Information Security Assignment: Security for V2V communications

Eric Laermans (eric.laermans@UGent.be)

2017-03-06

Contents

Autonomous cars, smart cars are one of today's big technological promises. The promised benefits include increased energy efficiency, reduced congestion, a significant reduction in traffic collisions, etc. There are still a few issues to be solved, e.g. interaction with traffic signs and traffic lights, interaction with pedestrians and cyclists, etc. but this is not the topic of this assignment.

An important element for this concept of autonomous cars are the vehicular communication systems, which include communications with smart traffic signs (for dynamic speed limits, traffic information, or other purposes) and vehicle-to-vehicle (V2V) communications. This may be very useful to allow platooning on an automated highway system. In this scenario vehicles join a platoon of several vehicles driving together with only minimal gaps (approximately 1 m) betweens vehicles to minimise air resistance and reduce traffic congestion.

The goal of this assignment is to develop the security protocol for these V2V communications. There will typically be 3 different phases in the communication:

- set-up of communication with other vehicles (e.g. when joining the platoon)
- normal communication (e.g. when driving in a platoon)
- termination of communication (e.g. when leaving the platoon)

You will have to deal with a few particularities of this application:

- the diversity of car manufacturers, which requires interoperability between different systems
- the technology should not be a source of accidents: safety is critical
- obviously the communications will be wireless, which has a negative impact on the reliability of a communication
- graceful degradation of the communication system is a requirement
- vehicles on a highway are driving at a speed of approximately 30 m/s, which means that hard real-time reactions are essential (25 ms is probably the maximal allowed reaction time)

- non-repudiable logging of communications may be very useful in case of a failure which causes an accident
- as the system involves safety malicious users may attempt to hack it
- the communications are fully automated: no intervention by the driver should be required

Try to think like a potential hacker and to analyse how you could crack or hurt the security you have designed.

Objective

Report

The main objective of this project is that you think about the correct security choices you have to make for such a system:

- Which security services are required (confidentiality, authentication, data-integrity, non-repudiation, etc.)?
- Against which attacks should these security services protect the system?
- Which countermeasures have been taken against these attacks?
- What are possible limitations and remaining vulnerabilities of your system?
- Which concrete security mechanisms (encryption algorithms, key lengths, etc.) do you use to implement these security services? Be sufficiently specific in the description of your choice.

You have to be able to justify these choices in the report you write about this (but also at the exam).

The report need not be lengthy (I do not expect a novel, eight pages —using normal font size and line space— is typically sufficient), but it shall be sufficiently complete, allowing me to understand your security choices.

Do not forget to mention the sources of your inspiration in the references.

Do not forget to write a conclusion to the assignment report.

And finally, a last note: "a picture is worth a thousand words". Adding a schematic explaining how messages are exchanged can be very useful.

Demonstration software

Besides the report you will write about the project, I also expect some small demonstration software.

- The main purpose of the software is to demonstrate the operation of the security mechanisms
- The functional aspects (e.g. the information exchanged between vehicles) are not essential for this assignment.

- Do *not* implement the cryptographic algorithms yourself. Rather use existing implementations.
- You need not set up any server. A proof-of-concept demonstration on a PC is sufficient. The purpose is that at the end of the assignment you can give me a demonstration of how your system works (e.g. on a laptop).
- I'll ask you to demonstrate how the software works (this can be done during the exam or we can schedule a separate appointment for that).

Practically

Groups

This project should be done in groups of 4 (if really needed 3) persons. So, your first task will be to agree upon the composition of these groups. I only expect a single report and a single demonstration per group. Please let me know as soon as possible the composition of the different groups (using Minerva's "Groups" functionality).

Deadline

The **final** deadline for the report of this project is **May 19, 2017 (22h00)**. The preferred submission channel is Minerva's "Dropbox".

As the exam period starts on May 29, it is not feasible for me to *guarantee* feedback about the assignment score before the exam. If you want guaranteed feedback before the exam, you can ask for this beforehand, but then I expect your report on May 9, 2017 (22h00) (10 days earlier). Otherwise, it will be "best effort" only.

Questions

If you have any further question, please contact me.