# Report Dagstuhl Seminar 10402
# Working Group on Security and Privacy

Frank Kargl (Moderator)
Levente Buttyan
David Eckhoff
Panagiotis Papadimitratos
Elmar Schoch

January 3, 2011

## 1 Introduction and Motivation

Security and Privacy protection are still considered to be among the major challenges for Inter-Vehicle Communication. While significant work has been done in this area in the past years, the very nature of IVC makes it extremely challenging to come up with a satisfying security and privacy solution. Some characteristics of IVC – for example node cooperation, high node mobility, or the dominance of broadcast communication – make traditional security mechanisms inappropriate. On the other hand, resource restrictions in on-board units and in the wireless channels will likely require to accept certain security - performance trade-offs. As none of the proposed solutions so far are without drawbacks, IVC security and privacy protection remain interesting and demanding research objectives. The goal of the security and privacy working group was to provide a judgement on the status of various security- and privacy-related issues and to discuss some solutions for still-open questions.

## 2 Discussions

Initial discussions were based on issues raised by Elmar Schoch in his invited talk. For security and privacy-protection, it is essential that we find the right level of protection. If we overdo security, this might negatively affect application performance and reduce IVC benefits in general. If too few security or privacy protection is provided, the security or privacy incidents that will likely result in a reduced trust of drivers in IVC systems and might thus severely damage deployment.

The discussion also touched the status of current security mechanisms and whether they are ready and sufficient for a day-1 IVC deployment. To answer this question, participants created a kind of overview map over research topics and issues.



Dagstuhl Seminar Proceedings 10402
Inter-Vehicular Communication
http://drops.dagstuhl.de/opus/volltexte/2011/2927

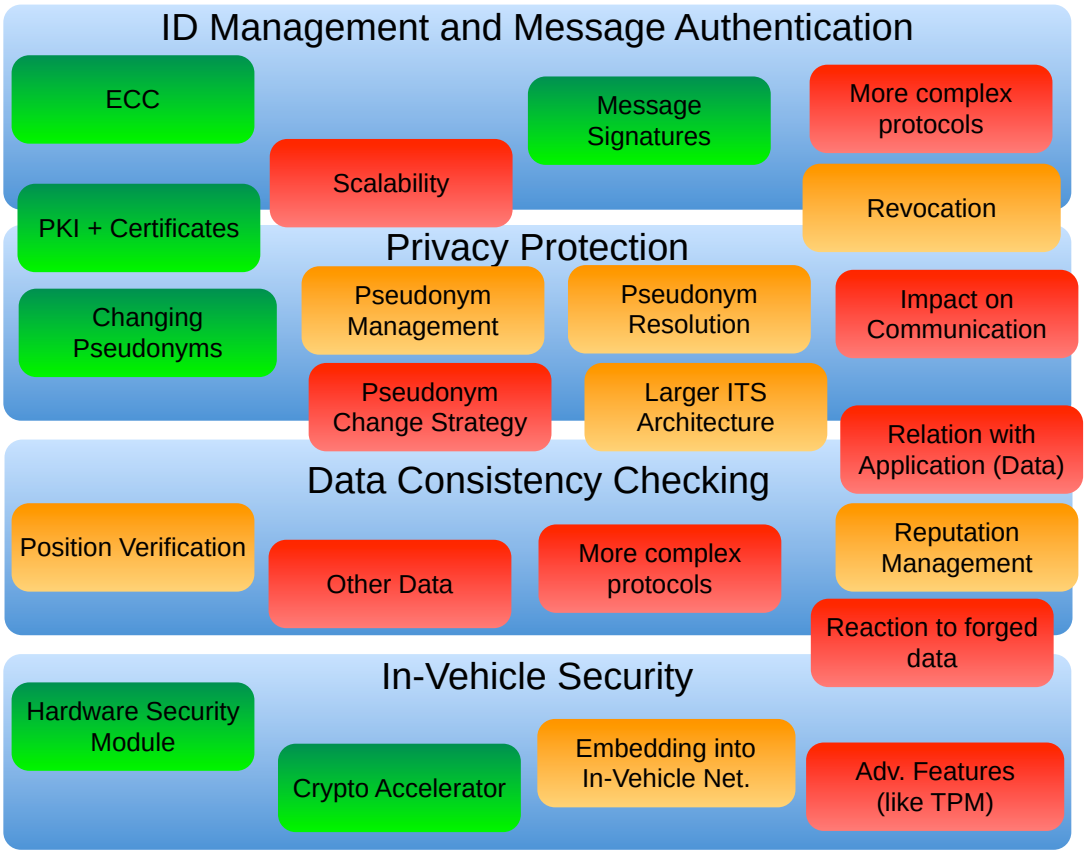


Figure 1: Research topics

### 2.1 Status of Research Challenges

Figure 1 shows the overview map over the various topics that were discussed among participants. Topics are grouped in 4 main categories:

