

Projet : Conception et analyse de protocoles cryptographiques

L'objectif de ce projet est d'apprendre à concevoir des protocoles cryptographiques et à les modéliser et les analyser à l'aide de l'outil ProVerif. Dans la première partie du projet, chaque groupe devra concevoir un protocole qui satisfait des contraintes données. Dans la deuxième partie du projet, tous les protocoles ainsi proposés seront analysés par chaque groupe. Les attaques trouvées devront être corrigées par les concepteurs du protocole attaqué.

Partie 1 (Conception d'un protocole d'échange de secret)

Vous devez concevoir un protocole qui permet à deux agents A et B de s'échanger un secret frais créé par A . À la fin de l'exécution du protocole, les deux agents A et B doivent partager la même donnée, qui doit rester confidentielle. Initialement, les agents A et B pourront connaître des clefs publiques et avoir une clef symétrique partagée avec un serveur. Par contre, on ne pourra pas supposer que A et B partagent déjà une clef symétrique k_{AB} .

La description du protocole, en pdf, en suivant le modèle donné en exemple pour Needham-Schroeder, doit être envoyée par mail aux responsables du cours (protocoles2020@inria.fr) le **mercredi 7 octobre à 23h59** au plus tard.

Propriétés de sécurité : À la fin de l'échange, les 3 propriétés de sécurité suivantes devront être satisfaites.

- Si B a fini pensant avoir reçu une clef K venant de A , alors A a bien envoyé K à B .
- Si A a fini en ayant envoyé une clé K à B alors B a bien reçu K de la part de A .
- Et bien sûr, la clé K est secrète entre A et B (et potentiellement le serveur).

Règles du jeu :

1. Le protocole doit être proposé en respectant la présentation type donnée en cours (pour Needham-Schroeder).
2. Il est interdit de proposer un protocole existant.
3. Le protocole devra être le moins "coûteux" possible pour la notion de coût définie ci-dessous. Le coût du protocole devra être précisé dans la description du protocole.
4. Plus votre protocole sera coûteux, plus vous partirez avec un malus élevé pour la deuxième partie du projet.
5. **Attention** : 20 points de malus par jour de retard (après le mercredi 7 octobre 2020).

Le coût d'un protocole P est défini comme la somme $f(P)$ des coûts de chaque message, dans une exécution normale du protocole. Étant donné un message $m = m_1, m_2, \dots, m_k$ (m_i ne commençant pas par une paire), le coût du message est la somme des $f(m_i)$ où f est définie récursivement :

$f(a)$	$=$	1	si a est un nom, une clef ou un nonce
$f(\{m\}_k^a)$	$=$	$1 + f(m) + f(k)$	chiffrement asymétrique
$f(h(m))$	$=$	$5 + f(m)$	hachage
$f(\{m\}_k^s)$	$=$	$10 + f(m) + f(k)$	chiffrement symétrique
$f(\langle m_1, m_2 \rangle)$	$=$	$50 + f(m_1) + f(m_2)$	paire

Note : les paires en tête des messages ne comptent pas. L'idée est qu'il est inutile de découper l'envoi d'un message en plusieurs envois, le coût reste identique. Seules les primitives mentionnées (chiffrement symétrique, chiffrement asymétrique avec clefs publiques, paire et hachage) pourront être utilisées. En particulier, la signature n'est pas autorisée.

Partie 2 (Attaques des protocoles)

À partir du **vendredi 9 octobre 2020**, il sera possible de commencer à attaquer les protocoles des autres groupes. Fin de la mise à jour des protocoles le **mercredi 4 novembre 2020** et fin des attaques le **vendredi 6 novembre 2020**.

Règles du jeu :

1. Chaque équipe part avec un score négatif correspondant au coût du protocole ($-f(P)$).
2. Si son protocole est attaqué, il faut proposer une nouvelle version.
Attention : au bout de 3 jours (ouvrés) sans correction, 20 points de malus par jour de délai.
3. Chaque première attaque trouvée sur un protocole (ou sa nouvelle version) rapporte 40 points à l'équipe qui l'a trouvée et l'équipe attaquée perd 40 points.
4. Si une nouvelle version est proposée, les anciennes versions ne peuvent plus être attaquées. Le malus est mis à jour avec le poids du nouveau protocole. L'ancien malus est oublié.
5. Comme pour les protocoles, les attaques devront être fournies sous la forme d'un fichier pdf, en respectant la présentation type donnée en cours (pour Needham-Schroeder). Le fichier décrivant une attaque sera envoyé au groupe attaqué avec copie aux responsables du cours (protocoles2020@inria.fr).
6. Pour être validée, une attaque devra être reconnue comme telle par le groupe attaqué. Mais la mauvaise foi n'est pas permise !
7. La feuille de score sera mémorisée à la fin de chaque semaine.
8. **Fin de championnat** : Plus aucun protocole ne sera accepté après mercredi 4 novembre pour laisser le temps aux autres équipes d'attaquer. **Attention** : si le dernier protocole proposé est attaqué, alors le malus retenu sera le poids du plus lourd protocole proposé par l'équipe au cours du championnat.

Jours ouvrés : tous les jours sauf week-end et les vacances du 26 au 30 octobre. Il est permis d'attaquer quand même !

Partie 3 (Analyse et modélisation en ProVerif)

Trois protocoles devront être modélisés et analysés à l'aide de l'outil ProVerif.

- au moins un des protocoles proposés par l'équipe
- au moins un protocole avec une attaque
- au moins un protocole sûr

Tous les protocoles modélisés et analysés devront être envoyés le **dimanche 15 novembre 2020** au plus tard, sous forme d'une archive comprenant tous les fichiers .pv des protocoles modélisés, avec une référence claire aux protocoles analysés (protocole-xy-v2.pv), ainsi qu'un fichier (un pour chaque fichier .pv) avec l'output obtenu par ProVerif (pour éviter les problèmes de version de ProVerif). Un grand soin devra être porté dans la modélisation des

protocoles et un maximum de propriétés devront être analysées. Pour chaque attaque trouvée par ProVerif, il faudra l'expliquer en la décrivant sous la forme d'un pdf comme pour les attaques trouvées en phase 2. Le cas échéant, il est possible de donner un pdf existant.

Notation : La note du projet **ne sera pas votre score dans le jeu**. Elle tiendra compte des aspects suivants :

- Implication dans le jeu.
- Modélisation en ProVerif
- Le jeu en lui-même rapporte des bonus sur la note finale du projet :
 - +2 points pour le groupe gagnant.
 - +1 point pour le groupe deuxième du jeu.
 - +1 point si 8 attaques ou plus ont été trouvées.