Envelope encryption et application au stockage dans le cloud et à la messagerie sécurisée

Mathieu Rambaud (TP)

L'envelope encryption est une technique utilisée par la plupart des clouds (AWS, Google, Azure) pour crypter les fichiers au repos, et chacun avec une clé distincte, afin de minimiser les conséquences en cas de récupération d'une clé par l'adversaire.

Pour minimiser le coût de stockage des clés (5$/mois dans un hardware sécurisé), les clés sont elles-mêmes cryptées à l'aide d'une master key. Cette master key est la seule qui reste dans un hardware sécurisé .

La partie implémentation du projet pourra consister à faire sa propre envelope encryption (à partir de openssl), par exemple pour l'intégrer à un client de stockage sur AWS (soit S3, soit DynamoDB) ou Google cloud ou Azure, possiblement en utilisant un hardware sécurisé à bas coût.

Ce travail pourra se faire avec deux stagiaires de M2 (de Versailles) jusqu'à fin novembre.

La partie bibliographique pourra consister au choix - à étudier la documentation du "client side encryption avec external key store" de l'un des clouds AWS/Google/Azure, et l'appliquer, pour pouvoir comprendre le fonctionnement en pratique et le présenter - à étudier un ou ces deux articles: https://eprint.iacr.org/2025/1512 (attaque sur le envelope key encryption de la messagerie sécurisée de Doctolib) et https://eprint.iacr.org/2023/1727 (comment faire de l'envelope encryption avec une master key symétrique).