SEVECOM - Secure Vehicle Communication

Tim Leinmüller*, Levente Buttyan+, Jean-Pierre Hubaux++, Frank Kargl**, Rainer Kroh*, Panos Papadimitratos++, Maxim Raya++, and Elmar Schoch**

+BME/CrySyS Lab, buttyan@crysys.hu
*DaimlerChrysler AG, Research Vehicle IT and Services, {rainer.kroh|tim.leinmueller}@daimlerchrysler.com
++School of Computer and Communication Sciences EPFL, Switzerland, {jean-pierre.hubaux|panos.papadimitratos|maxim.raya}@epfl.ch
**Ulm University, Media Informatics Department, {frank.kargl|elmar.schoch}@uni-ulm.de

***Abstract*— Vehicle to Vehicle communication (V2V) and Vehicle to Infrastructure communication (V2I) promise to improve road safety and optimize road traffic through cooperative systems applications. A prerequisite for the successful deployment of vehicular communications is to make them secure. The specific operational environment (moving vehicles, sporadic connectivity, etc.) makes the problem very novel and challenging.**

Because of the challenges, a research and development road map is needed. We consider SEVECOM [1] 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.

I. Introduction

Vehicle to Vehicle communication (V2V) and Vehicle to Infrastructure communication (V2I) bring the promise of improved road safety and optimized road traffic through cooperative systems applications. To this end a number of initiatives have been launched, such as the Car-2-Car consortium in Europe [2], or the VSCC 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 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 (moving vehicles, sporadic connectivity) makes the problem very novel and challenging. 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 an 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. Besides, following topics will be investigated in preparation of further work: Intrusion Detection, Data consistency, Secure positioning, 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 crypto-systems to the V2V/V2I environment.

As a start, SEVECOM will take into account existing results available from ongoing eSafety projects such as PREVENT or GST in terms of threat analysis and security architecture. Then, close liaison with new IST eSafety projects which will focus on C2C application and road network infrastructures is planned.

Some of the challenges addressed by SEVECOM will necessitate long term investigation that cannot be completed within SEVECOM. We have therefore assumed that a subsequent initiative/project (e.g. SEVECOM II) will be launched after SEVECOM. Therefore, we make a difference between items of work that are fully addressed within the time-span of SEVECOM and the items of work that will be input to a subsequent project. This also applies at the application level: entertainment applications will not be considered in this project. They are likely to be an objective for a later phase.

The remainder of this paper is organized as follows. In the next section, we will present V2V and V2I security issues that are going to be addressed in SEVECOM. Then section III will elaborate on the scientific and technical objective, followed by discussions on tamper resistant hardware IV and dedicated cryptosystems V for V2V and V2I communication. The problem of in-vehicle communication protection is addressed in section VI, while section VII discusses validation and testing of security mechanisms for vehicular communication. Finally, section VIII concludes this paper.

II. V2V and V2I Security Issues

A. Threats and Attacks

The self-organizing operation and the unique features of vehicular networks open vehicular communications to a wide range of exploits. Any wireless-enabled device that runs a rogue version of the vehicular communication protocol stack poses a threat. We denote such rogue devices deviating from the definition of protocols as *adversaries* or *attackers*. Next, we explore the most significant vulnerabilities of vehicular communications.

The jammer deliberately generates interfering transmissions that prevent communication. Since the network coverage area, e.g. along a highway, can be well-defined, at least locally, jamming is a low-effort exploit opportunity. An attacker can relatively easily, without compromising cryptographic mechanisms, and with limited transmission power, prevent communication in an area of the vehicular network.

It is possible that large areas of vehicular networks are fast '*contaminated*' by deliberately erroneous measurements and messages. For example, a single attacker can forge and transmit false hazard warnings (e.g. ice formation on the

pavement). These messages would then be taken up by all vehicles in both traffic streams, and relayed further across the network.