- ID Management and Message Authentication
- Privacy Protection
- Data Consistency
- In-Vehicle Security

There was general agreement among participants that these categories provide a good and complete coverage of the majority of past and recent research on IVC security and privacy activities. Within each of these activities, we found a number of research topics. The topics are not meant to be exhaustive, there are likely also other relevant topics. Still, they should give a broad overview over various issues that are covered in literature and that are discussed at scientific conferences and in standardization bodies. For each

of the topics, we tried to give an estimation of the maturity of the topic, encoded in colors with the following meaning:

**Green:** Topics are marked in green if there is a broad number of proposals available in literature and a general agreement among researchers and in standardization bodies which mechanisms to include for a first deployment of IVC security and privacy. Remaining work is of a more fine-grained nature.

**Yellow:** Yellow marks topics where there is a large variety of proposed security or privacy protection mechanisms in the literature but where a consensus how to solve this problem is not yet reached.

**Red:** There is comparatively few work on this topic, let alone an agreement how to solve the issue.

An example of a topic where there is general agreement is the use of ECC-based asymmetric cryptography for message authentication and integrity protection using public-private keypairs and certificates issued by a PKI [1, 2]. A matter of ongoing discussion is however, how vehicles would communicate with the PKI in case of certificate renewal (which happens especially often in case of use of pseudonyms), whether a 3G connection can be assumed to be present for this or whether other more sporadic communication channels must suffice.

Other areas of discussion that were raised by participants include scalability of mechanisms with respect to certain node densities, metrics for measuring the effectiveness of privacy protection mechanisms, and the availability and price of crytpo-accelerators for On-Board Units (OBUs). One topic of special importance is avoiding the overhead associated with secure broadcast communication and achieving scalable and efficient authentication of broadcast mechanisms.

### 2.2 IVC Broadcast Authentication

To approach the issue of efficient broadcast authentication, you first have to clearly identify the purpose why you apply it. The ultimate goal of applying security mechanisms to IVC is to ensure correctness of communicated data. That is, no attacker should be able to disseminate forged data in the network. Ensuring trust and integrity of packets as achieved with a 'key-pair / certificate / signature' solution is only one part of the solution, and one that comes at a very high overhead [3]. There are many proposed alternatives, some using symmetric cryptography instead of asymmetric [4] or hybrid solutions that use asymmetric or group cryptography only for distribution of symmetric keys [**?** ]. However, most of these solutions come at significant drawbacks and therefore the mainstream solution under discussion still relies on 'key-pair / certificate / signature'.

During the working group sessions, the participants discussed additional ways of achieving efficient broadcast communication that require additional refinement and discussion after the seminar.

Beyond the integrity and authenticity protection achieved by 'key-pair / certificate / signature', a further conclusion is that data consistency needs to be guaranteed by

additional mechanisms that cross-validate data received from various independent means that an attacker cannot influence in parallel. Some work proposes usage of characteristics of physical radio channels [5], others cross-validate received data with physical sensors.

## 3 Conclusion and Outlook

The discussions in the security working group provided a good overview over the current situation of security and privacy in Inter-Vehicle Communication. While there is no complete solution and agreement in all matters, it became clear that the questions to be solved are clear and that at least some are answered in a sufficient manner. The big challenge will be to find the right trade-off between strong security and privacy protection on the one hand and efficiency and low overhead on the other hand. If researchers and developers fail in either direction, this will inevitable lead to problems with vulnerable or inefficient and unusable systems.

## References


[1] Panos Papadimitratos, Levente Buttyan, Tamas Holczer, Elmar Schoch, Julien Freudiger, Maxim Raya, Zhendong Ma, Frank Kargl, Antonio Kung, and Jean-Pierre Hubaux. Secure Vehicular Communications: Design and Architecture. *IEEE Communications Magazine*, 46(11):2–8, November 2008.

[2] Frank Kargl, Panos Papadimitratos, Levente Buttyan, Michael Müter, Björn Wiedersheim, Elmar Schoch, Ta-Vinh Tongh, Giorgio Calandriello, Albert Held, Antonio Kung, and Jean-Pierre Hubaux. Secure Vehicular Communications: Implementation, Performance, and Research Challenges. *IEEE Communications Magazine*, 46 (11):2–8, November 2008.

[3] Elmar Schoch and Frank Kargl. On the efficiency of secure beaconing in vanets. In *ACM Conference on Wireless Security (WiSec '10)*, March 2010.

[4] Yih-Chun Hu and Kenneth P. Laberteaux. Strong vanet security on a budget. In *4th Annual Conference on Embedded Security in Cars (escar 2006)*, Berlin, Germany, November 2006. is-its.

[5] Fangming He, Hong Man, and Wei Wang. PLASMON: Physical Layer Assisted Security for Mobile OFDM Networks. In *2nd IEEE Vehicular Networking Conference (VNC 2010)*. IEEE, December 2010.