Family Name: .....

First Name: .....

Section: .....

Security Protocols and Applications (Part 2)

Final Exam

June 18th, 2009

Duration: 3:45

This document consists of 7 pages.

Instructions

Electronic comunication devices and documents are *not* allowed.

This exam contains 2 *independent* parts.

Answers for each part must be written on its separate sheet.

Answers can be either in French or English.

Questions of any kind will certainly *not* be answered. Potential errors in these sheets are part of the exam.

You have to put your full name on the first page and have all pages *stapled*.

1 Electronic Passport

1.1 Basics

E-passports can have different security features. For each of the following explain what kind of *attacks* they are supposed to protect from and what *conditions* must be met to make this protection actually work.

1. The Security Object (SOD) in the Logical Data Structure (LDS)

2. The basic access control (BAC)

3. The Active Authentication (AA)

1.2 Eve's attack

Eve has seduced Bob and got him to divorce from Alice. She is very disappointed. Not only did Bob lose the car to Alice over a strange coin flipping game, but he also didn't get anything from Alice's fortune, because it was all Alice's private money.

Eve discovered that Alice has stored all her fortune in a safe in bank. The bank uses very modern safes that only open when an authorized passport is placed in front of the safe. Eve does not have access to Alice's passport but she knows that Alice always carries it in her purse, which she puts on the passenger seat when driving. Before Bob hands over the car to Alice, Eve places some equipment under the passenger seat of the car in order to get access to the safe without stealing the passport.

The safes at Alice's bank work like this:

- The customer walks to the room containing the safes and declares which safe she wants to access.
- A clerk takes the passport of the customer into his hands and makes sure the customer is the legitimate owner of the passport by looking at the picture, the birth date and the expiration date.
- The clerk holds the passport in front of the safe.
- A tiny camera in the safe read the MRZ.
- an RFID reader within the safe reads the passport and compares it to a list of authorized users stored within the safe.
- The safe opens if the person is on the list of authorized users.

Eve plans to walk into the bank and pretend she is an authorized user of Alice's safe. She will give her passport to the clerk and play some tricks such that the safe opens when presented her passport. She knows Alice's birthday (Bob told her) and she knows the expiration date of Alice's passport (it is the same as Bob's as they got it together for their honey moon). She also knows that the serial number of Bob's and Alice's passport only differ by the last four digits.

Scenario I: Imagine the passport is protected with BAC:

1. Explain what kind of devices Eve needs to install under Alice's passenger seat.

2. Explain what kind of operations she has to carry out before she goes to the bank.

3. Explain what kind of devices she needs to carry into the bank.

4. Explain exactly what happens when the clerk holds the passport in front of the safe.

Scenario II Now imagine the passport is protected with AA

1. Explain what kind of devices Eve needs to install under Alice's passenger seat

2. Explain what kind of operations she has to carry out before she goes to the bank.

3. Explain what kind of devices she needs to carry into the bank.

4. Explain exactly what happens when the clerk holds the passport in front of the safe.

1.3 Protection:

1. What should the bank have done differently to avoid this problem (independently of BAC or AA)?

2. What standard element of the e-passport is supposed to protect against this type of attacks?

3. What could Alice have done to prevent the attack?

Any attempt to look at
the content of these pages
before the signal
will be severly punished.

Please be patient.