# Security Architecture for Vehicular Communication

Matthias Gerlach*, Andreas Festag**, Tim Leinmüller***, Gabriele Goldacker* and Charles Harsch**
*Fraunhofer Institute for Open Communication Systems (FOKUS), {Matthias.Gerlach |Gabriele.Goldacker}@fokus.fraunhofer.de,
**NEC Deutschland GmbH, {festag |harsch}@netlab.nec.de,
***DaimlerChrysler AG, Group Research and Advanced Engineering, Tim.Leinmueller@DaimlerChrysler.com

***Abstract*— Despite recent progress for vehicular communication in research, development, field tests, and standardization, security is still in an early phase though it represents a crucial part of the vehicular communication system.**

**So far, no vehicular security architecture has been proposed which integrates existing individual solutions for vehicle registration, data integrity, authentication, and so on. By description of different architectural perspectives, we identify the stakeholders and their responsibilities. Then, we focus on the functional layer view and highlight the concepts which jointly secure the vehicular communication. Based on these concepts, we present an implementation approach which introduces the security concepts into the protocol stack of a vehicular communication system.**

**The proposed security architecture follows a clean and modular design. It is the basis for our prototype implementation which will serve as a proof-of-concept. We will also submit this architecture to the ongoing standardization process of the *Car2Car Communication Consortium (C2C-CC)*.**

## I. Introduction

Vehicular communication based on wireless short-range technology enables spontaneous information exchange among vehicles and with road-side stations. It enables a plethora of new applications for safety, traffic efficiency, and infotainment using direct or multi-hop communication at low cost. For these applications, security is mandatory and an integral part of the whole system.

Security issues, and therefore also the integration of security in a vehicular communication system, cover aspects ranging from sensor data protection, secure communication, to tamper-proof hard- and software. Security affects all parts of the system. For the development of a secure system, a well-defined, modular and extensible structure and clearly defined application programming interfaces are necessary.

Security threats and the corresponding security requirements in vehicular environments have been described in detail in [1] and [2]. In a nutshell, the security measures shall prevent privacy violations, denial of service attacks against the system, and the insertion of forged data into the system.

### A. Related Work

Currently, there are a couple of projects concerning vehicular networks, such as *Network on Wheels* [3], *Willwarn* [4], and *GST* [5]. The *C2C-CC* [6] and *IEEE WAVE* (the 1609 suite of standards and IEEE 802.11p) represent the standardization efforts in Europe and the U.S., respectively. Concerning security in vehicular communication, the *SEVECOM* project started recently [7].

The security architecture developed by the *Vehicle Safety Communications Consortium (VSCC)* and subsequently submitted to *IEEE P1609.2* can be seen as the only approach for a security architecture in vehicular networks that is under standardization so far [8]. It defines a public-key-infrastructure (PKI)-based approach for securing messages sent in a vehicle-to-vehicle and vehicle-to-infrastructure fashion. The standard, however, does not address privacy issues, multi-hop communication, and how the network can be protected against malicious certified nodes.

Work by Hubaux and Raya addresses security issues in vehicular communication, mainly in a PKI setting. In [9], they discuss attacks on vehicular networks and security requirements, propose a PKI based solution and outline open issues. In [10], the authors propose different mechanisms for certificate revocation. They also discuss privacy issues in vehicular networks. In [11], assumptions, security requirements and principles, including architectural aspects, are discussed.

As it is simple to manipulate sensor information the plausibility of information should be assessed upon reception. Golle et al. provide a framework to detect and correct false information in [12].

In this paper, we present an architecture that is able to integrate these different existing solutions.

### B. Outline and Main Contributions

In this paper, we present a security architecture for vehicular communication, a security-enhanced vehicular communication system, and a corresponding protocol architecture. We furthermore describe an implementation concept which allows a structured and efficient integration of security into the system.

The main contributions of this paper are:

- the abstract description of a security architecture for vehicular communication using different views,
- the proposal of relevant security concepts and a description of their implementation on a node-local security system.

The different views cover the important security aspects in a systematic approach. The high level functional view can be used to identify responsibilities for the deployment of a vehicular communication security system; the implementation-near views described in Sec. IV propose concrete mechanisms

and a way to integrate them into a vehicular communication system.