Any node acting as a relay can disrupt communications of other nodes: it can *drop* or *corrupt* messages, or, *meaningfully modify* messages. This way the reception of valuable or even critical traffic notifications or safety messages can be manipulated. Moreover, attackers can *replay* messages, e.g. to illegitimately obtain services.

Message fabrication, alteration, and replay can also be used towards impersonation. Consider, for example, an attacker masquerading an emergency vehicle to mislead other vehicles to slow down and yield. Or, an adversary impersonating road-side units, spoofing service advertisements or safety messages.

With vehicular networks deployed, the collection of vehicle-specific information from overheard vehicular communications will become particularly easy. Then, inferences on the drivers' personal data could be made, and violate her or his *privacy*. An eavesdropping attacker, which could even be a service provider, could deploy several with 'strength' quantified by the number of network traffic sniffing points. The attacker extracts data such as time, location, vehicle identifier, technical descriptions, or trip details, and based on those derive private information.

Beyond exploits of communication protocols, the attacker may select to tinker with data (e.g. velocity, location, status of vehicle parts) at their source. Tampering with the on-board sensing and other hardware (e.g. real-time clocks), may, in fact, be relatively simple.

B. Requirements and Constraints

SEVECOM will further investigate vulnerabilities, model attackers, perform a risk analysis, and identify security requirements, in liaison with other related projects, including NoW, C2C-CC, GST, the eSafety projects CVIS, SafeSpot, Coopers, and COMeSafety. The methodology underlying the ISO 15408 standard on security evaluation (common criteria) will be used to carry out the threat and risk analysis. Beyond technical requirements, business and legal constraints and requirements will be taken into consideration.

Securing vehicular communications will require:

- Authentication and integrity, to prevent message modification and forgery
- Data consistency, to mitigate the impact of injecting authentic yet falsified measurements
- Non-repudiation, to prevent nodes from denying transmission of a message
- Privacy, to prevent the collection or extraction of private information from vehicular communications
- In-vehicle security, to protect the in-vehicle data access and resources

In addition, the network scale and dynamics will be taken into consideration. Vehicular networks will comprise hundreds of millions of highly mobile nodes, whose connectivity will change frequently and fast.

A large number of authorities and service providers will emerge, making interoperability of secure communication protocols a difficult problem. A multitude of road-side infrastructure devices may be available, while vehicles from foreign administrative domains may frequently need to communicate in a secure manner.

At the same time, the deployment of those networks will be gradual: initially, only a fraction of the vehicles will be equipped with communication and processing capabilities, while only a few highways will be covered by road-side infrastructure. The cost of such equipment will be a determining factor, while broad support of vehicular communication systems is essential for their effectiveness.

III. Scientific and Technical Objectives

SEVECOM vision is that future vehicular communication and inter-vehicular communication infrastructures will be widely deployed in order to bring the promise of improved road safety and optimized road traffic. SEVECOM addresses security of future vehicle communication networks, including both the security and privacy of inter-vehicular communication and of vehicle-infrastructure communication. Its objective is to define the security architecture of such networks, as well as to propose a road map for integration of security functions in these networks. More specifically, this means the following scientific and technical objectives will be addressed.

A. Threat and risk analysis

The variety of threats on safety applications will be identified: 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. The approach will be to use the underlying methodology behind the ISO 15408 standard on security evaluation (common criteria).

B. Specification of an security architecture

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. So far, vehicles have been identified by their license plate and their chassis number. SEVECOM will devise appropriate electronic identification schemes, along with the related key management.

Secure communication protocols. Unprotected routing protocols offer a large potential for malicious attacks like black hole routing or traffic redirection. Whereas there exists a significant number of proposals for secure topology-based routing protocols (like SAODV, SRP, or SDSR), secure position-based routing as used in VANETs is not well covered yet. SEVECOM will develop secure routing and authentication protocols as well as a framework for secure application protocols.

Tamper proof device and related protocols. In order to prevent the compromise of the private keys of a car, they should be stored in a tamper resistant unit within the car. This unit would not only store the keys, but it should also be able to perform cryptographic operations (e.g. generate digital signature) with them, therefore, the keys would never need to leave the unit. SEVECOM will identify requirements on the tamper resistant unit, the design of its protocols, and the decision on the crypto-systems used within the unit.

