Secure Vehicle Communication

Deliverable 1.1

VANETS Security Requirements Final Version

Project:	Sevecom
Project Number:	IST-027795
Deliverable:	D1.1
Title:	VANETS Security Requirements Final Version
Version:	V2.0
Confidentiality	Confidential, will be public
Authors:	Rainer Kroh (DaimlerChrysler) Editor
	Antonio Kung (Trialog), Frank Kargl (UUlm)
Date:	21 November 2006

Part of the Sixth Framework Programme

Funded by the EC - DG INFSO

Control Sheet

Version history			
Version number	Date	Main author	Summary of changes
0.0	05 May 2006	Antonio Kung, Rainer Kroh	Creation of template
0.1	13 June 2006	Rainer Kroh	Integration of Application Lists, Application Characteristics and Use Case Analysis
0.2	19 June 2006	Rainer Kroh	Update of Technical Use Cases
0.3	06 July 2006	Rainer Kroh	Integration of Methodology of Deliverable (from UUlm)
0.4	10 July 2006	Rainer Kroh	Integration of Introduction (from Trialog)
1.0	20 July 2006	Antonio Kung	Final: Version 1.0
1.1	23 August 2006	Rainer Kroh	Integration of Attack Use Cases
1.2	11 October 2006	Rainer Kroh	Integration of Security Concepts and mapping of C2C-CC use cases
1.3	20. October 2006	Elmar Schoch	Update of Security Requirements Engineering Process
2.0	21. November 2006	Rainer Kroh	Minor spelling corrections

Approval		
	Name	Date
Prepared	Rainer Kroh	10 July 2006
Reviewed	All Project Partners	14 July 2006
Authorized	Antonio Kung	20 July 2006

Circulation	
Recipient	Date of submission
Project partners	20 July 2006
European Commission	21 July 2006

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Intended Audience

This deliverable is an intermediate version of the final requirement deliverable that will be public. This intermediate version is intended for use within SEVECOM as well as for IST projects and working groups (e.g. C2C consortium) with which SEVECOM has liaison activities.

1.2 Abbreviations and Conventions

CALM:	Continuous Air interface for Long and Medium distance
DSRC:	Digital Short Range Communication
ECU:	Electronic Control Unit
GPS:	Global Positioning System
IVC:	Inter-Vehicle communication (equal to V2V + V2I)
PKI:	Public Key Infrastructure
OBU:	Onboard Unit
QoS:	Quality of Service
RSU:	Roadside Unit
TOC:	Transportation Operation Centre
TCU:	Telematics Control Unit
VANET:	Vehicle Adhoc Network
V2V:	Vehicle to Vehicle communication
V2I:	Vehicle to Infrastructure communication
VSCC:	Vehicle Safety Communication Consortium

1.3 Scope and Objectives of SEVECOM

SEVECOM addresses security of future vehicle communication networks, including both the security and privacy of inter-vehicular and vehicle-infrastructure communication. Its objective is to define the security architecture of such networks, as well as to propose a roadmap for progressive deployment of security functions in these networks.

Vehicle to Vehicle communication (V2V) and Vehicle to Infrastructure communication (V2I) bring the promise of improved road safety and optimised road traffic through co-operative systems applications. To this end a number of initiatives have been launched, such as the Car-2-Car consortium in Europe, and the DSRC in North America. A prerequisite for the successful deployment of vehicular communications is to make them secure. For example, it is essential to make sure that life-critical information cannot be modified by an attacker; it should also protect as far as possible the privacy of the drivers and passengers. The specific operational environment (e.g. moving vehicles, sporadic connectivity …) makes the problem very novel and challenging.

Because of the challenges, a research and development roadmap is needed. We consider SEVECOM to be the first phase of a longer term undertaking. In this first phase, we aim to define a consistent and future-proof solution to the problem of V2V/V2I security.

SEVECOM will focus on communications specific to road traffic. This includes messages related to traffic information, anonymous safety-related messages, and liability-related messages. The following research and innovation work is foreseen:

- Identification of the variety of threats: attacker's model and potential vulnerabilities; in particular, study of attacks against the radio channel and transferred data, but also against the vehicle itself through internal attacks, e.g., against TCU (Telematics Control Unit), ECU (Electronic Control Unit) and the internal control bus.
- Specification of architecture and of security mechanisms which provide the right level of protection. It will address issues such as the apparent contradiction between liability and privacy, or the extent to which a vehicle can check the consistency of claims made by other vehicles. The following topics will be fully addressed: key and identity management, secure communication protocols (including secure routing), tamper proof device and decision on crypto-system, privacy. The following topics will be investigated in preparation of further work: intrusion detection, data consistency, secure positioning and secure user interface.
- The definition of cryptographic primitives which take into account the specific operational environment. The challenge is to address (1) the variety of threats, (2) the sporadic connectivity created by moving vehicles

and the resulting real-time constraints, (3) the low-cost requirements of embedded systems in vehicles. These primitives will be adaptations of existing cryptosystems to the V2V/V2I environment.

The overall approach is the following:

- Take into account existing results available from on-going eSafety projects in terms of threat analysis and security architecture.
- Work in close liaison with new IST eSafety projects which will focus on C2C application and road network infrastructures. Common workshops will be held in order to reach a consensus on the security threats and the proposed mechanisms.
- Take into account on-going standardisation work at the level of security such as ISO15764 - Extended Data Link Security or ISO/CD20828 - Security Certificate Management, or at the level of communication (ISO2121x series on CALM - Continuous Air interface for Long and Medium distance)
- Integrate SEVECOM mechanisms into a use case development which is based on the V2V/V2I infrastructure used by eSafety projects.
- Investigate the necessary conditions for deployment. This includes the provision guidelines for security evaluation and certification, as well as the definition of a roadmap. This will include discussion on organisational issues (e.g. key and certificate management)

The project will work in close liaison with the Car-2-Car consortium; it will also establish strong connections with related efforts in the world, notably USA (DSRC, IEEE P1609) and Japan.

Sevecom covers a number of research topics. The table below lists them along with the expected achievement.

	Topic	Scope of work	Academic Partners (first name is leader)
A1	Key and identity management	Fully addressed in SEVECOM	EPFL, BUTE
A2	Secure communication protocols (including secure routing)	Fully addressed in SEVECOM	U.Ulm, BUTE
A3	Tamper proof device and decision on cryptosystem	Fully addressed in SEVECOM	BUTE
A4	Intrusion Detection	Investigation work	U.Ulm
A5	Data consistency	Investigation work	BUTE
A6	Privacy	Fully addressed in SEVECOM	EPFL, U.Ulm, BUTE
A7	Secure positioning	Investigation work	EPFL
A8	Secure user interface	Investigation work	U.Ulm

1.4 Scope and Objectives of Document

This document reports on the current results of the requirement analysis work carried out in SEVECOM. It contains

- an application list
- an analysis of application characteristics
- an analysis of application requirements
- a resulting analysis of application use cases
- technical use case descriptions

The final version of this deliverable will include complete requirement analysis with the following sections

- a threat analysis section
- an analysis of security requirements

2 Methodology for Deliverable

2.1 Introduction

Spontaneous communication between vehicles or between vehicles (V2V) and road-side infrastructure (V2I) is an important research area that several projects and initiatives like Fleetnet [1] and the VSC [3] have addressed during the recent years. Right now, work on the topic is being continued by a number of projects including, for example, NoW [2], CVIS [4], or Safespot [5].

These projects have suggested a long list of potential applications (e.g. in [8]), some of which address road safety issues or try to enhance driver and passenger comfort. Examples include warnings at intersections and at traffic lights, detection and warning of dangerous road conditions between cars, direct car-to-car messaging, and many more.

Likewise, considerable research has been done on specific topics involved in V2V/V2I-communication. Investigations and proposed solutions range throughout the ISO/OSI model, starting from optimised MAC layer approaches, work on message dissemination, and integration of infrastructure in the V2V network up to application implementation questions.

From the security point of view, it is obvious that all these mechanisms and applications may become the target of attackers that will try to interfere with the proper operation for fun or profit. For instance, some pranksters might send bogus warning messages to other cars, pretending that there are dangerous road conditions ahead. This might lead to cars slowing down or breaking, resulting in traffic jams or even accidents.

This is where the work of SEVECOM starts. The goal of SEVECOM is to develop future-proof mechanisms to secure vehicular communication (VC) to thwart such attacks.

The first step towards security mechanisms usually comprises an analysis of risks, weaknesses of the system, of threats and attacks. Yet in VC, the situation is different due to several facts.

- Largely undefined system
  In contrast to traditional security engineering, we don't have a specified system in the VC context. While many aspects have been investigated, large portions of the system including components, protocols and involved parties are not defined. Some standardisation efforts are under way, but mostly cannot yet be used.
- Broad variety of envisioned applications
  Previous and ongoing projects have brought up a very large number of potential application ideas for a multitude of scenarios. Additionally, though the intention of an application is usually clear, the implementation options are manifold.

These conditions have direct implications on the security design approach.

First, commonly used methods for security assessment including the Common Criteria [6] or Octave [7] are not useful, because they usually focus on security evaluation of established systems within commercial organisations. This clearly does not fit the problems faced in SEVECOM, where we want to assess the security problems in an application area, namely Vehicular Communication.

Second, the variety of applications makes it impossible to discuss the security of them all in detail. However, a simple incremental, use-case driven development is also not applicable, since it might be problematic to leave out an important application with distinguished properties or a combination of properties that is not covered by others. Furthermore, two different use cases could be closely related in certain aspects, so that essentially the same work would have been done twice.

In order to fulfil the goal of an overall security solution on VC, SEVECOM had to find new ways of extracting security requirements to cope with such conditions.

The new approach we developed for this is a kind of enhanced use case method. It allows for analysing a large set of applications, select typical representatives that will cover the requirements of a whole cluster of applications, and develop a security solution for this subset of applications which is expected to cover the requirements of all applications considered.

2.2 Process

Figure 1 shows the main steps in the entire requirements engineering process. In fact this process encompasses not only the requirements engineering, but also the outlines the later phases of security system development (yet it excludes any validation steps).

The basic concept is to first collect a widely complete application list and do a preliminary analysis of application characteristics and security requirements for all applications. The classification of properties for every application predicts key implementation decisions. The large collection of applications assures to some extent that no important application has been overlooked accidentally. By such a list, we get under control both the indefinite system properties as well as the variety of applications.

After that, a cluster analysis process is used to find clusters of applications that share similar characteristics and security requirements.

Next, a small subset of representative applications is selected for each of these clusters, which will be analysed in more detail. Application use-cases will now describe the regular operation of the applications and identify all needed components and protocols. The described systems will not have any security mechanisms in place, but simply describe the operation as needed from an application point-of-view.

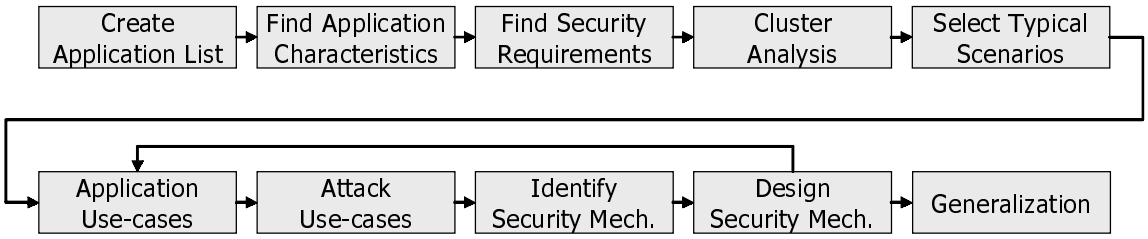

Figure 1: Steps of Security-Requirements Engineering using Cluster Analysis (SECA) process

So called attack use-cases describe potential attacks against the applications and their security requirements. This leads to a set of required security mechanisms that will prevent these attacks. The design of these mechanisms is the step next to last step. As the introduction of these security mechanisms might introduce changes to the application itself or even open up new opportunities for attacks, there is a look back to previous steps here.

Finally, the last step will check whether the found solutions will also apply to the other applications within each cluster.

2.2.1 Step 1: Create Application List

The goal of this step is to find a detailed list of potential applications for the area to be analyzed. For VC, this list will contain all applications that might be used in VC scenarios together with a short description of the application. Typically such a list will be the result of intensive discussions and brain-storming sessions.

The application list and the classification of properties is a key factor to get things structured. Because concrete security mechanisms can only be introduced in concrete system specifications, it helps a lot to get away from a vague system to a more structured definition. Though still on a high level, the application list allows the extraction of key system functionality and security requirements.

We gathered an application list based on our discussions and material provided by VSC [21] and others [22]. One major insight from that process is the extreme variety of domains, where VC could enable applications. Beyond the typical VANET scenarios, where vehicles warn each other of hazardous road situations, communicate to avoid collisions, help the driver ramping the highway or improve navigation by sending out traffic information, there are numerous different application areas. For instance, integrating traffic infrastructure like signs and traffic lights into the VC system could improve driving and support for authorities. Commercial infrastructure nodes might lead drivers to free parking lots and let them download the latest map updates for the navigation system. Similar to that, vehicle maintenance could be improved by wireless diagnostics or just-in-time repair notification. In summary, VC applications involve all situations in a vehicle's life - on the road, at home, in the garage, by warning, helping and facilitating.

In the later sections of this document (chapter 3) you find a list that the SEVECOM project developed based on own discussions and material provided by VSC [8] and others [9].

2.2.2 Step 2: Find Application Characteristics

The next step is needed to further understand details of the applications. One should find properties that describe characteristic aspects of the applications and can be used to distinguish different kinds of applications (chapter 4).

For VC, we defined properties that answer most relevant questions on the application, including general estimations on importance, technical requirements, and application situation.

After the properties are defined, each application needs to be classified in every property. Because there is no definite answer in most cases, estimates need to be given. Although it might be hard to actually answer these questions without having an application- and protocol description available, our own work has shown that experts are usually able to come up with pretty reasonable assumptions.

While we will give meaningful classes for each property here, the final values of the properties need to be given in a numerical form, describing e.g. the importance of the property for an application, where '0' stands for irrelevant, '1' for important and '2' for very important. This is necessary so the cluster analysis algorithm can determine numerical distances between properties and applications.

In the following, we introduce key properties, corresponding classification possibilities and the relation of the property to security.

Influence on safety

Among the various applications, we find different levels of influence on road safety. Many applications are **safety-critical**, like intersection collision avoidance, which is used in hazardous situations. Other applications are only intended to improve road safety to some extent which we then denominate as **safety-related**. For instance, missing a work zone warning is not likely to cause as much harm as missing a collision warning. A third category of applications is **not safety related** at all, e.g. a parking spot locator service. Regarding security, this characteristic directly indicates how much attention an application requires.

Driver involvement

Applications feature totally different extent of driver's involvement. Whereas in some cases the driver manually triggers messages, in other cases the vehicle creates messages autonomously without even notifying the driver. Also at the receiver's side, messages may be treated by the **vehicle only**, or they may demand the driver's **awareness**, **attention** or even **reaction**. This is also strongly related to security requirements. If a driver is intended to react immediately e.g. on a warning message, the message content must be absolutely trustable.

Interworking of communication

When it comes to communication, several important questions need answers. The first is to clarify which parties will be involved in the communication. For traditional VANETs, communication is only **car-to-car**, which means that cars trigger messages and deliver them to other cars. Yet in the whole scenario, also a lot of infrastructure nodes are involved whose capabilities and needs are obviously different than vehicles. For example, in an **infrastructure-to-car (I2C/I2V)** application, a traffic light might send state changes to vehicles. From the opposite perspective, vehicles might send SOS messages to infrastructure nodes with backend network to call for help (**car-to-infrastructure (C2I/V2I)**). Security is influenced, for instance, because infrastructural components of VANETs usually don't need privacy.

Direction of communication

Regarding security, it is important to distinguish between **one-way** and **two-way** communication. For example, in case of some warning applications, a vehicle might only get one packet and then has to decide whether to trust the contained information. Moreover, for typical two-way applications like electronic payment or wireless diagnostics, encryption of data is likely needed.

Forwarding of messages

While there are applications that only need **single-hop** communication, many typical ones distribute information **multi-hop**, using other nodes as forwarders. Both types of communication raise specific security questions, but secure routing is harder to obtain because routing by definition involves multiple -- potentially fraudulent -- nodes.

Addressing

Before messages can be sent out, one of the most important questions is who will receive them. In our application list, we have some applications that use **unicast** addressing whereas others **broadcast** information to a certain neighbourhood, but also many applications apply **geocast**. Much information in VC is position dependent; also the destination of messages is often specified geographically. Therefore, securing the position data also plays a vital role.

Timing constraints

Among the applications, timing constraints vary extremely. Whereas in some cases, timely delivery has highest priority (**highly time-critical**), time is **no critical issue** in other cases. For highly time-critical applications, we assume a maximum delay of ~ 500ms, for **time-critical** applications 1s and for applications for which **time is relevant** ~ 5s. Those applications with **no time constraints** may have delays of more than 10s. Particularly, applications with highly time-critical messages are sensitive to network disturbance.

2.2.3 Step 3: Find Security Requirements

Like in the previous step, you now have to provide a set of security requirements that will be relevant for the application (chapter 5). It is important to only describe requirements based on the application needs and not to include assumptions about potential security mechanisms here.

Referring to VC, security requirements include authentication requirements, integrity and confidentiality, privacy requirements, availability, and access control.

The values of these properties need to be described in a numerical form, where e.g. ’0’ stands for irrelevant, ’1’ for important and ’2’ for very important.

Authentication

Trust is crucial in safety-related applications, in which vehicles react according to legitimate messages they received. Authentication ensures that the sender of a message is correctly identified. With **ID authentication**, the receiver is able to verify a unique ID of the sender. The ID could be the license plate or chassis number of the vehicle. Yet, in many cases, the actual identity of nodes does not play an important role -- receivers are satisfied if they are able to verify that the sender has a certain property. Hence, **property authentication** is a security requirement that allows verifying properties of the sender, e.g. that the sender is a car, a traffic sign etc. For applications using location information, **location authentication** allows to verify that the sender is actually at the claimed position, or that the message location claim is valid.

Integrity

Applications requiring integrity specify that the transported information must not be altered between sender and receiver.

Confidentiality

Some applications require that only the sender and the intended receiver can access the content of a message, e.g. instant messaging between vehicles. Confidentiality specifies that transported information cannot be eavesdropped on its way between sender and receiver.

Privacy

Privacy is an important factor for the public acceptance and successful deployment of VANETs. It means that the driver is able to keep and control the information related to the vehicle (e.g. identity of the driver, the driving behaviour, the past and present location of the vehicle etc.) from other parties. Without privacy protection, VC provides a convenient way for an observer to track and identify the vehicle and its passengers, hence makes the Big Brother surveillance scenario more a reality than a fiction. But safety-related applications in VC also require trust between the communication partners, so total anonymous for privacy reason is not feasible. There are different security requirements for privacy, in this way the information of the vehicle and the driver can be protected as much as possible. For example, in "vehicle-based road condition warning", a car does not need to reveal its identity, but needs to provide its location information so that other cars can estimate e.g. the relevance of received warning messages. **ID privacy** specifies how much the identity of the sender should be kept secret. Depending on the applications, **location privacy** has different levels, which range from distributing location information freely throughout the network to totally keeping it private. Although privacy requirements apply for normal communications, public authorities wishing to have access to the identity or location information of cars may have **jurisdictional access**.

Availability

Some applications, particularly safety applications, require high availability of the communication system. For example, a post-crash/breakdown warning requires that the radio channel is available such that approaching cars can receive the warning message in time. If the medium is jammed e.g. by an attacker and therefore such messages don't arrive at the receivers in a very short time, the application gets useless.

Access control

Access control is necessary for applications that need fine-grained definition of the rights that a user or infrastructure component has. For instance, an authorized garage may be allowed to fully access wireless diagnostics, whereas other parties may only be granted limited access. Another form of access control can be the exclusion of misbehaving nodes (e.g. by an intrusion detection system using a trust management scheme) from the VANET by certificate revocation or other means.

Non-repudiation

Certain application need to track and reconstruct what was going on in the past. In our project, the non-repudiation requirement is also called **auditability**, by which senders or receivers can prove that messages have been received or sent respectively. For some applications, messages may only be stored for a very limited time (e.g. the last 10 seconds in a ring buffer) and made permanent only in case of an incident (e.g. crash).

First, the receiver should be able to authenticate the property that the sender actually is a car and that the location of the sender is correct. Otherwise, attackers may use an arbitrary wireless transmitter by the roadside or forge the location information to make upcoming cars believe the hazardous road condition ahead. Furthermore, property authentication can make sure that the sender is able to detect the road condition, e.g. a car equipped with ESP/VSC sensors in contrast to a car without appropriate sensors. The application also requires integrity, so the message cannot be altered during transmission (e.g. a message saying wet surface ahead altered by attacker to be icy road). Regarding privacy, as the sender is a private car, the identity of it should be kept private, too. Since it is not a safety critical application, the security requirements such as jurisdictional access and availability are set to medium value. Access control and non-repudiation only play a minor role, and confidentiality is not applicable because the warning is public information and the set of receivers is not known.

2.2.4 Step 4: Cluster Analysis

After describing all the different applications, the properties and security requirements, the next step is the grouping of applications in clusters with similar properties and security requirements (chapter 5.3). With this step, we can likely identify groups of applications with similar requirements and characteristics. As described earlier, the cluster analysis is intended to reduce the complexity of dozens of applications while in parallel; it should deliver a qualified selection of representative application use cases.

This can easily be done using statistics software like SPSS and delivers results like shown in the later sections of this document. We have used the k-means cluster analysis to do this analysis. According to the online-help, „this procedure attempts to identify relatively homogeneous groups of cases based on selected characteristics, using an algorithm that can handle large numbers of cases."

For the k-means cluster analysis, the user has to provide the number of clusters. It was initially clear that not more than 10 clusters should be considered, as otherwise the resulting amount of work for specifying the application use-cases etc. would get too high.

We have run the cluster analysis with cluster sizes from 5 to 10. According to the average and maximum distances from applications to the respective cluster centers, and the distribution of applications per cluster, we decided that 8 clusters is a reasonable number.

2.2.5 Step 5: Select Typical Scenarios

The selection of cluster representatives is a manual process. There are different strategies how to do so. One strategy is to use these applications which have the closest distance to the cluster centers, as they represent their cluster best. Another strategy would be to select the most "interesting" applications, whatever "interesting" means in the context of the research activities.

For our VC applications, we preferred applications that are also considered interesting e.g. by other projects like CVIS or Safespot and by consortiums like the C2C-CC (chapter 6.1).

2.2.6 Step 6: Application Use Cases

For all the selected applications, we have written detailed application use cases that describe the applications in terms of involved components and operation steps (chapter 6). For all examples we use an identical form so that applications and their description can be compared easily.

It is important to note that the applications are described "as is", i.e. without any security measures in place. This way, we are able to fully concentrate on the desired behaviour of the application. Possible security weaknesses are to be discovered in the next step.

2.2.7 Step 7: Attack Use Cases

In a next step, detailed descriptions of various attacks need to be found (chapter 7). We use a form similar to the application use case form for describing these attack use cases, as we call it. The form comprises a short risk analysis, including attack classifications and detailed descriptions. The categorization comprises e.g. the primary goal of the attack, used attack techniques and the severity of the attack. Descriptions are given for the attacker's goal in context, the attack procedure, the attacked system components, the effects of the attack, and pre-conditions for the attack as well as success and failure factors. These attack use cases consecutively allow finding weaknesses in the application scenarios.

2.2.8 Step 8: Identify Security Mechanisms

Based on the attack use cases, security primitives (chapter 8) can be identified. While reviewing all attack use cases, we can decide which primitives are useful against the corresponding attack. This transfer needs to be done in a discussion again, since there is no general definitions which mechanism helps against what attack.

Therefore, we revisited all attack use cases and discussed appropriate methods to thwart the attack. In an incremental way, we gathered a list of what we called “security concepts”, and estimated applicability and helpfulness against every attack use case. The classification knows three different categorizations:

- “++”: The security concept is very useful for the corresponding attack use case and is usually able to prevent the attack
- “+”: The concept can help against the attack though it does not guarantee the prevention or might not be wanted due to other considerations
- “O”: The concept might help to a certain degree, but it depends on the concrete implementation if it is likely to be overridden with only small effort by the attacker.

