Abstract—In order to reduce the amount of traffic accidents on the roads, new safety systems based on vehicular communication – which allows vehicles to exchange information with nearby vehicles – are being developed. Similar to wireless communication in other domains, this type of information exchange is threatened by various kinds of attacks that could outweigh the advantages of safety applications and cause additional risks for traffic participants. Therefore, it is necessary for applications to recognize attacks and stop eavesdroppers from gaining sensitive information about the vehicles’ occupants. The SeVeCom project dealt with those challenges and developed solutions that can be applied in realistic scenarios.

I. INTRODUCTION

Vehicular communication (VC) is able to extend the safety features of vehicles, thereby making driving safer by exchanging messages about status and dangerous situations between all traffic participants. Additionally, VC can make travelling more effective and more comfortable by, for example, recognizing traffic jams and distributing this information to following vehicles or simply establishing internet access for the occupants. Therefore, vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication are recent research topics and their deployment is pushed to develop the next generation of intelligent vehicles within the next years. But in addition to the new features and possibilities of VC, new challenges and threats appear and have to be addressed during the development process of VC networks and systems. Besides the permanently changing structure of the vehicular ad hoc network (VANET), malicious nodes can start a variety of attacks ranging from faked messages, replay and Sibyl attacks to network jamming in order to gain some kind of advantage. Also, privacy concerns arise, since messages can not be encrypted in many cases. This allows eavesdroppers to gather sensitive information and maybe track vehicles over a long period of time.

To develop solutions for these issues the SeVeCom project was founded, supported by the European Commission. The project started in February 2006, the final review took place in Brussels in April 2009. Its main goals were to secure V2V and V2I wireless communication and propose mechanisms to preserve the privacy of the involved participants.

As other related projects already coped with the realisation of inter-vehicular communication (e.g., Fleetnet, NOW, CVIS, Safespot, and Coopers), the SeVeCom approach was to develop a modular system supporting security and privacy features that can be easily integrated into existing network stacks. Thus, all projects that use a network stack that is structured similar to the linux netfilter concept can benefit from the results of the SeVeCom project.

Due to the help and fruitful cooperation of all SeVeCom partners (namely, Trialog (Coordinator), Daimler, Centro Ricerche Fiat (CRF), Ecole Polytechnique Fédéral de Lausanne (EPFL), Ulm University, Budapest University of Technology and Economics, Katholieke Universiteit Leuven, and Bosch), the project was able to reach its goals and achieve a number of relevant publications in the scientific area (e.g., [1], [2]).

In the following Sections we will present the SeVeCom security architecture and privacy mechanisms. Section III discusses details of the baseline architecture and implementation and is followed by a description of the certification tool (Section IV), which was used for conformance testing of the system.

II. SECURITY AND PRIVACY MECHANISMS

With inter-vehicular communication based applications, traffic jams can be detected and accidents can be avoided making our roads safer and driving more efficient. That is, collision or road condition warnings are generated by the vehicles themselves and broadcasted to surrounding vehicles. In this context, security is a major issue, because, for example, fraudulent information can provoke accidents or lead to traffic congestion.

In order to avoid these kinds of attacks, SeVeCom proposes a mechanism that allows the verification of the message senders’ authenticity. Therefore, the sensitive content of a message and meta information like a timestamp are signed with an asymmetric private key. The signature, the senders’ authenticity. Therefore, the sensitive content of a message and meta information like a timestamp are signed with an asymmetric private key. The signature, the senders

Author version. Definitive version at ieee.ieeeexplore.org
(CA), which vouches for the authenticity of the public key, are added to the message. By verifying the message with the public key and checking the certificate, the receiver is able to prove the authenticity and the message integrity.

However, this construction would still compromise the privacy of the drivers, because an attacker could track the itinerary of a vehicle by filtering all messages containing the same certificate. Our solution to this problem is to use short-term keys and certificates – combined to a so-called pseudonym – and to change these pseudonyms after a period of time.