The proposed architecture leaves room for combining different security mechanisms to extend the system, e.g. to react to new threats. Further, its structure gives application developers the means to customize the confidence evaluation provided by the security system. Parts of this architecture are already implemented and the experience gained has been fed back into the security architecture.

This remainder of this paper is organized as follows: Sec. II describes the high level view of the security architecture, its functional layers and involved actors. Sec. III describes the proposed security concepts for the vehicular security system. Sec. IV provides details on the implementation specific view, and how the above concepts can be integrated in a modular fashion. Sec. V concludes the paper and outlines future work.

## II. Security Architecture

Describing an architecture using different viewpoints is common practice in software engineering [13]. We specify four different views:

- the functional layer view,
- the organizational / component view,
- the reference model view, and
- the information centric view.

In Sections II-A and II-B, we describe the high level view of the architecture, namely the *functional layers* and the *organizational and component view*, whereas we leave the implementation-near views – the *reference model view* and the *information-centric view* – to Sec. IV.

### A. Functional Layers View

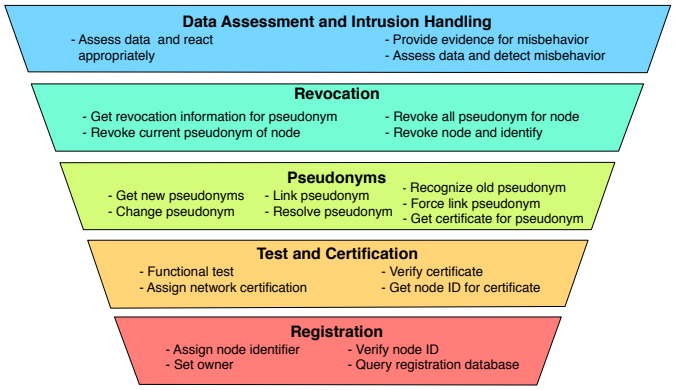


Fig. 1. Functional layers of the security architecture including use case names for each layer

The functional layers depicted in Fig. 1 describe a decomposition of the security system into groups of use cases for a specific functionality. While the lowest layer is concerned with vehicle and application registration and identification, the higher layers are concerned with proper system operation, appropriate security measures and user privacy protection (see [14] for more details).

The decomposition describes a complete view of a security solution under rather general security and application requirements. Hence, a concrete security solution may not need all components or even all layers or to be present.

The lowest layer is concerned with the *registration* of nodes, i.e., OBUs and RSUs[1]. This implies the mapping of an acquirer or owner – the legal entity who bought the unit – to the identifier of a node. The registration layer basically contains the registration database that may contain any relevant information about a vehicle, like its vehicle identification number, its color, the brand. An *identifier* is defined as "an object that can act as a reference to something that has an identity, " as defined by Stoneburner in [15]. An identity makes an object unique within a set of other objects. The registration process is a common process for vehicular environments; in general, it is used in scenarios where accountability (of a human) is an issue. Typically, the more applications may affect human lives, security designs require stricter accountability.

The *test and certification layer* is responsible for assessing the correctness of operation of a node. This process ensures that only nodes with verified properties may actively participate in the communication. One or several digital certificates issued by the testing authority vouch for the correct operation of the node. In addition, different roles may be assigned to a node. Certificates in the certification layer shall not be used for the communication. The test and certification process is a protective measure against the unauthorized insertion of data into the network. It is a means to control the fulfillment of requirements with respect to the performance, behavior and reliability of a system.

The *pseudonym layer* provides a basic level of anonymity by introducing the possibility to use changing pseudonyms that cannot be linked by unauthorized parties (a) to the vehicle, (b) to the acquirer and (c) among each other. Pseudonyms shall express the same roles as the certificate issued for the node. They are used for the communication system and are equivalent to a certified MAC/IP address that is bound to a cryptographic key. Changing pseudonyms provide a fair amount of privacy to the users while allowing for revoking (escrowing) privacy if required by some applications. Privacy provision of the system can be important even to meet the regulatory requirements of certain countries. The requirement for escrow depends on the impact of failing security on the system users. Clearly, if life or the functionality of the whole transportation system are at stake, revocation is more important than if failing security only results in a couple of false messages (a mere nuisance).

