LASEC

Family Name: .....

First Name: .....

Section: .....

Security Protocols and Applications (Part 2) — Solutions

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)

   The SOD prevents the creation of faked passports. It is based on the fact that electronic signatures can not be faked and that the reader can validate the key of the authority that signs the passport.

2. The basic access control (BAC)

   The BAC prevents unauthorized reading of the passport. To be efficient the key, based on the MRZ, must be random enough to render brute force attacks unpracticable.

3. The Active Authentication (AA)

   The AA prevents cloning of the passport. To be efficient, it must not be possible to extract the private key from the passport.

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.

   She needs an RFID reader

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

   She needs to
   - *try all 10'000 possible values of the serial number in order to find which one opens the passport.*
   - *copy the complete content of the passport into a chip located in her passport.*
   - *write Alice's MRZ on her passport*

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

   She needs her passport and a chip in the passport (or a transmitter in her purse) that can respond with Alice's data

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

   - *The camera reads Alice's MRZ on Eve's passport.*
   - *The RFID reader uses the MRZ as a key to read Alice's passports content*
   - *After verification of the signature of the SOD the safe is convinced that the passport is genuine and opens the door*

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

   She needs an RFID reader and a transmitter to communicate with the reader (e.g. a cell phone).

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

   She needs to

   - *try all 10'000 possible values of the serial number in order to find which one opens the passport.*
   - *copy the complete content of the passport into a chip located in her passport.*
   - *write Alice's MRZ on her passport*
   - *make sure Alice is in the car when she enters the bank.*

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

   She needs

   - *her passport with Alice's MRZ on it*
   - *a transmitter that can respond to the RFID reader with Alice's data.*
   - *a cell phone that can send the AA challenge to Alice's passport in the car and receive its response.*

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

   - *The camera reads Alice's MRZ on Eve's passport.*
   - *The RFID reader uses the MRZ as a key to read Alice's passports content from Eve's transmitter.*
   - *The RFID reader sends a challenge to the passport*
   - *Eve's cell phone sends the challenge to Alice's car.*
   - *The RFID reader in the car reads the passport and sends it the challenge.*
   - *The cell phone in the car sends the response of the challenge back to Eve's cell phone.*
   - *Eve's transmitter sends the response back to the reader in the safe.*
   - *The reader in the safe is convinced by the SOD and the response to the challenge the passport is genuine and authentic.*

1.3 Protection:

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

   The clerk should verify that the electronic content of the passport matches the passport holder

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

   The biometric information, e.g. a phot) to make sure the customer is the legitimate owner of the passport.ograph or a fingerprint

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

   She could have placed the passport into a metal envelope.

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

Please be patient.