Comparaison de protocole d'accord de clé authentifié avec « forward secrecy »

Encadrant : Sébastien Canard, Télécom Paris, sebastien.canard@telecom-paris.fr

Description :

Un protocole d'accord de clé authentifié (AKA pour Authenticated Key Agreement) est une protocole permettant à des parties de mutuellement s'authentifier, tout en échangeant une clé cryptographique qui peut ensuite être utilisée pour protéger une grande quantité de données en confidentialité et en intégrité. C'est une mécanisme que nous utilisons quotidiennement, par exemple lorsque nous allons sur Internet ou quand nous utilisons nos téléphones mobiles. Il est habituellement demandé à ce genre de protocole d'assurer à la fois une authentification mutuelle (chaque partie authentifie l'autre), et le secret de la clé finalement partagée (seuls les deux protagonistes la connaisse).

Bien souvent, ces protocoles sont exécutés plusieurs fois entre les deux mêmes protagonistes. Nous parlons alors de sessions. Ainsi, une autre propriété de sécurité est parfois recherchée : celle de « forward secrecy », qui garantit que la divulgation future des clés secrètes « long terme » (qui sont conservées d'une session à une autre) ne compromet pas les clés de session échangées jusque-là.

Le projet va s'intéresser à deux protocoles d'accord de clé authentifié :
- le premier s'appuie sur des mécanismes de cryptographie à clé publique, et notamment le protocole Diffie-Hellman et un mécanisme de signature numérique. Il s'appelle Sigma, dont une variante correspond au protocole TLS1.2 utilisé sur Internet entre un navigateur et un serveur. Ce protocole a notamment été étudié dans l'article [DG21] ;
- le second s'appuie uniquement sur des mécanismes de cryptographie à clé secrète. Il s'appelle SAKE et a été décrit et étudié dans l'article [ACF20].

Objectifs :

L'objectif du projet consistera à faire la comparaison la plus exhaustive entre les deux protocoles Sigma et SAKE. Cette comparaison s'appuiera sur une implémentation réelle des deux systèmes et devra prendre en compte plusieurs critères à définir, tels que la complexité d'implémentation, les temps de réponse, la facilité de gestion des clés cryptographiques, etc.
Le projet devra en grande partie suivre les étapes suivantes :
1. lecture des deux articles (les preuves de sécurité pourront être passées dans un premier temps) ;
2. définition des critères de comparaisons ;
3. implémentation des deux protocoles ;
4. rédaction d'un document donnant les conclusions de comparaisons selon les critères définis à la seconde étape.

Références :

[DG21] Hannah Davis, Felix Günther: Tighter Proofs for the SIGMA and TLS 1.3 Key Exchange Protocols. ACNS (2) 2021: 448-479. Disponible : https://eprint.iacr.org/2020/1029.

[ACF20] Gildas Avoine, Sébastien Canard, Loïc Ferreira: Symmetric-Key Authenticated Key Exchange (SAKE) with Perfect Forward Secrecy. CT-RSA2020: 199-224. Disponible : https://eprint.iacr.org/2019/444.