The *revocation layer* is concerned with excluding nodes from the system. It contains a database of revoked pseudonyms and distributes this data to all nodes in the system if necessary, depending on the scale of the revocation decision. The scale can range from only node-local to system-wide revocation. A reaction to detected attacks carried out by a node is to exclude this node from the system. Other reasons not directly owed

[1]OBU – On Board Unit, RSU – Road Side Unit

to system operation, such as a stolen unit or prevention of criminal activity may also require a revocation service.

The *data assessment and intrusion handling layer* is responsible for assessing data, auditing them and detecting and handling misbehavior. Misbehavior and faulty nodes can sometimes not be distinguished, we use the word misbehavior to also include faulty nodes. The decision to ignore data or to initiate the revocation process is taken in this layer. If revocation of nodes is an issue, an authority and appropriate mechanisms must exist to decide if a node must be revoked. In large networks, where automatic detection and reaction is necessary, this layer is particularly important. Besides system-wide detection of malicious and false data, node-local detection and reaction is necessary to minimize the impact of malicious or malfunctioning nodes.

### B. Organizational and Component View

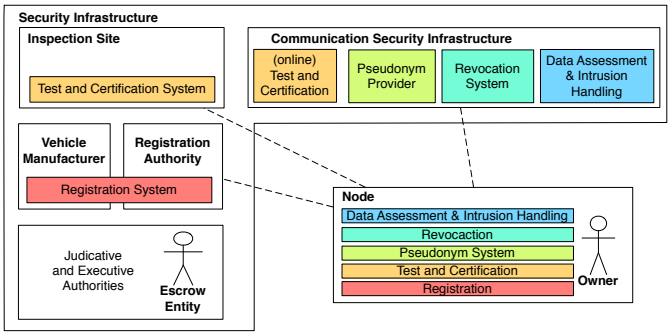


Fig. 2. The organizations and components in a vehicular communication security system

This view describes actors and components that are part of the security system. In Fig. 2, the different components – systems, humans, organizations and authorities – are depicted. The main building blocks in the security architecture are the security infrastructure and the node. The figure also depicts which functionality resides in which component of the system.

The *security infrastructure* contains

- the vehicle manufacturer and the registration authority for the registration of nodes
- the inspection site for test and certification of nodes
- the "Escrow" which includes the escrow entity with the authoritative power to identify – i.e., void the anonymity of – and revoke nodes
- the communication security infrastructure, which includes the communication systems, processing and databases necessary to carry out online testing, pseudonym provision for nodes, revocation of nodes and infrastructure based data assessment and intrusion handling.

Vehicle manufacturer and registration authority together cover two major tasks: first, the assignment of a unique identifier to the vehicle and the corresponding OBU and second the registration of the vehicle owner and his vehicle with the appropriate authority. For RSUs, the owner would be the respective authority or company operating it.

The inspection site can be seen as a placeholder for an organization where the OBU or RSU can be functionally tested; upon completing the test successfully, a certificate is issued for the node. This certificate in turn can be used to get valid pseudonyms for network operation using the communication security infrastructure.

The escrow entity represents courts, police officers, and technical staff that together decide if a node shall be revoked or not under certain circumstances. Its involvement depends on the level of revocation, from temporarily revoking a pseudonym to the identification of the owner of the vehicle.

The *node* contains the counterpart modules for each functionality of the security system. In some cases the whole functionality of a layer can be implemented by the node. It can be registered, certified, revoked and can get new pseudonyms for network operation. A node is linked to the *owner* which – similar to the current status in transportation – is responsible for the regular maintenance of the vehicle and the communication system.

The dotted lines between the node and the security infrastructure indicate that the components communicate. For the registration, the owner of the car would communicate with the authority directly. For the test and certification process, a wired and a wireless connection can be assumed for, e.g., test vector upload and network protocol testing, respectively. Interaction with the communication security infrastructure depends on which module is involved. It is important to note that we assume sporadic access to the infrastructure. Some modules, such as the pseudonym provider and online test and certification may need reliable and on-demand connectivity, that could be provided by cellular technologies. As discussed in [10], distributing revocation information can also be achieved by simple terrestrial broadcast.

