used by the NDM to authenticate the vehicle. Furthermore, digital certificates were used as authentication keys for authentication between the automotive company, the

software supplier, and the NDM.

In [50], 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 before any of them can be transmitted. The hash of the first fragment is used as an initial fragment containing a digital signature over the first hash, 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. [51] give a detailed presentation of a remote software download procedure including some remote diagnostics, which utilises the HSM designed within the EVITA project.

Efforts are also made by ISO to create a standardized diagnostics protocol, DoIP [9], and some initial tests have been performed by Johanson et al. [52]. 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 [53–55].

To conclude, we find that very little has been done regarding secure remote diagnostics. Instead, a majority of the proposals addresses 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.

1.6 Conclusion

In this thesis, we have presented work to adopt a structured approach to securing the connected car. We have described a model of the connected car infrastructure and presented a taxonomy of its entities to facilitate the derivation of security mechanisms. We have also conducted a security analysis of the interaction between the connected car and the repair shop that exhibits the usefulness of our proposed model of the connected car infrastructure.

Many new services are expected to be introduced in the vehicle and since the vehicle is safety-critical, it is vital that the vehicle is secured, so that these new services cannot violate with the safety and security mechanisms of the vehicle. One such new service that was analysed is remote diagnostics. Here some problems were detected and remedies were proposed. However, the model of the connected car infrastructure is general and the model as well as the taxonomy are believed to be applicable in many similar situations.

References

[1] S. You, M. Krage, and L. Jalics. “Overview of Remote Diagnosis and Maintenance for Automotive Systems”. *2005 SAE World Congress*. Detroit, MI, USA, Apr. 2005. DOI: 10.4271/2005-01-1428.

[2] M. Shavit, A. Gryc, and R. Miucic. “Firmware Update Over The Air (FOTA) for Automotive Industry”. *14th Asia Pacific Automotive Engineering Conference*. Hollywood, California, USA, Aug. 2007. DOI: 10.4271/2007-01-3523.

[3] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, et al. "Experimental Security Analysis of a Modern Automobile". *Proceedings of the 31st IEEE Symposium on Security and Privacy (SP)*. 2010, pp. 447–462. DOI: 10.1109/SP.2010.34.

[4] 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.

[5] D. K. Nilsson, U. E. Larson, and E. Jonsson. "Creating a Secure Infrastructure for Wireless Diagnostics and Software Updates in Vehicles". *Proceedings of the 27th International Conference on Computer Safety, Reliability, and Security (SAFECOMP '08)*. Newcastle upon Tyne, UK, 2008, pp. 207–220. ISBN: 978-3-540-87697-7. DOI: 10.1007/978-3-540-87698-4_19.

[6] E. Kelling, M. Friedewald, T. Leimbach, M. Menzel, P. Säger, H. Seudié, and B. Weyl. *Specification and evaluation of e-security relevant use cases*. EVITA Project, Deliverable D2.1, v1.2. Dec. 2009.

[7] R. Uzcategui and G. Acosta-Marum. Wave: A tutorial. *Communications Magazine, IEEE* **47**.5 (May 2009), 126–133. ISSN: 0163-6804. DOI: 10.1109/MCOM.2009.4939288.

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

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

[10] *The CALM Handbook*. v3 (060326). The CALM Forum Ltd. 1 Beverly Hall, Halifax, West Yorkshire, HX2 6HS, UK, Mar. 2006. URL: http://www.isotc204wg16.org/pubdocs/The\CALM\Handbookv6-070301.pdf (visited on 08/06/2011).

[11] *C2C-CC Manifesto*. v1.1. CAR 2 CAR Communication Consortium. Aug. 2007. URL: http://www.car-to-car.org/ (visited on 08/06/2011).

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

[13] 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.

[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] 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.

[16] R. Brooks, S. Sander, J. Deng, and J. Taiber. Automobile Security Concerns. *Vehicular Technology Magazine, IEEE* **4**.2 (June 2009), 52–64. ISSN: 1556-6072. DOI: 10.1109/MVT.2009.932539.