Based on the security concepts, which only describe an abstract measure against attacks, the next step is to propose concrete mechanisms that will implement these concepts.

2.2.9 Step 9: Design Security Mechanisms

With this step, we leave the threat and requirements engineering and the design phase of our process begins. Based on the identified threats and required mechanisms, one will now design and propose e.g. cryptographic protocols or a system design which will provide the necessary security functionality.

Introducing security mechanisms may lead to additional attack vectors, e.g. on a PKI system needed to manage the identities in our example. Therefore there is a loop in the process going back to step 7 where additional attacks targeting the security system can be described.

It may also part of this step to analyze the effectiveness and efficiency of the proposed methods. This can e.g. be done using simulations or formal methods.

2.2.10 Step 10: Generalization

Up to this point, we have only considered the selected cluster representatives. Though the clustering is a step to reduce complexity in a qualified way, it does not guarantee that the security mechanisms designed for the application representatives are also valid for all other applications. Therefore, in a final step, we will now have to analyze whether the security mechanisms will also work with the other applications that are to be realized.

3 Applications Lists

3.1 Assist driver with signage

3.1.1 Traffic signal violation warning

Traffic signal violation warning uses infrastructure-to-vehicle communication to warn the driver to stop at the legally prescribed location if the traffic signal indicates a stop and it is predicted that the driver will be in violation.

The in-vehicle system will use information communicated from infrastructure located at traffic signals to determine if a warning should be given to the driver. The communicated information would include traffic signal status and timing, traffic signal stopping location or distance information, and directionality. The type of road surface and weather conditions near the traffic signal may also be communicated as this could be used to estimate braking distance.

3.1.2 Stop sign violation warning

Stop sign violation warning uses infrastructure-to-vehicle communication to warn the driver if the distance to the legally prescribed stopping location and the speed of the vehicle indicate that a relatively high level of braking is required for a complete stop.

The in-vehicle application will use information communicated from the infrastructure to provide the warning. The communicated information would include stopping location or distance information, and directionality. The type of road surface and weather conditions near the stopping location may also be communicated as this could be used to better estimate braking distance. As an alternative to DSRC, digital maps and GPS could be used.

3.1.3 General in-vehicle signage

Show (important) traffic signs inside the vehicle (e.g. adaptive signs) or display warning if a sign is ignored by the driver (e.g. speeding).

The in-car system can determine whether the signage applies to this car (e.g. height restrictions) and filter displayed information accordingly.

3.2 Assist driver at intersections

3.2.1 Left turn assistant

The Left Turn Assistant provides information to drivers about oncoming traffic to help them make a left turn at a signalized intersection without a phasing left turn arrow. When turning left at an intersection, drivers get a notification if they have to yield to traffic from the left, right, or from ahead. Communication is based on C2C communication where information on position, speed, and direction is exchanged. Communication is triggered by approaching intersection which can be discovered either map based or by infrastructure beaconing (e.g. from traffic signals).

3.2.2 Intersection collision warning

Warn vehicles at an intersection, when a collision would be probable, e.g. warn driver if he is going to accelerate from stop although another vehicle is approaching.

Infrastructure sensors and/or DSRC communications can be used to detect all vehicles, their position, velocity, acceleration, and turning status while approaching an intersection. Weather status and the road shape/surface type can be variables for calculating the likelihood of a collision. The in-vehicle unit determines when a collision is imminent and issues a warning to the driver.

3.2.3 Pedestrian crossing information

This application provides an alert to vehicles if there is danger of a collision with a pedestrian that is on a designated crossing.

The presence of a pedestrian is detected through infrastructure sensing equipment, including the “walk” button that pedestrians press before crossing an intersection. Another option is to detect pedestrians by on board sensors (e.g. radar) and distribute this information to other vehicles.

A broadcast message with information regarding the pedestrian (position, direction, speed) is transmitted from roadside units or other vehicles to vehicles approaching the crossing area.

Application areas may also include warning about deer and other wild animals crossing the street.

3.3 Assist authorities

3.3.1 Emergency vehicle approaching warning

Emergency vehicle approach warning is implemented by vehicles that are stopped or vehicles that are slowing to warn approaching vehicles. An OBU mounted on the emergency vehicle transmits to warning messages to all vehicles ahead of it. These messages are received by the OBU on-board the approached vehicles and passed to the driver for evaluation the potential hazard or to the on-board computer for automatic evaluation or both.

This application provides the driver a warning to yield the right of way to an approaching emergency vehicle.

The emergency vehicle broadcast message would include information regarding its position, lane information, speed and intended path. The in-vehicle application will use this information to alert the driver.

3.3.2 Emergency vehicle signal pre-emption

This application allows an emergency vehicle to request right of way from traffic signals in its direction of travel.

Emergency vehicle signal pre-emption allows the emergency vehicle to override intersection signal controls. The intersection mounted roadside unit verifies that the request has been made by an authorized source and alters the traffic signal and timing to provide right of way to the emergency vehicle. This application may need to be integrated with the Approaching Emergency Vehicle Warning application.

Emergency vehicle signal pre-emption in a multiple traffic signal network is implemented with intersection mounted, stationary, RSU communicating with each other and with emergency vehicle mounted, mobile, RSU as they approach. As a stationary RSU collects data to identify an approaching emergency vehicle it sends information to the local signal controller and the surrounding stationary RSU that allows the emergency vehicle to proceed through its’ intersection and others in its path with a green light.

3.3.3 Emergency vehicle at scene warning

While at an accident scene, emergency vehicles warn oncoming motorists from either direction that there is a road obstacle ahead.

3.3.4 Vehicle safety inspection

Authorities may use C2C or I2C communication to check the safety status of cars and esp. commercial vehicles like trucks. Data checked might include the date of last safety inspection, maximum and current load, data from the tachograph, etc.

Based on this data, authorities may signal to the driver that he can proceed freely or needs to stop e.g. at an upcoming inspection for further checking.

3.3.5 Electronic license plate

The electronic license plate allows the reading of vehicle license plates via wireless interface.

Must only be available to authorized comm. partners! Possibly the car also checks automatically if its license is still valid and refuses to operate otherwise.

3.3.6 Electronic driver's license

There are two stages of implementing electronic driver’s license. First, the driver has to issue his license to the car - one could imagine that a car would not start without driver’s license (which has some problematic aspects like emergencies!).

As a second step, one could imagine that the driver's license could be requested wirelessly by police.

3.3.7 In-vehicle Amber alert (crime haunt)

This application sends Amber Alert information to the in-vehicle unit.

The Amber Alert response program utilizes the resources of the law enforcement and the media to notify the public when children are suspected to be kidnapped. The vehicle being sought after could be excluded from receiving the message.

Information is provided to the driver through the in-vehicle application.

3.3.8 Stolen vehicles tracking

When a car is reported to being stolen, infrastructure and/or other cars send messages, informing the car about this status. Properly also in-board tampering detectors may be used to detect that a cars has been stolen.

Stolen cars send information regarding their location and status to other cars which relay this information to the authorities.

3.4 Assist road users upon accident

3.4.1 Post-crash/breakdown warning

This application warns approaching traffic of a disabled vehicle (disabled due to an accident or mechanical breakdown) that is stuck in or near traffic lanes, as determined using map information and GPS.

The application assumes communication, digital map, and GPS are still operable and may require a bottom-mounted antenna for rollover situations. This should have the greatest benefit in poor visibility and inclement weather situations and may reduce the potential for a secondary crash.

Vehicle to vehicle: A disabled vehicle will warn approaching vehicles of its position.

Alternative: Other vehicles approaching the site may detect the obstacle by in-board sensors (e.g. radar) and send the warning in place of the disabled vehicle.

3.4.2 SOS services

The in-vehicle application will send SOS messages after airbags are deployed, a rollover is sensed, or the vehicle otherwise senses a life-threatening emergency.

An occupant could also initiate the message for a non-crash related medical or other emergency.

Vehicle to infrastructure: The emergency message will be sent from the vehicle to a roadside unit and then forwarded to the nearest local authority for immediate assistance.

Vehicle to vehicle: The emergency message will be sent from the vehicle to a passing vehicle, which stores and then relays the message when in range of a roadside unit. It will then be forwarded to the nearest local authority for immediate assistance.

3.4.3 Pre-crash sensing

Pre-crash sensing can be used to prepare for imminent, unavoidable collisions.

Based on position information obtained by beaconing, the car can determine whether a crash is about to occur.

This application could use communication in combination with other sensors to mitigate the severity of a crash. Countermeasures may include pre-tightening of seatbelts, airbag pre-arming, front bumper extension, etc.

3.4.4 Event data recording

Near crash data and crash data such as position, speed, deceleration, yaw, roll are collected and used to reconstruct accidents, to determine potential safety problem in cars, ...

3.5 Assist driver on special road conditions

3.5.1 Work zone warning

Work zone warning delivers warning and additional information on a work zone to cars. Data could include speed limit, lane closures/changes etc.

Information on work zone may also be relevant to vehicles further away from the scene.

3.5.2 Curve-speed warning (rollover warning)

Curve speed warning aids the driver in approaching curves at appropriate speeds.

This application will use information communicated from roadside beacons located ahead of approaching curves. The communicated information from roadside beacons would include curve location, curve speed limits, curvature, and bank and road surface condition. The in-vehicle system would determine, using other on-board vehicle information, such as speed and acceleration whether the driver needs to be alerted.

3.5.3 Vehicle-based road condition warning

This in-vehicle application will detect marginal road conditions using on-board systems and sensors (e.g. stability control, ABS), and transmit a road condition warning to approaching vehicles using geocast.

Road condition information can be used by vehicle safety applications in the receiving vehicle. For example, an application can be designed to work in the vehicle to calculate maximum speed recommendations based on road conditions and upcoming road features (e.g. curve, bank, intersection, or stop sign) and notify the driver appropriately.

3.5.4 Infrastructure-based road condition warning

This infrastructure-based application will detect marginal road conditions using infrastructure systems and sensors (e.g. fog-detectors, temperature sensors, etc.), and transmit a road condition warning to approaching vehicles using geocast.

Information is forwarded by other vehicles.

Road condition information can be used by vehicle safety applications in the receiving vehicle. For example, an application can be designed to work in the vehicle to calculate maximum speed recommendations based on road conditions and upcoming road features (e.g. curve, bank, intersection, or stop sign) and notify the driver appropriately.

3.6 Assist on vehicle maintenance

3.6.1 Safety recall notice

This application allows the distribution of safety recalls sent directly to vehicles via roadside units, and/or in-home PCs.

The on-board system can use on-board diagnostics to evaluate, whether the safety recall applies to this car, e.g. if a defective part is actually installed in the car.

A reminder of a safety recall that requires immediate attention can be provided through a warning lamp or other methods

3.6.2 Just-in-time repair notification

This application communicates in-vehicle diagnostics to the infrastructure and advises the driver of nearby available services.

The roadside unit can pass information to an OEM technical support center for assessment. This information could be used to advise the driver of potential maintenance required.

3.6.3 Wireless Diagnostics

Service staff can access the on-board diagnostics without requiring physical access to the in-board systems. This can speed up turn-around times at service locations. In some cases, problems may also be fixed by correcting software-based problems without the need to drive the car to a special location.

3.6.4 Software update/flashing

Software update/flashing includes up- and download of data without requiring a physical connection to the vehicle.

Examples include: Transfer of registration data, diagnostic data, repair record data, new engine and electronics control programs, onboard computer program updates, map databases, music, video, and on-board sensor data at high transfer rates to any device in the vehicle.

3.7 Assist driver in dangerous traffic situations

3.7.1 Cooperative (forward) collision warning

Cooperative collision warning collects surrounding vehicle locations and dynamics and warns the driver when a collision is likely.

The vehicle receives data regarding the position, velocity, heading, yaw rate, and acceleration of other vehicles in the vicinity. Using this information along with its own position, dynamics, and roadway information (map data), the vehicle will determine whether a collision with any vehicle is likely. In addition, the vehicle will transmit position, velocity, acceleration, heading, and yaw rate to other vehicles.

3.7.2 Emergency electronic brake lights

When a vehicle brakes hard, the Emergency Electronic Brake light application sends a message to other vehicles following behind.

This application will help the driver of following vehicles by giving an early notification of lead vehicle braking hard even when the driver's visibility is limited (e.g. a large truck blocks the driver's view, heavy fog, rain). This information could be integrated into an adaptive cruise control system.

3.7.3 Blind spot warning / lane change warning

Blind spot:

This application warns the driver when he intends to make a lane change and his blind spot is occupied by another vehicle. The application receives periodic updates of the position, heading and speed of surrounding vehicles via vehicle-to-vehicle communication. When the driver signals a lane change or turn intention, the application determines the presence or absence of other vehicles/pedestrians/bicyclists in his blind spot. In case of a positive detection, a warning is provided to the driver.

Lane change:

This application provides a warning to the driver if an intended lane change may cause a collision with a nearby vehicle. The application receives periodic updates of the position, heading and speed of surrounding vehicles via vehicle-to-vehicle communication. When the driver signals a lane change intention, the application uses this communication to predict whether or not there is an adequate gap for a safe lane change, based on the position of vehicles in the adjacent lane. If the gap between vehicles in the adjacent lane will not be sufficient, the application determines that a safe lane change is not possible and will provide a warning to the driver.

3.7.4 Wrong way driver warning

Cars heading in the wrong direction in one-way streets or on highways will receive a warning.

Other vehicles driving in the correct direction will also be alerted of the upcoming vehicle. The wrong-way car will be detected by its position beacons or by infrastructure.

3.7.5 Rail collision warning

Railroad collision avoidance aids in preventing collisions between vehicles and trains on intersecting paths. Drivers of cars get informed about upcoming trains, which is of importance especially at crossings without gates.

Infrastructure to vehicle: This application will use information communicated from roadside beacons located near railroad crossings. The communicated information from roadside beacons would include data about approaching trains such as position, heading, and velocity.

Vehicle to vehicle: This application will use information communicated from a train. The communicated information would include data about the approaching train such as position, heading, and velocity.

3.8 Assist driver in normal traffic

3.8.1 Highway merge assistant

This application warns a vehicle on a highway on-ramp if another vehicle is in its merge path (and possibly in its blind spot).

The merging vehicle uses its navigation information to recognize that it is on an on-ramp. The in-vehicle system monitors information received from other vehicles in the area regarding their position, speed and heading. The system warns the driver if one of the vehicles is in the merge path and is considered a potential collision threat.

3.8.2 Visibility enhancer

This application senses poor visibility situations (fog, glare, heavy rain, white-out, night, and quick light-to-dark transitions) either automatically or via user command.

Vehicle-to-vehicle communication is used to obtain position, velocity and heading of nearby vehicles. The application uses this information with its own GPS and map database for visibility enhancement that may range from simple (veer left or right indications) to complex (superimposed road and vehicles on inside of windshield) implementations.

3.8.3 Cooperative adaptive cruise control

Cooperative adaptive cruise control will use vehicle-to-vehicle communication to obtain lead vehicle dynamics and enhance the performance of current adaptive cruise control (ACC).

Enhancements that could be made to ACC include stopped vehicle detection, cut-in vehicle detection, shorter headway distance following, improved safety, etc. The application can be enhanced by communication from the infrastructure, which could include intelligent speed adaptation through school zones, work zones, off-ramps, etc.

3.8.4 Cooperative platooning

In contrast to Adaptive Cruise Control, platooning is envisioned to take control over vehicles (steering, …)

3.8.5 Cooperative glare reduction / headlamp aiming

This application uses DSRC to allow a vehicle to automatically switch from high-beams to low-beams when trailing another vehicle.

Each vehicle broadcasts its position and heading in low-light situations. If one vehicle calculates that another vehicle in front of it is within a specified range, it will switch from high-beams to low-beams.

3.8.6 Adaptive drivetrain management

Adaptive drivetrain management uses information provided by the infrastructure regarding road features ahead, such as grades, to assist the engine management system of a vehicle in stabilizing its transmission.

Roadside units communicate road features (e.g. curves, grades) that enable the vehicles to anticipate appropriate shift patterns. The goal of the application is to improve fuel economy, emissions and transmission shifting performance. As an alternative to communication, digital maps and GPS could be used.

3.9 Improve traffic management

3.9.1 Intelligent traffic flow control

This infrastructure application uses vehicle-to-infrastructure communication and thereby facilitates traffic light signal phasing based on real-time traffic flow.

Vehicles send a message regarding their position, heading, and speed to the traffic signal infrastructure, which processes the information from each direction and determines the optimal signal phasing based on the real-time information. This application would improve traffic flow.

3.9.2 Road surface conditions to TOC

Vehicles send current location along with status of specific on-board sensors (e.g., traction control, anti-lock braking, transmission speed, etc.) and an activation history of vehicle control devices (steering, brakes, etc.) to the Transportation.

Operations Center which processes these data to determine road surface conditions at vehicle location

Previous title: "Vehicle Probes Provide Road Surface Conditions Data"

3.9.3 Vehicle probes provide weather data to TOC

Vehicles send current location and direction along with status of on-board sensors (precipitation, temperature, traction control, rain, sun level, etc.) and status of on-board devices (wipers, headlamps, heat and air conditioning, etc) to the Transportation Operations Center which processes these data to determine weather information at vehicle location.

3.9.4 Crash data to TOC

In crash situations, vehicles send information to TOC, so e.g. routes in navigation systems can be adapted to prevent the crash site.

3.9.5 Origin and destination to TOC

Vehicle stores route data that is sent to the TOC for use in real-time by operators and archived for planning purposes

3.10 Improve navigation

3.10.1 Parking spot locator

Application should deliver information about unoccupied parking lots to vehicles. Cars send or request parking information from a central TOC.

3.10.2 Enhanced route guidance and navigation

Up-to-date and localized navigation information is sent to vehicles via roadside units.

Information that could be sent includes construction advisories, detours, right and left turn restrictions, closed roads, traffic jams, and parking restrictions. This information may be temporary or too recent to appear in published navigation maps.

Roadside units send enhanced route guidance and navigation information to the vehicle, which processes it and possibly merges it with its navigation system.

Cars need to specifically request the information from the roadside unit.

3.10.3 Map download/update

The car navigation system can download up-to-date maps from the TOC.

3.10.4 GPS correction

Road-side Units can transmit GPS correction data for differential GPS.

3.10.5 Cooperative positioning improvement

Based on map-data, error measurements from other cars, etc., vehicles can try to reduce GPS positioning errors.

3.11 Improve passenger comfort

3.11.1 Instant messaging (between vehicles)

This application enables a vehicle to send an instant message to another vehicle.

If e.g. an occupant notices any problem (e.g. flat tires, missing gas cap, open trunk, etc.), it can send a message to the corresponding vehicle. The message could be chosen from a list of pre-defined or customized messages. Messages could also be typed by co-drivers or sent as audio-recording. Recipients may be selected either from a list of pre-configured partners (e.g. when travelling in a group of cars) or using a graphical interface that shows the position of other cars around.

3.11.2 Point-of-interest notification

When passing interesting spots, drivers get a notification with information on that PoI.

3.11.3 Internet service provisioning / info fuelling

Enabler for all Internet-based services like web browsing, e-mail, multimedia download, concierge services, etc.

3.11.4 Mobile access to vehicle data (PDA, Mobile Phone,…)

This includes vehicle data access (settings, diagnostics, traffic information, navigation system) from your PDA or cell-phone.

This device might support a more convenient user interface to modify settings, plan routes, etc.

3.12 Improve vehicle-related services

3.12.1 Fleet management

Logistic companies can use DSRC to

- send driver advisories and information
- support location tracking and scheduling
- optimize routing
- download mission and instructions

3.12.2 Area access control

Control access e.g. to

- parking gates
- commercial vehicle electronic clearance
- border crossings

Access control is implemented by installing RSUs at the entry and exit points of restricted areas, such as shipping yards, warehouses, airports, transit-only ramps and other areas. The RSU receives authorized

identity codes or access codes from approaching OBU equipped vehicles and transmits a message to proceed or that entry is not allowed. The message could be displayed in the vehicle via in-vehicle signing.

3.12.3 Electronic payment

Realizes electronic payment in cases like

- fast food drive through
- gas stations
- parking fees
- toll fees

3.12.4 Rental car processing

The rental car processing application allows a vehicle to exit the rental car parking area after being rented and re-enter the parking area where the rental fee is automatically deducted from the driver's charge account or other monetary account.

Other RSU are installed so that the rental agency can identify the location of the rental vehicle in the rental lot.

3.12.5 Hazardous material cargo tracking

Tracking of vehicles containing hazardous cargo is implemented by installing RSUs at the entry and exit points of shipping areas, such as shipping yards, warehouses, airports, and other areas. The RSUs collect an identity code and, if desired, a cargo list from approaching or leaving OBU equipped vehicles and send that information to a tracking program. Tracking information can also be obtained from the RSU data of weigh-station clearance points and border crossings.

4 Application Characteristics

4.1 General Characteristics

4.1.1 Safety-related

Application has a safety function (is intended to improve driving safety to some extent), yet it is not safety-critical e.g. in terms of latency of the messages. This has impact on the design of security mechanisms, because safety messages must not be forged or altered. In addition, safety messages usually concern many receivers, which mean that they should not be encrypted or only encrypted with a mechanism that many receivers can decrypt.

4.1.2 Safety critical

Application has severe impact on safety improvement (e.g. used in hazardous situations). In this case, latency plays a vital role, which means that security protocol overhead and processing times should be kept at a minimum for instance.

4.1.3 In-car

Application strongly involves in-car systems, e.g. in-car sensors or software systems. This is the case, for instance, if vehicle software is updated or integral parts of the vehicle like brakes or engine are influenced.

This has security implications because these parts are critical for safe operation of the vehicle.

4.1.4 Driver involvement

Defines, in which way the driver is involved in the application. This may range from no involvement by notifications of any kind (e.g. by an information display), or even may require him to react.

In the table, we use the following numerical codes:

0 = car autonomous/no driver involved

1 = driver awareness

2 = driver attention

3 = driver reaction necessary

4.1.5 Wireless communication

Wireless Communication (C2C, C2I, and I2C) is involved. Does NOT encompass in-car wireless (e.g. Bluetooth used with mobile or PDA)

4.1.6 Sender/Destination

4.1.6.1 C2C

Car to Car: Car originates communication to other car

4.1.6.2 C2I

Car to Infrastructure: Car originates communication with infrastructure

4.1.6.3 I2C

Infrastructure to Car: Infrastructure originates communication with car

4.1.7 Communication Characteristics

4.1.7.1 Single-Hop

We assume a single-hop range of at least 150m in normal road conditions. In case of curve- or turn-applications, the range may be shorter.

4.1.7.2 Multi-Hop

Multi-Hopping is assumed to be realized by a position-based routing protocol.

4.1.7.3 Relevancy-based

Messages are transported passively, using a content- and situation-based relevancy calculation. With this transport mechanism, messages can be spread in an area even with very low network connectivity.

4.1.7.4 One-way

Messages are sends without response

4.1.7.5 Two-way

Messages are sends with response

4.1.7.6 Periodic

Application encompasses periodic sending of messages. The periodic sending of messaging way be off by default and may be triggered by some external events, like setting the indicators or activating the blue light in an emergency vehicle.

4.1.8 Addressing

4.1.8.1 Unicast

Receiver is a unique network entity (e.g. a vehicle, RSU, Access point etc)

4.1.8.2 Broadcast

Receivers are all network entities that receive a packet.

In case of single-hop: Every receiver in wireless transmission range

In case of multi-hop: TTL-limited flooding

4.1.8.3 Geocast

All network entities receiving a packet must check their own position to decide whether they are intended to process the packet.

In case of single-hop: Only those entities in the defined region are receivers. No relaying.

In case of multi-hop: If already in the target region, flood the packet within the region. If outside the target region, forward the packet to the target region based on routing protocol, then flood.

4.1.9 Time constraints

Application messages are somehow time-critical

Classes:

0.5 = message is highly time-critical (~ 0.5 seconds)

1 = time critical (~ 1 second)

5 = time is relevant (~ 5 seconds)

10 = time is no critical issue (> 10 seconds ok)

4.2 Security Characteristics

4.2.1 Authentication

4.2.1.1 ID authentication

Receiver should be able to verify unique ID of sender.

