Information Security Assignment: Security Design for a Smartphone Car Access App

Eric Laermans (eric.laermans@UGent.be)

2025-02-26

Contents

Smart cards have been widely used for car access (opening and closing the car, starting the car, etc.) due to their convenience and security features. These cards typically use Near Field Communication (NFC) or Radio Frequency Identification (RFID) technology to communicate with the car's access system. A new tendency in car access is to replace these smart cards by a smartphone application.

The goal of this assignment is to think thoroughly about the security aspects that would be required for a secure smartphone application that can replace a smart card for car access.

I expect you to address the following aspects:

- The app should allow users to unlock, start, and manage their car.
- The app should include a secure method for transferring access rights to another person without transferring the smartphone. This should allow the identification of the driver when a fine for some traffic violation must be paid or when an accident occurs.
- It should be possible to block the possibility to start the car if the driving licence of the user has been revoked.
- Consider the advantages and drawbacks in comparison to a smart card based solution.
- The app should include some application level security. It is not sufficient to rely on underlying secure communication protocols (e.g. TLS) only (although you can include them in your security solution).
- Try also to think like a potential hacker and to analyse how you could crack the security you have designed.
- Do not forget the ease-of-use requirement.

Objectives

Report

The *main objective* of this assignment is that you think about the correct security choices you have to take into account to *design* 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 (communication protocols, encryption algorithm, key lengths, etc.) do you use to implement these security services? Be sufficiently specific in the description of your choice.
- Which measures have been taken to protect the users' privacy?

You are expected to justify your choices in the final report you write about this assignment. The report need not be lengthy (I do not expect a novel, 8 to 12 pages using normal font size and line space is typically sufficient), but it shall be sufficiently complete: someone reading the report should be able to understand how your system works and how it could be implemented. A couple of additional tips for the final report:

- Do not forget to mention the sources of your inspiration in the references.
- If you use Copilot or some other AI, you must clearly mention what the contribution of this AI is and you have to be able to explain this contribution.
- Do not forget to write a conclusion to the assignment report.
- "A picture is worth a thousand words". Adding a schematic explaining how messages are exchanged in a protocol and the structure of these messages can be very useful.

Demonstration software

Besides the report you will write about the assignment, I also expect some proof-of-concept demonstration software.

- The main purpose of the software is to demonstrate the operation of the security mechanisms and the operation of your application. A feature rich implementation is not asked for. The software should be seen as a means to facilitate the explanation of the design choices you have made.
- Show how the required security services can be verified.
- It may be useful to illustrate a few possible attacks and how the security of your systems prevents them from being successful.

- Do *not* implement the cryptographic algorithms yourself. Rather use existing implementations.
- Your proof-of-concept demonstration may slightly differ from the system you've worked out in the report if this simplifies the implementation (e.g. using RSA instead of ECC), but don't forget to mention and explain the differences.
- You need not set up any server (but it is not forbidden either) or develop a mobile app. 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).
- You will be able to demonstrate how the software works during the presentation (see next section).

Presentation

You will show your results in a presentation, where you explain how the security works and show the demonstration of the proof-of-concept software. The presentations will be organised online using MS Teams. A 30 minutes time slot will be scheduled for each group in the second half of May or in June. We'll try to find a time slot which is sufficiently convenient for most group members and myself. Not all group member need to be present during the presentation (although that would be better of course), but at least a majority of the group is expected to join.

Practically

Deadlines

Groups

This assignment should be done in groups of 6 (if needed 5) 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. Forming the groups is left to the responsibility of the students. I expect the groups to be formed by **Friday, March 07, 2025 (22h00)**. Use Ufora's "Groups" functionality to compose the groups.

Intermediate reports

I expect from each group a *concise* intermediate report via the Ufora "Assignments" tool on the following dates:

- Friday, March 21, 2025 (22h00)
- Friday, April 4, 2025 (22h00)
- Friday, April 25, 2025 (22h00)

Please include your group number and the names of the group members in the report. I expect a brief description of the vision of your project, the current status (i.e. work done), a short term planning with respect to the overall assignment schedule and contributions

of each group member (task + estimate of time spent) in each intermediate report. If there are changes in your vision or in the overall planning, it could be useful to describe these briefly.

Be honest in your reporting. There may be periods where some of you haven't been able to do much because of other obligations, or you may not have achieved the goals of your previous planning. Your score won't depend on these intermediate reports. The goal of these intermediate reports is for me to keep an oversight of the assignment progress in all groups and to identify possible "free-rider problems" in time.

Final report

The **final** deadline for the report of this assignment is **Friday, May 9, 2025 (22h00)**[1]. You shall submit the final report using Ufora's "Assignment" tool. I shall try to provide feedback on the assignments before May 26.

Questions

If you have any assignment related question that may be of general interest, please use the "Discussions" module in Ufora. For other questions you can contact me by email.

[1] If you need an extension of this deadline by a few days, do not hesitate to ask.