## III. Security Concepts

For a security architecture for vehicular communication a large set of relevant security concepts exists, including concepts for

- node identification,
- digital signatures and certificates,
- pseudonyms for location privacy protection[2],
- detection of protocol violation,
- plausibility checks,
- tamper-resistant devices,
- access control policies,
- software certification,
- in-vehicle network security,
- secure positioning, and more.

While most of them are not specific to vehicular communication, their application has already been discussed in the literature. Examples are tamper-resistant devices, node identification using an electronic license plate (see Sec. I-A). Others, like software certification and in-vehicle network

[2]In this work, we assume location privacy protection by anonymization through pseudonyms.

security, do not directly concern the communication though they are important and closely related.

In this paper, we focus on four main concepts which we consider to be most relevant for the implementation of the security architecture. We see *digital signatures* as the enabler of a flexible and efficient crypto-based security solution that is easy to administer. Further, *plausibility checks* increase the confidence information that is transmitted and processed by the applications. Third, we introduce *confidence values* as a measure to express the credibility of data. Finally, we consider *pseudonyms and intelligent pseudonym change*.

### A. Digital Signatures and Certificates

Asymmetric cryptography provides authentication, integrity, and non-repudiation of received messages. In order to provide secure multi-hop communication, the network security module provides a combination of hop-by-hop and end-to-end signatures. For secure routing, the routing header is divided into *immutable* and *mutable* fields. Immutable are those fields that remain unchanged from sender to destination , e.g., destination and source addresses and source position. Mutable fields, such as sender address, sender position and time-to-live (TTL), are allowed to be altered by intermediate nodes. For packets being sent via multiple wireless hops, two signatures are added: an end-to-end signature is created by the source node over the immutable fields of the packet header. Additionally, a hop-by-hop signature is added for the mutable fields. On reception of a data packet a node verifies both signatures, and replaces the hop-by-hop signature by a new one for the altered mutable fields and keeps the end-to-end signature. Eventually, the combination of end-to-end signatures results in a trusted forwarding chain [16].

### B. Cross-Layer and Cross-Application Plausibility Checking

Plausibility checks compare received information with the expected value by means of heuristics. Typically, statements about the range of a certain value are made. The concept specifically addresses security issues of active safety applications in VANETs. It is one of the main components to feed input to the confidence evaluation system of the security architecture.

Plausibility checks can be applied at different protocol layers, mainly at network and application layer. By alignment of algorithms for plausibility checks and their combination/fusion into a confidence justification their efficiency can be improved. Also, a plausibility check for received data from one application can incorporate data from other applications and hence utilize the redundancy of the transmitted information.

In order to realize the cross-layer and cross-application plausibility checks we propose an instance, which collects as much information from any information source available. Sources include the communication system, applications as well as vehicle sensors and in-vehicle sensor systems (radar, ABS, ESP, ...). The collected data is used by a plausibility checking module in every vehicle to create an independent view of its current status, its current (physical) environment and current or previous neighboring vehicles. Then, upon the reception of warning messages, the messages (their content, origin, etc. ) are evaluated and compared to the vehicle's own estimation of the current situation, which results from the previously collected data.

### C. Confidence Valuation of Data

Different mechanisms for assessing data and nodes include certification, plausibility checking etc. Typically, these algorithms – given some data – decide if the data can be accepted or not. This leads to the undue suppression of data if a particular algorithm has too high "security requirements" to let information pass the test. For example, consider an algorithm that would only accept certificates that have been issued a minute or less ago to minimize the system's vulnerability window.

This undue suppression can be avoided, if confidence evaluation and filtering is separated into two blocks. We propose to model the confidence evaluation of data carried out by the security system using confidence values for credibility-assessed data. Each security algorithm may evaluate the data and attach a value, the confidence value to the data. This confidence value expresses the normalized confidence of the security system in the piece of data. Is is represented by a value between 0 and 1 that can be interpreted as the "probability that the given value reflects the status of the real world".