Privacy. SEVECOM will elaborate a scheme preserving the anonymity of the vehicles (and therefore of the drivers and passengers) when needed. This scheme will respect the constraint of liability identification whenever required (typically in the event of a collision).

The following topics will be investigated in preparation of further work:

Intrusion Detection. Some aspects of malicious behavior cannot be prevented by securing e.g. authentication or routing protocols by cryptographic means. This is especially true for selfish behavior, where nodes deny spending own resources on supporting overall connectivity. SEVECOM will design an intrusion detection system that uses sensors to detect this and other malicious behavior and take appropriate actions.

Data consistency. A car may transmit fraudulent data about road congestion, or its own position, speed, etc. for malicious or for rational reasons. Therefore, the security of car-to-car communications relies not only on verifying the integrity and the authenticity of the received data, but also on the capability of detecting and potentially correcting fraudulent data. SEVECOM will study the fundamental limits of the potential solutions to this problem, and the design of detection and correction mechanisms (within the identified limits) based on checking the consistency of the received data.

Secure positioning. Technology makes it already possible to position a vehicle (by means of GNSS or terrestrial antennas). This work item will propose mechanisms by which this operation can be secured, meaning that the (correct) information about the position of a vehicle at a given moment cannot be modified by an internal or external attacker. In IVC, life-critical applications, such as collision avoidance, require both precision and security in both ad hoc and infrastructure scenarios. No such system has been defined yet in academic research or industrial projects. Hence, a scientific and technical objective of SEVECOM will be to pave the road for the design of a secure positioning system, possibly in the follow-up phases after this project.

Secure user interface. Usual security systems cannot work completely autonomously. At some points user interaction is required. Examples include user authentication or decisions whether to trust another party that enters the system and has no known trust status. Badly designed user interfaces often lead users to wrong decisions or false actions which can severely degrade the security of the whole system. Although the overall goal of SEVECOM must be the creation of a autonomous security subsystem that restricts the communication with the end user to an absolute minimum, for the remaining few interactions SEVECOM will focus on trying to find first answers, how a suitable user interface should look like.

Design of cryptographic primitives. An important factor in addressing the security issues of IVC is the choice of the underlying crypto-system which take into account the specific operational environment. The challenge is to address the variety of threats, the sporadic connectivity created by moving vehicles and the resulting real-time constraints, the low-cost requirements of embedded systems in vehicles. The initial comparison in [4] of the performance of existing crypto-systems in a IVC environment shows that some of them are suitable for IVC. Thus one of the technical objectives of SEVECOM will be to refine this feasibility study and devise the modifications required to adapt one of the available crypto-systems to IVC, such as the necessity of a cryptographic hardware accelerator.

IV. Tamper resistance

Implementing security services for VANETs requires vehicles to store sensitive data (e.g. cryptographic keys, event logs, etc.) [4]. Clearly, such sensitive data needs to be protected from unauthorized access. However, this is particularly challenging in VANETs, because the vehicles operate in a hostile environment, where vehicle owners and maintenance service providers have unsupervised access to them. In addition, owners and service providers may have strong incentives to tamper with the vehicles (e.g. a car owner may want to delete the content of the car's Event Data Recorder in order to escape from liability after an accident).

Unfortunately, the timely detection of the compromise of sensitive information stored in vehicles seems to be impossible in VANETs due to the lack of any real-time, centralized control. Although tampering with vehicles may be detected during regular inspections by the authority, this may happen only months or years after the sensitive data are compromised and likely misused. Moreover, since the detection of tampering itself may not reveal any information about the time of the attack, ensuring liability based on data stored in vehicles becomes nearly impossible.

In order to cope with this problem, vehicles must be equipped with *tamper resistant* modules, and the system (data, software, and hardware) should be structured in such a way that sensitive information is stored and processed exclusively within these modules.