[17] M. Jenkins and S. M. Mahmud. "Security Needs for the Future Intelligent Vehicles". *2006 SAE World Congress*. Detroit, Michigan, USA, Apr. 2006. DOI: 10.4271/2006-01-1426.

[18] 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. ISBN: 1-58113-828-8. DOI: http://doi.acm.org/10.1145/996566.996771. URL: http://doi.acm.org/10.1145/996566.996771.

[19] *Secure Vehicle Communication (SeVeCOM)*. URL: http://www.sevecom.org/ (visited on 07/25/2012).

[20] 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.

[21] 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.

[22] 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. URL: http://downloads.hindawi.com/journals/es/2007/074706.pdf.

[23] 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.

Washington, DC, 2010, pp. 21–21. ISBN: 888-7-6666-5555-4. URL: http://dl.acm.org/citation.cfm?id=1929820.1929848.

[24] 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.

[25] 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. ISBN: 978-0-88986-758-1. URL: http://portal.acm.org/citation.cfm?id=1713277.1713292.

[26] 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. URL: http://dx.doi.org/10.1007/978-3-540-88181-0_11.

[27] T. Hoppe, S. Kiltz, and J. Dittmann. "Security Threats to Automotive CAN Networks – Practical Examples and Selected Short-Term Countermeasures". *Proceedings of the 27th International Conference on Computer Safety, Reliability, and Security (SAFECOMP '08)*. SAFECOMP '08. Springer-Verlag, Berlin, Heidelberg. Newcastle upon Tyne, UK, Sept. 2008, pp. 235–248. ISBN: 978-3-540-87697-7. DOI: http://dx.doi.org/10.1007/978-3-540-87698-4_21. URL: http://dx.doi.org/10.1007/978-3-540-87698-4_21.

[28] J. D. Howard and T. A. Longstaff. A Common Language for Computer Security Incidents. Sandia Report: SAND98-8667 (1998). URL: http://www.cert.org/research/taxonomy_988667.pdf.

[29] 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.

[30] 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. Oak Ridge, Tennessee, 2008, 30:1–30:3. ISBN: 978-1-60558-098-2. DOI: 10.1145/1413140.1413174.

[31] 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. URL: http://academypublisher.com/jnw/vol04/no07/jnw0407552564.pdf.

[32] 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.

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

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

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

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

[37] C. Szilagyi and P. Koopman. "Flexible Multicast Authentication for Time-Triggered Embedded Control Network Applications". *Dependable Systems Networks. IEEE/IFIP International Conference on*. Dependable Systems Networks, 2009. DSN '09. IEEE/IFIP International Conference on. June 2009, pp. 165–174. DOI: 10.1109/DSN.2009.5270342.

[38] 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". *Vehicular Technology Conference (VTC Fall), 2011 IEEE*. San Francisco, CA, Sept. 2011. DOI: 10.1109/VETECF.2011.6093081.

[39] 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. DOI: 10.1109/IVS.2008.4621263.

[40] 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.

[41] 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. URL: http://www.mirlabs.org/jias/hoppe.pdf.

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

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

[44] 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. DOI: 10.1109/VETECF.2008.260.

[45] 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. DOI: 10.1007/978-3-540-75101-4_4.

[46] *E-safety Vehicle Intrusion Protected Applications (EVITA)*. URL: http://www.evita-project.org/ (visited on 07/25/2012).

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

[48] 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.

[49] 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)*. National Automotive Center and Vectronics Technology. Traverse City, Michigan, June 2005, pp. 145–155.

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

[51] M. 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*. Vol. 6596. Lecture Notes in Computer Science. 2011, pp. 224–238. ISBN: 978-3-642-19785-7. DOI: 10.1007/978-3-642-19786-4_20.

[52] 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)*. IARIA. Barcelona, Spain, Oct. 2011, pp. 226–231.

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

[54] A. Weimerskirch. "Secure Software Flashing". *SAE Int. J. Passeng. Cars - Electron. Electr. Syst.* Vol. 2. 1. 2009, pp. 83–86.

[55] 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. ISBN: 978-3-540-28428-4. URL: http://dx.doi.org/10.1007/3-540-28428-1_3.