

Modélisation et analyse de protocoles en ProVerif

L'objectif de ce TP est d'apprendre à exprimer la confidentialité et l'authentification en ProVerif.

1. Installer ProVerif sur votre ordinateur. Pour cela, suivre les instructions de la page : <https://prosecco.gforge.inria.fr/personal/bblanche/proverif/>
2. Modéliser le protocole de Needham-Schroeder à clefs publiques et retrouver l'attaque vue en cours, sur le secret de N_b .

$$\begin{aligned} A &\rightarrow B \quad \{A, N_a\}_{pub(B)} \\ B &\rightarrow A \quad \{N_a, N_b\}_{pub(A)} \\ A &\rightarrow B \quad \{N_b\}_{pub(B)} \end{aligned}$$

Vous pouvez partir du squelette de fichier proposé sur la page du cours.

3. Montrer que le protocole corrigé est sûr pour le secret de N_b .

$$\begin{aligned} A &\rightarrow B \quad \{A, N_a\}_{pub(B)} \\ B &\rightarrow A \quad \{B, N_a, N_b\}_{pub(A)} \\ A &\rightarrow B \quad \{N_b\}_{pub(B)} \end{aligned}$$

4. Si on modifie la correction proposée, montrer qu'il existe de nouveau une attaque (à l'aide de ProVerif).

$$\begin{aligned} A &\rightarrow B \quad \{A, N_a\}_{pub(B)} \\ B &\rightarrow A \quad \{N_a, N_b, B\}_{pub(A)} \\ A &\rightarrow B \quad \{N_b\}_{pub(B)} \end{aligned}$$

Indice : L'attaque suppose que :

- (a) les identités puissent être confondues avec un nonce
- (b) Le message $\{N_a, N_b, B\}_{pub(A)}$ soit parenthésé comme suit : $\{\langle N_a, \langle N_b, B \rangle \rangle\}_{pub(A)}$.

5. Montrer en ProVerif que le protocole de Needham-Schroeder corrigé assure bien l'authentification mutuelle de ses participants. Il s'agit de modéliser la propriété "si B termine une session croyant avoir parlé à A, avec les valeurs N_a et N_b ; alors A a terminé une session croyant avoir parlé à B, avec les valeurs N_a et N_b ".
6. Le protocole suivant n'est pas un bon protocole d'échange de clef.

$$A \rightarrow B \quad \{A, K_{ab}\}_{pub(B)}$$

Pourquoi ? Retrouver l'attaque en ProVerif.