To obtain such pseudonyms, a vehicle is equipped with a set of long-term keys for identification to a trusted CA from which it periodically receives certificates for several short-time keys, maybe hundreds or thousands. Car manufacturers, as well as regional, national, or international traffic administrations could act as trusted authorities that generate these certificates. In the SeVeCom system, one short-term public key and the correlating certificate are combined to a pseudonym. Frequent pseudonym changes – which imply to change keys for signature creation – make it difficult for an eavesdropper to track a vehicle over a long period of time. Thus, it prevents eavesdroppers from relating a message to a particular vehicle or to another message. Nonetheless, a receiver is able to verify message integrity and authenticity with the public keys of the CA.

Of course, all identifiers that could be used to connect messages before and after a pseudonym change also have to be changed. This includes MAC and possibly IP addresses.

The same architecture can also be used to secure the communication of vehicles with road side units. The only difference will be that RSUs will not change keys and certificates, because there is no need to protect the privacy of the RSUs.

III. BASELINE ARCHITECTURE AND IMPLEMENTATION

The SeVeCom architecture is designed to support inter-vehicular communication, making applications more robust and reliable. Also, some privacy aspects arising form the use of secure communication are addressed. A baseline architecture was specified (see Figure 1a), and the most important modules were implemented in a prototype in order to be able to prove the feasibility and the advantages of the architecture. The SeVeCom system can be integrated into existing network stacks via an adaptable hooking mechanism.

The system is built on independent modules implementing different security mechanisms, which allows to react flexibly to future security solutions. These modules are instantiated and controlled by the Security Manager. Depending on scenarios and policies, the Security Manager can start the SeVeCom modules with different configurations and dynamically enable or disable some of the Secure Communication Components.

The Pseudonym Manager (PM) takes care of pseudonym storage and pseudonym validity checks. It decides when to change a pseudonym and in parallel triggers the MAC address changes. When it runs out of pseudonyms, it contacts an external Pseudonym Provider (a trusted CA) and submits new public keys for certification.

Long-term-key identifiers and certificates are managed by the Identification & Trust Management Module, which also provides services like public key registration and revocation.

Keys and signatures are created/verified by the Crypto Support Module (CSM), which also checks the validity of certificates. It has either access to a cryptographic library or to a tamper resistant Hardware Security Module that holds private keys and performs cryptographic operations and is physically protected against unauthorized readout of private key material. For efficiency reasons, and to limit the security payload attached to the messages, keys, certificates, and signatures are based on Elliptic Curve Cryptography (ECC), as they are significantly smaller than their RSA and DSA counterparts.

Incoming and outgoing messages are routed to the Secure Communication Components which add/verify signatures and pseudonyms by the help of CSM and PM. In the prototype, beaconing messages, unicast messages, and geo- and TTL restricted flooding messages are supported. TTL restricted flooding messages are limited by a time-to-live counter, which has to be decreased every time the message is forwarded. An attacker could try to increase the TTL in order to enlarge the region inside the message will be distributed, which could lead to higher bandwidth usage and channel congestion. Therefore the counter is secured by a hash chain; thus, an attacker cannot increase the TTL. The timestamp of the message is checked mandated. This way also replay attacks will be recognized and the messages discarded or marked as not trustworthy.

The In-car Security Module is the gateway to other car systems and sensors, e.g., GPS and speed sensors. An intrusion detection system controls and monitors all information exchanged between the network stack and the in-car systems. A firewall restricts access to in-vehicle systems to protect them from attacks due to vehicular communications.

The SeVeCom System is connected to the network stack via Inter Layer Proxies (ILPs), which are integrated between several layers of the stack. The Secure Communication Components can register at one or several ILPs during the initialization phase. When a message arrives at an ILP, an event is triggered, which is handled by one or several of the Secure Communication Components. Those components process the message and possibly modify it. Via a return value, they indicate to the ILP whether the message was modified and whether it should be dropped or forwarded to the next layer of the stack.

