



project name

Title of the report

Verified by,
Technolution B.V.

person that verifies
title of person

Accepted by,
customer name

person that accepts
title of person

Document information:

Title : Title of the report
Customer : customer name
Author(s) : Nol
Version : 0.0
Date : 21 June, 1996
File : eSecurity part A2 A3.doc
Project : project name
Project number : T00001

Document change control:

Version	Date	Author	Comments	Review	Style

Document distribution:

<p><u>Company A</u> <Make sure that the person who orders this document agrees with the distribution. That person must check this list> Name 1 Name 2 Name n</p> <p><u>Internal</u> Name 1 Name 2 Name n</p>
--

This report was created by:

Technolution B.V.
Zuidelijk Halfrond 1
P.O. Box 2013
2800 BD Gouda
The Netherlands

Tel. +31(0)182 59 40 00
Fax +31(0)182 53 97 36
www.technolution.nl

© Technolution B.V.

Nothing of this report may be multiplied and/or published by print, photocopy, microfilm, electronic or otherwise, without previous consent of Technolution B.V.

SYNOPSIS

TABLE OF CONTENTS

1.	INTRODUCTION	1
1.1	Context	1
1.2	Purpose of this report.....	1
1.3	Structure of this report	1
2.	ARCHITECTURES	2
2.1	Overview architecture current systems	3
2.1.1	NOW	3
2.1.2	GST.....	3
2.1.3	CVIS.....	3
2.1.4	COOPERS.....	3
2.1.5	Safespot	3
2.2	General model	3
2.2.1	Architecture	3
2.2.2	Behaviour	4
3.	ROLES	5
4.	ATTACKS	6
5.	OPEN ISSUES	ERROR! BOOKMARK NOT DEFINED.
6.	REFERENCES	7
7.	GLOSSARY	8

1. INTRODUCTION

1.1 Context

From meeting:

- Focus 1: Data protection
 - Impact of eSafety (applications) and telematic services onto security (data protection, article 29 aspects, etc.).
- Focus 2: Intrusion
 - Impact of security on Safety and on other aspects (e.g. socio-economical impact)
 - hardware and software security, attacks, manipulations, DoS, in car communication, car-to-car, car-to infrastructure, etc)

Goal: Derived from a profound threat and attack scenario **qualified recommendations need to be developed** regarding the technology requirements (networks, architecture, systems & components and their interaction), which are complemented by advice regarding the legal provisions and standardisation needs for implementation.

1.2 Purpose of this report

1.3 Structure of this report

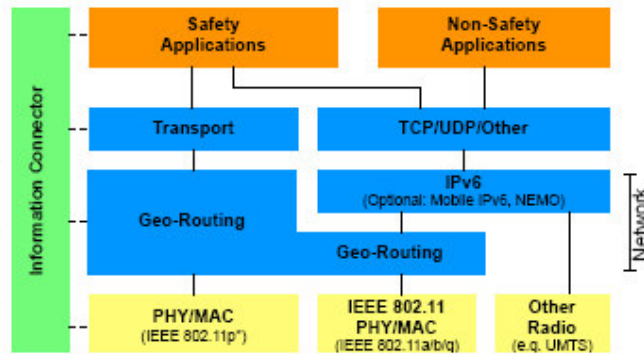
2. PLAN

2.1 Activities

- Compare models used for in-car system from different projects like NOW, CVIS, COOPERS, Safespot
- Construct a general model (architecture) and behaviour in different stages of the life-cycle of the vehicle.
- Assume technologies used TCPIP, IEEE 804.11x, VANET's, WAVE, ...
- Identify vulnerabilities, counter measures

2.2 Open issues

- Document templates?
- Contact persons other technology projects like COOPERS, Safespot, NOW?
- Focus: what is not clear to me is what the appropriate effort is to accomplish the goal of this working group. I think that this working group is important because of its ability to formulate recommendations in the field of 'vehicular security'. So the focus is not to find the solutions but to find the problems.
- Report content:
 - Style: Self containing or survey?
 - Is it possible/usefull to do this only for a general model, or should analysis always address an implementation? What aspects will be overlooked when dealing with a general model only?
- How to cooperate / assign work packages
- As Frank suggested: there is a strong dependence with line of attention A4. How to deal with this? Merge activities?



