



Sevecom

SEcure VEHicular COMMunication

Sevecom is an EU-funded project that focuses on providing a full definition and implementation of security requirements for vehicular communications.

The **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 optimised road traffic through cooperative systems applications.

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

With the goal of enhancing the immunity of future road safety applications against a wide range of security threats, **Sevecom** focuses on communications specific to road traffic. Three major aspects will be examined.

- Threats, such as bogus information, denial of service or identity cheating.
- Requirements, like authentication, availability, and privacy.
- Operational Properties, including network scale, privacy, cost and trust.

More Information:

www.sevecom.org

Contact us:

Name: Antonio Kung
 Organisation: Trialog
 Telephone: +33-1-44 70 61 00
 E-mail: antonio.kung@trialog.com

Sevecom Mission and Objectives

Vehicular communications (VC) and inter-vehicular communications (IVC) bring the promise of improved road safety and optimized 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, or 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 (moving vehicles, sporadic connectivity, etc.) 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 VC/IVC 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, Secure user interface.

The definition of cryptographic primitives which takes 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 VC environment.

Sevecom will maintain close links with other IST projects dealing with cooperative systems, as well as with European and international initiatives in this area.

Project Acronym:	Sevecom
Project Reference:	IST-2004-027795
Contract Type:	Specific Targeted Research Project (STReP)
Start Date:	01/01/2006
Duration:	36 months
End Date:	31/12/2008
Project Cost:	4.674.048 €
EC project funding:	2.998.983 €

Participants:

The project is coordinated by Dialog, the consortium consists of the following partners: BMU, DaimlerChrysler, EPFL, CRF, Philips and Ulm University.