Security Protocols and Verification
Project Presentation

Project : Design and Analysis of Cryptographic Protocols

The goal of this project is to learn do design cryptographic protocols, as well as how to model and analyze them in Tamarin. In the first phase of the project, each team will design a protocol respecting the given constraints. In the second phase, all these protocols will be attacked by the other teams. All successful attacks must be corrected by the designers of the protocol.

Phase 1 (Design of a secret exchange protocol)
You will design a protocol allowing two agents A and B to exchange a secret freshly generated by A. At the end of the protocol, both A and B need to share the same value, which also needs to stay secret. Initially, agents A and B can know all public keys (in particular each other's public keys), and even share a symmetric key with an honest server S. However, they have no mutually shared key K_{AB}.

The protocol description, following the format given in following example for the Needham-Schroeder protocol, must be sent to `jannik.dreier@loria.fr` using the title "[CHAMPIONSHIP] Protocol XXX" (where XXX is you team name) at latest on **October 3, 23h59**.

Security Properties: At the end of the message exchange, the following three security properties must be ensured:

- If B finishes a protocol run and thinks that he received a key K from A, then A effectively sent K to B.
- If A finishes a protocol run during which he sent K to B, then B has effectively received K from A.
- Finally, the key K must stay secret among A and B (and potentially the server S).
- In each session, a new fresh key K is exchanged.

Rules:

1. The protocol must be described using the template given in class for the Needham-Schroeder protocol.
2. It is forbidden to use an existing protocol.
3. The protocol must be the least "costly" with respect to the cost function defined below. The cost must be given in the protocol description.
4. The more costly your protocol is, the more negative point you will have at the start of the second phase of the project.
5. **Be careful:** 20 additional negative points for every day of delay (after October 3).

The cost of a protocol P is defined as the sum $f(P)$ of all costs of all messages in a normal execution of the protocol P. Given a message $m = m_1, m_2, \cdots, m_k$ (m_i does not start with a pair), the cost of the message $f(m_i)$ is defined recursively as follows:

$$\begin{array}{rcll} f(a) & = & 1 & \text{if } a \text{ is a name, a key or a nonce} \\ f(\{m\}_k) & = & 1 + f(m) + f(k) & \text{asymmetric encryption} \\ f(\mathsf{h}(m)) & = & 20 + 0.5 * f(m) & \text{if } m \text{ does not contain } \mathsf{h} \\ f(\mathsf{h}(m)) & = & 20 + f(m) & \text{otherwise} \\ f(\{\!|m|\!\}_k) & = & 10 + f(m) + f(k) & \text{symmetric encryption} \\ f(\langle m_1, m_2 \rangle) & = & 50 + f(m_1) + f(m_2) & \text{pair} \end{array}$$

Note: pairs at the beginning of messages do not count. This means that it is useless to cut a message into several messages, as the cost stays the same.
Note 2: triplets are counted as a pair inside a pair, i.e., $\langle m_1, m_2, m_3 \rangle$ is actually interpreted and counted as $\langle \langle m_1, m_2 \rangle, m_3 \rangle$, and similarly for quadruplets etc.
Note 3: Only the given primitives (symmetric and asymmetric encryption, hashing, pairs) can be used. In particular, signatures are not allowed.

Phase 2 (Protocol Attacks)
Starting from **October 13** it is possible to attack the protocols designed by the other groups. Protocols cannot be corrected any more after November 23, and attacks cannot be submitted any more after November 28, 23h59.

Rules:

1. Each team starts with a negative score, which is the cost of its protocol ($-f(P)$).
2. If your protocol gets attacked, you must fix it by proposing a new version.
   Be careful: after 3 (working) days without correction, an additional penalty of 20 points per (working) day of delay applies.
3. Every team finding the an attack on a protocol (or a "corrected" version) will be awarded 40 points, the attacked team looses 40 points. Note: even if several attacks are found on protocol version, a team cannot loose more than 40 points. Similarly, a team finding multiple attacks on one protocol (version) will only be awarded 40 points.
4. When a valid attack or a new version of a protocol is published, the old versions of the protocol can no longer be attacked.
5. When a protocol is updated, the initial negative score is also updated with the cost of the new version, the old score is "forgotten".
6. As for the protocols, attacks must be described in a pdf file named `AttackedTeamVXbyAttackingTeam.pdf` (where `AttackedTeam` and `AttackingTeam` are the names of the attacked and attacking team respectively, and `X` is the attacked protocol version) following the template give in class for the Needham-Schroeder protocol. The attack file must be sent to the team that proposed the protocol, with a copy to `jannik.dreier@loria.fr`.
7. To be considered valid, an attack must be recognized by attacked team. But stay honest!

8. The scoreboard will be updated every week, and is available on the class website on ARCHE.

9. **End of the competition:** No new versions are accepted after November 23 to allow the other teams to attack. **Be careful:** if the last version of a protocol is successfully attacked, the cost will be the highest cost of all the protocol version developed by a team, and not the cost of the last version.

Working days : all days except for the week-end, and the holidays from October 25 to November 2. Attacking is allowed any time!

Phase 3 (Modeling and Analysis using Tamarin)
Three protocols need to be modeled and analyzed using Tamarin.

- at least one protocol designed by the team
- at least one protocol with an attack
- at least one secure protocol

All the models have to be submitted inside a single compressed file on ARCHE, by one member of the team, on **November 28, 23h59**, latest.
The compressed file must contain the .spthy files of the modeled protocols, with a clear filename (e.g., protocol-xy-v2.spthy), as well as Tamarin's output for each of these files (e.g., protocol-xy-v2-OUTPUT.spthy, to avoid problems with different versions of the tool). Don't hesitate to add a README if for some file Tamarin needs to be run with particular options (e.g., `--auto-sources` or a particular heuristic).
Use great care when modeling the protocols and specifying the properties. In particular, do not hesitate to comment your model as you would comment code!
All discovered attacks have to be explained in a pdf file as for the attacks found in phase 2 (you can reuse an existing file if possible!).

Grading: The final grade of the project **is not your score in the competition**. It will rather be based on:

- Your participation in the competition
- The quality of your Tamarin models and the results obtained
- The competition itself however allows to obtain bonus points:
  - +2 points for the winning team
  - +1 point for the second team
  - +1 point if 8 or more attacks were found by a team
  - +1 point of none of the protocols proposed by a team has been successfully attacked