Information Security Assignment: Security for a (Car) Key App

Eric Laermans (eric.laermans@intec.UGent.be)

2016-03-10

Contents

Smartphone apps are often available for the most diverse applications. One company even uses a smartphone app as a car key for shared cars: no more need for special key cards or other dedicated hardware that needs to be distributed to the users, the user smartphone will do.

The goal of this assignment is to work out the security for such a key app. The app must have the following functionality:

- booking a car
- (un)locking the car
- starting the car
- billing the user for the time and distance travelled

The key app may be generalised for other "key" applications, e.g. access to a hotel room, to an apartment for rent, etc.

Do not forget to consider the following security aspects:

- users need to be registered and their driver's license needs to be checked
- only the legitimate user who has booked the car should be able to unlock and to start a car
- billing should be non-repudiable
- ideally the system should work even when there is no network coverage (except for the booking part), e.g. in some very rural areas or in an underground parking lot
- ideally the security of the app shouldn't rely on underlying network security (3G or 4G), the app should be able to operate securely over an unsecured WiFi network (the car being the access point) or over NFC (Near Field Communication)
- Try also to think like a potential hacker and to analyse how you could crack or hurt the security you have designed.
- Do not forget the ease-of-use requirement.

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?

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. collecting billing data) are not essential for this assignment.
- Do *not* implement the cryptographic algorithms yourself. Rather use existing implementations.
- You need not write a smartphone app or 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 13, 2016**. The preferred submission channel is Minerva's "Dropbox".

As the exam period starts on May 23, it is not feasible for me to guarantee feedback about the assignment score before the exam. If you want feedback before the exam, you can ask for this beforehand, but then I expect your report on May 3, 2016 (10 days earlier).

Questions

If you have any further question, please contact me.