As an example, take a simple plausibility check: if a node in the one-hop neighborhood (i.e., in the reception radius) claims a position outside the reception radius, the respective position is assumed to be false. This sensor has been described as the *acceptance range threshold (ART)* test in [17]. Once a message passes the ART test, the application using the information can only assume that the real position is somewhere within the acceptance range, i.e., an attacker could have faked any position within that radius.

A helpful property of confidence values the possibility to combine them to obtain new confidence values for combined algorithms. Further, with respect to the implementation of a system, the implementer can define a minimum required confidence value in the data he receives and can then choose the appropriate security mechanism. Alternatively, newly deployed security measures may provide a higher confidence due to better checks, such that applications requiring a high confidence become more usable.

### D. Pseudonymity and Context Mixes

Frequently changing pseudonyms protect the location privacy of vehicles. Like this, a vehicle cannot be traced longer than the pseudonym is stable. Changing pseudonyms only provide sufficient anonymity when changed in the right situations, i.e., where the anonymity set is sufficiently large. We propose to incorporate this requirement in the pseudonym change algorithm and call this approach *context mix*: a node only changes its pseudonym if it is in a situation that is considered private, i.e., if there are enough (similar) nodes around that can be confused with the node after the change.

We call these situations *mix contexts*. As an example, a mix context could be when many nodes stand at the traffic lights.

A sketch of the context mix algorithm is as follows: first, the vehicle permanently assesses its neighborhood. Second, once the vehicle detects $K$ vehicles with a similar direction in the neighborhood that are within the confusion radius (e.g., just 10m away), it changes its pseudonym, expecting neighboring vehicles to react similarly. Finally, after changing the pseudonym, all vehicles assess if their pseudonym change has been successful.

As discussed in [18], this algorithm can be enhanced using a minimum stable time to prevent too many changes and an indication that the node is ready to change its pseudonym.

In [19], Schoch et al. discuss the impact of pseudonym changes on geographic routing. In order to prevent network instabilities due to inaddressable nodes, Fonseca et al. discuss the addressability of nodes with its old pseudonym after a pseudonym change in [20].

## IV. Implementation Approach

For implementation of the different security concepts we identify two primary design options. It is common to both options that the communication system provides anonymity and security for sending, forwarding, and reception of data packets, controlled by a core security application. The main difference between the options lies in the way confidence assessment and filtering is implemented.

In the first option, individual applications implement security functions autonomously (Fig. 3). The second option relieves applications of implementing security functions as much as possible; it integrates these into the core security application as a service that applications can use. The first option reduces the dependency between applications and hence, decreases implementation complexity. But then confidence assessment across applications would hardly be feasible since it requires a structured exchange of confidence values among the different applications in the node.

Cross-application confidence assessment can be accomplished by the second approach, but requires application knowledge within the core security application and an efficient information exchange between communication system, core security application, and applications. As confidence assessment can be based on algorithms that are independent of the specific application logic, the second approach appears to be beneficial. In our implementation approach both options coexist and the application designer can decide which option to use. The remaining part of this section focuses on the second option.

From a high-level perspective, the reference model that is currently discussed in the *C2C CC*, is enhanced by components as shown in Fig. 4, notably a core security application, confidence filter, and the network security component, which are explained below. In order to realize the complex cross-layer and cross-application interaction, we make use of three implementation concepts, namely information connector, confidence tagging, and confidence filter modules.

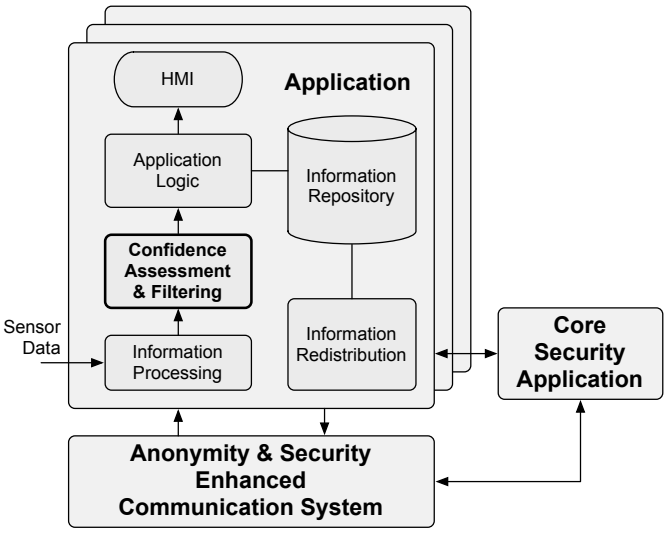


Fig. 3. Local application components: confidence assessment and filtering on a per-application basis