Alternative term: "Entity authentication"

4.2.1.2 Property authentication

Receiver should be able to verify that sender has a certain property, e.g. sender is a car, a traffic sign, ...

4.2.1.3 Location authentication

Receiver should be able to verify that sender is actually at the claimed position or that message location claim is valid.

4.2.2 Integrity

Receiver should be able to verify that transported information has not been altered between sender and receiver (or in other words, receiver should detect tampered information).

4.2.3 Confidentiality

Sender and receiver want to assure that transported information can not be eavesdropped on its way

4.2.4 Privacy

4.2.4.1 ID privacy

Sender does not want to reveal its identity

4.2.4.2 Location privacy

Sender does not want to reveal its location

0: location information can be freely distributed throughout the network

1: current location information is relevant for neighbouring nodes, collection of sequences of location information for user tracking should be prevented

2: other nodes (knowing the identity of a node) in the network can not retrieve the (exact) location of this node

4.2.4.3 Jurisdictional access

In addition to privacy requirements: Though privacy requirements apply for normal communication, public authorities want to have access to identity or location of node

4.2.5 Availability

Application is sensitive to Denial of service, i.e. availability is critical

4.2.6 Access control

Application needs a somehow fine-grained definition, if and what a user or infrastructure component is allowed to do (e.g. forbid map usage outside Europe).

Another form of access control would be the exclusion of misbehaving nodes from the VANET by certificate revocation or other means, e.g. an intrusion detection system using a trust management scheme.

4.2.7 Auditability

Application needs to track/reconstruct what was going on in the past. This might also include non-repudiation requirements, where senders or receivers can prove that messages have been received or sent respectively. For some applications, messages may only be stored for a very limited time (e.g. the last 10 seconds in a ring buffer) and made permanent only in case of an incident (e.g. crash).

5 Application Requirements Analysis

5.1 Generic Characteristics

							Sender/Dest			Comm. Char.					Addressing			
Application	Gen. Characteristics	Safety-related	Safety critical	In-car	Driver involvement	Wireless communiatio	C2C	C2I	I2C	Single-Hop	Multi-Hop	Relevancy-based	One-way	Two-way	Periodic	Unicast	Broadcast	Geocast	Time constraints
Assist driver with signage																			
Traffic signal violation warning		X	X		3	X			X	X			X		X			X	1,0
Stop sign violation warning		X	X		3	X			X	X			X		X			X	1,0
General in-vehicle signage		X			1	X			X	X			X		X			X	1,0
Assist driver at intersections																			
Left turn assistant		X			2	X	X		X	X			X		X			X	0,5
Intersection collision warning		X	X		3	X	X		X	X			X		X			X	0,5
Pedestrian crossing information		X			2	X	X		X	X			X		X			X	1,0
Assist authorities																			
Emergency vehicle approaching warning		X	X		3	X	X				X		X		X			X	1,0
Emergency vehicle signal preemption		X	X		0	X		X			X			X		X			1,0
Emergency vehicle at scene warning		X	X		2	X	X				X	X	X					X	5,0
Vehicle safety inspection		X		X	0	X	X		X	X				X		X			10,0
Electronic license plate				X	0	X	X		X	X				X		X			10,0
Electronic driver's license				X	0	X	X		X	X				X		X			10,0
In-vehicle Amber alert (crime haunt)					1	X			X	X			X		X		X		10,0
Stolen vehicles tracking				X	0	X	X	X	X	X				X		X	X		10,0
Assist road users upon accident																			
Post-crash/breakdown warning		X	X		2	X	X				X	X	X		X			X	0,5
SOS services		X	X		0	X	X	X			X		X		X	X			5,0
Pre-crash sensing		X	X	X	0	X	X			X			X		X		X		0,5
Event data recording				X	0														10,0
Assist driver on special road conditions																			
Work zone warning		X			2	X			X		X	X	X		X			X	5,0
Curve-speed warning (rollover warning)		X		X	2	X			X	X			X		X			X	1,0
Vehicle-based road condition warning		X			2	X	X				X	X	X		X			X	5,0
Infrastructure-based road condition warning		X			2	X			X		X	X	X		X			X	5,0
Assist on vehicle maintainance																			
Safety recall notice				X	1	X			X	X		X		X		X			10,0
Just-in-time repair notification				X	1	X		X		X				X		X			10,0
Wireless Diagnostics				X	0	X			X	X				X		X			10,0
Software update/flashing				X	0	X			X	X				X		X			10,0
Assist driver in dangerous traffic situations																			
Cooperative (forward) collision warning		X	X		3	X	X				X		X		X			X	0,5
Emergency electronic brake lights		X	X		3	X	X				X		X					X	0,5
Blind spot warning / lane change warning		X	X		2	X	X			X			X		X			X	0,5
Wrong way driver warning		X	X		3	X	X		X		X	X	X		X			X	1,0
Rail collision warning		X	X		2	X	X		X	X			X		X		X		1,0
Assist driver in normal traffic																			
Highway merge assistant		X		X	2	X	X			X			X		X		X		1,0
Visibility enhancer		X			1	X	X			X			X		X			X	1,0
Cooperative adaptive cruise control		X			1	X	X				X		X		X			X	0,5
Cooperative platooning		X	X		0	X	X				X			X	X			X	0,5
Cooperative glare reduction / headlamp aiming		X			0	X	X				X		X		X			X	1,0
Adaptive drivetrain management				X	0	X			X	X			X		X			X	5,0
Improve traffic management																			
Intelligent traffic flow control					0	X		X		X			X		X	X	X		10,0
Road surface conditions to TOC					0	X		X		X			X			X			10,0
Vehicle probes provide weather data to TOC					0	X		X		X			X			X			10,0
Crash data to TOC					0	X		X		X			X			X			10,0
Origin and destination to TOC					0	X		X		X			X			X			10,0
Improve navigation																			
Parking spot locator					1	X		X			X			X	X	X			10,0
Enhanced route guidance and navigation				X	1	X		X		X		X		X		X			10,0
Map download/update				X	0	X		X		X				X		X			10,0
GPS correction				X	0	X			X	X			X		X		X		5,0
Cooperative positioning improvement				X	0	X	X			X			X		X			X	5,0
Improve passenger comfort																			
Instant messaging (between vehicles)					1	X	X				X		X			X			5,0
Point-of-interest notification					1	X			X	X			X				X		10,0
Internet service provisioning / info fueling					1	X		X	X		X			X		X			1,0
Mobile access to vehicle data (PDA, Handy,...)				X	1	X				X				X		X			1,0
Improve vehicle-related services																			
Fleet management					1	X			X	X				X		X			10,0
Area access control					1	X			X	X				X		X			1,0
Electronic payment				X	3	X			X	X				X		X			1,0
Rental car processing				X	1	X			X	X				X		X			5,0
Hazardous material cargo tracking					0	X			X	X				X		X			5,0

5.2 Security Characteristics

		Authentic.					Privacy					
	Security	ID authentication	Property auth.	Location auth.	Integrity	Confidentiality	ID privacy	Location privacy	jurisdictional acc.	Availability	Access control	Auditability
Assist driver with signage												
Traffic signal violation warning		0	2	2	2	0	0	0	0	1	0	1
Stop sign violation warning		0	2	2	2	0	0	0	0	1	0	1
General in-vehicle signage		0	2	2	2	0	0	0	0	1	0	0
Assist driver at intersections												
Left turn assistant		0	2	2	2	0	2	1	0	1	0	1
Intersection collision warning		0	1	2	2	0	2	1	0	1	0	1
Pedestrian crossing information		0	1	1	2	0	2	1	0	1	0	1
Assist authorities												
Emergency vehicle approaching warning		0	2	1	2	0	0	0	0	2	1	2
Emergency vehicle signal preemption		0	2	1	2	0	0	0	0	2	1	1
Emergency vehicle at scene warning		0	2	1	2	0	0	0	0	1	0	0
Vehicle safety inspection		2	0	0	2	2	1	1	1	0	2	1
Electronic license plate		2	0	0	2	2	1	1	1	0	2	1
Electronic driver's license		2	0	0	2	2	1	1	1	0	2	1
In-vehicle Amber alert (crime haunt)		0	2	0	2	1	0	0	0	0	0	0
Stolen vehicles tracking		2	0	0	2	2	0	0	0	1	0	0
Assist road users upon accident												
Post-crash/breakdown warning		0	2	2	2	0	2	0	1	2	0	1
SOS services		2	0	1	2	1	2	0	2	2	0	2
Pre-crash sensing		0	2	2	2	0	2	0	0	2	0	0
Event data recording		1	0	0	2	2	0	0	0	2	2	2
Assist driver on special road conditions												
Work zone warning		0	2	2	2	0	0	0	0	1	0	0
Curve-speed warning (rollover warning)		0	2	2	2	0	0	0	0	1	0	0
Vehicle-based road condition warning		0	2	2	2	0	2	0	1	1	0	0
Infrastructure-based road condition warning		0	2	2	2	0	0	0	0	1	0	0
Assist on vehicle maintainance												
Safety recall notice		2	0	0	2	2	0	0	0	0	2	1
Just-in-time repair notification		2	0	0	2	2	0	0	0	0	2	1
Wireless Diagnostics		2	0	0	2	2	0	0	0	0	2	1
Software update/flashing		2	0	0	2	2	0	0	0	0	2	1
Assist driver in dangerous traffic situations												
Cooperative (forward) collision warning		0	2	2	2	0	2	0	0	2	0	2
Emergency electronic brake lights		0	2	2	2	0	2	0	0	2	0	2
Blind spot warning / lane change warning		0	1	2	2	0	2	0	0	2	0	2
Wrong way driver warning		0	2	2	2	0	2	0	2	2	0	2
Rail collision warning		0	2	2	2	0	0	0	0	2	0	1
Assist driver in normal traffic												
Highway merge assistant		0	1	2	2	0	2	0	0	1	0	1
Visibility enhancer		0	1	2	2	0	2	0	0	1	0	0
Cooperative adaptive cruise control		0	1	2	2	0	2	0	0	1	0	1
Cooperative platooning		0	1	2	2	0	2	0	2	1	0	2
Cooperative glare reduction / headlamp aiming		0	1	1	2	0	2	0	0	1	0	1
Adaptive drivetrain management		0	2	2	2	0	0	0	0	1	0	0
Improve traffic management												
Intelligent traffic flow control		0	2	2	1	0	2	0	0	0	0	0
Road surface conditions to TOC		0	2	2	1	0	2	0	0	0	0	0
Vehicle probes provide weather data to TOC		0	2	2	1	0	2	0	0	0	0	0
Crash data to TOC		1	2	2	1	0	1	0	0	0	0	0
Origin and destination to TOC		0	2	2	1	1	2	1	0	0	0	0
Improve navigation												
Parking spot locator		0	2	1	2	0	2	1	0	1	0	0
Enhanced route guidance and navigation		0	2	1	2	0	2	1	0	1	2	0
Map download/update		0	2	0	2	0	2	1	0	1	2	0
GPS correction		0	2	2	2	0	0	0	0	0	0	0
Cooperative positioning improvement		0	2	2	2	0	2	0	0	0	0	0
Improve passenger comfort												
Instant messaging (between vehicles)		2	0	0	2	2	1	1	0	0	0	0
Point-of-interest notification		0	0	0	2	0	0	0	0	0	0	0
Internet service provisioning / info fueling		2	0	0	2	2	2	2	0	0	1	0
Mobile access to vehicle data (PDA, Handy,...)		2	0	0	2	2	0	0	0	0	2	0
Improve vehicle-related services												
Fleet management		2	0	0	2	2	0	0	0	1	2	1
Area access control		2	0	1	2	2	0	0	0	2	2	2
Electronic payment		2	0	0	2	2	1	0	0	1	2	2
Rental car processing		2	0	0	2	1	0	0	0	1	0	1
Hazardous material cargo tracking		2	0	0	2	2	0	0	0	1	0	2

5.3 Cluster Results

Application	Cluster	Distance
Assist driver with signage		
Traffic signal violation warning	8	1,0783
Stop sign violation warning	8	1,0783
General in-vehicle signage	8	0,9651
Assist driver at intersections		
Left turn assistant	4	1,4985
Intersection collision warning	4	1,5273
Pedestrian crossing information	4	1,7059
Assist authorities		
Emergency vehicle approaching warning	8	2,5158
Emergency vehicle signal preemption	8	2,4713
Emergency vehicle at scene warning	8	1,872
Vehicle safety inspection	5	1,2067
Electronic license plate	5	1,1429
Electronic driver's license	5	1,1429
In-vehicle Amber alert (crime haunt)	2	1,7985
Stolen vehicles tracking	2	2,3675
Assist road users upon accident		
Post-crash/breakdown warning	4	1,2230
SOS services	1	0,0000
Pre-crash sensing	4	2,2704
Event data recording	7	2,3909
Assist driver on special road conditions		
Work zone warning	8	1,0429
Curve-speed warning (rollover warning)	8	1,1808
Vehicle-based road condition warning	4	1,6551
Infrastructure-based road condition warning	8	1,0429
Assist on vehicle maintainance		
Safety recall notice	7	1,0047
Just-in-time repair notification	7	1,0047
Wireless Diagnostics	7	1,0393
Software update/flashing	7	1,0393
Assist driver in dangerous traffic situations		
Cooperative (forward) collision warning	4	1,4830
Emergency electronic brake lights	4	1,7510
Blind spot warning / lane change warning	4	1,4244
Wrong way driver warning	4	2,2503
Rail collision warning	8	1,8196
Assist driver in normal traffic		
Highway merge assistant	4	1,8194
Visibility enhancer	4	1,5584
Cooperative adaptive cruise control	4	1,0476
Cooperative platooning	4	2,3141
Cooperative glare reduction / headlamp aiming	4	1,4501
Adaptive drivetrain management	8	1,4608
Improve traffic management		
Intelligent traffic flow control	6	1,2152
Road surface conditions to TOC	6	0,7872
Vehicle probes provide weather data to TOC	6	0,7872
Crash data to TOC	6	1,4311
Origin and destination to TOC	6	1,3276
Improve navigation		
Parking spot locator	6	2,1345
Enhanced route guidance and navigation	3	0,527
Map download/update	3	0,527
GPS correction	8	2,1527
Cooperative positioning improvement	6	2,2228
Improve passenger comfort		
Instant messaging (between vehicles)	5	2,2132
Point-of-interest notification	2	1,6025
Internet service provisioning / info fueling	5	2,0086
Mobile access to vehicle data (PDA, Handy,...)	7	1,8428
Improve vehicle-related services		
Fleet management	7	1,0047
Area access control	7	2,008
Electronic payment	7	1,5992
Rental car processing	7	1,9576
Hazardous material cargo tracking	7	1,9984

5.4 Sorted Cluster Results

Application	Cluster	Distance
SOS services	1	0,0000
In-vehicle Amber alert (crime haunt)	2	1,7985
Stolen vehicles tracking	2	2,3675
Point-of-interest notification	2	1,6025
Enhanced route guidance and navigation	3	0,527
Map download/update	3	0,527
Left turn assistant	4	1,4985
Intersection collision warning	4	1,5273
Pedestrian crossing information	4	1,7059
Post-crash/breakdown warning	4	1,2230
Pre-crash sensing	4	2,2704
Vehicle-based road condition warning	4	1,6551
Cooperative (forward) collision warning	4	1,4830
Emergency electronic brake lights	4	1,7510
Blind spot warning / lane change warning	4	1,4244
Wrong way driver warning	4	2,2503
Highway merge assistant	4	1,8194
Visibility enhancer	4	1,5584
Cooperative adaptive cruise control	4	1,0476
Cooperative platooning	4	2,3141
Cooperative glare reduction / headlamp aiming	4	1,4501
Vehicle safety inspection	5	1,2067
Electronic license plate	5	1,1429
Electronic driver's license	5	1,1429
Instant messaging (between vehicles)	5	2,2132
Internet service provisioning / info fueling	5	2,0086
Intelligent traffic flow control	6	1,2152
Road surface conditions to TOC	6	0,7872
Vehicle probes provide weather data to TOC	6	0,7872
Crash data to TOC	6	1,4311
Origin and destination to TOC	6	1,3276
Parking spot locator	6	2,1345
Cooperative positioning improvement	6	2,2228
Event data recording	7	2,3909
Safety recall notice	7	1,0047
Just-in-time repair notification	7	1,0047
Wireless Diagnostics	7	1,0393
Software update/flashing	7	1,0393
Mobile access to vehicle data (PDA, Handy,...)	7	1,8428
Fleet management	7	1,0047
Area access control	7	2,008
Electronic payment	7	1,5992
Rental car processing	7	1,9576
Hazardous material cargo tracking	7	1,9984
Traffic signal violation warning	8	1,0783
Stop sign violation warning	8	1,0783
General in-vehicle signage	8	0,9651
Emergency vehicle approaching warning	8	2,5158
Emergency vehicle signal preemption	8	2,4713
Emergency vehicle at scene warning	8	1,872
Work zone warning	8	1,0429
Curve-speed warning (rollover warning)	8	1,1808
Infrastructure-based road condition warning	8	1,0429
Rail collision warning	8	1,8196
Adaptive drivetrain management	8	1,4608
GPS correction	8	2,1527

6 Application Use Case Analysis

6.1 Reference Applications

As shown in the sorted cluster analysis (chapter 5.4) we have selected the following 10 applications as references for the Use Case Analysis:

- SOS services
- Stolen vehicles tracking
- Map download/update
- Intersection collision warning
- Vehicle-based road condition warning
- Electronic license plate
- Road surface conditions to TOC
- Software update/flashing
- Emergency vehicle signal pre-emption
- Work zone warning

These Application Use Cases will be described in more details based on the following template:

Use Case	
Creator	
Goal in Context	
Scope & Level	Application use case
Preconditions	
Success End Condition	
Failed End Condition	
Involved components (Any logical components, both hardware and software that are involved in application implementation)	
Trigger	
Operation description (Complete textual description of application operation)	

Characteristics	

Safety relation	No relation		Safety relevant		Safety critical			
In-car system								
Driver involvement								
Communication	C2C		C2I		I2C			
	One-way		Two-way		Single-Hop		Multi-Hop	
	Unicast		Broadcast		Geocast		Relevancy	
Timing	Timing constraints				Periodic messages			
Security requirements								
ID Authentication								
Property auth.								
Location auth.								
Integrity								
Confidentiality								
ID privacy								
Location Privacy								
Jurisdict. Access								
Availability								
Access control								
Auditability								

Threats	**Criteria**	
	Motivation	
	Target	
	Skill of attacker	
	Technical effort	
Classification of risks		

Description of Threat Criteria

Threats Motivation	What is or could be the motivation of the attacker • "fame" • money • joke • harm • ...
Threat Target:	• who: User/Driver, Vehicle, OEM, VANET communication system, infrastructure, application, • what: Privacy, Health, system function, Finances...
Skill of the Attacker:	• low (e.g. script kiddies) • mid (experienced user) • high (expert)

Technical effort:	• Direct physical vehicle access (Garage or User/Driver) • Wireless access (Local VANET or Remote (Internet))
Classification of risk:	• low • mid • high

6.2 SOS services

Use Case	SOS services
Creator	Tamás Holczer and Laszlo Csik, BUTE
Goal in Context	Car 2 Car or Car to Infrastructure application
Scope & Level	Application use case
Preconditions	Airbags are deployed, a rollover is sensed, or the vehicle otherwise senses a life-threatening emergency.
Success End Condition	The emergency message is forwarded to the nearest local authority for immediate assistance.
Failed End Condition	The local authority does not receive the emergency message.
Involved components (Any logical components, both hardware and software that are involved in application implementation)	Sensors (sense the accident) On board unit (put the message together, send the message) Tamper proof hardware (sign the message) Communication interface (send the message)
Trigger	Airbags are deployed, a rollover is sensed, or the vehicle otherwise senses a life-threatening emergency.
Operation description (Complete textual description of application operation)	After an accident car C sends an emergency message to the nearest local authority. The route of the message can be many kinds. The message can be sent directly to a Road Side Unit (RSU). If no RSU is reachable, then C broadcasts the emergency message to cars in range. Each of them tries to forward the message to a RSU, or hops the message. The RSU forwards the message directly to the nearest local authority.

Characteristics								
Safety relation	No relation		Safety relevant	x	Safety critical	x		
In-car system	In-car system not involved, just triggers							
Driver involvement	No driver involvement needed							
Communication	C2C	x	C2I	x	I2C			
	One-way	x	Two-way		Single-Hop		Multi-Hop	x
	Unicast	x	Broadcast		Geocast		Relevancy	
Timing	Timing constraints		x	Periodic messages				
	Timing constraint: time relevant (~5 sec)							
Security requirements								
ID Authentication	2, ID authentication is needed to avoid forged alerts							

Property auth.	0, No property authentication required
Location auth.	1, Location of car C should be authenticated to avoid forged alerts.
Integrity	2, Integrity of the message must be ensured to avoid misleading alerts.
Confidentiality	1, The alert message can be encrypted (optional), only the ID and place must be hidden.
ID privacy	2, The ID of car C must be hidden from the other users.
Location privacy	0, No location privacy required
Jurisdict. Access	2, Public authorities must access the place and ID data of the accident.
Availability	2, This application should always be available anywhere, anytime.
Access control	0, Everyone should access the application, no access control needed.
Auditability	2, Car C should be able to prove, that he called the ambulance. Car M should be able to prove, that he forwarded the message to an RSU.

Threats	**Criteria**	
	Motivation	Fame, joke, flood local authority with alerts, harm user
	Target	Application, User
	Skill of attacker	Low-Mid
	Technical effort	Wireless access Physical access
Classification of risks	Low-mid	

6.3 Stolen vehicles tracking

Use Case	Stolen vehicle tracking
Creator	Cosenza Stefano, Centro Ricerche FIAT
Goal in Context	I2C and C2I application to individuate an eventual stolen vehicle and to track, consequently, its position.
Scope & Level	Application use case
Preconditions	The licence plate of the stolen car or any other unique characteristic (chassis number) is present in police database.
Success End Condition	The vehicle is recognised by a node of the infrastructure
Failed End Condition	The vehicle is not recognised by a node of the infrastructure (the identity could be hide)
Involved components (Any logical components, both hardware and software that are involved in application implementation)	Electronic licence plate mounted on the car, in alternative the licence plate or the chassis number should be reported in the messages exchanged between the car and the infrastructure. A specific inquiry can be sent by the infrastructure, to know the licence plate/chassis number from the on coming vehicles. A specific box (as a black box) should reply to the inquiries coming from the node for legal reason.
Trigger	The passage of the vehicle nearby nodes of the infrastructure.

Operation description (Complete textual description of application operation)	All the node near the borders of the city and some specific or random nodes can be dedicated to inquiry the vehicles passing by. A node sends a periodic message, asking for the licence plate and/or chassis number of the vehicle. The answer from the vehicle is compared with the data contained in stolen vehicle police database. If the comparison has a success, then all the nodes around the first one can be activate to track the stolen car. The "stolen car" can be informed by the infrastructure of its condition and since that moment it can pass its position to all nodes and vehicles it crosses.

