Sujet de stage

Intitulé du stage

Analyse et optimisation du contrôle d'accès cryptographique dans des environnements multi-domaines

Contexte

Le chiffrement par contrôle d'accès (ACE pour Access Control Encryption en anglais) est un nouveau paradigme qui permet un contrôle d'accès à grain fin avec une mise en œuvre cryptographique, en donnant des droits à des utilisateurs pour les messages qu'ils sont autorisés à lire (donc déchiffrer), mais aussi ceux qu'ils sont autorisés à écrire (donc chiffrer).

Pour contrôler les flux d'informations au sein d'un même système ou entre des systèmes appartenant à différents domaines de sécurité, la cryptographie classique et des schémas de chiffrement plus évolués (tels que les schémas de chiffrement basés sur les attributs [2] ou les schémas de chiffrement par prédicat [3]) ne suffisent pas. Ils permettent d'appliquer un contrôle d'accès sur les autorisations en lecture mais un expéditeur malveillant peut toujours diffuser des messages sensibles en clair. En outre, il est tout aussi important de contrôler qui peut écrire à qui.

Le chiffrement ACE tel qu'introduit par Damgård *et al.* [1] résoud ce problème en introduisant une partie supplémentaire, l'assainisseur (*sanitizer* en anglais). Tout message communiqué entre un expéditeur et un destinataire doit passer par cet assainisseur qui applique un certain traitement au message avant de le diffuser au destinataire. De cette façon, les schémas ACE empêchent un écrivain d'envoyer des messages à des personnes avec lesquelles il n'est pas autorisé à communiquer.

Deux schémas récents, basés sur cette approche, seront étudiés au cours de ce stage :

- **Cross-Domain Access Control Encryption (CD-ACE)** : Proposé par Wang et Chow[5], ce schéma permet de gérer des politiques d'accès complexes avec des chiffrés de taille constante. Il se distingue par sa capacité à fonctionner dans des *environnements multi-domaines*, où les clés sont gérées par des autorités séparées (*sender authority* et *receiver authority*). Ce schéma utilise des signatures préservant la structure et des preuves à zero-knowledge, permettant une gestion efficace des droits d'accès sans compromettre l'anonymat des utilisateurs.
- **Cross-Domain Attribute-Based Access Control Encryption (CD-ABACE)** : Introduit par Sedaghat et Preneel[4], ce schéma étend l'ACE en utilisant des *politiques basées sur les attributs* des utilisateurs plutôt que sur des identités fixes. Cela permet une gestion plus fine des droits d'accès, adaptée à des environnements multi-domaines complexes, tout en maintenant une taille constante des chiffrés et des clés, indépendamment du nombre de destinataires ou d'attributs. Le CD-ABACE permet ainsi d'implémenter des politiques d'accès plus expressives, mais laisse des questions ouvertes sur la préservation complète de l'anonymat et la gestion des attributs dans des politiques complexes.

Objectifs

Ce stage vise à explorer les deux schémas de chiffrement ACE et CD-ABACE, et à identifier des améliorations pour rendre ces schémas plus efficaces, sécurisés et adaptés à des environnements réels multi-domaines.

Tâches proposées

1. **Revue de la littérature** : Comprendre en profondeur les schémas ACE et CD-ABACE, en étudiant leurs forces et faiblesses dans des environnements inter-domaines.
2. **Implémentation des schémas** : Développement d'un prototype pour les deux schémas à l'aide de bibliothèques cryptographiques modernes, et évaluation des performances (temps de calcul, taille des chiffrés, etc.).
3. **Analyse comparative** : Comparer les performances des deux schémas dans différents scénarios d'application, comme la gestion de grands nombres d'utilisateurs ou d'attributs.
4. **Optimisation** : Proposer des améliorations aux schémas existants, notamment pour renforcer leur *résilience aux fuites* et améliorer la gestion des politiques d'accès et des clés dans des environnements complexes.
5. **Étude de la sécurité et de l'anonymat** : Explorer des moyens d'améliorer l'anonymat des utilisateurs et de garantir la sécurité même en cas de compromission partielle du système.

Résultats attendus

— Une comparaison détaillée des performances des deux schémas dans divers contextes d'application.
— Des propositions d'amélioration concernant la résilience aux fuites, la gestion des politiques d'accès et l'anonymat.
— Un prototype optimisé démontrant la faisabilité de ces schémas dans des environnements réels.

Poursuite en thèse

En fonction des résultats obtenus durant le stage, une **proposition de thèse** pourra être envisagée, portant sur l'amélioration des systèmes ACE dans des applications à grande échelle. Cette thèse pourrait approfondir la résilience aux fuites, la gestion des politiques d'accès dynamiques et l'anonymat.

Profil recherché

— Étudiant en Master 2 ou école d'ingénieurs, avec des compétences en cryptographie et cybersécurité.
— Bon niveau de programmation.
— Bon niveau d'anglais.

Modalités

Dates : Le stage est prévu pour se dérouler de février-mars 2025 à août-septembre 2025, mais n'hésitez pas à nous contacter si vous souhaitez le démarrer plus tôt. Les candidatures seront traitées au fil de l'eau : nous vous encourageons à candidater le plus tôt possible.

Équipe d'encadrement :

Clara Bertolissi (clara.bertolissi@univ-amu.fr)

Alexis Bonnecaze (alexis.bonnecaze@univ-amu.fr)

Kevin Thiry-Atighehchi (kevin.atighehchi@uca.fr)

Gratification : La gratification prévue est a priori la gratification minimale d'un stage en France (soit 4.35 euros par heure).

Pour candidater : Envoyez un email aux trois encadrants (cf email ci-dessus) avec une lettre de motivation, un CV, votre relevé de notes de M1 ou équivalent, et les éléments dont vous disposez pour votre M2 ou équivalent.

Références

[1] Ivan Damgård, Helene Haagh, and Claudio Orlandi. Access control encryption : Enforcing information flow with cryptography. In *Theory of Cryptography Conference*, pages 547–576. Springer, 2016.

[2] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM conference on Computer and communications security*, pages 89–98, 2006.

[3] Jonathan Katz, Amit Sahai, and Brent Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In *Advances in Cryptology–EUROCRYPT 2008 : 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings 27*, pages 146–162. Springer, 2008.

[4] Mahdi Sedaghat and Bart Preneel. Cross-domain attribute-based access control encryption. In *International Conference on Cryptology and Network Security*, pages 3–23. Springer, 2021.

[5] Xiuhua Wang and Sherman SM Chow. Cross-domain access control encryption : Arbitrary-policy, constant-size, efficient. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 748–761. IEEE, 2021.