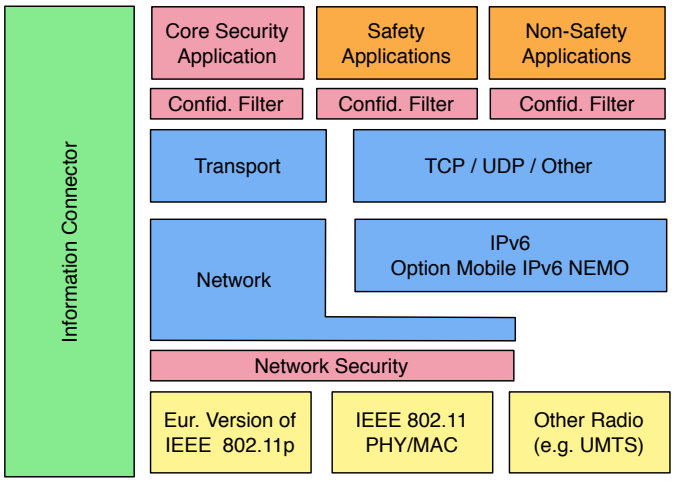


Fig. 4. The reference model view on the security system

### A. Core Security Application

Many safety applications need similar data. It is probable that a modular design of the system will employ a publish-subscribe-like mechanism for vehicular safety information elements. These information elements can be exchanged by application modules and allow for a common data format between safety applications.

The core security application is responsible for privacy protection, pseudonym change, getting new pseudonyms, and cross layer confidence tagging. The choice of implementing these security concepts as a module in the application domain (that in turn contains submodules) reduces the complexity of the system by re-use of confidence evaluated information elements. The core security application contains those confidence evaluation modules that are common to many applications.

### B. Confidence Evaluation and Filtering

Confidence evaluation and filtering can be done for one application only, or – if the particular information element is relevant for several applications – as a module within the core security application. The security system (i.e., the network layer security and the modules in the core security application) attaches *confidence values* to information elements that are exchanged by the different components within the system – a process we dub *tagging*. As described above, confidence values indicate the confidence the security system has in a particular piece of information.

The *confidence filter* evaluates the confidence information derived by the system and permits to dynamically adapt the confidence threshold. This allows different security requirements for applications and represents the interface between the security system and the application.

### C. Multi-Layer Addressing for Pseudonymity

In order to assure anonymity in vehicular communication, a node chooses randomly-generated identifiers referred to as pseudonyms[3] that change over time. Triggered by the *core security application*, the communication system addresses, including addresses for MAC, ad hoc routing, and IPv6, as well as the corresponding certificate are changed.

The certificate is an integral part of a pseudonym representing authorizations for the communication system and (if necessary) application domains. As the certificate format, the WAVE certificate format [8] has been chosen as it represents an extensible and compact format suitable for vehicular environments.

## V. Summary and Outlook

We have presented a security architecture for vehicular communication networks. The architecture is based on different views on the architecture as is common practice in software engineering. We distinguish the high-level views and the implementation-near views.

The former, i.e., the functional layers and the organizational structure, describe how the overall security system should look like. In the functional layer view we have shown how to stack the various existing security mechanisms and algorithms while we show how the functions can be distributed over different authorities and entities in the organizational view. The latter, i.e., the local application components and the reference model view, describe how the system can actually be implemented. We have described an implementation design for the security system in the vehicle's on-board unit and presented the information flow among the architecture components.

