Université Paris 7 DESS Logiciels Fondamentaux
U.F.R d'informatique Année 2002-2003

TP 10 – Modelisation d'un protocole cryptographique

1 Needham Schroeder [1978]

Deux personnes ont une information secrete qu'ils desirent se transmettre. Mais le reseau n'est pas sûr, et les messages peuvent etre ecoutés, detournés, dupliqués par une troisieme personne.

Pour securiser l'ensemble, on se place dans un contexte de cryptographie à cle publique, c'est à dire que tout le monde possède un couple clé, verrou, les verrous sont connus de tous et peuvent etre utilisés pour securiser les messages à destination d'une personne. Par contre les clés sont privées, et seul celui qui la connait peut deverrouiller un message codé par le verrou correspondant.

Voici le protocole proposé par Needham-Schroeder lorsqu'il y a deux interlocuteurs :

Alice envois le message $< N_A, A >$ codé par le verrou de B (Il est destiné à Bob) Il contient le secret qu'elle desire partager, et son identitee pour que Bob sache de qui il s'agit. Ensuite, lorsqu'elle recoit un message qui lui est destiné (codé par son propre verrou), elle le dechiffre. Si ce message contient N_A suivit de quelque chose, elle a la reponse qu'elle attendait de Bob et le quelque chose est l'information N_B que Bob desire partager. Elle lui confirme qu'elle a bien recut N_B en envoyant en accusé de reception le message N_B, codé par le verrou de Bob, et termine.

Symetriquement, si Bob recoit un message codé par son verrou, il le dechiffre. Il comprend quel est le secret qu'on lui propose et qui le lui a envoyé. Il envoit alors un message $< N_A, N_B >$ codé par le verrou de son interlocuteur. (Il confirme à Alice qu'il a recut N_A, et lui apprend N_B). Finalement il attend la confirmation d'Alice qu'elle a bien recut N_B, et alors il termine.

Pendant 17 ans ce protocole a été supposé correct, et utilisé tel quel.
Nous allons chercher à le verifier avec Spin.

2 Modelisation avec Spin

1. Dans un premier temps, proposez un modele pour Alice et pour Bob. Celui ci devra :
   - Etre symetrique, c'est a dire que Alice ou Bob peut initier la communication

- Le reseau est modelise par un canal de taille 1
- Les messages sont codes, c'est a dire qu'ils sont compose de triplet $cle(m_1, m_2)$, et un acteur ne peut retirer un message du canal que si la cle est la sienne.
- votre modele doit verifier la validite des messages recut, et eventuellement detecter des incoherences.

2. On va supposer maintenant qu'il y a un troisieme personage dans le reseau : un Intrus malicieux qui peut choisir de ne pas respecter le protocole. Du point de vue d'Alice et de Bob, il s'agit d'un interlocuteur comme un autre. Comment modifier Alice et Bob pour au depart faire le choix de l'interlocuteur ? Quelle sont a present les constantes publiquement connues ?
3. L' Intrus, des lors qu'il voit passer un message qui lui est destine, et qui contient NA ou NB, peut les utiliser pour constituer un message. Ecriver un modele pour l'Intrus qui lui permette de :
   - perdre les messages
   - decoder les messages qui lui sont destines
   - composer des messages perfides
4. Simulez les 3 processus ensembles, et essayez de trouver une situation ou Alice et Bob parlent avec l'intrus, mais Bob pense etre en comunication avec Alice.
5. Ecrivez une formule qui englobe ce comportement.
6. Pouvez vous retrouver cette execution avec Spin ? Si non, essayez de reduire l'espace de recherche (brisez les symetries, quels sont les domaines des variables ...)