The convergence layer separates the SeVeCom code from the implementation of the network stack. Therefore, an adaptation of the SeVeCom system to a new network stack is possible with reasonable effort. Only parts of the convergence layer have to be modified, while the other components remain unchanged.
For the baseline implementation, the ACUp\textsuperscript{7} network stack was enhanced by the SeVeCom security system, which implements the concepts presented above. The whole setup is running on Denso Wireless Security Units (WSU), which use a draft 802.11p network protocol implementation using a frequency band at 5.9 GHz dedicated for vehicular communication. This setup could be directly integrated in any ordinary vehicle.

The crypto operations are performed by a crypto library instead of a Hardware Security Module, because of project runtime constraints. Due to the limited resources of the Denso hardware (the Denso boxes contain a 400 MHz PPC processor) and the complexity of the cryptographic algorithms, the number of messages that can be signed/verified per second is not enough for deployment. However, using an HSM or future car systems with enough computational power will allow to cope with large vehicle densities occurring, for example, in traffic jams.

We want to thank our SeVeCom partners, who contributed to the prototype implementation, especially the groups from EPFL and Budapest University of Technology and Economics.

IV. Certification Tool (Test Lab)

To test the functionalities of the system, a conformance tester which respects the ISO9646 standard has been developed. The test architecture is described in terms of TTCN3 (Testing and Test Control Notation), a conformance testing methodology and framework. TTCN3 is a language standardised by ISO for the specification of tests for real-time and communicating systems, developed within the framework of standardised conformance testing (ISO/IEC 9646). This language allows to stimulate our security communication stack (known as system under test) with relevant events and to check its behaviour. Our tester has two main purposes: to test the conformance of the security payload (or security data) and to test the conformance of the protocols. Indeed, several types of messages are managed by the stack, each with its specific protocol.

Using the TTCN3 Terminology our test lab architecture contains the following components (see figure below):

- the implementation under test (IUT) which is the implementation that must be tested. It is considered as a black box.
- system under test (SUT): The whole test system including hardware, software etc. It contains the implementation under test (IUT).
- the upper tester (UT) which is composed of that part of the tester that communicates with the IUT at the upper interface. We can see that it communicates through a TCP/IP socket with the IUT. It plays the role of the local applications (see fig 1).
- the lower tester (LT) which is that part of the tester that communicates with the IUT at the lower interface. The information exchanged between the IUT and the wireless hardware is capture using a tcp dump like tool. Information can also be injected in order to simulate the reception of data through this communication means. It plays the role of the remote applications.

\textsuperscript{7}The ACUp (AKTIV Communication Unit with 802.11p) project is a network stack developed by BMW Group and implemented by Cirquent GmbH. It is used in the AKTIV project as well as in the context of the C2C-CC (Car-2-Car Communication Consortium).
the abstract test suite (ATS) which defines the test suite that must be executed in order to verify the correct behaviour of the implementation under test (IUT). The IUT is stimulated by sequences of test events and its responses are checked versus expected results.

V. CONCLUSION

The SeVeCom project has designed a security architecture for vehicle-to-vehicle and vehicle-to-infrastructure communication. By using cryptographic signatures, message authenticity and integrity can be verified, and different kinds of attacks can be recognized. Using pseudonyms, communication cannot directly be linked to a vehicle or an individual, and pseudonym and MAC address changes prevent eavesdroppers from tracking vehicles over a long period of time.

A test laboratory has been developed, which allows to verify the conformance of the security enhanced communication stack and the used protocols in different scenarios. Finally, a proof-of-concept prototype was implemented, which demonstrates the feasibility of the architecture.

SeVeCom results are now being considered in other projects such as CVIS and standardization bodies like in ETSI TC ITS WG 5 and the European eSecurity working group.

REFERENCES