As a whole, the paper provides a clear and modular security architecture as a basis for implementation. As next steps we complete the prototype implementation, conduct experiments in order to justify the security overhead, and promote the architecture in ongoing standardization efforts in the *C2C-CC*.

[3]More precisely, the pseudonyms are pseudo-random since they can be linked to the true identity by an authority.


## Acknowledgements

This work has been carried out in the *NOW – Network on Wheels* [3] project supported by the German Ministry for Education and Research under contract No. 01AK064.


## References


[1] A. Aijaz, B. Bochow, F. Dötzer, A. Festag, M. Gerlach, R. Kroh, and T. Leinmüller, "Attacks on Inter Vehicle Communication Systems - an Analysis," The Network on Wheels Project, Tech. Rep., 2005. [Online]. Available: http://www.network-on-wheels.de/documents.html

[2] M. Gerlach, "Assessing and Improving Privacy in VANETs," in *Proceedings of Fourth Workshop on Embedded Security in Cars (ESCAR)*, November 2006.

[3] The Network on Wheels (NOW) Project, "NOW website," 2004. [Online]. Available: http://www.net-on-wheels.de

[4] The Willwarn Project, "The Willwarn Project Website," 2005. [Online]. Available: http://www.prevent-ip.org/willwarn

[5] The Global Systems of Telematics (GST) Project, "GST website," 2005. [Online]. Available: http://www.gstproject.org

[6] The Car-to-Car Communication Consortium (C2C-CC), "C2C-CC website," 2006. [Online]. Available: http://www.car-to-car.org

[7] The Secure Vehicle Communication (SeVeCOM) Project, "SeVeCOM home." [Online]. Available: http://www.sevecom.org/

[8] "IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages," 2006. [Online]. Available: http://ieeexplore.ieee.org/servlet/opac?punumber=11000

[9] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing Vehicular Communications," *IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications*, October 2006.

[10] M. Raya, D. Jungels, P. Papadimitratos, I. Aad, and J.-P. Hubaux, "Certificate Revocation in Vehicular Networks," Laboratory for Computer Communications and Applications (LCA), EPFL, Tech. Rep. LCA-REPORT-2006-006, 2006.

[11] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, "Securing Vehicular Communications - Assumptions, Requirements, and Principles," in *Proceedings of Fourth Workshop on Embedded Security in Cars (ESCAR)*, 2006.

[12] P. Golle, D. Greene, and J. Staddon, "Detecting and Correcting malicious data in VANETs," in *Proceedings of the first ACM workshop on Vehicular ad hoc networks (VANET)*, October 2004, pp. 29–37.

[13] IEEE, "IEEE standard 1471-2000: IEEE recommended practice for architectural description of software-intensive systems," 2000.

[14] M. Gerlach, "Use Cases for a Vehicular Security System," Fraunhofer FOKUS, Tech. Rep. to appear, 2007.

[15] G. Stoneburner, "Underlying Technical Models for Information Technology Security, Tech. Rep. NIST Special Publication 800-33, December 2001. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf

[16] F. Armknecht, A. Festag, D. Westhoff, and K. Zeng, "Cross-Layer Privacy Enhancement and Non-Repudiation in Vehicular Communication," in *Proceedings of 4th Workshop on Mobile Ad-Hoc Networks (WMAN)*, Bern, Switzerland, March 2007.

[17] T. Leinmüller, E. Schoch, and F. Kargl, "Position verification approaches for vehicular ad hoc networks," *IEEE Wireless Communications Magazine*, October 2006.

[18] M. Gerlach and F. Güttler, "Privacy in VANETs using Changing Pseudonyms - Ideal and Real (Poster Presentation)," in *Proceeedings of 65th Vehicular Technology Conference VTC2007-Spring*, April 2007.

[19] E. Schoch, F. Kargl, T. Leinmüller, S. Schlott, and P. Papadimitratos, "Impact of Pseudonym Changes on Geographic Routing in VANETs," in *Proceedings of Third European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS 2006)*, September 2006.

[20] E. Fonseca, A. Festag, R. Baldessari, and R. Aguiar, "Support of Anonymity in VANETs – Putting Pseudonymity into Practice," in *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC)*, Hong Kong, March 2007.