Characteristics								
Safety relation	No relation	X	Safety relevant		Safety critical			
In-car system	Yes							
Driver involvement	No							
Communication	C2C	X	C2I	X	I2C	X		
	One-way		Two-way	X	Single-Hop	X	Multi-Hop	
	Unicast	X	Broadcast	X	Geocast		Relevancy	
Timing	Timing constraints				Periodic messages			
Security requirements								
ID Authentication	2							
Property auth.	0 Not relevant							
Location auth.	0							
Integrity	2 the integrity of the messages must be guaranteed							
Confidentiality	2 the data exchanged are strictly private							
ID privacy	0 Not so important							
Location privacy	1							
Jurisdict. Access	2 The authorities have access to some specific information on the vehicle							
Availability	1 Some random point can be dedicated to inquiry the vehicles							
Access control	1							
Auditability	2							

Threats	**Criteria**	
	Motivation	Joke (if it is not real), money
	Target	All the vehicles
	Skill of attacker	High
	Technical effort	Wireless
Classification of risks	Low-medium	

6.4 Map download/update

Use Case	Map download/update
Creator	Albert Held and Rainer Kroh, DaimlerChrysler

Goal in Context	The car navigation system can download up-to-date maps from the Service Centre
Scope & Level	Application use case
Preconditions	Navigation system is running Service Centre in the infrastructure is available Communication link vehicle<->infrastructure is available
Success End Condition	Downloaded/updated map could be used
Failed End Condition	Downloaded/updated map could not be used
Involved components (Any logical components, both hardware and software that are involved in application implementation)	Communication unit Navigation system Download server
Trigger	User activates download/update function
Operation description (Complete textual description of application operation)	The user, the vehicle system or the service centre detects that the map of the navigation system should be updated. The vehicle security system checks the rights of the user/navigation system to communicate to the service centre. The service centre checks the access rights of the user/navigation system and the navigation system loads the map. If no new map data are available – the map in the vehicle is up-to-date – the service centre sends a special “no update available” message to the navigation system. The navigation system installs the new/updated map. The navigation system returns a “map data up-to-date” message.

Characteristics								
Safety relation	No relation		Safety relevant		Safety critical			
In-car system	X							
Driver involvement	Car autonomous or driver awareness							
Communication	C2C		C2I	X	I2C	X		
	One-way		Two-way	X	Single-Hop	X	Multi-Hop	
	Unicast	X	Broadcast		Geocast		Relevancy	
Timing	Timing constraints			>10s	Periodic messages			
Security requirements								
ID Authentication	0							
Property auth.	2							
Location auth.	0							
Integrity	2							
Confidentiality	0							
ID privacy	2							
Location privacy	1							
Jurisdict. Access	0							
Availability	1							

Access control	2
Auditability	0

Threats	**Criteria**	
	Motivation	Money (Joke)
	Target	Navigation system
	Skill of attacker	Mid-high
	Technical effort	Wireless access
Classification of risks	mid	

6.5 Intersection collision warning

Use Case	Intersection collision warning
Creator	Mateusz Masiukiewicz, Hans-J. Reumerman, Philips
Goal in Context	Warn vehicles of imminent collision with other vehicles or vulnerable road users at a signalled or non-signalled intersections using Car 2 car / Infrastructure 2 car application
Scope & Level	Application use case
Preconditions	Vehicles are equipped with navigation system (road maps); they frequently send beacon messages. Intersections are equipped with sensors to detect vulnerable road users.
Success End Condition	Driver receives warning (information) about other cars heading to the intersection, or vulnerable road users to consider
Failed End Condition	Driver receives no warning (information) about (a) other cars heading for the intersection or (b) unexpected presence of vulnerable road users.
Involved components (Any logical components, both hardware and software that are involved in application implementation)	Radar Sensors, cameras etc. to detect if intersection is occupied Wireless radio in every car Wireless radio in intersection equipment or variable traffic signs and traffic sign recognition in vehicle Navigation system (road maps + positioning system) in every car Traffic Rule base to decide upon right of way
Trigger	Navigation system sends message about approaching intersection Intersection signals unexpected obstacle (either through variable message sign or wireless link)
Operation description (Complete textual description of application operation)	Navigation system sends message about approaching intersection. Application checks if car has right of way on this intersection or not. Car gathers beacon messages from other nodes and send beacon by itself. By beacon messages analysis application creates intersection state, analyse driver's behaviour and car state (if turn indication is on, on which lane car is heading, speed, velocity). Knowing intersection state, car condition and right of way on this intersection application displays information "ok" or warning. Warning message depends on intersection state, e.g. "stop", "car on right", "fast heading from left". Cars can signal their intended driving direction to the intersection infrastructure Road infrastructure can also be used, especially when local road intersect with main road. Then car receives intersection state from infrastructure.

Characteristics												
Safety relation	No relation		Safety relevant		x	Safety critical		X				
In-car system	(cameras and traffic sign recognition)											
Driver involvement	3 – driver reaction is necessary											
Communication	C2C		X	C2I		?	I2C		X			
	One-way	X	Two-way		Single-Hop		X	Multi-Hop				
	Unicast		Broadcast		Geocast		X	Relevancy				
Timing	Timing constraints			0,5s	Periodic messages				X			
	Highly time critical											
Security requirements												
ID Authentication	0 – No											
Property auth.	1- Yes – beacon messages must come from a car or RSU only											
Location auth.	2- Yes – beacon message and application warning/information are valid only locally											
Integrity	2 – Yes – beacon message cannot be changed (especially position, speed, direction data)											
Confidentiality	0 – No											
ID privacy	2 – Yes – privacy must be guaranteed											
Location Privacy	1 – Yes – location privacy should be guaranteed (no tracking possible)											
Jurisdict. Access	0 – No											
Availability	1 – Yes											
Access control	0 – No											
Auditability	1 - Yes											

Threats	Criteria	
	Motivation	Joke, harm, get right of way
	Target	Vehicle safety
	Skill of attacker	High (for wireless access), Low (for disabling sensors and traffic signs)
	Technical effort	Wireless access to car or RSU, manipulate sensors, disable variable traffic signs
Classification of risks	high	

6.6 Vehicle-based road condition warning

Use Case	Vehicle-based road condition warning
Creator	Frank Kargl, UULM
Goal in Context	Vehicles that detect hazardous road conditions send warnings to other approaching vehicles, so that their drivers can adapt their behaviour accordingly.
Scope & Level	Application use case
Preconditions	None
Success End Condition	Drivers receive warnings before reaching hazardous road segments
Failed End Condition	System fails to warn drivers

Involved components (Any logical components, both hardware and software that are involved in application implementation)	Sensors for detection of hazardous road conditions, e.g. - ABS, ASR, or ESP/VSC sensors can detect slippery or icy roads - rain sensors that are used for starting the wipers can detect wet roads On-board processing and wireless communication units
Trigger	Sensors detecting potential hazardous road conditions
Operation description (Complete textual description of application operation)	Sensors constantly monitor road conditions and create a risk-estimation for multiple classes of hazards (e.g. slippery road, wet road, strong wind …). When at least one of these parameters exceeds a given threshold, the car starts emitting geocast messages that are sent to all nearby road segments which lead to this position. The messages contain the risk-estimations for all hazard-classes. Vehicles receiving such a message will forward the message according to the general geocast-/relevancy-based-forwarding strategy. Vehicles receiving such a message will additionally issue an optical/acoustical warning to the driver. Options: - The warning might be modulated according to the estimated strength of the hazard contained in the message. - Vehicles may apply consistency checks with own sensors or messages received from other cards to detect false-alarms.

Characteristics								
Safety relation	No relation		Safety relevant	X	Safety critical			
In-car system								
Driver involvement								
Communication	C2C	X	C2I		I2C			
	One-way	X	Two-way		Single-Hop		Multi-Hop	X
	Unicast		Broadcast		Geocast	X	Relevancy	X
Timing	Timing constraints			5s	Periodic messages			X
Security requirements								
ID Authentication	0							
Property auth.	2							
Location auth.	2							
Integrity	2							
Confidentiality	0							
ID privacy	2							
Location privacy	0							
Jurisdict. Access	1							
Availability	1							
Access control	0							
Auditability	0							

Threats	**Criteria**	
Forging of warnings	Motivation	Joke, Vandalism
	Target	Driver
	Skill of attacker	Low

	Technical effort	Wireless Access
Suppression of warnings	Motivation	Joke, Vandalism, Harm
	Target	Driver
	Skill of attacker	Low
	Technical effort	Wireless Access
Classification of risks	low-medium	

6.7 Electronic license plate

Use Case	Electronic License Plate (ELP) reading
Creator	Panos Papadimitratos, EPFL
Goal in Context	Infrastructure (roadside/static or mobile) queries vehicles to obtain their ELP
Scope & Level	Application use case
Preconditions	Assignment of identity and credentials to vehicles
Success End Condition	The queried vehicle returns its ELP number
Failed End Condition	Forged or stolen or no ELP is acquired by the querying infrastructure unit.
Involved components (Any logical components, both hardware and software that are involved in application implementation)	On-board processing and wireless communication units, infrastructure processing and communication units.
Trigger	Varies; vehicle approaching the infrastructure, or vehicle requests a service, or vehicle violates a rule.
Operation description (Complete textual description of application operation)	• Infrastructure generates a ELP request message (ELP-REQ); message is signed • Infrastructure transmits the ELP-REQ, which can be targeted to a specific vehicle or all vehicles receiving the message • Vehicle receives and validates ELP-REQ; if successful (authentic, recent), vehicle returns its ELP encrypted (Step (3) for each of the vehicles that received ELP-REQ in case of a broadcast/geocast).

Characteristics								
Safety relation	No relation	x	Safety relevant		Safety critical			
In-car system	Yes							
Driver involvement	No							
Communication	C2C	x	C2I	x	I2C	x		
	One-way		Two-way	x	Single-Hop	x	Multi-Hop	
	Unicast	x	Broadcast		Geocast		Relevancy	

Timing	Timing constraints	x	Periodic messages	
Security requirements				
ID Authentication	2			
Property auth.	0			
Location auth.	0			
Integrity	0			
Confidentiality	0			
ID privacy	1			
Location privacy	1			
Jurisdict. Access	1			
Availability	0			
Access control	2			
Auditability	1			

Threats	**Criteria**	
	Motivation	Vehicle tracking, impersonation.
	Target	Vehicle identity.
	Skill of attacker	Varies. Depends on system implementation.
	Technical effort	Varies. Depends on system implementation.
Classification of risks	High.	

6.8 Road surface conditions to TOC

Use Case	Road surface conditions to Transportation Operation Centres
Creator	Antonio Kung, Trialog
Goal in Context	Vehicles send current location along with status of specific on-board sensors (e.g., traction control, anti-lock braking, transmission speed, etc.) and an activation history of vehicle control devices (steering, brakes, etc.) to the Transportation Operations Center which processes these data to determine road surface conditions at vehicle location
Scope & Level	Application use case
Preconditions	Vehicle is equipped a list of on-board sensors and is either logging information on current location and surface conditions or can do it in real-time Interworking standards for road surface condition descriptions put in place
Success End Condition	Road surface conditions have been transmitted
Failed End Condition	Properties or location not authenticated
Involved components (Any logical components, both hardware and software that are involved in application implementation)	Transportation operations center Roadside equipment On-board unit with wireless communication unit On-board sensors Control activation logging system (e.g. steering./brake/windshield/… events)

Trigger	Vehicle is in the range of a roadside equipment
Operation description (Complete textual description of application operation)	• Vehicle and Roadside equipment create a communication link, with property and location authentication capability • Vehicle sends location information and surface condition data. In order to cope with the wide range of sensors that could be available in a vehicle (high-end very accurate sensors available in trucks versus low-cost sensors in mid-size vehicles), a category property is added. • Vehicle optionally sends information on vehicle control devices. • Optionally, possibly on request from roadside equipment, and if the vehicle has appropriate storage capability, vehicle sends surface condition data on previous zone (e.g. to cope with the fact that the beacon 2 km before is out of order).

Characteristics								
Safety relation	No relation	X	Safety relevant		Safety critical			
In-car system	No							
Driver involvement	No							
Communication	C2C		C2I		X	I2C		
	One-way	X	Two-way		Single-Hop	X	Multi-Hop	
	Unicast	X	Broadcast		Geocast		Relevancy	
Timing	Timing constraints			>10 s	Periodic messages			
Security requirements								
ID Authentication	0							
Property auth.	2							
Location auth.	2							
Integrity	1							
Confidentiality	0							
ID privacy	2							
Location Privacy	0							
Jurisdict. Access	0							
Availability	0							
Access control	0							
Auditability	0							

Threats	**Criteria**	
• Forging of road conditions • Denying information	Motivation	Joke, harm
	Target	(who) Infrastructure (what) operation
	Skill of attacker	Medium
	Technical effort	Wireless Access

Classification of risks	Low-medium

6.9 Software update/flashing

Use Case	Software update/flashing
Creator	Albert Held, Rainer Kroh, DaimlerChrysler
Goal in Context	Download and update software, data and configurations of the vehicle system with a control centre to keep the vehicle components up-to-date
Scope & Level	Application use case
Preconditions	Vehicle-system is running Vehicle does not move Control Centre in the infrastructure is available Communication link vehicle <-> infrastructure is available
Success End Condition	New SW can be used, new configuration is activated
Failed End Condition	New SW / data / configuration cannot be used
Involved components (Any logical components, both hardware and software that are involved in application implementation)	Communication unit On-boar processing unit Memory unit (Flash, disk, …) Download Server
Trigger	User activates download and update function
Operation description (Complete textual description of application operation)	The user, the vehicle system or the control centre detects that the software or configuration of the vehicle should be updated. The vehicle system connects to the control centre. The control centre checks the access rights of the user/vehicle and the vehicle system could load the SW/configuration. The vehicle security system checks rights / licenses associated with the downloaded SW / configuration and enable the usage of SW / configuration. The vehicle system performs a backup of the current data/configuration (but only from the affected parts) and installs the new components. Afterwards the vehicle system performs a self test, assess the current SW/configuration and finishes with the information for the user that the update was successful

Characteristics								
Safety relation	No relation	X	Safety relevant		Safety critical			
In-car system	X							
Driver involvement	Car autonomous or driver awareness							
Communication	C2C		C2I	X	I2C	X		
	One-way		Two-way	X	Single-Hop	X	Multi-Hop	
	Unicast	X	Broadcast		Geocast		Relevancy	
Timing	Timing constraints				Periodic messages			
Security requirements								
ID Authentication	2							
Property auth.	0							

Location auth.	0
Integrity	2
Confidentiality	2
ID privacy	0
Location privacy	0
Jurisdict. Access	0
Availability	0
Access control	2
Auditability	1

Threats	**Criteria**	
	Motivation	Money, (Joke)
	Target	Vehicle system functions
	Skill of attacker	Mid-High
	Technical effort	Direct physical access, Wireless access
Classification of risks	high	

6.10 Emergency vehicle signal pre-emption

Use Case	Emergency vehicle signal pre-emption
Creator	Mateusz Masiukiewicz and Hans-J. Reumerman, Philips
Goal in Context	Emergency vehicles can control traffic lights, dynamic lane marks or other infrastructure elements to avoid or escape from traffic jams and accelerate the time of arrival at an emergency scene or hospital
Scope & Level	Application use case
Preconditions	Emergency vehicle is registered in system. Infrastructure elements are directly or indirectly controlled by emergency vehicle. Emergency vehicle uses standard emergency flashers and standard traffic rules apply
Success End Condition	Emergency vehicle changes right of way from traffic signals in its direction of travel.
Failed End Condition	Emergency vehicle doesn't change right of way from traffic signals in its direction of travel.
Involved components (Any logical components, both hardware and software that are involved in application implementation)	Wireless radio Road side unit attached to infrastructure Navigation system incl. up to date traffic situation route planning software considering signal pre-emption options
Trigger	Turning on emergency vehicle's siren.

Operation description (Complete textual description of application operation)	Navigation system or emergency control centre advices optimal route considering signal pre-emption options. Emergency vehicle (EV) heading to intersection with traffic lights communicate either directly with traffic lights' RSU or indirectly via other vehicles using a Multi-Hop link. EV is being authorized by RSU and traffic lights are changed.

Characteristics								
Safety relation	No relation		Safety relevant	x	Safety critical	X		
In-car system	No							
Driver involvement	No							
Communication	C2C		C2I	X	I2C			
	One-way		Two-way	X	Single-Hop		Multi-Hop	X
	Unicast	X	Broadcast		Geocast		Relevancy	
Timing	Timing constraints			1,0s	Periodic messages			
	Less time critical							
Security requirements								
ID Authentication	0 – no - RSU doesn't need to know real ID of a car, just must be sure that car is allowed to use this service							
Property auth.	2 – yes - RSU must be sure that it's communicating with emergency vehicle or received valid identifier from EV through ordinary car							
Location auth.	1 – yes – application is location sensitive							
Integrity	2 – yes							
Confidentiality	0 – no							
ID privacy	0 – no							
Location Privacy	0 – no							
Jurisdict. Access	0 – no							
Availability	2 – yes – availability is critical, if signal pre-emption option is indicated to route planner							
Access control	1 – only dedicated vehicles may use this application							
Auditability	1 - yes							

Threats	**Criteria**	
	Motivation	Time, joke, harm, gain right of way, minimize travel time
	Target	human life, traffic control
	Skill of attacker	High
	Technical effort	Wireless access
Classification of risks	Medium (compared to current risks of emergency drivers), High (for hacker faking an EV and confusing traffic control)	

6.11 Work zone warning

Use Case	Workzone warning
Creator	Frank Kargl, UULM
Goal in Context	Delivers a warning and additional information on a work zone to cars. Data could include speed limit, lane closures/changes, etc.
Scope & Level	Application use case
Preconditions	None
Success End Condition	Drivers receive warnings before reaching workzone
Failed End Condition	System fails to warn drivers
Involved components (Any logical components, both hardware and software that are involved in application implementation)	Infrastructure at workzone site with wireless communication unit. On-board processing and wireless communication units Warning mechanism
Trigger	None (periodic activity at workzone site)
Operation description (Complete textual description of application operation)	The communication unit at the workzone site periodically emits geocast messages that are sent to all nearby road segments which lead to this position. The messages contain information on the workzone, like speed limits, lane closures/changes, etc. Vehicles receiving such a message will forward the message according to the general geocast-/relevancy-based-forwarding strategy. Vehicles receiving such a message will additionally issue an optical/acoustical warning to the driver.

Characteristics								
Safety relation	No relation		Safety relevant	X	Safety critical			
In-car system								
Driver involvement								
Communication	C2C		C2I		I2C			X
	One-way	X	Two-way		Single-Hop		Multi-Hop	X
	Unicast		Broadcast		Geocast	X	Relevancy	X
Timing	Timing constraints			5s	Periodic messages			X
Security requirements								
ID Authentication	0							
Property auth.	2							
Location auth.	2							
Integrity	2							
Confidentiality	0							
ID privacy	0							
Location privacy	0							
Jurisdict. Access	0							
Availability	1							
Access control	0							

Auditability	0

Threats	**Criteria**	
Forging of warnings	Motivation	Joke, Vandalism
	Target	Driver
	Skill of attacker	Low
	Technical effort	Wireless Access
Suppression of warnings	Motivation	Joke, Vandalism, Harm
	Target	Driver
	Skill of attacker	Low
	Technical effort	Wireless Access
Classification of risks	low-medium	

7 Attack Use Case Analysis

As described in 2.2.7 a detailed descriptions of various attacks on the reference applications will be specified. The attack descriptions should allow finding weaknesses in the application scenarios.

7.1 SOS services

Use Case	**Forging of SOS Messages**							
Related appl. use case	SOS services							
Creator	Tamas Holczer, BUTE							
Primary Attack Goal	DoS	X	Inform. Theft		Intrusion		Tampering	
Used Techniques	Masquer.		Eavesdrop.		Auth. Violation		Loss/Modific.	
	Repudiat.		Forgery	X	Sabotage			
Goal in Context **(Textual description of attackers goal/motivation)**	Local authority may be alerted. Ambulance, fire department, and police may be called without reason.							
Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Wireless communication							
Pre-requirements for attack	Wireless communication equipment, capable of creating and sending forged messages							
Attack description (Complete textual description of attack operation)	Attacker places itself near the target area and emits forged messages. The local authority receives SOS message and sends the ambulance and/or other departments to the location of the forged accident. If occurs a real accident in the vicinity meanwhile, then the ambulance can not help there. If many forged alerts emitted in different places, then the local authority can not notice the real problems.							
Attack success factors **(Reasons why attack may succeed)**	Local authority receives SOS message, and sends the ambulance to the location.							
Attack failure factors **(Reasons why attack may fail)**	Local authority may be able to detect false alerts.							
Effects of attack **(regarding driver and road traffic)**	The attack will cause a denial of service at the ambulance; no help arrives to real accidents.							
Severity	low	X	medium		high		fatal	

Use Case	**Eavesdropping of SOS Messages**							
Related appl. use case	SOS services							
Creator	Tamás Holczer, BUTE							
Primary Attack Goal	DoS		Inform. Theft	X	Intrusion		Tampering	
Used Techniques	Masquer.		Eavesdrop.	X	Auth. Violation		Loss/Modific.	
	Repudiat.		Forgery		Sabotage			
Goal in Context **(Textual description of attackers goal/motivation)**	An eavesdropper can collect information about accidents in its vicinity.							

Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Wireless communication							
Pre-requirements for attack	Wireless communication equipment, capable of interpret of SOS messages.							
Attack description (Complete textual description of attack operation)	Attacker places itself near the target area and eavesdrop SOS messages. From the messages it can deduce the place the time, and most importantly the victim of the accident.							
Attack success factors (Reasons why attack may succeed)	The identity of the victim of the accident is not hidden in the SOS message.							
Attack failure factors (Reasons why attack may fail)	The identity of the victim of the accident is hidden in the SOS message.							
Effects of attack (regarding driver and road traffic)	The anonymity of the persons involved in the accident is violated.							
Severity	low	X	medium		high		fatal	

Use Case	**Blocking SOS Messages (DoS)**							
Related appl. use case	SOS services							
Creator	Tamás Holczer, Laszlo Csik - BUTE							
Primary Attack Goal	DoS	X	Inform. Theft		Intrusion		Tampering	X
Used Techniques	Masquer.		Eavesdrop.		Auth. Violation		Loss/Modific.	X
	Repudiat.		Forgery		Sabotage		DoS	X
Goal in Context (Textual description of attackers goal/motivation)	Attacker tries to prevent SOS messages to reach local authority, in order to delay the arrival of Police, Ambulance or Fire department.							
Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Wireless communication, Road side units							
Pre-requirements for attack	Wireless jamming equipment or physical attack against a road side unit							
Attack description (Complete textual description of attack operation)	The Attacker places itself near the target area and tries to interfere with the wireless signals in order to jam all wireless communication. Other solution can be to shade the sender or / and the receiver interface. The goal of the attacker is to prevent SOS messages to reach local authorities which might delay the arrival of the ambulance / police.							
Attack success factors (Reasons why attack may	The SOS message cannot reach Local Authority							

succeed)								
Attack failure factors (Reasons why attack may fail)	Another car may inform local authority							
Effects of attack (regarding driver and road traffic)	The attack causes delay in the emergency service, which might be dangerous.							
Severity	low	X	medium		high		fatal	

7.2 Stolen vehicles tracking

Use Case	**Denial of Service**							
Related appl. use case	Stolen vehicles tracking							
Creator	Stefano Cosenza, CRF							
Primary Attack Goal	DoS	X	Inform. Theft		Intrusion	X	Tampering	
Used Techniques	Masquer.		Eavesdrop.		Auth. Violation		Loss/Modific.	
	Repudiat.		Forgery		Sabotage	X		
Goal in Context (Textual description of attackers goal/motivation)	To interrupt the communication and the exchange of information to hide the vehicle.							
Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	To interrupt the service there could be several options: Physically turn off the ECU dedicated to the communication. Bypass the ECU to guarantee the functionality of the in – vehicle network To modify/substitute the software (wireless/wired equipment).							
Pre-requirements for attack	Wireless/wired communication equipment Direct access to the electrical cable of the vehicle							
Attack description (Complete textual description of attack operation)	Attacker has the possibility to access the vehicle. From the inside the attacker can operate on the system and in particular on the communication engine, inhibiting either the power supply or the SW to communicate, or manipulating the HW so to guarantee the functionality of the vehicle.							
Attack success factors (Reasons why attack may succeed)	The communication is inhibited							
Attack failure factors (Reasons why attack may fail)	Dedicated electronic control units (not attacked) continue to communicate with the infrastructure, sending messages containing data about licence plate or chassis number. The SW modifications are not able to inhibit the communication.							
Effects of attack (regarding driver and road traffic)	The vehicle does not respond to any interrogation from the infrastructure or the other vehicles: it is not possible to track its position.							
Severity	low		Medium	X	high		fatal	

Use Case	**Masquerade/impersonate as another vehicle**
Related appl. use case	Stolen vehicle tracking
Creator	Stefano Cosenza, CRF

Primary Attack Goal	DoS		Inform. Theft		Intrusion		Tampering	
Used Techniques	Masquer.	X	Eavesdrop.		Auth. Violation		Loss/Modific.	
	Repudiat.		Forgery		Sabotage	X		
Goal in Context **(Textual description of attackers goal/motivation)**	To stole a vehicle.							
Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Wireless communication equipment; SW modification of the original data; HW modification of the original data (substitution of the black box containing: licence plate and/or chassis number);							
Pre-requirements for attack	Wireless communication equipment. Direct access to the vehicle and its internal electronic control unit.							
Attack description (Complete textual description of attack operation)	Attacker has the possibility to access the vehicle. From the inside the attacker can substitute or by pass the black box containing the basic information on the vehicle. In this case the stolen vehicle loses its real identity to appear, inside the infrastructure network, as another car.							
Attack success factors **(Reasons why attack may succeed)**	The attacker is able to modify via SW the basic information of the vehicle (chassis number, licence plate). The attacker has a direct access to the vehicle and he is able to modify via HW the basic information of the vehicle (chassis number, licence plate).							
Attack failure factors **(Reasons why attack may fail)**	The attacker is not able to modify via SW the information contained in the vehicle The attacker has not a direct access to the vehicle and consequently he is not able to change the identity parameters of the car.							
Effects of attack **(regarding driver and road traffic)**	Once modified the data of the vehicle, the car appears as another vehicle inside the network and it cannot be tracked by the authorities.							
Severity	low		medium		high	X	fatal	

Use Case	**Masquerade/impersonate as authority**							
Related appl. use case	Stolen vehicle tracking							
Creator	Stefano Cosenza, CRF							
Primary Attack Goal	DoS		Inform. Theft		Intrusion		Tampering	
Used Techniques	Masquer.	X	Eavesdrop.		Auth. Violation		Loss/Modific.	
	Repudiat.		Forgery		Sabotage	X		
Goal in Context **(Textual description of attackers goal/motivation)**	To track vehicles position to steal at the first occasion available. To provoke undesired effects on the normal working of the vehicle.							
Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Wireless communication							

Pre-requirements for attack	Wireless communication equipment and a very expert attacker.
Attack description (Complete textual description of attack operation)	If the target of the attack is a specific vehicle, the attacker must be able to track it all the time and everywhere, using the infrastructure network. In this sense the attacker must be able to log in the infrastructure network as authority operator (with all the relative attributes) to download the necessary information on the vehicle position. If the attacker chooses a vehicle to steal or to disturb it, the attacker should be in the proximity of the vehicle so to simulate a problem on the vehicle (the power off of the engine, the stall of the electronic system) as a break of an important component.
Attack success factors (Reasons why attack may succeed)	Driver ignores to be tracked. Drivers are not able to distinguish between a real mechanic/electronic problem and an injected one.
Attack failure factors (Reasons why attack may fail)	The attack cannot fail if the system (infrastructure network, on board unit) recognises the attacker as an authority.
Effects of attack (regarding driver and road traffic)	The position of a target vehicle is known in real time. If the attacker is able to simulate the authority, the driver has not means to oppose.

