Project : Design and analysis of cryptographic protocols

The aim of this project is to learn how to design cryptographic protocols and how to model and analyse them using the ProVerif tool. During the first part of the project each team (of 2 students) will design a protocol which meets the constraints detailed below. In the second part of the project the proposed protocol will be analyzed by each team. Any attacks found will have to be corrected by the protocol designers.

The subject of all e-mails must contain the string "[Prot_Comp]".

Part 1 (Design of a key exchange protocol)
The aim is to design a protocol that allows two agents A and B to exchange a key which has been freshly generated during the session. At the end of the protocol both agents need to share the same, confidential and mutually authenticated key. Initially, both agents A and B will know their public encryption keys. They may also share a symmetric key with a trusted server. However, you may *not* suppose that A and B initially share a symmetric key.

Rules:

1. The protocol must be presented in the same style as the examples provided.
2. A pdf file with a detailed description of the protocol must be submitted no later than **January 9** by e-mail to steve.kremer@inria.fr.
3. It is *not* allowed to propose an existing protocol (or a direct variant).
4. The cost of the protocol must be as low as possible according to the cost function defined below. The cost of the protocol must be included in the protocol description.
5. The more costly the protocol is, the higher will be the initial *malus* of the second phase of the project.

The cost $f(P)$ of the protocol P is defined to be the sum of the costs of each message in a normal execution of the protocol.
Given a message $m = \langle m_1, \langle m_2, \cdots, m_k \rangle\rangle$, such that none of the m_i is a pair, the cost $f(m)$ is defined to be $\sum_{1 \leq i \leq k} f(m_i)$ where f is defined inductively as follows:

$f(a)$	$=$	1	if a is an identity, a key, a constant or a nonce
$f(\{m\}_k^a)$	$=$	$1 + f(m) + f(k)$	public key encryption
$f(h(m))$	$=$	$5 + f(m)$	hash function
$f(\{m\}_k^s)$	$=$	$10 + f(m) + f(k)$	symmetric encryption
$f(\langle m_1, m_2 \rangle)$	$=$	$50 + f(m_1) + f(m_2)$	pair

No cryptographic primitives other than public key encryption, symmetric encryption, hash function and pairs may be used.

Part 2 (Protocol attacks)
From January 10 onwards teams may start attacking each other's protocols.

Rules:

1. Each team starts with a negative score equal to the cost of the protocol, i.e. $-f(P)$.
2. A team is allowed to change their protocol if either their protocol has been attacked, or their new protocol has a lower cost.
3. Any new attack on a protocol (or on a new version of the protocol) adds 20 points to the attacking team. The team having designed the protocol loses 20 points. A same team may attack a same protocol multiple times if the attacks are different and the protocol has not been fixed.
4. Once a protocol has been fixed, the previous version may not be attacked any more.
5. After a protocol has been attacked, the designers have 3 days (not counting weekends, or holidays) to fix their protocol. Beyond this delay any further day removes an additional 20 points from the designer team.
6. As for the protocol, attacks must be provided in a pdf file, and presented in a similar way as the examples. The file describing the attacks must be sent to the group under attack and to the course instructor (steve.kremer@inria.fr).
7. For an attack to be valid, the attacked team must acknowledge the attack. In case the teams do not agree the course instructor will judge the validity of the attack.
8. The score board will be updated on the following dates: January 16, January 21, January 24, January 28.

Part 3 (Protocol models and analysis on ProVerif)
The proposed protocols have to be modelled and analysed using the ProVerif tool. Some attacks will certainly be discovered using this tool (but attacks may also be discovered by hand).
Each group will have to submit 3 ProVerif source files and a short report to the course instructor (steve.kremer@inria.fr) by January 30:

- one file with a proof of a property;
- one file with an attack; there should also be an explanation of the attack (see example files for describing attacks)
- one file of your choice (a model you think interesting).

These files should contain comments and must come with a short report explaining which protocols have been analysed and describing the attacks found using ProVerif.
The submission should consist of a single archive file (.zip or tar.gz – no other formats) containing all .pv protocol files with a clear reference to the analysed protocols (protocol-xy-v3.pv). The quality of the protocol modelling and of the analysed properties for each protocol will be an important aspect of the evaluation.

Grading: The project grade **will not be the score in the competition**. Your grade will depend on the following aspects:

- Implication in the competition.
- Modelling in ProVerif.
- The competition will attribute bonus points:
  - +2 points for the winners.
  - +1 point the team ranked second.
  - +1 point if 8 or more attacks were found.