The benchmark standard that specifies the requirements on tamper resistant modules is the FIPS 140 standard [5]. The FIPS 140 specification defines four levels of tamper resistance with an increasing degree of security. Systems evaluated at level 1 are not required to implement any physical protection measures, while level 4 devices need to provide strong resistance against physical tampering attempts. The latter category of devices are usually enclosed in tamper resistant packaging, they include tamper detection sensors, which detect abnormal environmental conditions (e.g. temperature, pressure, supply voltage, or clock frequency), and circuitry (powered by an internal battery) that reacts to the alarms raised by the sensors by erasing all sensitive data immediately from memory.

Smart cards are often considered to provide some level of tamper resistance, and they are widely used as trusted system components in hostile environments. However, systems that use smart cards often rely on additional security mechanisms too, such as video surveillance or a central transaction processing facility that detects anomalies and distributes blacklists of cards suspected to be compromised in real-time. When such additional measures are not used, smart cards become less effective as a protection mechanism (see e.g. payTV systems). Due to the very nature of VANETs, it may not be feasible to extend the level of protection provided by smart cards with additional security mechanisms. Therefore, smart cards may not be the ideal candidates as security modules for vehicles. Further disadvantages of smart cards include the lack of a battery, and hence, the lack of a secure, on-board clock. In addition, most of the smart cards do not really resist to physical attacks of a determined attacker (although there exist smart cards that are evaluated at FIPS 140 level 3). On the positive side, we must mention that smart cards are very cheap relative to the price of a vehicle.

On the other extreme of the spectrum of tamper resistant devices, one can find cryptographic coprocessors such as the IBM 4758 PCI board [6]. These devices provide a very high level of security, but their price is considerably higher than that of smart cards. Indeed, the coprocessor hardware itself can cost several hundreds of dollars, not even counting the additional cost of the software and the increased maintenance costs. Therefore, high-end cryptographic coprocessors may not be ideal security modules for vehicles either.

PKCS	Sig size (bytes)	$T_{tx}(Sig)$ (ms)
RSA	256	0.171
ECDSA	56	0.038
NTRU	197	0.131

TABLE I
SIZE AND TRANSMISSION TIME OF PKCS

PKCS	Generation (ms)	Verification (ms)
ECDSA	3.255	7.617
NTRU	1.587	1.488

TABLE II
COMPARISON OF SIGNATURE GENERATION AND VERIFICATION TIMES ON A MEMORY-CONSTRAINED PENTIUM II 400 MHZ WORKSTATION

Clearly, one needs to find a trade-off between the cost of and the level of security provided by the security module. In order to find the best trade-off, one needs to understand the security requirements of VANET applications, as well as the characteristics of the operating environment of VANETs (including the attacker model). Based on this understanding, one can determine the level of security that needs to be provided, and then select an appropriate class of tamper resistant devices with affordable cost. Then, the design of the security architecture can be based on the selected device type. In the SeVeCom Project, we intend to investigate these issues, and come up with recommendations to be considered by the vehicle manufacturers.

V. CHOICE OF THE CRYPTOSYSTEM

It is important to choose a Public Key Cryptosystem (PKCS) with an acceptable implementation overhead in the vehicular context [4]. There are two factors that affect the choice of a particular PKCS: (1) the execution speeds of the signature generation and the verification operations, and (2) the key, signature, and certificate sizes.

There are several candidate PKCS (we consider only the currently standardized systems) for VANET. To assure the future security of the cryptographic material, and taking into account the deployment schedule of VANET technology, we assume a security level at least equivalent to RSA 2048 (which is supposed to survive until 2030) and we list figures for public key and signature sizes:

1) RSA Sign: the key and signature sizes are large (256 bytes).
2) ECC (Elliptic Curve Cryptography): it is more compact than RSA (28 bytes), faster in signing but slower in verification.
3) NTRUSign[1]: the key size is between the two above (197 bytes), but it is much faster than the others in both signing and verification.