Severity	low		medium		high	X	fatal	

7.3 Map download/update

Use Case	**Unauthorized Access**							
Related appl. use case	Download and update of maps for the car navigation system							
Creator	Rainer Kroh, Albert Held, DC							
Primary Attack Goal	DoS		Inform. Theft	X	Intrusion		Tampering	
Used Techniques	Masquer.	X	Eavesdrop.	X	Auth. Violation	X	Loss/Modific.	
	Repudiat.		Forgery		Sabotage			

Goal in Context (Textual description of attackers goal/motivation)	Get unauthorized access to map content and the owner of the content loses revenue
Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Wireless communication, user identity, authentication process/protocol
Pre-requirements for attack	Wireless communication equipment, knowledge about user identity (Masquerade)
Attack description (Complete textual description of attack operation)	Attacker could use different techniques to get unauthorized access on map data. • If it is possible for the attacker to catch an identity of an authorized user it could be used for the access. • The map content could be eavesdropped while being transferred to the car • Manipulation of authentication data or exploit weakness in the authorization protocol/process allows access on the map content
Attack success factors (Reasons why attack may	Un-allowed usage of map content

succeed)	Earning money by selling the map content							
Attack failure factors (Reasons why attack may fail)	Identity theft by the attacker fails Map content is encrypted Map content is free of charge (no authentication necessary) Map content is vehicle bounded							
Effects of attack (regarding driver and road traffic)	Owner of data loses revenue User have to pay for map download/update							
Severity	low		medium		high	X	fatal	

Use Case	**Manipulation of map content**							
Related appl. use case	Download and update of maps for the car navigation system							
Creator	Rainer Kroh, Albert Held, DC							
Primary Attack Goal	DoS		Inform. Theft		Intrusion		Tampering	X
Used Techniques	Masquer.	X	Eavesdrop.		Auth. Violation		Loss/Modific.	X
	Repudiat.		Forgery	X	Sabotage	X		
Goal in Context (Textual description of attackers goal/motivation)	Harm in-vehicle (safety-critical) systems which rely on correct map content Mislead navigation system to influence traffic situations							
Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Wireless communication, map content server							
Pre-requirements for attack	Wireless communication equipment, knowledge about map content server identity, knowledge about map format							
Attack description (Complete textual description of attack operation)	Manipulation of the map content could be realized by • Attacker eavesdrops and manipulates the content transferring between map content server and vehicle. • A faked map content server misused the identity of an trusted content server and transfers manipulated map content to the vehicles In both cases the navigation system receives the manipulated content and navi-system and/or in-vehicle systems could react in a defective manner on this data.							
Attack success factors (Reasons why attack may succeed)	Unreliable behaviour of in-vehicle system and navigation-system Exertion of influence on road traffic							
Attack failure factors (Reasons why attack may fail)	Driver ignores routing recommendations of the navigation-system							
Effects of attack (regarding driver and road traffic)	User could not trust the unreliable navigation-system In-vehicle systems could influence or harm driving behaviour Exertion of influence on road traffic							
Severity	low		medium	X	high		fatal	

7.4 Intersection collision warning

Use Case	**Tracking Cars**
Related appl. use case	Intersection collision warning

Creator	Hans-J. Reumerman, Philips							
Primary Attack Goal	DoS		Inform. Theft		Intrusion	X	Tampering	
Used Techniques	Masquer.		Eavesdrop.		Auth. Violation	X	Loss/Modific.	
	Repudiat.		Forgery	X	Sabotage			
Goal in Context **(Textual description of attackers goal/motivation)**	If the RSUs at every intersection can be controlled, it becomes very easy to track the routes of all cars e.g. within a city.							
Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Wireless communication, backbone interconnecting RSUs							
Pre-requirements for attack	Wireless communication equipment Means to authenticate as road authority and intrude into the road side unit control system. Address and query road side units. Store large amount of messages and/or upload data to server by means of long range communication link. Means to effectively scan through large databases.							
Attack description (Complete textual description of attack operation)	Attacker addresses road side units and queries identity of vehicles having passed. Various attackers circulate in a city and combine forces to upload data to a server, which runs matching algorithms. Alternatively, the attacker authenticates itself e.g. as maintenance staff and enters into the RSU control system to read out messages and beacons received by any RSU.							
Attack success factors **(Reasons why attack may succeed)**	Route of selected car can be plotted. Selected car can be spotted in real time.							
Attack failure factors **(Reasons why attack may fail)**	Cars change their identity according to a secret algorithm, so attacker can not correlate different ID's to the same car.							
Effects of attack **(regarding driver and road traffic)**	Attacker can profile selected road users and predict the driving behaviour and habits as well as potential traffic rule violation. This knowledge can be used for criminal or commercial intentions.							
Severity	low	X	medium		high		fatal	

Use Case	**Forge RSU Warning Messages**							
Related appl. use case	Intersection collision warning							
Creator	Hans-J. Reumerman, Philips							
Primary Attack Goal	DoS		Inform. Theft		Intrusion		Tampering	
Used Techniques	Masquer.		Eavesdrop.		Auth. Violation	X	Loss/Modific.	
	Repudiat.		Forgery	X	Sabotage	X		
Goal in Context **(Textual description of attackers goal/motivation)**	Creating wrong warning messages and cause unneeded braking by drivers. This could then lead to congestion or even accidents. Sabotage safety features of critical intersections. Enjoy control over road side infrastructure and enjoy confusing drivers. Manipulate route planners of other vehicles by marking intersections as congested to offload traffic from own route. Create chaos to more easily escape from police.							

Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Wireless communication, backbone interconnecting RSUs, road sensors and signals							
Pre-requirements for attack	Wireless communication equipment, capable of creating and sending forged messages							
Attack description (Complete textual description of attack operation)	Attacker modifies or inhibits warning message issued by intersection collision warning equipment. Attacker could also interfere with the status inquiry protocol running between RSU and approaching or leaving vehicles. In other cases the attacker will confuse the road side sensors e.g. by mimicking a vehicle approaching the intersection at high speed, or blocking the intersection.							
Attack success factors (Reasons why attack may succeed)	Drivers will react according to a fictitious warning. RSU signals will wrongly interpret status signals from leaving or approaching vehicles.							
Attack failure factors (Reasons why attack may fail)	Driver relies on external signals rather than on the electronic warnings. Basic intersection control will most likely remain an independent system that can not be influenced by electronic messages. Therefore it will not be possible to block the entire intersection or to enable green lights for all directions. Only extended safety features such as dynamic road signals are targeted.							
Effects of attack (regarding driver and road traffic)	Drivers might brake apparently without reason. This can not be anticipated by following vehicles, and causes accidents. Drivers will be confused by contradicting signals from road side signals and in-vehicle warnings. Stress will be increased. False Warnings will lower user acceptance. Missed warnings will increase risk for accident. Drivers that relied on additional safety features like left-turn warning will be at risk.							
Severity	low		medium	X	high		fatal	

Use Case	**Confuse Navigation Data and Traffic Management**							
Related appl. use case	Intersection collision warning							
Creator	Hans-J. Reumerman, Philips							
Primary Attack Goal	DoS		Inform. Theft		Intrusion		Tampering	
Used Techniques	Masquer.		Eavesdrop.		Auth. Violation	X	Loss/Modific.	X
	Repudiat.		Forgery	X	Sabotage			
Goal in Context (Textual description of attackers goal/motivation)	Enjoy control over road side infrastructure and enjoy confusing drivers. Manipulate route planners of other vehicles by marking intersections as congested to offload traffic from own route. Create chaos to more easily escape from police. Mark certain roads as blocked that lead to business competitors or guide people towards visiting specific places, shopping malls, etc.							
Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Wireless communication, backbone interconnecting RSUs with traffic control or road operator; traffic management database of road operators: communication link between to radio broadcast stations, traffic centers or police							
Pre-requirements for attack	Wireless communication equipment, capable of creating and sending forged messages about traffic state; routing/navigation software to create a meaningful series of blocked intersections							

Attack description (Complete textual description of attack operation)	Attacker marks a number of intersections as blocked, in order to intrigue vehicle's navigation systems into proposing a different route that suits the need of the attacker. Alternatively, the messages of different intersections are forged such that a traffic center proposes a deviation and broadcasts this over the air.							
Attack success factors (Reasons why attack may succeed)	Traffic is offloaded from certain streets or suburbs. Traffic is routed into desired region.							
Attack failure factors (Reasons why attack may fail)	The traffic center correlates the intersection messages to warnings received from individual vehicles and detects the attack. Subsequent congestion warnings may be received from the region originally proposed as deviation, so the navigation system proposes yet another route or gives up.							
Effects of attack (regarding driver and road traffic)	Drivers are annoyed because the proposed route is not optimal or (starts getting congested more easily). In other cases, the drivers accept the deviation if traffic runs smoothly. Still it might lead to decreased trust in system warnings.							
Severity	low		medium	X	high		fatal	

Use Case	**Attention Splitter**							
Related appl. use case	Intersection collision warning							
Creator	Andre Barroso, Philips							
Primary Attack Goal	DoS	X	Inform. Theft		Intrusion		Tampering	
Used Techniques	Masquer.		Eavesdrop.		Auth. Violation	X	Loss/Modific.	X
	Repudiat.		Forgery	X	Sabotage	X		
Goal in Context (Textual description of attackers goal/motivation)	Induce third party vehicle collision for criminal purposes (e.g. insurance claim, road rage, terrorism).							
Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Approaching vehicles in the intersection. Event Priority Scheduler. Authentication Mechanism.							
Pre-requirements for attack	Cars approaching intersection in collision route, preferably in blind spot areas. Collision warning messages issued by RSU or approaching cars. Wireless communication equipment, capable of creating and sending attention splitter messages which have the same or higher priority than collision warning messages.							
Attack description (Complete textual description of attack operation)	Attacker sends one or more messages having equal or higher priority than a collision warning message. Drivers approaching the intersection, distracted by the attention-splitter messages, fail to react to collision warnings. Cars collide.							
Attack success factors (Reasons why attack may succeed)	Human inability to react to multiple events in a short period of time. Difficulty in filtering false imminent threats in a timely manner.							

Attack failure factors (Reasons why attack may fail)	Driver reacts to collision warning first and ignores attention splitter. System is able to correctly identify that attention splitters are not real threats.							
Effects of attack (regarding driver and road traffic)	Intersection Collision							
Severity	low		medium		high		fatal	X

Use Case	**Collision Warning Relay**							
Related appl. use case	Intersection collision warning							
Creator	Andre Barroso, Philips							
Primary Attack Goal	DoS	X	Inform. Theft		Intrusion		Tampering	
Used Techniques	Masquer.		Eavesdrop.	X	Auth. Violation	X	Loss/Modific.	X
	Repudiat.		Forgery	X	Sabotage	X		
Goal in Context (Textual description of attackers goal/motivation)	Induce third party vehicle collision for criminal purposes (e.g. insurance claim, road rage, terrorism), sabotage confidence in the warning system, Irritate drivers.							
Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	OBU warning system							
Pre-requirements for attack	Cars approaching intersection in collision route. Eavesdropper of collision warning messages issued by RSU or approaching cars. Wireless communication equipment, capable of replaying captured warnings as attention splitter messages.							
Attack description (Complete textual description of attack operation)	Attacker snoops legitimate intersection collision warning messages and later replays them as attention splitters.							
Attack success factors (Reasons why attack may succeed)	Human inability to react to multiple events in a short period of time. Difficulty in filtering false imminent threats in a timely manner. Intersection collision messages must have high priority.							
Attack failure factors (Reasons why attack may fail)	System is able to correctly identify that attention slitters are not real threats.							
Effects of attack (regarding driver and road traffic)	Confusion and accidents							
Severity	low		medium		high	X	fatal	

7.5 Vehicle-based road condition warning

Use Case	**Forging of Warning Messages**							
Related appl. use case	Application-based road condition warning							
Creator	Frank Kargl, UULM							
Primary Attack Goal	DoS	X	Inform. Theft		Intrusion		Tampering	
Used Techniques	Masquer.		Eavesdrop.		Auth. Violation		Loss/Modific.	

	Repudiat.		Forgery	X	Sabotage			
Goal in Context **(Textual description of attackers goal/motivation)**	Issue false warnings so that drivers get irritated and may go slower than necessary. Due to hard breaking, rear-end collisions may occur.							
Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Wireless communication							
Pre-requirements for attack	Wireless communication equipment, capable of creating and sending forged messages							
Attack description (Complete textual description of attack operation)	Attacker places itself near the target area and emits forged messages warning e.g. because of slippery or icy road conditions. The destination area for the geocast may be selected based on topographic features or simply set to a maximum area so that as many cars as possible will be affected. Messages will be automatically distributed in the destination region and drivers will receive warning messages, to which they are supposed to react accordingly.							
Attack success factors **(Reasons why attack may succeed)**	Drivers will recognize the warning and slow down.							
Attack failure factors **(Reasons why attack may fail)**	If there are no cars in the one-hop neighbourhood to distribute the messages, the attack fails. Drivers might simply ignore the warnings.							
Effects of attack **(regarding driver and road traffic)**	The attack will cause the drivers to slow down; causing traffic jams or in worst case rear-end collisions.							
Severity	low	X	medium		high		fatal	

Use Case	**Suppression of warning messages**							
Related appl. use case	Vehicle-based road condition warning							
Creator	Frank Kargl, UULM							
Primary Attack Goal	DoS	X	Inform. Theft		Intrusion		Tampering	
Used Techniques	Masquer.		Eavesdrop.		Auth. Violation		Loss/Modific.	X
	Repudiat.		Forgery		Sabotage			
Goal in Context **(Textual description of attackers goal/motivation)**	Prevent warning messages from reaching the driver							
Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Wireless communication							
Pre-requirements for attack	Either jamming device or wireless communication equipment, that can be controlled by the attacker to behave in a non-conforming way							

Attack description (Complete textual description of attack operation)	Attacker places itself near the target area. Case 1) Attacker emits a jamming signal that prevents wireless communication between regular network nodes Case 2) Attacker receives messages that he should forward to other nodes. Instead, messages are dropped Case 3) Attackers prevents communication e.g. by manipulation the IEEE 802.11 medium access, e.g. not respecting the DIFS and sending small packets before others are able to transmit.							
Attack success factors (Reasons why attack may succeed)	Attacker is successfully able to prevent communication, e.g. because the jamming succeeds or the attacker outperforms all others in MAC							
Attack failure factors (Reasons why attack may fail)	Case 1) Jamming is not effective, because of insufficient power, wrong frequencies, DSSS, etc. Case 2) Messages are routed through other nodes Case 3) Attacker is not able to outperform others							
Effects of attack (regarding driver and road traffic)	Drivers will not be warned and can therefore not react to dangerous road conditions in time.							
Severity	low	X	medium		high		fatal	

Use Case	**Eavesdropping and tracking**							
Related appl. use case	Vehicle-based road condition warning							
Creator	Frank Kargl, UULM							
Primary Attack Goal	DoS		Inform. Theft	X	Intrusion		Tampering	
Used Techniques	Masquer.		Eavesdrop.	X	Auth. Violation		Loss/Modific.	
	Repudiat.		Forgery		Sabotage			
Goal in Context (Textual description of attackers goal/motivation)	Collect information about vehicles and their positions							
Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Wireless communication							
Pre-requirements for attack	Wireless communication equipment, to receive and analyze warning messages							
Attack description (Complete textual description of attack operation)	The attacker places itself near one or many area where warnings are likely to be emitted. Attacker may even force warnings e.g. by putting water on the street. Next, the attacker promiscuously receives all transmitted messages and stores the locations and vehicle-IDs in a database for later analysis.							
Attack success factors (Reasons why attack may succeed)	Messages are sent as broadcast and can be received and analyzed by everybody.							
Attack failure factors (Reasons why attack may fail)	Cars will not detect hazard and do not send messages.							
Effects of attack (regarding driver and road	Privacy of vehicle drivers is diminished.							

traffic)								
Severity	low		medium	X	high		fatal	

Use Case	**Impersonation of other cars**							
Related appl. use case	Vehicle-based road condition warning							
Creator	Frank Kargl, UULM							
Primary Attack Goal	DoS		Inform. Theft		Intrusion		Tampering	X
Used Techniques	Masquer.	X	Eavesdrop.		Auth. Violation		Loss/Modific.	
	Repudiat.		Forgery	X	Sabotage			
Goal in Context **(Textual description of attackers goal/motivation)**	Make (faked) warning messages appear to come from other participants to harm their reputation.							
Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Wireless communication							
Pre-requirements for attack	Wireless communication equipment, capable of creating and sending forged messages with wrong identities							
Attack description (Complete textual description of attack operation)	Attacker places itself near the target area and emits forged messages warning e.g. of slippery or icy road conditions. Message origin will be set to the IDs of other vehicles. Messages will be automatically distributed in the destination region and drivers will receive warning messages, to which they are supposed to react accordingly. If the forged warning messages are detected and the system or authorities will try to punish the responsible origin, they will falsely accuse the wrong vehicle/person.							
Attack success factors **(Reasons why attack may succeed)**	There must be reputation systems or event data recorders that consider or record the origin of a message in their actions. Sending of wrong messages has negative consequences (e.g. loss of reputation, lawsuits, etc.)							
Attack failure factors **(Reasons why attack may fail)**	Forged messages are simply ignored.							
Effects of attack **(regarding driver and road traffic)**	Loss in reputation							
Severity	low		medium	X	high		fatal	

7.6 Electronic license plate

Use Case	**Impersonation of infrastructure node**							
Related appl. use case	Electronic license plate							
Creator	Panos Papadimitratos, EPFL							
Primary Attack Goal	DoS		Inform. Theft	X	Intrusion	X	Tampering	X
Used Techniques	Masquer.	X	Eavesdrop.		Auth. Violation	X	Loss/Modific.	
	Repudiat.		Forgery	X	Sabotage			
Goal in Context **(Textual description of attackers goal/motivation)**	Masquerade as an infrastructure node (including public vehicles, such as police cars) and initiate an ELP reading protocol.							

Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Wireless communication, on-board hardware							
Pre-requirements for attack	Wireless communication equipment, capable of creating and sending forged messages; equipment for extracting credentials from the OBU							
Attack description (Complete textual description of attack operation)	The attacker initiates the ELP reading protocol, forging messages accordingly. It misleads the victim nodes to respond with their ELPs. Prior to that, the attacker may tamper with the infrastructure node and extract its credentials.							
Attack success factors (Reasons why attack may succeed)	The attacker is either capable of forging messages if the infrastructure node is not authenticated, or it has compromised and utilizes the infrastructure node's credentials, before they expire or be revoked.							
Attack failure factors (Reasons why attack may fail)	Infrastructure or public vehicle nodes are equipped with credentials that cannot be compromised by the attacker, or in such case, they are promptly revoked.							
Effects of attack (regarding driver and road traffic)	Compromise of ELP, i.e., private information.							
Severity	low		medium	X	high		fatal	

Use Case	**Impersonation of vehicle / forging of ELP**							
Related appl. use case	Electronic license plate							
Creator	Panos Papadimitratos, EPFL							
Primary Attack Goal	DoS		Inform. Theft	X	Intrusion	X	Tampering	X
Used Techniques	Masquer.	X	Eavesdrop.		Auth. Violation	X	Loss/Modific.	
	Repudiat.		Forgery	X	Sabotage			
Goal in Context (Textual description of attackers goal/motivation)	Masquerade as an infrastructure node or a public vehicle and initiate an ELP reading protocol.							
Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Wireless communication, on-board hardware							
Pre-requirements for attack	Wireless communication equipment, capable of creating and sending forged messages; equipment for extracting credentials from the OBU; methods for generating apparently valid yet illegitimate ELP numbers							
Attack description (Complete textual description of attack operation)	The attacker injects forged messages in response to an ELP-REQ message. It responds with a fake ELP. Prior to that, the attacker may tamper with the OBU of other vehicles and extracts and credentials ELP numbers a							

Attack success factors (Reasons why attack may succeed)	The attacker is either capable of forging messages if the ELP is not cryptographically verifiable. Or it has compromised and utilizes the credentials of other vehicles before they expire or be revoked.							
Attack failure factors (Reasons why attack may fail)	Vehicles are equipped with credentials that cannot be compromised by the attacker, or in such case, they are promptly revoked.							
Effects of attack (regarding driver and road traffic)	Impersonation; illegitimate access; avoidance of tracking by the authorities; compromise of ELP, i.e., private information.							
Severity	low		medium	X	high		fatal	

7.7 Road surface conditions to TOC

Use Case	**Tracking**							
Related appl. use case	Road surface condition to TOC							
Creator	Antonio Kung, Trialog							
Primary Attack Goal	DoS		Inform. Theft	X	Intrusion		Tampering	
Used Techniques	Masquer.		Eavesdrop.	X	Auth. Violation		Loss/Modific.	
	Repudiat.		Forgery		Sabotage			
Goal in Context (Textual description of attackers goal/motivation)	Tracking the moves of a person possibly in some specific area							
Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Wireless communication.							
Pre-requirements for attack	Wireless communication equipment, to receive and analyse messages. This equipment is located in some predetermined locations.							
Attack description (Complete textual description of attack operation)	Attacking equipment log received data Logged data is then analysed off-line on a simple PC Results concerning person is obtained further to decrypting software available on the net using grid computing technology. This takes a few days.							
Attack success factors (Reasons why attack may succeed)	Network analysers are not expensive							
Attack failure factors (Reasons why attack may fail)	-							
Effects of attack (regarding driver and road traffic)	Privacy at stake							
Severity	low		medium		high	X	fatal	

Use Case	**Impersonation**							
Related appl. use case	Road surface condition to TOC							
Creator	Antonio Kung, Trialog							
Primary Attack Goal	DoS		Inform. Theft		Intrusion		Tampering	X

Used Techniques	Masquer.	X	Eavesdrop.		Auth. Violation		Loss/Modific.	
	Repudiat.		Forgery	X	Sabotage			
Goal in Context **(Textual description of attackers goal/motivation)**	Creating an alibi							
Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Wireless communication.							
Pre-requirements for attack	Wireless communication equipment, to receive and analyse messages							
Attack description (Complete textual description of attack operation)	Attacking equipment impersonate an entity and sends data on behalf of car FOO and user BAR							
Attack success factors **(Reasons why attack may succeed)**	Network analysers are not expensive							
Attack failure factors **(Reasons why attack may fail)**	Cryptographic effort to forge a person.							
Effects of attack **(regarding driver and road traffic)**	Criminal activities							
Severity	low		medium		high	X	fatal	

Use Case	**Denial of service 1**							
Related appl. use case	Road surface condition to TOC							
Creator	Antonio Kung, Trialog							
Primary Attack Goal	DoS	X	Inform. Theft		Intrusion		Tampering	
Used Techniques	Masquer.	X	Eavesdrop.		Auth. Violation		Loss/Modific.	
	Repudiat.		Forgery	X	Sabotage			
Goal in Context **(Textual description of attackers goal/motivation)**	Prevent cars to drive in an area							
Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Wireless communication.							
Pre-requirements for attack	Wireless communication device A playing the role of a car. Has the following requirement • Can impersonate simultaneously different cars. For instance could include have hardware capabilities to provide the illusion that signals come from different cars, or is from a moving element. • Is remotely controlled and can be located in a specific position (no need for a car) Wireless communication device B playing the role of a RSE. Has the following							

	requirement • Can impersonate simultaneously different cars. For instance could include have hardware capabilities to provide the illusion that signals come from different cars, or is from a moving element. • Is remotely controlled and can be located in a specific position
Attack description (Complete textual description of attack operation)	Attacker launches programs which remotely • Instruct devices B to send information to all real cars so that they avoid section of route • Instruct devices A to send road surface conditions to TOC
Attack success factors (Reasons why attack may succeed)	Equipment is not expensive
Attack failure factors (Reasons why attack may fail)	Plausibility checks could be possible if real cars still drive in the area
Effects of attack (regarding driver and road traffic)	Criminal activities

Severity	low		medium		high	X	fatal	

Use Case	**Denial of service 2**							
Related appl. use case	Road surface condition to TOC							
Creator	Antonio Kung, Trialog							
Primary Attack Goal	DoS	X	Inform. Theft		Intrusion		Tampering	
Used Techniques	Masquer.	X	Eavesdrop.		Auth. Violation		Loss/Modific.	
	Repudiat.		Forgery	X	Sabotage			

Goal in Context (Textual description of attackers goal/motivation)	Denial of service to harm service operator
Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Wireless communication.
Pre-requirements for attack	Wireless communication devices playing the role of a car. Has the following requirement • Can impersonate simultaneously different cars. For instance could include have hardware capabilities to provide the illusion that signals come from different cars, or is from a moving element. • Is remotely controlled and can be located in a specific position (no need for a car) ▪

Attack description (Complete textual description of attack operation)	Attacker launches programs which remotely • Instruct devices A to send road surface conditions to TOC							
Attack success factors (Reasons why attack may succeed)	Equipment is not expensive							
Attack failure factors (Reasons why attack may fail)	Plausibility checks could be possible							
Effects of attack (regarding driver and road traffic)	Criminal activities							
Severity	low		medium		high	X	fatal	

7.8 Software update/flashing

Use Case	**Manipulation of data**							
Related appl. use case	Update/flashing of in-vehicle software							
Creator	Rainer Kroh, Albert Held, DC							
Primary Attack Goal	DoS		Inform. Theft		Intrusion		Tampering	X
Used Techniques	Masquer.		Eavesdrop.		Auth. Violation		Loss/Modific.	X
	Repudiat.		Forgery		Sabotage			
Goal in Context (Textual description of attackers goal/motivation)	Changing the content of the download to provoke malfunctioning or un-allowed access to vehicle systems							
Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Wireless communication							
Pre-requirements for attack	Wireless communication equipment							
Attack description (Complete textual description of attack operation)	The attacker eavesdrop the transfer between content server and vehicle and manipulate the transferred content. The manipulation could also be done on encrypted content and may lead to malfunctions of in-vehicle systems							
Attack success factors (Reasons why attack may succeed)	Unreliable behaviour of in-vehicle system and/or access on vehicle systems							
Attack failure factors (Reasons why attack may fail)	Manipulation of downloaded content will be detected by vehicle systems							

Effects of attack (regarding driver and road traffic)	User could not trust the unreliable in-vehicle systems In-vehicle systems could influence or harm driving behaviour							
Severity	low		medium		high		fatal	X

Use Case	**Injection of malicious Software**							
Related appl. use case	Update/flashing of in-vehicle software							
Creator	Rainer Kroh, Albert Held, DC							
Primary Attack Goal	DoS		Inform. Theft		Intrusion	X	Tampering	
Used Techniques	Masquer.		Eavesdrop.		Auth. Violation		Loss/Modific.	
	Repudiat.		Forgery	X	Sabotage			
Goal in Context (Textual description of attackers goal/motivation)	Injection of malicious software to take over control of the in-vehicle systems							
Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Wireless communication, content server							
Pre-requirements for attack	Wireless communication equipment, knowledge about content server identity, knowledge about software format							
Attack description (Complete textual description of attack operation)	Manipulation of the map content could be realized by • Attacker eavesdrops and injects malicious code in the content-transfer between map content server and vehicle. • A faked content server misused the identity of an trusted content server and transfers malicious code to the vehicles In both cases the in-vehicle system receives the malicious content and the in-vehicle systems could react in a defective manner on this data or the attacker took over control of the system							
Attack success factors (Reasons why attack may succeed)	Take over control of in-vehicle system							
Attack failure factors (Reasons why attack may fail)	Malicious software will be detected from in-vehicle system							
Effects of attack (regarding driver and road traffic)	User could not trust the unreliable in-vehicle system In-vehicle systems could influence or harm driving behaviour Attacker has entire access on the vehicle							
Severity	low		medium		high		fatal	X

Use Case	**Eavesdropping**							
Related appl. use case	Update/flashing of in-vehicle software							
Creator	Rainer Kroh, Albert Held, DC							
Primary Attack Goal	DoS		Inform. Theft	X	Intrusion		Tampering	
Used Techniques	Masquer.		Eavesdrop.	X	Auth. Violation		Loss/Modific.	
	Repudiat.		Forgery		Sabotage			
Goal in Context (Textual description of attackers goal/motivation)	Get un-allowed access to commercial in-vehicle software to use it or to earn money							

Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Wireless communication							
Pre-requirements for attack	Wireless communication equipment							
Attack description (Complete textual description of attack operation)	Attacker could eavesdrop and store the content transfer of in-vehicle software between content server and vehicle. The stored software could be used by the attacker itself or sold to third parties. Therefore the owner of the software loses revenue.							
Attack success factors (Reasons why attack may succeed)	Acquire proprietary commercial in-vehicle software Earning money by selling the in-vehicle software							
Attack failure factors (Reasons why attack may fail)	Transfer could not be eavesdropped In-vehicle software is vehicle-bounded							
Effects of attack (regarding driver and road traffic)	Owner of software loses revenue Buyer of eavesdropped software could lose OEMs warrantee							
Severity	low		medium		high	X	fatal	

Use Case	**Unauthorized access / Impersonation**							
Related appl. use case	Update/flashing of in-vehicle software							
Creator	Rainer Kroh, Albert Held, DC							
Primary Attack Goal	DoS		Inform. Theft	X	Intrusion		Tampering	
Used Techniques	Masquer.	X	Eavesdrop.		Auth. Violation	X	Loss/Modific.	
	Repudiat.		Forgery		Sabotage			
Goal in Context (Textual description of attackers goal/motivation)	Get unauthorized access to in-vehicle software and the owner of the content loses revenue							
Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Wireless communication, user/vehicle identity, authentication process/protocol							
Pre-requirements for attack	Wireless communication equipment, knowledge about user/vehicle identity (Masquerade)							
Attack description (Complete textual description of attack operation)	Attacker could use different techniques to get unauthorized access on in-vehicle software. • If it is possible for the attacker to catch an identity of an authorized user/vehicle it could be used for the access. • Manipulation of authentication data or exploit weakness in the authorization protocol/process allows access on transferred in-vehicle software							
Attack success factors (Reasons why attack may	Acquire proprietary commercial in-vehicle software							

succeed)	Earning money by selling the in-vehicle software							
Attack failure factors (Reasons why attack may fail)	Identity theft by the attacker fails In-vehicle software is vehicle-bounded							
Effects of attack (regarding driver and road traffic)	Owner of data loses revenue User have to pay for software download/update							
Severity	low		medium		high	X	fatal	

7.9 Emergency vehicle signal pre-emption

Use Case	**Impersonate Emergency vehicle**							
Related appl. use case	Emergency vehicle (EV) signal pre-emption							
Creator	Hans-J. Reumerman, Philips							
Primary Attack Goal	DoS		Inform. Theft		Intrusion		Tampering	
Used Techniques	Masquer.	X	Eavesdrop.		Auth. Violation	X	Loss/Modific.	
	Repudiat.		Forgery	X	Sabotage	X		
Goal in Context (Textual description of attackers goal/motivation)	Get the right of way; accelerate rescue workforce beyond what is needed; eavesdrop on communication between rescue workforce; mitigate public safety; deteriorate public order by provoking traffic jams: extend the time needed for rescue operation							
Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Wireless links, routing instances, communication road side units, road side infrastructure (traffic lights, barriers, etc.), emergency vehicles							
Pre-requirements for attack	Wireless communication equipment capable of receiving and deciphering EV messages, as well as of creating, encoding and sending forged messages							
Attack description (Complete textual description of attack operation)	Attacker assumes the role of en EV and emits artificial warning signals to control traffic lights or alert other vehicles on approaching EV. Attacker could also prepare roadside infrastructure to accept proprietary or modified signals and thus takes over the control of a particular road signal or sensor. By changing the originator field in messages from “standard vehicle” to EV, the message priority may be artificially increased and/or the transmit power is allowed to be increased.							
Attack success factors (Reasons why attack may succeed)	Other vehicles will slow down and/or pull right, traffic lights will switch according to attackers desired intention. Attacker is addressed by other rescue staff and eavesdrop safety relevant information. Attacker controls part of the road side infrastructure.							
Attack failure factors (Reasons why attack may fail)	Encoding or decoding of public safety messages might fail, which uncovers the attack. The emergency vehicle control centre may discover strange or unexpected signals from infrastructure connected to a backbone network and disable the road side infrastructure.							
Effects of attack (regarding driver and road traffic)	The attack will cause traffic jams and deteriorate the quality and reaction time of rescue operations. It will disturb the communication between EV and control centre and put the EV crew at risk							
Severity	low		medium		high		fatal	X

Use Case	**Manipulation of Emergency Vehicle messages**

Related appl. use case	Emergency vehicle (EV) signal pre-emption							
Creator	Hans-J. Reumerman, Philips							
Primary Attack Goal	DoS		Inform. Theft		Intrusion		Tampering	
Used Techniques	Masquer.		Eavesdrop.		Auth. Violation	X	Loss/Modific.	X
	Repudiat.		Forgery	X	Sabotage	X		
Goal in Context **(Textual description of attackers goal/motivation)**	Accelerate rescue workforce beyond what is needed; eavesdrop on communication between rescue workforce; mitigate public safety; deteriorate public order by provoking traffic jams: extend the time needed for rescue operation							
Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Wireless links, routing instances, communication road side units, road side infrastructure (traffic lights, barriers, etc.), emergency vehicles							
Pre-requirements for attack	Wireless communication equipment capable of receiving EV messages, as well as of creating and sending forged messages							
Attack description (Complete textual description of attack operation)	Messages are received and identified as EV-originated messages. Upon forwarding the message will be deleted, doubled, changed, extended or shortened. Also the destination area or destination address may be modified. By changing the originator field in messages from “standard vehicle” to EV, the message priority may be artificially increased and/or the transmit power is allowed to be increased.							
Attack success factors **(Reasons why attack may succeed)**	Manipulating certain fields of en AV message will cause indeterminist behaviour of receiving vehicles and drivers. Some vehicles will slow down and/or pull right; others may ignore the message or react in a different way. Traffic lights may not switch according to EV desired intention.							
Attack failure factors **(Reasons why attack may fail)**	Message may be discarded by the application in case certain encoding rules or checksums are violated. The emergency vehicle control centre may discover strange or unexpected signals from infrastructure connected to a backbone network and disable the road side infrastructure							
Effects of attack **(regarding driver and road traffic)**	The attack will cause traffic jams and deteriorate the quality and reaction time of rescue operations. Due to unexpected behaviour EV crew will be put at risk and stress will be increased.							
Severity	low		medium		high	X	fatal	

7.10 Work zone warning

Use Case	**Forging of messages**							
Related appl. use case	Workzone warning							
Creator	Elmar Schoch, UULM							
Primary Attack Goal	DoS	X	Inform. Theft		Intrusion		Tampering	
Used Techniques	Masquer.	X	Eavesdrop.		Auth. Violation		Loss/Modific.	
	Repudiat.		Forgery	X	Sabotage			
Goal in Context **(Textual description of attackers goal/motivation)**	Send incorrect information about workzone to other vehicles. This may then cause other drivers try to bypass the imaginary bottleneck and therefore jam other roads. For the traffic on the concerned road, it may also lead to jams because drivers brake for caution.							

Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Application protocol Authentication – if in place
Pre-requirements for attack	Wireless communication equipment, protocol stack that allows creating valid messages, application logic is known
Attack description (Complete textual description of attack operation)	Attacker places itself in the vicinity of the targeted area or drives along with others on the road and starts to emit forged messages. The destination region of such a message may be selected arbitrarily – either according to the topographic situation or set to a maximum allowed range (if in place) to reach as many vehicles as possible. The rest is done automatically by the routing/message dissemination mechanisms and the effect then depend on drivers' reaction.
Attack success factors (Reasons why attack may succeed)	Drivers react on message by taking another route or by braking. Note that this is actually the intention of the application!
Attack failure factors (Reasons why attack may fail)	Drivers ignore warnings (which renders the application useless if many do so), vehicle density is too low for sufficient message distribution
Effects of attack (regarding driver and road traffic)	In case that drivers take a bypass route, potential waste of fuel and time. In case of high vehicle density and braking vehicles, there may develop autogenously traffic jams.

Severity	low	X	medium		high		fatal	

Use Case	**Suppression of messages**							
Related appl. use case	Workzone warning							
Creator	Elmar Schoch, UULM							
Primary Attack Goal	DoS	X	Inform. Theft		Intrusion		Tampering	
Used Techniques	Masquer.		Eavesdrop.		Auth. Violation		Loss/Modific.	X
	Repudiat.		Forgery		Sabotage			

Goal in Context (Textual description of attackers goal/motivation)	By suppressing workzone warning messages, the attacker may cause irritations for drivers that may lead to hazardous situations. Moreover, missing information about workzones reduces traffic efficiency that was intended to be improved by such messages.
Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Wireless communication by jamming radio (creating noise to disturb medium access or to cancel existing transmissions) Routing/Message dissemination
Pre-requirements for attack	Wireless communication equipment, eventually aware of routing mechanisms
Attack description (Complete textual description of attack operation)	First, the attacker needs to listen actively on the wireless medium. One way to suppress workzone warnings is to prohibit medium access which generally makes communication impossible in the wireless communication range of the attacker. A more sophisticated approach would be to evaluate the content of a transmission while it is sent and then created noise when it is clear that the transmission is a workzone warning. On the routing layer, the attacker is able to drop packets at will. So, the simplest way is to drop all passing packets with workzone information. Again, with more elaborate methods, the routing protocol(s) may be exploited to reroute packets which then may be dropped.

Attack success factors (Reasons why attack may succeed)	When workzone messages do not reach the intended receivers, they might get confused if suddenly the workzone appears or they might be angry because if they had been informed, they had taken a different route to save time.							
Attack failure factors (Reasons why attack may fail)	If it is clear to drivers that the warning is just additional information and the normal efforts of announcing workzones to drivers using traffic signs etc. are not reduced, the attack is mostly useless.							
Effects of attack (regarding driver and road traffic)	Traffic efficiency may be reduced							
Severity	low	X	medium		high		fatal	

Use Case	**Manipulation of traffic sign location**							
Related appl. use case	Workzone warning							
Creator	Elmar Schoch, UULM							
Primary Attack Goal	DoS		Inform. Theft		Intrusion		Tampering	X
Used Techniques	Masquer.		Eavesdrop.		Auth. Violation		Loss/Modific.	
	Repudiat.		Forgery		Sabotage	X		
Goal in Context (Textual description of attackers goal/motivation)	As effect, workzone warnings will appear in wrong places, leading also to effects like hazardous situations or reduced traffic efficiency							
Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Equipment that emits workzone warnings (e.g. traffic signs)							
Pre-requirements for attack	Physical access to equipment							
Attack description (Complete textual description of attack operation)	Relocate workzone warning sender equipment							
Attack success factors (Reasons why attack may succeed)	Drivers recognize the warning and get confused, thinking that they missed corresponding signs somewhere							
Attack failure factors (Reasons why attack may fail)	Drivers ignore warning because a workzone is not there (nevertheless reducing trustability of the whole system)							
Effects of attack (regarding driver and road traffic)	Confusing and therefore hazardous situations, reduced traffic efficiency, lower trustability of system							
Severity	low	X	medium		high		fatal	

Use Case	**Manipulation of message content**							
Related appl. use case	Workzone warning							
Creator	Elmar Schoch, UULM							
Primary Attack Goal	DoS		Inform. Theft		Intrusion		Tampering	X
Used Techniques	Masquer.		Eavesdrop.		Auth. Violation		Loss/Modific.	X

	Repudiat.		Forgery		Sabotage			
Goal in Context **(Textual description of attackers goal/motivation)**	Create wrong information on existing workzones. This may lead to accidents, e.g. if cars respect a – manipulated – speed limit.							
Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Routing – to reach "faster" distribution than the original message Message integrity checking mechanisms (if in place)							
Pre-requirements for attack	Wireless communication equipment including the complete communication stack to be able to be part of network							
Attack description (Complete textual description of attack operation)	The attacker modifies received workzone warning messages (e.g. by setting a different speed limit) and forwards them again. If the attacker wants to reach more distribution of the manipulated message, he may also influence routing.							
Attack success factors **(Reasons why attack may succeed)**	Drivers may get confused about wrong information or even cause accidents due to manipulated data.							
Attack failure factors **(Reasons why attack may fail)**	Drivers recognize the manipulation and ignore warning							
Effects of attack **(regarding driver and road traffic)**	Potential accidents, reduced trustability of system							
Severity	low		medium	X	high		fatal	

8 Identify Security Mechanisms

Based on the analysis of the different attack use cases of chapter 7 we have identified the following security concepts that would be needed to prevent these attacks. In the table you find the list of such concepts in the first column and where we find that these concepts should be applied. These are only abstract concepts and solutions/realizations of all or some of these concepts that are suitable for VANETs will be described in detail in our Deliverable 2.1 “Security Architecture and Mechanisms for V2V/V2I”.

	SOS services			Stolen vehicle tracking			Map download	
	1.1	1.2	1.3	2.1	2.2	2.3	3.1	3.2
	Forging of SOS message	Eavesdropping of SOS messages	Blocking SOS messages	Denial of service	Masquerade as other vehicle	Masquerade as authority	Unauthorized access	Manipulation of map content
Identification & Authentication Concepts								
Identification	O				O		O	
Authentication of sender	++		O		+	++	++	++
… and sender is					stolen vehicle		vehicle	server
Authentication of receiver		+	O					
Property authentication	+							
Authentication of intermediate nodes		O						
Privacy Concepts								
Resolvable anonymity	++							
Total anonymity								
Location obfuscation								
Integrity Concepts								
Encryption		++						+
Integrity protection								++
Detection of protocol violation			++					
Jamming protection			++					
Tamper-resistant comm. system				++	++			
DRM								++
Replay protection								
Consistency/context checking	+							
Attestation of sensor data	+							
Location verification								
Access Control/Authorization Concepts								
Access control								
Firewall/Checkpoint								
Closed user groups								
Filtering (e.g at intermediate nodes)								
Sandbox								

	Intersection collision avoidance					Vehicle-based road condition warning			
	4.1	4.2	4.3 (na	4.4	4.5	5.1	5.2	5.3	5.4
	Tracking	Forge RSU warning messages	Confuse navigation data	Attention splitter	Collision warning relay	Forging of warning messages	Suppression of warning messages	Eavesdropping and tracking	Impersonation of other cars
Identification & Authentication Concepts									
Identification						O			
Authentication of sender		++				O			++
… and sender is									
Authentication of receiver									
Property authentication		+				++			+
Authentication of intermediate nodes									
Privacy Concepts									
Resolvable anonymity						O			
Total anonymity	++							++	
Location obfuscation	O								
Integrity Concepts									
Encryption								+	
Integrity protection									
Detection of protocol violation							++		
Jamming protection							++		
Tamper-resistant comm. system						+			
DRM									
Replay protection		+			++				
Consistency/context checking				++		++			
Attestation of sensor data				+		+			
Location verification									
Access Control/Authorization Concepts									
Access control									
Firewall/Checkpoint									
Closed user groups									
Filtering (e.g at intermediate nodes)									
Sandbox									

	El. license plate		Road surface cond. to TOC			
	6.1	6.2	7.1	7.2	7.3	7.4
	Impersonation of infrastructure node	Impersonation of vehicle or forging ELP	Tracking	Impersonation	Denial of service 1	Denial of service 2
Identification & Authentication Concepts						
Identification		**O**				
Authentication of sender	**++**	**++**		**++**	**++**	
… and sender is	infra-structure	vehicle			vehicle	
Authentication of receiver						
Property authentication					**+**	**+**
Authentication of intermediate nodes					**O**	
Privacy Concepts						
Resolvable anonymity					**+**	
Total anonymity			**++**			
Location obfuscation			**O**			
Integrity Concepts						
Encryption			**+**			
Integrity protection						
Detection of protocol violation						
Jamming protection						
Tamper-resistant comm. system	**++**	**+**		**+**		
DRM						
Replay protection		**+**			**+**	**+**
Consistency/context checking					**+**	**+**
Attestation of sensor data					**+**	**O**
Location verification					**O**	
Access Control/Authorization Concepts						
Access control						
Firewall/Checkpoint						
Closed user groups					**++**	
Filtering (e.g at intermediate nodes)						**++**
Sandbox						

	Software update/flashing				EV signal preemption		Workzone warning			
	8.1	8.2	8.3	8.4	9.1	9.2	10.1	10.2	10.3	10.4
	Manipulation of data	Injection of malicious software	Eavesdropping	Unauthorized access / impersonation	Impersonate emergency vehicle	Manipulation of EV messages	Forging of messages	Suppression of messages	Manipulation of traffic sign location	Manipulation of message content
Identification & Authentication Concepts										
Identification										
Authentication of sender	++	+		O	++	++	+			
… and sender is	OEM	OEM/ Svc prov			EV	EV	RSU			
Authentication of receiver	+	+		+						
Property authentication					++	++	+			
Authentication of intermediate nodes										
Privacy Concepts										
Resolvable anonymity										
Total anonymity										
Location obfuscation										
Integrity Concepts										
Encryption			+		O					
Integrity protection	+	+				++				++
Detection of protocol violation								++		
Jamming protection								++		
Tamper-resistant comm. system									+	
DRM			++	++						
Replay protection										
Consistency/context checking						O	+		+	+
Attestation of sensor data										
Location verification									++	+
Access Control/Authorization Concepts										
Access control				++						
Firewall/Checkpoint		++								
Closed user groups										
Filtering (e.g at intermediate nodes)										
Sandbox		+								

The values of the properties in the tables describe our estimation of usefulness of the security concepts to help against the specific attacks, where 'O' stands for possible, '+' for useful and '++' for very useful (see also 2.2.8)

9 Design Security Mechanisms

As described in 2.2.9 this will be the actual design phase of our process. The description and the results of the design phase of the security mechanisms for VANETs will be done as part of WP2 Security Architecture and therefore specified in detail in Del 2.1 “Security Architecture and Mechanisms”.