(b) Protocol architecture

3.2.2 Behaviour

In this section I suggest we enter basic functionality. It will give us a baseline for identifying vulnerabilities. A paper of Matthias Gerlach suggests to use use cases. I'm not sure, but this might work out well for the functional part. Functional aspects are however responsible for only a part of vulnerabilities of a system. Another source of vulnerabilities is utilisation of specific technology (TCP/IP, Linux, OSGi,). This part depends a lot on project specific choices.

3.2.2.1.1 Platform

- Storing keys
- Sensor access

3.2.2.1.2 C2C (or V2V)

- VANET context

3.2.2.1.3 C2I (or V2I)

- VANET context (roadside)
- TCP/IP context (services)

4. ROLES

Mind the phases of the life-cycle of the

- Development phase
 - Hardware- and software developer
- Production phase
 - Manufacturer
- Operating phase
 - dealer, Owner, User, anybody
- Maintenance phase
 - Authorized garage, Brand own, Non brand own
 - Unauthorized garage
- De-Installation phase
- Re-Installation

5. ATTACKS

- Analysis/ attack models
- Type of attacks
- Types of attackers
- Threads
- Kinds of attacks
- Intrusion detection
- Standard attacks
- exploits

Input meeting:

- The activity can take input from existing work for threat identification
- Examples:
 - Manipulation of hardware, software, parameters, transactions
 - Unauthorized use of collected data (e.g. for location tracking...)
 - Implementation trapdoors and trojan horses
 - Denial of service
 - Unauthorized access
 - Unauthorized commands
 - Unintended risks, for example by interferences on the communication system, failures of CAN gateway, overload of CAN gateway by entertainment system
 - Levels of threats
 - Levels of damages

6. REFERENCES

[1] xxx

- Network-on-wheels (NOW)
 - <http://www.network-on-wheels.de/documents.html>
 - [http://www.network-on-wheels.de/downloads/NOW TechReport Attacks on Inter Vehiclu e Communications.pdf](http://www.network-on-wheels.de/downloads/NOW_TechReport_Attacks_on_Inter_Vehiclu_e_Communications.pdf)
 - <http://www.network-on-wheels.de/downloads/now-ap24-20070501secuc-dv1.pdf>
- Secure Vehicular Communication (SeVeCOM)
 - <http://www.sevecom.org/Pages/JournalPublications.html>
 - <http://www.sevecom.org/Pages/PublicationsProject.html>
 - [http://www.sevecom.org/Deliverables/Sevecom Deliverable D1.1_v1.0.pdf](http://www.sevecom.org/Deliverables/Sevecom_Deliverable_D1.1_v1.0.pdf)
 - to be published on 6th – 8th June 2007: Architecture for Secure and Private Vehicular Communications
- EPFL
 - <http://infoscience.epfl.ch/>
 - <http://infoscience.epfl.ch/getfile.py?recid=94375&mode=best>
 - <http://infoscience.epfl.ch/getfile.py?recid=94377&mode=best>
 - <http://infoscience.epfl.ch/getfile.py?recid=94374&mode=best>
 - <http://infoscience.epfl.ch/getfile.py?recid=87501&mode=best>
 - <http://infoscience.epfl.ch/getfile.py?recid=90806&mode=best>
- CAR 2 CAR Communication Consortium
 - <http://www.car-2-car.org/>
 - C2C CC manifesto (location not yet identified)
- Medien Informatik Ulm
 - <http://medien.informatik.uni-ulm.de/forschung/publikationen.xml>
 - <http://medien.informatik.uni-ulm.de/~frank/research/escar2006.pdf>
 - <http://medien.informatik.uni-ulm.de/forschung/publikationen/escar2006.pdf>

7. GLOSSARY

Sample entry example of a glossary entry.
VANET Vehicular Network