Given that in DSRC the minimal data rate is 6Mbps (for safety messaging it is typically 12Mbps), the transmission overhead (at 12Mbps) corresponding to all the above options is acceptable as shown in Table I.

Table II gives approximative execution times of signature generation and verification for ECDSA (Elliptic Curve Digital Signature Algorithm) and NTRUSign on a Pentium II 400 Mhz with memory constraints.

In conclusion, we can notice that in terms of performance, ECDSA and NTRU outperform RSA. Compared to each other, the advantage of ECDSA is its compactness, whereas NTRU's is superior speed. The conclusive decision should depend on case-specific evaluations (e.g., considering the computing platforms that will be installed on vehicles equipped with DSRC).

[1]The NTRU cryptosystem is recent and has so far undergone considerable scrutiny. It is being standardized by the IEEE P1363 Working Group (Standard Specifications For Public-Key Cryptography).

VI. IN-VEHICLE COMMUNICATION PROTECTION

Active safety applications rely on trusted usage of car sensor data, but to focus only on VANET security is not sufficient enough. Therefore the protection against outside and inside attacks on vehicle sensor data based on an in-vehicle security middleware will be investigated. Besides the conceptions of in-vehicle firewalls mechanisms the development of an intrusion detection system (in-vehicle IDS combined with VANET IDS) and concepts for the integration of secure execution environments in an in-vehicle architecture will be made (e.g. "sandboxes" based on tamper-proof devices (Software and Hardware)). Additionally specifications for a secure enforcement of security policies and safeguarding of in-vehicle processes will be evaluated and "Minimize Loss" through an autonomous, self-healing security management (e.g. definition of security system status and system recovery) will complete this task.

The consideration of current AUTOSAR activities [7] to secure the flashing and updating of electronic/telematics control units (ECUs/TCUs) and a liaison with the security activities in the STREP Electronic Architecture and System Engineering for Integrated Safety Systems (EASIS, [8]) support our activities.

VII. VALIDATION AND TESTING OF SECURITY MECHANISMS

When working on a security system, validation and testing of the design, specification, and implementation becomes a predominant subject. If the security system fails to thoroughly address potential security holes or even worse introduce new ones, the invested work and resources are for nothing.

Therefore, the approaches developed in SEVECOM need to be validated and tested on multiple levels. First, cryptographic protocols and other architectural components need to be analyzed whether they actually meet the formal specifications and security goals. Next, the actual prototype implementation of the various components need to be checked, whether it really implements the architecture and adheres to these specifications.

As SEVECOM intends to also prepare the industrial deployment of the designed system, the test and validation mechanisms need to be automated where possible in order to test new versions or implementations by other manufacturers.

SEVECOM will take the following steps to approach these tasks:

- Evaluate and decide on approaches for specification validation
- Validate the security and correctness of the specification
- Evaluate and decide on approaches for implementation validation
- Implementation validation
- Quantitative analysis
- Implementation validation of prototype implementation
- Quantitative analysis

- Prepare validation methods for deployment

A. Approaches for Specification Validation

Here, the project will identify the steps that SEVECOM will take to ensure the security and correctness of its results. When defining an security architecture, this architecture usual comprises a number of sub-components like protocols, algorithms, etc. Research activities in the area of formal proof of security systems have led to a number of methods based on state-machines, modal logic, or algebras [3]. This task will identify suitable instruments that will be used to validate the correctness of the architecture and formal specification developed throughout the project with regard to the security goals identified earlier. It will then select a representative set for development and demonstration. Performance criteria as well as metrics will also be defined. Finally, these instruments will be applied to the architecture and formal specification of SEVECOM

B. Approaches for Implementation Validation

Like for the specification, the correctness of the actual implementation needs to be verified. Before deploying software into a car, it needs to be tested and validated. In particular, platforms and/or technology components from different suppliers must exhibit the required level of trust and security. The validation must be aware of technical standards (e.g. NIST or SECG). Additionally, legal standards - like the European directive on Digital Signatures for example - have to be considered. Cost and complexity requirement will also be taken into account. A future goal is an automatic test suite that checks the conformance. SEVECOM will investigate the approaches that are possible to test both the correctness of both lab test developments and real-world use cases. Approaches to be considered are:

Protocol and Interface testing. Related standards (e.g. ISO/IEC 9646-1:1994(E)) will be considered. Automated protocol generation/testing will also be considered (e.g. the Protos Project from Oulu University, Finland [11], or the COCOS compiler from Rostock University, Germany)

Tests of the overall system (overall behavior, integration in lab test and use case development, trial attacks, etc.)