10 Generalization

The final step of the security requirements process and security system development will be the analysis whether the security mechanisms will also work with the other applications that are to be realized. This will be done also in Del 2.1 “Security Architecture and Mechanisms”.

11 References

[1] Franz, W., Wagner, C., Maihöfer, C., Hartenstein, H.: Fleetnet: Platform for intervehicle communications. In: Proc. 1st Intl. Workshop on Intelligent Transportation, Hamburg, Germany (2004)

[2] Now - network on wheels project. http://www.network-on-wheels.de (2005)

[3] US Vehicle Safety Communication Consortium. (http://www-nrd.nhtsa.dot.gov/pdf/nrd-12/CAMP3/pages/VSCC.htm)

[4] CVIS project. (http://www.ertico.com/en/activities/efficiency__environment/cvis.htm)

[5] Safespot project. (http://www.safespot-eu.org/)

[6] Common criteria portal

[7] Octave information security risk evaluation

[8] VSC: Task 3 final report: Identify intelligent vehicle safety applications. Technical report, U.S. Department of Transportation (2005)

[9] Doetzer, F., Kosch, T., Strassberger, M.: Classification for traffic related intervehicle messaging. In: Proceedings of the 5th IEEE International Conference on ITS Telecommunications, Brest, France (2005)

[10] Nuseibeh, B., Easterbrook, S.: Requirements engineering: a roadmap. In: ICSE - Future of SE Track. (2000) 35–46

[11] Devanbu, P.T., Stubblebine, S.G.: Software engineering for security: a roadmap. In: ICSE - Future of SE Track. (2000) 227–239

[12] Och Dag, J.N., Regnell, B., Carlshmare, P., Andersson, M., Karlsson, J.: Evaluating automated support for requirements similarity analysis in market-driven development. In: REFSQ 01: Seventh International Workshop on Requirements Engineering: Foundation for Software Quality. (2001)

[13] Park, S., Kim, H., Ko, Y., Seo, J.: Implementation of an efficient requirements analysis supporting system using similarity measure techniques. Information and Software Technology 42(6) (2000) 429–438

[14] Palmer, J., Liang, Y.: Indexing and clustering of software requirements specifications. Information and Decision Technologies 18(4) (1992) 283–299

[15] Toms, M., Cummings-Hill, M., Curry, D., Cone, S.: Using cluster analysis for deriving menu structures for automotive mobile multimedia applications. In: SAE 2001. (2001)

12 Annex A: Technical Use Cases

Besides of the 10 Reference Application Use Cases which was resulted from our cluster analysis there are additional technical use cases which was described by various partners of SEVECOM and could be seen as a pre-work for the requirements analysis.

12.1 BUTE

12.1.1 Traffic signal violation warning

Use Case	Traffic signal violation warning
Creator	BUTE: Tamás Holczer, Laszlo Csik
Goal in Context	Car 2 Car or Car to Infrastructure application
Scope & Level	Application use case
Preconditions	Vehicle receives state of road signal, vehicle is to violate the signal
Success End Condition	The driver of the vehicle violating the traffic signal is warned
Failed End Condition	The driver of the vehicle violating the traffic signal is not warned
Involved components (Any logical components, both hardware and software that are involved in application implementation)	Road Side Unit (RSU) Display On board unit (decide to warn or not) Tamper proof hardware (check the signature of the message) Communication interface (receive the message)
Trigger	Vehicle is to violate traffic signal
Operation description (Complete textual description of application operation)	The in-vehicle system will use information communicated from infrastructure located at traffic signals to determine if a warning should be given to the driver. The communicated information would include traffic signal status and timing, traffic signal stopping location or distance information, and directionality.

Characteristics								
Safety relation	No relation		Safety relevant		Safety critical	x		
In-car system	In-car system involved							
Driver involvement	The driver is warned to brake							
Communication	C2C		C2I		I2C	x		
	One-way	x	Two-way		Single-Hop	x	Multi-Hop	
	Unicast		Broadcast		Geocast	x	Relevancy	
Timing	Timing constraints			x	Periodic messages			x
	Timing constraint: time relevant (~1 sec)							
Security requirements								
ID Authentication	No ID authentication needed							

Property auth.	The sender must be a valid traffic signal
Location auth.	The location of the traffic signal must be authenticated
Integrity	Integrity of the message must be ensured to avoid misleading alerts.
Confidentiality	No confidentiality needed
ID privacy	No ID privacy needed
Jurisdict. Access	No jurisdictional access needed
Availability	This application should always be available anywhere, anytime.
Access control	Everyone should access the application, no access control needed.
Auditability	No auditability needed

Threats	**Criteria**	
	Motivation	Joke, harm
	Target	Vehicle safety, speed of traffic
	Skill of attacker	High
	Technical effort	Wireless access
Classification of risks	Low	

12.1.2 Protected signing

Use Case A	Protected signing	
Goal in Context	Car 2 Car and Car 2 Infrastructure application	
Scope & Level	C2C,C2I infrastructure, Primary Task	
Preconditions	The car wants to send an authenticated message	
Success End Condition	Signature generation successful	
Failed End Condition	Signature generation fails	
Primary, **Secondary Actors**	Protected Signing Device In-Car module	
Trigger	An In-Car module generates an outgoing message, sends it to Protected Signing Device	
Description	**Step**	**Action**
	1	Protected Signing Device receives outgoing message
	2	Protected Signing Device verifies the privilege of message sender device
	3	Protected Signing Device generates Signature on the Message
	4	Protected Signing Device returns signed message
Extensions	**Step**	**Branching Action**
	2a	Message sender device has no right to request signature
	2b	Malicious subsystem tries to get access to the credentials
	3b	The access is detected by the protection
	5	Signature request rejected

Sub-variations		Branching Action

Related information	
Priority	Important
Performance	10 milliseconds
Frequency	Frequent
Channels to actors	In-Car wired communication
Open issues	Device verification
Due Date	
Any other management information	
Superordinates	
Subordinates	

Threats	Criteria	
	Motivation	Joke, Harm safety, Harm Privacy
	Target	Vehicle safety, Vehicle privacy
	Skill of attacker	Mid-High
	Technical effort	Wired connection to Tamper Proof Module
Classification of risks	Medium	

12.1.3 Exchange of platooning information

Use Case	Exchange of platooning information
Creator	BUTE: Tamás Holczer, Laszlo Csik
Goal in Context	Car 2 Car application
Scope & Level	Application use case
Preconditions	Some vehicles go on highway in platoon, known platooning information (location, velocity)
Success End Condition	Platooning information is exchanged
Failed End Condition	Platooning information is not exchanged
Involved components (Any logical components, both hardware and software that are involved in application implementation)	Vehicles in platoon On board unit (put the message together, send the message) Tamper proof hardware (sign the message) Communication interface (send the message)
Trigger	Elapsed time after the last information exchange

Operation description (Complete textual description of application operation)	This application functions only in the control role and improves highway traffic flow and capacity by allowing short-range headway distance following in platoon architecture. The application combines vehicle data with position and map data. The application reduces the amount of time a human controls the vehicle thereby reducing opportunities for driver error. For proper function, vehicles with this application may be required to use dedicated highway lanes. Longitudinal control of the vehicle is provided in order to maintain the short-range headway following within a platoon (similar to adaptive cruise control). Lateral control via automated steering provides lane-keeping and lane change manoeuvres of platoon vehicles in a coordinated manner.

Characteristics									
Safety relation	No relation		Safety relevant		Safety critical	x			
In-car system	Steering, accelerating, decelerating								
Driver involvement	No driver involvement needed								
Communication	C2C	x	C2I		I2C				
	One-way		Two-way	x	Single-Hop		Multi-Hop	x	
	Unicast		Broadcast		Geocast	x	Relevancy		
Timing	Timing constraints			x	Periodic messages			x	
	Timing constraint: time critical (~0.5 sec)								
Security requirements									
ID Authentication	No ID authentication needed								
Property auth.	The car must be a member of the group of valid car								
Location auth.	Location of the cars should be authenticated								
Integrity	Integrity of the message must be ensured to avoid accidents								
Confidentiality	No confidentiality needed								
ID privacy	The ID of the car must be hidden from the other users.								
Jurisdict. Access	Public authorities must access the ID data information in case of an accident.								
Availability	This application should available only for whole roads (not parts of the road)								
Access control	Everyone should access the application, no access control needed.								
Auditability	Cars should be able to prove, what kind of information they sent and received.								

Threats	**Criteria**	
	Motivation	Fame, joke, harm user
	Target	Vehicle, User
	Skill of attacker	High
	Technical effort	Wireless access
Classification of risks	Low-mid	

A.1 DaimlerChrysler

12.1.4 Read vehicle data

Use Case 1	**Read vehicle data**

Goal in Context	Read vehicle data via an attached mobile device	
Scope & Level	In-vehicle protection, Summary	
Preconditions	Mobile device can communicate with car-system Mobile device is “known” to the vehicle (registered) User is “known” to the vehicle (registered)	
Success End Condition	Information/data ware transferred from the vehicle to the mobile device	
Failed End Condition	No information/data is transferred to the mobile device	
Primary, **Secondary Actors**	Vehicle, mobile Device Driver, Passenger	
Trigger	Driver/passenger executes a program/function on the mobile device	
Description	**Step**	**Action**
	1	Mobile device/User identifies itself to the vehicle
	2	Vehicle checks identity of mobile device and user
	3	Vehicle checks access rights of mobile device and user
	4	Vehicle prepares data
	5	Vehicle sends data to the mobile device
Extensions	**Step**	**Branching Action**
	3a	Access Rights not granted by Vehicle: Goto: 6
	6	Vehicle sends error message to the device
Sub-variations		**Branching Action**

Related information	
Priority	Top
Performance	100 milliseconds
Frequency	Depending on the application: every second, minutely - hourly
Channels to actors	Wireless, wired communication, display, keyboard
Open issues	Usage of a Transaction on the vehicle side
Due Date	
Any other management information	
Superordinates	
Subordinates	

Threats	**Criteria**	
	Motivation	Joke
	Target	Vehicle privacy
	Skill of attacker	Low – mid
	Technical effort	Wireless access

Classification of risks	low

12.1.5 Write vehicle data

Use Case 2	**Write vehicle data**	
Goal in Context	Write vehicle data via an attached mobile device	
Scope & Level	In-vehicle protection, Summary	
Preconditions	Mobile device can communicate with car-system Mobile device is “known” to the vehicle (registered) User is “known” to the vehicle (registered)	
Success End Condition	Information/data were transferred from the mobile device to the vehicle	
Failed End Condition	No information/data is transferred to the vehicle	
Primary, **Secondary Actors**	Vehicle, mobile Device Driver, Passenger	
Trigger	Driver/passenger executes a program/function on the mobile device	
Description	**Step**	**Action**
	1	Mobile device/User identifies itself to the vehicle
	2	Vehicle checks identity of mobile device and user
	3	Vehicle checks access rights of mobile device and user
	4	Vehicle sends “ready to receive data” to mobile device
	5	Vehicle receives data and writes data
	6	Vehicle send “success” message to mobile device
Extensions	**Step**	**Branching Action**
	3a	Access Rights not granted by Vehicle: Goto: 7
	7	Vehicle sends error message to the device
Sub-variations		**Branching Action**

Related information	
Priority	Top
Performance	Depending on the amount of data seconds - minutes
Frequency	Depending on the application: minutely - hourly
Channels to actors	Wireless, wired communication, display, keyboard
Open issues	Usage of a Transaction on the vehicle side
Due Date	
Any other management information	
Superordinates	
Subordinates	

Threats	Criteria	
	Motivation	“Fame”, money, joke
	Target	Vehicle privacy, vehicle system functions
	Skill of attacker	mid – high
	Technical effort	Wireless access
Classification of risks	high	

12.1.6 Display security state

Use Case 3	Display security state	
Goal in Context	Display the security state of a vehicle	
Scope & Level	In-vehicle protection, Summary	
Preconditions	Vehicle-system is running	
Success End Condition	Status is correctly displayed, no end!	
Failed End Condition	No status is displayed, status is displayed incorrectly, no end!	
Primary, **Secondary Actors**	Vehicle	
Trigger	None	
Description	**Step**	**Action**
	1	Vehicle security system checks state
	2	Vehicle security system displays state
Extensions	**Step**	**Branching Action**
Sub-variations		**Branching Action**

Related information	
Priority	Top
Performance	100 milliseconds
Frequency	ongoing
Channels to actors	display
Open issues	
Due Date	
Any other management information	
Superordinates	
Subordinates	

Threats	Criteria	
	Motivation	-

	Target	Vehicle privacy
	Skill of attacker	-
	Technical effort	-
Classification of risks	low	

12.1.7 Recover secure state

Use Case 4	**Recover secure state**	
Goal in Context	If a security relevant incident happened, the system re-established a secure state.	
Scope & Level	In-vehicle protection, Summary	
Preconditions	Vehicle-system is running Security State displayed indicates a problem	
Success End Condition	Secure Status is recovered	
Failed End Condition	Secure Status cannot be recovered	
Primary, **Secondary Actors**	Vehicle User (driver)	
Trigger	User executes a function	
Description	**Step**	**Action**
	1	Vehicle security system resets the vehicle system
	2	Vehicle security system performs recovery procedure
	3	Vehicle security system checks system's security state
	4	Vehicle security system displays "ok" state
Extensions	**Step**	**Branching Action**
	4a	(Secure state cannot be recovered) Vehicle security system still indicates the problem
Sub-variations		**Branching Action**

Related information	
Priority	Top
Performance	Up to 2 minutes
Frequency	?
Channels to actors	Display, keypad,
Open issues	
Due Date	
Any other management information	
Superordinates	

Subordinates	

Threats	**Criteria**	
	Motivation	Money, OEM image loss
	Target	Vehicle system function
	Skill of attacker	High
	Technical effort	Direct physical vehicle access
Classification of risks	low	

12.1.8 Check configuration

Use Case 5	**Check configuration**	
Goal in Context	Check the configuration of the vehicle system with a control center to keep the vehicle's configuration up-to-date.	
Scope & Level	In-vehicle protection, Car-to-Infrastructure, Summary	
Preconditions	Start-up of the vehicle-system Control center in the infrastructure is available Communication vehicle-infrastructure is available	
Success End Condition	Configuration is checked	
Failed End Condition	Configuration cannot be checked	
Primary, **Secondary Actors**	Vehicle, control center	
Trigger	Start up of the vehicle system	
Description	**Step**	**Action**
	1	Vehicle system connects to control center (mutual authentication)
	2	Vehicle system loads up-to-date configuration information from control center
	3	Vehicle system assess current configuration and compares it with downloaded configuration
	4	Vehicle informs driver that configuration is up-to-date
Extensions	**Step**	**Branching Action**
	4a	Vehicle informs driver that configuration is not up-to-date
Sub-variations		**Branching Action**

Related information	
Priority	Top
Performance	Up to 5 seconds
Frequency	Daily - weekly

Channels to actors	display
Open issues	
Due Date	
Any other management information	
Superordinates	
Subordinates	

Threats	**Criteria**	
	Motivation	Money, Joke
	Target	Vehicle system function
	Skill of attacker	High
	Technical effort	Direct physical access, Wireless access
Classification of risks	mid - high	

12.1.9 Update SW / data / configuration

Use Case 6	**Update SW / data / configuration**	
Goal in Context	Update SW, data and configurations of the vehicle system with previously downloaded SW / data (see Use Case Download Software)	
Scope & Level	In-vehicle protection, Car-to-Infrastructure, Summary	
Preconditions	vehicle-system is running vehicle does not move new SW / data was downloaded correctly	
Success End Condition	New SW can be used, new configuration is activated	
Failed End Condition	New SW / data / configuration cannot be used	
Primary, **Secondary Actors**	Vehicle, User (driver, passenger)	
Trigger	User activates Update – function	
Description	**Step**	**Action**
	1	Vehicle security system checks rights of the user
	2	Vehicle system performs backup of the current data / configuration (only affected parts)
	3	Vehicle system installs new components
	4	Vehicle system performs a self test and assess current configuration, SW
	5	Vehicle informs driver that update was successful
Extensions	**Step**	**Branching Action**
	5a	Vehicle system restores data configuration
	6	(test not successful) Vehicle informs driver that update was not performed

Sub-variations		Branching Action

Related information	
Priority	Top
Performance	minutes
Frequency	Weekly - monthly
Channels to actors	Display, keypad
Open issues	
Due Date	
Any other management information	
Superordinates	
Subordinates	

Threats	Criteria	
	Motivation	Money, (joke)
	Target	Vehicle system function
	Skill of attacker	mid high
	Technical effort	Direct physical access, Wireless access
Classification of risks	high	

12.1.10 Download SW / data /media

Use Case 7	Download SW / data /media	
Goal in Context	Download SW / data / media files form a service center in the infrastructure.	
Scope & Level	In-vehicle protection, Car-to-Infrastructure, Summary	
Preconditions	vehicle-system is running Service center in the infrastructure is available Communication vehicle-infrastructure is available	
Success End Condition	SW / data / media are downloaded	
Failed End Condition	SW / data / media are not downloaded	
Primary, Secondary Actors	Vehicle, download server (service center, music store, etc.) driver / passenger	
Trigger	Driver, passenger activates a function of the vehicle system and selects Software / data / media to download	
Description	Step	Action
	1	Vehicle security system checks access rights of the user

	2	Vehicle system connects to service center
	3	Vehicle system loads SW / data / media
	3	Vehicle security system checks rights / licenses associated with the downloaded SW / data and enables usage of SW / data
	4	Vehicle system informs driver SW / data / media is downloaded
Extensions	**Step**	**Branching Action**
	2a	Vehicle display “no rights” message
	4a	Vehicle system deletes downloaded SW / data Vehicle system informs driver
Sub-variations		**Branching Action**

Related information	
Priority	Top
Performance	minutes
Frequency	Daily - weekly
Channels to actors	Display, keypad
Open issues	
Due Date	
Any other management information	
Superordinates	
Subordinates	

Threats	**Criteria**	
	Motivation	Joke
	Target	Vehicle system functions
	Skill of attacker	high
	Technical effort	Wireless access
Classification of risks	low	

A.2 University of Ulm

12.1.11 Secure Key Material Exchange

Use Case UULM 3	**Secure Key Material Exchange**
Goal in Context	Deliver or obtain secret key material securely to and from vehicle
Scope & Level	In-Vehicle security, sub-function
Preconditions	Driver has data device containing key material, input mechanism (e.g. RFID reader)

Success End Condition	Secret key material is transferred to and from the car in a secure way	
Failed End Condition	Leakage of secret key material, which may be used for malicious activities	
Primary, **Secondary Actors**	Vehicle, In-Vehicle electronics Vehicle owner, vehicle maintenance staff, possible malicious entities	
Trigger	Secret key exchange is necessary (e.g. due to system malfunction etc.)	
Description	**Step**	**Action**
	1	Insert data device into reader
	2	Authenticate data device
	3	Signal authenticity of data device to driver
	4	Locate key material
	5	Request copy confirmation from driver
	6	Copy and install key material
Extensions	**Step**	**Branching Action**
	2a	Authentication failure: stop process
	3a	Authentication failure: alert user
Sub-variations		**Branching Action**

Related information	
Priority	High
Performance	No special performance requirements
Frequency	Months or eventually years
Channels to actors	Various ways imaginable (cable connection, Near-Field communication, direct user input, key cards, …)
Open issues	
Due Date	
Any other management information	
Superordinates	
Subordinates	

12.1.12 Trustable Warning Message Content

Use Case UULM 2	**Trustable Warning Message Content**
Goal in Context	Car 2 Car application that is intended to distribute warning messages (e.g. accident, slippery road, traffic jam, …) as reliably as possible.
Scope & Level	Car2Car communication, Summary
Preconditions	Vehicle owns number of physical sensors, probably also electronic maps. Information is distributed in the VANET. Vehicles maintain trust ratings of other vehicles in the VANET.
Success End Condition	Bogus information reaching the vehicle is detected and discarded in a large number of cases

Failed End Condition	Vehicles displays/reacts also on a substantial part of injected, probably bogus messages	
Primary, **Secondary Actors**	Vehicle, In-Vehicle electronics Driver, possible malicious entities	
Trigger	Vehicle receives information from other vehicle or infrastructural network entities	
Description	**Step**	**Action**
	1	Receive message
	2	Check trust rating of sender
	3	Apply consistency check
	4	
	5	
	6	
	7	
Extensions	**Step**	**Branching Action**
	2a	Trust rating below threshold: Discard message
	3a	Consistency check fails: Discard message, Adapt trust rating of sending node
Sub-variations		**Branching Action**

Related information	
Priority	Top
Performance	Performance-critical in case of urgent information
Frequency	On demand
Channels to actors	Wireless communication
Open issues	
Due Date	
Any other management information	
Superordinates	
Subordinates	

12.1.13 Trustable Hazard Warning Distribution

Use Case A	**Trustable Hazard Warning Distribution**
Goal in Context	Car 2 Car application that is intended to distribute warning messages (e.g. accident, slippery road, traffic jam, …) as reliably as possible.
Scope & Level	Car2Car communication, Summary
Preconditions	Information about hazard (e.g. slippery) available at vehicle level, working wireless communication protocols

Success End Condition	Information has reached a large amount of addressed vehicles, information reaches destination vehicles with original content	
Failed End Condition	Information is lost, information is modified during its dissemination	
Primary, **Secondary Actors**	Vehicle Driver, possible malicious entities	
Trigger	Vehicle detects hazardous road condition	
Description	**Step**	**Action**
	1	Create or receive message
	2	Check if inside distribution area
	3	Process message
	4	Forward message as broadcast
	5	
	6	
	7	
Extensions	**Step**	**Branching Action**
	2a	If outside distribution area: drop message
Sub-variations		**Branching Action**

Related information	
Priority	Top
Performance	Best effort delivery success ratio, timely delivery (exact value depending on application)
Frequency	On demand
Channels to actors	Multi-Hop wireless communication
Open issues	
Due Date	
Any other management information	
Superordinates	
Subordinates	

A.3 EPFL

12.1.14 Identity and key management – Temporary identity and credential assignment

Use Case A	**Identity and key management – Temporary identity and credential assignment**
Goal in Context	This use ensures that a roaming vehicle can obtain temporary identities and credentials is equipped with its unique electronic identity, cryptographic keys and credentials
Scope & Level	V2V, V2I, I2V communication

Preconditions	Vehicle is equipped and can present the necessary valid long-term credentials; network policy and services require temporary identification	
Success End Condition	Temporary identity and credentials are obtained and securely stored in the tamper-resistant and trusted computing module of the vehicle	
Failed End Condition	No temporary identity and credentials are established; temporary identity and credentials are established and shared by multiple vehicles	
Primary, **Secondary Actors**	Infrastructure, vehicle Authority	
Trigger	Vehicle entering a network region/domain	
Description	**Step**	**Action**
	1	Vehicle obtains network region/domain policy
	2	Vehicle requests temporary identity and credentials
	3	Infrastructure/network authority validates request; if success,
	4	Infrastructure/network authority grants temporary identity and credentials
	5	Vehicle validates the grant response and stores the temporary identity and credentials
	6	Local authority stores in the vehicle (not necessarily in the trusted component) its own credentials necessary to validate the temporary, as well as a set of public keys for other authorities it certifies.
Extensions	**Step**	**Branching Action**
	1-6	Temporary credentials are one-time
	1-6	Temporary credentials are communicated encrypted to the vehicle trusted component, which regulates their use
Sub-variations		**Branching Action**

Related information	
Priority	Top
Performance	On-the-fly; e.g., <10sec.
Frequency	
Channels to actors	Wireless, wire-line
Open issues	Types of transactions that require temporary identities and credentials Properties of such temporary material Linkability to long-term identity and credentials
Due Date	
Any other management information	
Superordinates	
Subordinates	

Threats	**Criteria**	
	Motivation	Access to services; avoidance of identification; 'freedom' to mount a broad range of attacks.
	Target	Illegitimate participation and access to data and services.
	Skill of	High or medium, depending on the system implementation

	attacker	(and 'importance' of temporary credentials). For example, obtaining forged radio frequency identification (RFID) tags may be relatively simple, compared to an attacker that defeats the on-line protocol reflected by Steps 1-6.
	Technical effort	'Off-line' manipulation (credential acquisition) or protocol specific attacks.
Classification of risks	High to low. Illegitimate participation to the system is unwanted, independently of the type of misbehaviour. Yet, temporary credentials grant in general weaker access rights than long-term ones; for example, unauthorized access to a service (e.g., download of a map) may not constitute a risk per se.	

