TP Chiffrement Basé Attributs (ABE) pour l'automobile connectée

Documentation

Légende : l → lien, p → papier.

l1 Reliable Efficient LIbrary for Cryptography (RELIC) ,
https://github.com/relic-toolkit/relic

l2 Open ABE library by 'the' Brent Waters
https://github.com/zeutro/openabe

l3 Open ABE déjà tout compilé
https://lelien

p1 Survey on ABE schemes
Zhi Qiao, Shuwen Liang, Spencer Davis, and Hai Jiang. Survey of attribute based encryption.15th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), pages 1–6, 2014.

p2 Praveen Kumar P., Syam Kumar P., and Alphonse P.J.A. Attribute based encryption in cloud computing: A survey, gap analysis, and future directions. Journal of Network and Computer Applications, 108:37–52, 2018.

Choix du chiffrement

Objectifs

Dans ce TP l'objectif est de concevoir et utiliser des solutions cryptographiques pour un problème concret. Le travail est prévu pour ressembler le plus possible à des décisions qu'ont à prendre des responsables crypto dans l'indstrie.

Les voitures connectées, comme leur nom l'indique, sont en connexion quasi-permanante avec de multiples utilisateurs de leur données. Ces communications permettent le retour d'informations (itinéraires, circulation, météo) basé sur les informations fournies. Ces entreprises et les institutions (police, assurances ...) qui utilisent ces données ne peuvent pas chacun établir une connexion avec la voiture (explosion de la bande passante). Pour résoudre ce probleme, on impose que les voitures n'aient qu'un seul interlocuteur pour les informations montantes : un stockage cloud.

Il suffit donc aux consommateurs de données de venire réclammer celles-ci auprès du cloud, sans nouvelle connexion avec la voiture. On supposera que les utilisateurs de donnée et le cloud ont des capacités de calcul et de stockage très élevées. Il reste donc au calculateur embarqué dans la voiture la charge de chiffrer les données, afin de pouvoir spécifier qui sont les utilisateurs ayant le droit de déchiffrer celles-ci.
On demande spécifiquement que le contrôle d'accès puisse se faire de façon simple et instinctive par le conducteur, qui peut la modifier à tout moment.

Question 1

Dans ce contexte, quel chiffrement par attributs semble le plus adapté ? Key-Policy ou Ciphertext-Policy ?

Question 2

Il existe de très nombreuses versions de cet ABE. Choisissez en fonction des complexités le schéma ABE correspondant le mieux au problème. (Ce genre do données se trouve compilée dans des papiers 'surveys' [p1] qui se chargent pour vous de résumer les points clefs de dizaines de schémas) On note att le nombre d'attributs positionnés, $|U|$ le nombre total d'attributs, l le nombre de feuilles de l'arbre d'accès (lignes de la LSSS). On ignore le paramètre de sécurité.

	Setup	Keygen	Encrypt	Decrypt	|PK|	|SK|	|CT|
Schéma 1	$O(\|U\|)$	$O(l)$	$O(att)$	$O(1)$	$O(\|U\|)$	$O(l)$	$O(att)$
Schéma 2	$O(1)$	$O(l^2\|U\|)$	$O(1)$	$O(att \times l)$	$O(1)$	$O(\|U\|)$	$O(\|U\|)$
Schéma 3	$O(\|U\|)$	$O(\|U\|)$	$O(\|U\|)$	$O(l)$	$O(1)$	$O(l)$	$O(att)$
Schéma 4	$O(\|U\|^2)$	$O(l\|U\|)$	$O(att)$	$O(att \times l)$	$O(1)$	$O(\|U\|)$	$O(att)$

Design a partir d'un cahier des charges

Objectifs

Liste des utilisateurs de données :

- Institutions : Assurance, Police, Justice
- Constructeur / équipementiers
- Employeur / propriétaire du véhicule
- Services Ext.

Cahier des charges :

- Si un attribut spécifie un destinataire, celui-ci est en capacité de déchiffrer.
- Toutes les données sont chiffrées avec au moins un attribut correspondant à son type, et un pour la date. Les differents types peuvent être :
  - Etat du moteur
  - Vitesse
  - GPS
  - Temperature
  - Poids
  - Charge de la batterie (vehicules elec.)
- On suppose la voiture équipée d'un détecteur de panne et d'accident. Lorsque ceux-ci sont activés, chiffrer avec l'attribut *panne* ou *accident* correspondant est obligatoire.
- Si il y a une panne, l'assurance doit avoir accès à l'état du moteur et de la batterie.
- Si il y a un accident, l'assurance doit avoir accès à la vitesse et aux données GPS.
- Si la vitesse dépasse 150kmh, la police doit avoir accès a celle-ci.

- En cas d'accident, la police à accès à toutes les données.
- Les données moteur et batterie doivent toujours être accessible à leur constructeur.
- L'employeur (propriétaire du véhicule dans des cas de taxi ou de fret) à accès aux données GPS, de batterie et de poids, uniquement dans les plages horaires rémunérées du conducteur.
- L'employeur ne peut pas avoir de données, meme si elles lui sont spécifiquement destinnées hors de ces plages horaires.
- L'utilisateur doit pouvoir élargir l'ensemble des destinataires. Il spécifiera donc des attributs supplémentaires ciblant des services extérieurs en echange des services proposés.

Question 3

Pour chacun des utilisateurs de données, déterminez l'arbre d'accès de leur clef secrète.

Implementation sur OpenABE

Objectifs

OpenABE est une librairie créée par des chercheurs majeurs dans le domaine du chiffrement par attributs.

Celle-ci propose un des ABE ayant le plus d'expressivité possible. Le schéma propose une gestion des attributs par seuils (les attributs peuvent avoir la forme : $Age > 18$). Cela permet d'avoir des attributs qui sont des timestamps et donc de créer des clefs limitées dans le temps. Ce méchanisme de peremption (decay) des clefs permet de mettre en place de la *révocation* de clefs si nécessaire.

De plus, l'univers des attributs est infini. Pour obtenir la valeur liée a un attribut (att_i^+ dans le cours), un utilisateur souhaitant chiffrer n'a qu'a hacher la chaine de caractères correspondant au nom de l'attribut. Ainsi, la clef publique est courte

De plus les performances élevées sont conséquence de la librairie sous-jacente RELIC qui implémente les calculs sur les courbes elliptiques les plus rapides de l'état de l'art. La performance du tout est équivalente à RSA sur des chiffrements avec peu d'attributs.

Question 4

Téléchargez la version Pré-Compilée de OpenABE. Créez un script permettant de vérifier que les messages envoyés dans les cas suivants sont bien accessibles que par les bonnes personnes, En respectant bien entendu le cahier des charges établi précédemment.

- Un conducteur de taxi se déplaçant normalement pendant ses horaires de travail.
- Un conducteur propriétaire de sa voiture qui partage les données de température a *weather.io*, les données GPS a *Mapping* et *Gmaps*, et la charge de sa batterie a *zapp.com*
- Un conducteur roulant a 160 kmh à 3h du matin, alors qu'une panne moteur lui cause un accident.

⋆ *Question 5*

Le méchanisme de révocation de clefs par expiration permet de donner des clefs permettant de *tout* déchiffrer pour un temps donné. Implémentez une telle clef, donnée a la justice permettant de lire toutes les données du dernier véhicule de 2h a 4h du matin.