Secure Vehicle Communication

Deliverable 6.1

Project Presentation

Project:	Sevecom
Project Number:	IST-027795
Deliverable:	D6.1
Title:	Project Presentation
Version:	v1.0
Confidentiality:	Public
Author:	TRIALOG
Date:	03 February 2006

Part of the Sixth Framework Programme
Funded by the EC - DG INFSO

Table of Contents

1 DOCUMENT HISTORY 3

2 PROJECT DATA 4

3 LIST OF PARTICIPANTS 4

4 COST AND FUNDING 5

5 PROJECT PRESENTATION 5

5.1 MAIN GOALS 5
5.2 KEY ISSUES 5
5.3 TECHNICAL APPROACH 6
5.4 EXPECTED ACHIEVEMENTS AND IMPACT 6

6 CO-ORDINATOR CONTACT DETAILS 7

1 Document History

Version	Status	Date
v0.9	draft	03/02/2006
v1.0	final	28/03/2006

2 Project Data

Contract Number	IST-027795
Project Acronym	SeVeCom
Project Name	Secure Vehicle Communication
Priority Component	2.4.12 eSafety - Co-operative Systems for Road Transport
Project Logo	

3 List of Participants

No.	Consortium Partners
1	**TRIALOG**, Project Co-ordinator 25 rue du Général Foy 75008 Paris, France
2	**Ecole Polytechnique Fédérale de Lausanne** Ecublens 1015 Lausanne, Switzerland
3	**DaimlerChrysler AG** Wilhelm-Runge-Straße 11 P.O. Box 23 60 89081 Ulm, Germany
4	**Philips GMBH Zweigniederlassung Forschungslaoratorien** Weisshausstrasse 2 P.O. Box 21 D-52066 Aachen, Germany
5	**Budapesti Müszaki És Gazdasagtudomanyi Egyetem** **(Budapest University of Technology and Economics)** Muegyetem Rakpart 3 1111 Budapest, Hungary
6	**Centro Ricerche FIAT Societa Consortile per Azioni** Strada Torino 50 10043 Orbassano (TO), Italy
7	**Universität Ulm** P.O. Box 89069 Gruener Hof 5C 89073 Ulm, Germany

4 Cost and Funding

Total Cost	4 674 048.00 Euros
Commission Funding	2 998 983.00 Euros

5 Project Presentation

5.1 Main Goals

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

5.2 Key Issues

Vehicle to Vehicle communication (V2V) and Vehicle to Infrastructure communication (V2I) bring the promise of improved road safety and optimised 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 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. 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. 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 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 cryptosystems to the V2V/V2I environment.

5.3 Technical Approach

The overall approach is the following :

- Take into account existing results available from on-going eSafety projects such as PREVENT or GST in terms of threat analysis and security architecture.
- Work in close liaison with new IST eSafety projects which will focus on C2C application and road network infrastructures. Common workshops will be held in order to reach a consensus on the security threats and the proposed mechanisms.
- Take into account on-going standardisation work at the level of security such as ISO15764 - Extended Data Link Security or ISO/CD20828 - Security Certificate Management, or at the level of communication (ISO2121x serie on CALM - Continuous Air interface for Long and Medium distance).
- Integrate SeVeCom mechanisms into an use case development which is based on the V2V/V2I infrastructure used by eSafety projects.
- Investigate the necessary conditions for deployment. This includes the provision guidelines for security evaluation and certification, as well as the definition of a roadmap. This will include discussion on organisational issues (e.g. key and certificate management).

The project will work in close liaison with the Car-2-Car consortium; it will also establish strong connections with related efforts in the world, notably the USA with DSRC, IEEE P1609 (previously P1556) and Japan.

5.4 Expected Achievements and Impact

SeVeCom covers a number of research topics. The table below lists them along with the expected achievement.

	Topic	Scope of work
A1	Key and identity management	Workable solution
A2	Secure communication protocols (including secure routing)	Workable solution
A3	Tamper proof device and decision on cryptosystem	Workable solution
A4	Intrusion Detection	Investigation
A5	Data consistency	Investigation
A6	Privacy	Workable solution
A7	Secure positioning	Investigation
A8	Secure user interface	Investigation

6 Co-ordinator Contact Details

Company	TRIALOG
Contact person	Antonio Kung
Address	25 rue du Général Foy 75008 Paris, France
Telephone	+33 1 44 70 61 03
Fax	+33 1 42 94 80 64
e-mail	antonio.kung@trialog.com