12.1.15 Identity Management – Vehicle Registration

Use Case A	**Identity Management – Vehicle Registration**	
Goal in Context	This use case ensures that the vehicle is equipped with its unique electronic identity, cryptographic keys and credentials	
Scope & Level	V2V, V2I, I2V communication prerequisite	
Preconditions	Vehicle owner/user presents the necessary physical credentials	
Success End Condition	Identity, credentials, and keys are securely stored in the tamper-resistant and trusted computing module of the vehicle	
Failed End Condition	Identity, credentials, and keys secure storage in the tamper-resistant and trusted computing module of the vehicle fails	
Primary, **Secondary Actors**	Authority, vehicle Vehicle owner/user	
Trigger	Initialization necessary for the vehicle to operate within the network	
Description	**Step**	**Action**
	1	User presents physical credentials
	2	Authority and vehicle trusted component (TC) establish an off-line secure channel.
	3	Authority assigns vehicle identity and stores it in TC.
	4	TC generates vehicle private/public key pair and provides the public key to the authority.
	5	The authority certifies the vehicle public key and stores the certificate in TC.
	6	The authority stores in the vehicle (not necessarily in TC) its own public key and certificate, as well as a set of public keys for other authorities it certifies.
Extensions	**Step**	**Branching Action**
	3-5	Repeat steps 3 to 5 for each key pair in a set of multiple keys
	5	The authority stores one or more attribute certificates.
Sub-variations		**Branching Action**
	3-5	Different key pairs are associated with different attribute certificates.
	3-5	The vehicle obtains anonymous credentials, which do not reveal the vehicle's unique identity

Related information	
Priority	Top
Performance	Offline; e.g., <10min
Frequency	Once per year for the full procedure Step 6 otherwise on demand when vehicle needs to operate in a network area administered by a foreign authority,
Channels to actors	Wireline (non RF in general)
Open issues	Unique identity Types of keys and credentials Capabilities (processing, storage) of the on-board unit and TC.
Due Date	
Any other management information	
Superordinates	
Subordinates	

Threats	**Criteria**	
	Motivation	Avoidance of identification; 'freedom' to mount a broad range of attacks.
	Target	Illegitimate participation and access to data and services.
	Skill of attacker	High or irrelevant (from the vehicular system's point of view). High if the attacker tampers with the technical part of the process, irrelevant (yet always high) if the attacker can forge or misuse physical credentials (Step 1 above).
	Technical effort	Manipulation of the bootstrapping process or tampering with the TC and the stored data.
Classification of risks	High; illegitimate participation to the system is unwanted, independently of the type of misbehaviour or, more general, the deviation from the system enforceable policy.	

12.1.16 Identity Management – Identity Escrow

Use Case A	**Identity Management – Identity Escrow**	
Goal in Context	This use case ensures that the vehicle unique identity is hidden during its communications but can be retrieved with the help of an authority	
Scope & Level	V2V, V2I, V2I	
Preconditions	Vehicle equipped with anonymous credentials; authority holding the identity of the vehicle; log trail of transactions	
Success End Condition	A log trail of anonymous transactions is linked to the vehicle	
Failed End Condition	An anonymous transaction is linked to a vehicle different from the one that performed it, or to no vehicle among those registered with the authority	
Primary, **Secondary Actors**	Authority, infrastructure Vehicle	
Trigger	Administrative reasons or node faulty behaviour	
Description	**Step**	**Action**

	1	Fault detector or authority triggers request, providing a log trail
	2	Authority validates request; if success,
	3	Authority retrieves the identity of the vehicle that performed the transactions
	4	Authority responds with requested identity to the authorized entity
Extensions	**Step**	**Branching Action**
	1	The request is directed to a distinct system entity (authority) that validates it, and then, in case of success, directs it to the authority that holds the set of identities
	4	The authority responds to the requester, or responds to a third designated entity
Sub-variations		**Branching Action**

Related information	
Priority	Top
Performance	Varies; on-the-fly if immediate action is to follow the 'opening' of the identity; e.g., <10sec. Offline; e.g., <10min.
Frequency	On demand
Channels to actors	Wireless, wire-line
Open issues	Structure of authority Reasons that trigger revelation of the identity Authority to request and perform the identity revelation
Due Date	
Any other management information	
Superordinates	
Subordinates	

Threats	**Criteria**	
	Motivation	Avoidance of identification and attribution of liability in case of faulty/malicious behaviour.
	Target	Accountability
	Skill of attacker	High or irrelevant. Depending on the context, the attacker could elect an elaborate strategy of actions that constitute misbehaviour yet impede the irrefutable attribution of liability, Or depending on the system implementation, an attacker might succeed in impersonating other entities and thus cause a false identification. Or, the attacker could attempt to penetrate the authority servers. Nonetheless, the success of the identification per se can be achieved (if impersonation is successfully mitigated) irrespective of the success of any subsequent actions (e.g., irrefutable liability).
	Technical effort	Wiretapping, eavesdropping of wireless communication, or, actively, initiation of a protocol (e.g., impersonating a road-side unit)
Classification of risks	Varies, depending on the type of misbehaviour or, more general, the underlying deviation from the system enforceable policy, as well as the (urgency of) actions subsequent to the identification.	

12.1.17 Identity and key management – Revocation of credentials

Use Case A	**Identity and key management – Revocation of credentials**	
Goal in Context	This use ensures that the vehicle's credentials can be revoked when necessary	
Scope & Level	V2V, V2I, I2V communication	
Preconditions	System-wide policies governing the use and validity of the credentials of the system entities	
Success End Condition	Vehicle (node, in general) revoked credentials can no longer be validated by any other correct network node	
Failed End Condition	Vehicle (node, in general) credentials remain in use and are accepted as valid by correct nodes, in spite of their revocation	
Primary, **Secondary Actors**	Authority, vehicle, infrastructure	
Trigger	Credential expiration or authority decision	
Description	**Step**	**Action**
	1	Authority decides that vehicle credential(s) is (are) to be revoked
	2	Authority updates a data structure that describes or reflects revoked credentials
	3	Authority communicates the revoked credentials information to nodes that need to verify the validity of these credentials
Extensions	**Step**	**Branching Action**
	3	Authority distributes the revoked credentials information to all nodes throughout its domain
	3	Authority provides multiple points of access to the revoked credentials information, and provides it on demand to all requesting nodes
Sub-variations		**Branching Action**
	3	Authority communicates revocation information to other authorities

Related information	
Priority	Top
Performance	Varies; from <10sec to 'manual' access
Frequency	On-demand, upon a new revocation decision Periodic with varying frequency depending on the network domain locality
Channels to actors	Wireless, wire-line
Open issues	Required properties (e.g., timeliness and extent) of the revocation services provided by the authority Tolerance and trade-offs between different methods
Due Date	
Any other management information	
Superordinates	
Subordinates	

Threats	**Criteria**	

	Motivation	Avoid eviction in case of faulty/malicious behaviour
	Target	Administrative processes and protocols
	Skill of attacker	High; an attacker may elect an elaborate strategy to avoid the authority's decision of eviction, forge or misuse credentials, or manipulate the process that leads to the authorities' decision for revocation.
	Technical effort	Varies, from 'off-line' actions to message and credential fabrication and transmission/use.
Classification of risks	Varies, depending on the type of misbehaviour or, more general, the underlying deviation from the system enforceable policy. E.g., a vehicle that requires a minor service poses (at least, within a short period of time from the malfunction detection from the OBU) a lower risk than an active attacker that tampers with all messages that it relays in the network.	

12.1.18 Identity Management – Anonymous credentials and transactions

Use Case A	**Identity Management – Anonymous credentials and transactions**	
Goal in Context	This use ensures that the vehicle can anonymously perform transactions	
Scope & Level	V2V, V2I communication	
Preconditions	Vehicle is equipped with anonymous credentials	
Success End Condition	Vehicle performs the transaction without revealing information beyond that provided in the used anonymous credential	
Failed End Condition	Vehicle does not complete the transaction or information beyond what is necessary is revealed (leaked)	
Primary, **Secondary Actors**	Vehicle, infrastructure (road side unit), server	
Trigger	User input, location or time trigger	
Description	**Step**	**Action**
	1	Vehicle presents anonymous credentials
	2	Vehicles or infrastructure or servers accessible through the infrastructure, the credential verifiers, validate the credentials
	3	Verifier of credentials grants service or access
Extensions	**Step**	**Branching Action**
Sub-variations		**Branching Action**

Related information	
Priority	Top
Performance	On-the-fly; e.g., <10sec.
Frequency	On-demand, on-line transactions and communication
Channels to actors	Wireless, wire-line
Open issues	Types of credentials Types of transactions

	On-board unit and trusted components processing capabilities
Due Date	
Any other management information	
Superordinates	
Subordinates	

Threats	**Criteria**	
	Motivation	Surveillance (and consequently harm or profit)
	Target	Private information
	Skill of attacker	High, medium. Depending on the context; e.g., an attacker can locate itself next to an infrastructure access point, deploy multiple eavesdroppers, or penetrate a location/transaction data base.
	Technical effort	Wiretapping, eavesdropping of wireless communication, or, actively, initiation of a protocol (e.g., impersonating a road-side unit)
Classification of risks	Varies, depending on the implementation of the system that is targeted for extracting the private information from.	

A.4 Trialog

12.1.19 V2I and V2C Authentication QoS

Use Case A	**V2I and V2C Authentication QoS**	
Goal in Context	Car 2 Car application. Will ensure that V2I and V2C mutual authentication takes into account QoS needs (response time)	
Scope & Level	C2C infrastructure, Summary	
Preconditions	Car A is running Car B is running Roadside equipment R is close to A	
Success End Condition	Car A and roadside equipment have exchanged C2C application payload Car A and B have exchanged C2C application payload	
Failed End Condition		
Primary, **Secondary Actors**	In-Vehicle platform, Roadside Platform	
Trigger	C2C application event	
Description	**Step**	**Action**
	1	A reaches a point where V2C communication with R is possible
	2	A and R exchange credentials sufficiently rapidly
	3	R transmits data traffic info T to A
	4	A reaches a point where C2C communication with B is possible
	5	A and B exchange credentials sufficiently rapidly

	6	A transmits data traffic info T to B
Extensions	**Step**	**Branching Action**
Sub-variations		**Branching Action**

Related information	
Priority	
Performance	
Frequency	
Channels to actors	
Open issues	Privacy and Identity Management
Due Date	
Any other management information	
Superordinates	
Subordinates	

Threats	**Criteria**	
	Motivation	Denial of service
	Target	Infrastructure
	Skill of attacker	Low – mid
	Technical effort	Simulating large number of V2V/V2I to create QoS problems
Classification of risks	Low occurrence, high impact	

12.1.20 Public Key Infrastructure Deployment

Use Case A	**Public Key Infrastructure Deployment**	
Goal in Context	Organise and deploy public key infrastructure for Car 2 Car application.	
Scope & Level	C2C infrastructure, Summary	
Preconditions	Infrastructure requiring the assignment of individual keys to CVIS entities has been finalised and standardised	
Success End Condition	PKI infrastructure in place. Deployment can take place)	
Failed End Condition		
Primary, **Secondary Actors**	In-Vehicle platform, Roadside Platform, Registration Authority, Certificate Authority, Country, Europe	
Trigger	Pan-European deployment decision	
Description	**Step**	**Action**
	1	Europe and Countries agree for pan-European Interworking,

		compatible with C2C PKI architecture scheme
	2	Country A consults with national stakeholders (e.g. a car manufacture, a road operator, a national certificate authority) and defines a national PKI infrastructure for vehicles and for road side equipment. They also negotiate with Europe and pan-European business stakeholders an Interworking scheme
	3	C2C applications can be used in country A.
	4	Country B consults with national stakeholders (e.g. a car manufacture, a road operator, a national certificate authority) and defines a national PKI infrastructure for vehicles and for road side equipment. They also negotiate with Europe and pan-European business stakeholders an Interworking scheme.
	5	In-Vehicle platforms and Roadside platforms or country B are deployed with certificates
	6	C2C applications can be used in country A and B. Vehicles from A and B can interwar in either countries
Extensions	**Step**	**Branching Action**
Sub-variations		**Branching Action**

Related information	
Priority	
Performance	
Frequency	
Channels to actors	
Open issues	Political organisation and agreement
Due Date	
Any other management information	
Superordinates	
Subordinates	

Threats	**Criteria**	
	Motivation	National Protectionism
	Target	Infrastructure pan-European Interworking
	Skill of attacker	Low – mid
	Technical effort	Incompatible PKI infrastructure
Classification of risks	Low occurrence, high impact	

12.1.21 Operation Data Monitoring

Use Case A	**Operation Data Monitoring**

Goal in Context	Car 2 Car application. Will ensure that some operation data can be collected. This use case will lead to liability management considerations	
Scope & Level	C2C infrastructure, Summary	
Preconditions	Data collected are organised according to a partition arrangement In-Vehicle Platforms and/or Roadside platforms have monitoring capabilities Monitored data can be collected at transferred to a Control Centre	
Success End Condition	Data Collected	
Failed End Condition		
Primary, **Secondary Actors**	Stakeholder, Regulator, Infrastructure operator	
Trigger	Deployment of data collecting capability	
Description	**Step**	**Action**
	1	Stakeholder A (e.g., Manufacturer, operator, regulator) decide for data collecting capability
	2	Stakeholder A make deals with deployment stakeholder U to collect data of certain type compliant to regulator rules
	3	The infrastructure operator plans for a subsequent deployment of new bundles in charge of collecting data.
Extensions	**Step**	**Branching Action**
Sub-variations		**Branching Action**

Related information	
Priority	
Performance	
Frequency	
Channels to actors	
Open issues	Liability Management
Due Date	
Any other management information	
Superordinates	
Subordinates	

Threats	**Criteria**	
	Motivation	Preventing identification for unlawful purposes
	Target	Infrastructure stakeholder point of observation
	Skill of attacker	Low – mid
	Technical effort	Access to an operation data point of observation • wireless level • infrastructure level

Classification of risks	Low occurrence, high impact	

12.1.22 Operation Data Protection

Use Case A	**Operation Data Protection**	
Goal in Context	Car 2 Car application. Will ensure that operated data are strictly partitioned according to an arrangement. This use case will lead to privacy and identify management considerations at the architecture level. In particular stakeholders will no be able to access data from other partitions	
Scope & Level	C2C infrastructure, Summary	
Preconditions	Vehicle Platforms have monitoring capabilities Monitored data can be collected at transferred to a Control Centre	
Success End Condition	The partition arrangement prevents stakeholders to combine collected data and infer further information. No correlation capability is possible unless all credentials of all stakeholders are made available (e.g. through a judge order)	
Failed End Condition		
Primary, **Secondary Actors**	Regulator, In-Vehicle platform, Roadside Platform, Business stakeholder, Infrastructure operator	
Trigger	Deployment creates privacy concern	
Description	**Step**	**Action**
	1	Regulator orders a data partition arrangement. C2C/V2C infrastructure architecture supports the definition of such arrangements including modification of arrangements overtime
	2	Business stakeholder A and B make deals with deployment stakeholder U to collect data of certain type compliant to regulator rules (a business stakeholder could be a service provider, a telecom operator, a facility management company etc.. a deployment stakeholder could be a manufacturer, a telecom operator, a service provider)
	3	Deployment stakeholder U collects data for business stakeholder A and B (for instance a telecom operator can collect diagnosis data on behalf of a certain car manufacturer). U can only collect data for A. It cannot analyse of A because it lacks the data identification credential which only A knows. Likewise, if U provides B data to A by accident, this cannot be analysed.
	4	After several years of operations and growth, Regulator sees that data collected for A converge into patterns allowing some unexpected inferences. It orders the infrastructure to evolve into a new data arrangement. The infrastructure architecture supports that.
	5	The infrastructure operator plans for a subsequent deployment of new bundles in charge of collecting data according to the new arrangement
Extensions	**Step**	**Branching Action**
Sub-variations		**Branching Action**

Related information	
Priority	
Performance	
Frequency	
Channels to actors	
Open issues	Privacy and Identity Management
Due Date	
Any other management information	
Superordinates	
Subordinates	

Threats	**Criteria**	
	Motivation	Accessing private data, Stealing business data
	Target	Driver privacy, Vehicle privacy, Stakeholder business data
	Skill of attacker	Low – mid
	Technical effort	Access to an operation data point of observation • wireless level • infrastructure level
Classification of risks	Low occurrence, high impact	

13 Annex B: Inputs from Other Projects

13.1 C2C Communication Consortium (C2C-CC)

The Application Working Group of the C2C-CC is currently working (status October 2006) on the descriptions of the C2C relevant applications. Currently the WG is specifying the following 6 applications which cover the C2C use cases:

1. V2V Cooperative Awareness
2. V2V Unicast Exchange
3. V2V Decentralized Environmental Notification
4. Infrastructure to Vehicle (one-way)
5. Local RSU Connection
6. Internet Protocol Roadside Unit Connection

The WG has also defined the terms for the description of the applications

Term	Definition
Actor	Identifies a person(identified by role), a computer system or component or organization interacting with the system under discussion.
Scenery	Location and circumstances of a scenario. E.g. highway scenery.
Scenario (=Use case instance)	A specific sequence of actions and interactions between actors and the system under discussion; it is also called a use case instance. It is one particular story of using a system, or one path through the use case. They describe concrete system behaviours by summarizing behaviour traces of existing or planned systems.
Use Case	A collection of related success and failure scenarios that describe actors using a system. The Rational Unified Process defines a use case as “a set of use cases instances, where each instance is a sequence of actions a system performs that yields an observable result of value to a particular actor”. This is more ore less the equivalent of the definition given by Jacobson” a behaviorally related sequence of transactions in a dialogue with the system”.
Application	According to a definition provided by Wikipedia an application is a solution running on a computer system which supports goal(s) of users. The application is based on a system architecture – often a layered architecture composed of a presentation tier, business logic tier and a persistence tier. An application may comprise several functional elements or functional building blocks. In this way an application may cover and support a set of use cases including corresponding scenarios.
Application Instance	Identifies a specific selection of functional elements of an application.

Figure 2: Definition of Terms for the C2C-CC applications

Use cases with similar requirements, resulting in common communication mechanisms, are grouped in these 6 applications.

Applications	V2V Cooperative Awareness	V2V Unicast Exchange	V2V Decentralized Environmental Notification	Infrastructure to Vehicle (one-way)	Local RSU Connection	Internet Protocol Roadside Unit Connection
Use Cases (C2C-CC)	V2V Merging Assistance	Pre-Crash Sensing/Warning	Slow Vehicle Warning	Hazardous Location I2V Notification	Automatic Access Control	SOS Services
	Cooperative Forward Collision Warning	V2V Merging Assistance	Post-Crash Warning	Traffic Signal Violation Warning	Personal Data Synchronisation at home	Just-In-Time Repair Notification
	Emergency Electronic Brake Lights	Cooperative Vehicle-Highway Automation System (Platoon)	In-Vehicle Amber Alert	Stop Sign Violation Warning	Infrastructure based Cooperative merging Assistance	Media Download
	V2V Lane Change Assistance	Instant Messaging	Safety Recall Notice	Limited Access Warning	Remote Diagnostics	Map Downloads and Updates
	Approaching Emergency Vehicle Warning		Traffic Jam Ahead Warning	Green light optimal speed advisory	Free-Flow Tolling	Enhanced Route Guidance and Navigation
	Highway/Rail Collision Warning		Hazardous Location V2V Notification	V2I Traffic Optimization	Drive-through payment	Fleet Management
	Wrong Way Driving Warning		Safety Service Point	GPS Correction	Vehicle Computer Program Updates	
	Cooperative Glare Reduction		Decentralised Floating Car Data	Adaptive Drive-train Management		
	Cooperative Adaptive Cruise Control			Point of Interest Notification		

Table 1: C2C-CC Applications and Use Cases

13.1.1 Mapping of C2C-CC Use Cases on Sevecom Application Use Cases

Currently (status October 2006) the C2C-CC WG Applications has not specified in detail all use cases shown in Table 1. But to emanate from the use case titles the greyed cells in the table show the direct mapping of the C2C-CC use cases to the Sevecom use cases. For all use cases left some mapping efforts will be explained in the following.

The Use Cases of the column “V2V Decentralized Environmental Notification” provide information about events and roadway characteristics that are probably interesting to vehicles or drivers for a certain time in a certain area. Therefore these use cases could be mapped on Sevecom use cases of the categories “Assist Driver on special road conditions” (3.5) and “Assist driver in dangerous traffic situations (3.7). The same mapping could be done with the C2C-CC use cases “Hazardous Location I2V Notification” and “Limited Access Warning”.

The Use Cases “Green light optimal speed advisory” and “V2I Traffic Optimization” could be seen as characteristic of the Sevecom application use case “Intelligent traffic flow control” (3.9.1)

“Infrastructure based Cooperative merging Assistance” could be seen as a specification of the Sevecom use case “Highway merge assistant” (3.8.1).

"Free-Flow Tolling" and "Drive-through payment" could be fulfilled by the Sevecom use cases ""Area access control" (3.12.2) and "Electronic Payment" (3.12.3).

"Vehicle Computer Program Updates" is similar to the Sevecom use case "Software update/flashing" (3.6.4) and "Media Download" could be handled by the Sevecom use case "Internet service provisioning/info fuelling" (3.11.3)

Only for the C2C-CC use case "Personal Data Synchronisation at home" there is no obvious mapping on one of the Sevecom application use cases noticeable, but the security requirements could be similar to the Sevecom use cases "Software update/flashing" and "Internet service provisioning/info fuelling".

The more encompassing Sevecom application use case list still includes additional use cases which are not "directly" described by the C2C-CC WG, but Table 2 shows a possible mapping of these use cases to the C2C-CC applications.

Applications (C2C-CC)	**V2V Cooperative Awareness**	**V2V Unicast Exchange**	**V2V Decentralized Environmental Notification**	**Infrastructure to Vehicle (one-way)**	**Local RSU Connection**	**Internet Protocol Roadside Unit Connection**
Use Cases (Sevecom)	Left turn assistant		Emergency vehicle at scene warning	General in-vehicle signage	Emergency vehicle signal pre-emption	Parking spot locator
	Intersection collision warning		Stolen vehicle tracking	Pedestrian crossing information	Vehicle safety inspection	
			Visibility enhancer	Curve-speed warning	Electronic license plate	
				Cooperative positioning improvement	Electronic driver's licence	
					Stolen vehicle tracking	
					Vehicle probes provide weather data to Transportation Operations Center (TOC)	
					Crash data to TOC	
					Origin and destination to TOC	
					Rental car processing	
					Hazardous material cargo tracking	

Table 2: Mapping of some Sevecom use cases to C2C-CC applications

Only the Sevecom use cases "Event data recording" and "Mobile access to vehicle data (PDA, Mobile Phone, …)" could not be allocated to the C2C-CC applications because there is no communication link needed ("Event data recording") or the communication link ("Mobile access to vehicle data") is not considered by the C2C-CC.

As a first estimation all C2C-CC applications and the appending use cases should be fulfilled by the Sevecom requirements and the constitutive security mechanisms, which will be specified in the Sevecom Deliverable 2.1 "Security Architecture and Mechanisms". A concluding evaluation if the Sevecom security mechanisms are

really useful for the C2C-CC use cases should be part of the last step of the Sevecom requirements process (“Step 10: Generalization”).