Homework 1

Model a protocol and analyze it using Proverif

Deadline: 8.10.2020

Step 1. Alice comes to a government authority and receives a document. The document contains a secret key, which can be activated when using a corresponding PIN code. The authority writes down into a public table (which anyone can see) the public key of Alice.

- There can be arbitrarily many honest users getting their cards.
- The attacker can receive any number of cards as well, but he cannot choose the identity himself (e.g. he cannot pretend to be Alice who is already registered as an honest user).
- Add a query which verifies that the attacker indeed cannot learn a secret key that belongs to an honest user.

Step 2. Alice and Bob use the credentials of their cards and the public table to authenticate each other and exchange a symmetric key for further communication.
You can reuse any existing authenticated key exchange protocol here. Verify that:

- The attacker cannot learn the key shared between two honest parties.
- The attacker cannot impersonate Alice or Bob to each other (verify agreement of Alice and Bob on the same key).

**Step 3.** Alice lost her card. The attacker has found it. Alice blocked the card, and now needs to wait until she gets a new one.

- Output the secret key of the ID card into the public network. The query checking that “the attacker cannot learn the secret key of an honest party” should now fail.
- Blocking a card can be modeled e.g. using phases, so that the operations involving the card belong to the phases prior to the event when Alice lost her card.
- You do not need to model receiving a new card.

**Step 4.** Alice and Bob now want to exchange some secrets using the previously exchanged key. Is it safe assuming that Alice lost her card? Check at least the following:

- Can the attacker guess the secret if he only has the card, but not the PIN? Ensure that it is not possible.
- Can the attacker guess the secret if we has both the card and the PIN (which Alice probably wrote down onto a paper and put into the same wallet that she has lost)? This depends on which particular key exchange protocol Alice and Bob have used. You do not need to ensure this property, just verify it.