Proposition de projet M2 Cybsersécurité IP Paris

Récupération confidentielle d'information avec vérification

Mots-clefs :
Private Information Retrieval (PIR), Stockage/recherche dans le nuage.

Laboratoire d'accueil : INRIA Saclay/LIX, équipe Grace

Encadrante: Françoise Levy-dit-Vehel (ENSTA-IP Paris & INRIA Saclay).

Description du sujet :

La problématique est celle d'un client souhaitant récupérer un enregistrement d'une base de données distante, répliquée ou distribuée sur plusieurs serveurs, sans révéler aux serveurs une quelconque information sur le numéro d'enregistrement. Cette problématique est connue sous le nom de "récupération confidentielle d'information", ou "Private Information Retrieval" (PIR).

A ISIT'2022, Ke et Zhang [1] ont proposé une nouvelle fonctionnalité pour un protocole de PIR : le client peut détecter une réponse incorrecte des serveurs. Cette fonctionnalité de PIR augmenté, appelé PIR-RV (PIR with result verification) constitue une relaxation de celle identifiant les serveurs malveillants, qui avait été proposée à ACNS 2014, mais est suffisante dans beaucoup de scenarii. Les auteurs introduisent dans [1] une construction de PIR-RV dans le cas de deux serveurs, basée sur un protocole de PIR de Woodruf et Yekhanin de 2005. Cette année, les mêmes auteurs ont proposé à ACNS 2023 [2] une généralisation de leur protocole, permettant de faire du PIR avec vérification pour $k \geq 2$ serveurs, avec l'hypothèse minimale qu'au moins un serveur est honnête.

Dans une phase préliminaire du projet, il s'agit de bien comprendre la fonctionnalité de PIR et les définitions de sécurité associées. Ensuite, l'étudiant mettra en oeuvre le protocole de PIR-RV à deux serveurs et évaluera ses performances, en termes de complexité de communication, coût de stockage, temps de calcul. En particulier, il appliquera ce protocole à la récupération confidentielle de clefs PGP pour diverses tailles de bases de données de clefs OpenPGP.

Dans une deuxième phase du projet, l'étudiant explorera un travail dû à Colombo et. al. en 2023 [3], introduisant la notion de PIR authentifié, notée ici Auth-PIR (avec une version multi-serveurs et une version à un serveur). Il s'agit d'un protocole à l'issue duquel le client est soit assuré de l'intégrité de l'enregistrement obtenu, soit détecte un comportement anormal d'un serveur et arrête le protocle avec l'assurance que le numéro de l'enregistrement voulu n'a pas été dévoilé. Il

comparera ensuite les protocoles PIR-RV et Auth-PIR, notamment en termes de garanties de securité, de complexités de communication et de fonctionnalités offertes.
Dans le cas de deux serveurs, il rapprochera les performances de PIR-RV obtenues lors de la première phase du projet à celles de Auth-PIR (décrites dans [3]), pour l'application à la base de données de clefs OpenPGP.

Un dernier volet du projet consistera en l'étude de la généralisation à k serveurs du protocole PIR-RV de Ke et Zhang, parue cette année [2]. Si le temps le permet, d'autres variantes de PIR pourront être abordées (multi-query PIR notamment).

Bibliographie :

[1] Pengzhen Ke, Liang Feng Zhang : Two-Server Private Information Retrieval with Result Verification. ISIT 2022.
[2] Pengzhen Ke, Liang Feng Zhang : Private Information Retrieval with Result Verification for more servers. ACNS 2023.
[3] Simone Colombo, Kirill Nikitin, Henry Corrigan-Gibbs, David J. Wu, Brian Ford : Authenticated Private Information Retrieval. USENIX 2023.

Livrables :
Rapport présentant la problématique du PIR, ses modèles de sécurité, et les fonctionnalités additionnelles proposées dans [1] et [3].
Mise en œuvre du protocole décrit dans [1] et comparaison avec [3].