Penetration testing. Project external people (sometimes referred to as a tiger team) with full knowledge of the technical implementation will try to undermine the security of the system and information. This task will need to run in parallel with the development task, because instrumentation mechanism might be required (e.g. logging of some data, unit testing interfaces, etc.). It will identify the possibilities for implementation validation, and select a representative set for development and demonstration.

Next, the selected methods will be applied to the lab test developments and necessary test components will be developed. At a later stage of the project, these methods will then be applied to the use case implementations. Necessary test components will be extended and enhanced during this task.

In addition to the methods described above, we will analyze our security architecture with respect to quantitative aspects. This includes overhead, runtime behavior like latencies or scalability. This can be achieved by means of simulations, using discrete event simulators like ns-2, Glomosim, OPNET Modeler or JiST/SWANS, by using numerical calculations or by measuring certain values in the lab test and use case developments.

C. Prepare validation methods for deployment

An additional requirement for SEVECOM is to prepare the designed systems for deployment in industry. This also includes testing facilities that will allow manufacturers of in-car systems to easily test their implementations like it has been done with the prototypes.

So SEVECOM needs to investigate how existing industrial conformance testing tools (e.g. test protocols, APIs) can be enhanced to support specific security related testing. Such enhancements need to be developed and applied to the laboratory prototype.

VIII. Conclusions

V2V and V2I communication will play an important role for eSafety applications. Currently, there are several ongoing and upcoming projects in Europe and the US that investigate and develop V2V and V2I technologies, which have security as a common requirement. Ongoing projects like *Network on Wheels (NoW) [9]* and *GST* [10] partially address security issues and have worked out several important aspects to consider. SEVECOM will pick up and continue this work, particularly in close liaison with the recently started IST eSafety projects like CVIS, Safespot and Coopers, to ensure that SEVECOM threat analysis is consistent with eSafety projects.

Besides, SEVECOM will support standardization committees. This may mean to extend existing standard (e.g. CALM, Road vehicle security) or defining specific APIs (e.g. at the OSGi level). For this work, SEVECOM will closely cooperate with the car-to-car communication consortium [2]. Apart from the European initiatives led by the C2C-CC, SEVECOM will also establish strong connections with related efforts in the world, notably in the USA (DSRC, IEEE P1556) and in Japan.

It is expected that a number of common workshop with eSafety projects as well as with other stakeholders will be held. This will allow SEVECOM in particular to identify further challenges for the longer term than the first project phase.

References

[1] http://www.sevecom.org/
[2] http://www.car-to-car.org/
[3] Formal Verification of Cryptographic Protocols: A Survey. Catherine Meadows, Advances in Cryptology - Asiacrypt '94, LNSC 917, Springer-Verlag, 1995, pp. 133-150.
[4] M. Raya and J.-P. Hubaux. The Security of Vehicular Ad Hoc Networks. In *Proceedings of the ACM Workshop on Security in Ad hoc and Sensor Networks (SASN)*. October 2005.
[5] FIPS PUB 140-2. Security Requirements for Cryptographic Modules. NIST Information Technology Laboratory. May 2001.
[6] IBM Cryptographic Products. IBM PCI Cryptographic Coprocessor. General Information Manual. May 2002.
[7] http://www.autosar.org
[8] http://www.easis-online.org
[9] http://www.network-on-wheels.de/
[10] http://www.gstproject.org/
[11] http://www.ee.oulu.fi/research/ouspg/protos/