Une politique de contrôle d'accès à grains fins aux données pour les systèmes de transport intelligents

Rémi Adelin, Eric Alata, Vincent Migliore, Vincent Nicomette

Une politique de contrôle d'accès à grains fins aux données pour les systèmes de transport intelligents

Rémi Adelin, Éric Alata, Vincent Migliore, Vincent Nicomette
LAAS-CNRS, Université de Toulouse, CNRS, Toulouse, France
{prénom}.{nom}@laas.fr

***Abstract*—Le développement des systèmes de transport intelligents entraîne de nombreux échanges de données entre des acteurs aux desseins différents. Les conducteurs sont en général très peu au fait des destinataires et du devenir de leurs données. Un enjeu primordial est donc de rétablir le contrôle des conducteurs sur leurs données. Cet article présente une solution basée sur une politique fine de contrôle d'accès aux données qui repose sur l'usage du chiffrement par attributs.**

I. Introduction

Les véhicules sont aujourd'hui indissociables de nos activités quotidiennes. Le nombre de voitures immatriculées chaque année ne cesse d'ailleurs d'augmenter [1], [2]. Ces véhicules sont dotés d'une multitude de capteurs, actionneurs et calculateurs qui permettent d'améliorer la conduite et le confort de l'utilisateur au travers de multiples services. Le passager peut ainsi visionner des films ou exécuter des applications téléchargées d'un catalogue.

D'autres services vont au-delà des besoins du conducteur et peuvent intéresser d'autres acteurs. Par exemple, un capteur de température est bien sûr utile au conducteur mais il fournit également une donnée qui peut être utilisée en entrée de modèles de prévisions météorologiques. Le véhicule peut ainsi se transformer en sonde météorologique mobile que peut exploiter un service météorologique, sans avoir à la déployer elle-même. La géolocalisation du conducteur, utilisée pour le guider dans son trajet, permet d'avoir une vision plus fine du trafic global pour ainsi aider les autres conducteurs à mieux se positionner dans la circulation. Ainsi, la confrontation des données issues de plusieurs véhicules est devenue indispensable pour fournir des services. Ces données doivent donc être stockées et accessibles par les constructeurs et équipementiers pour pouvoir appliquer des traitements. Le choix de stockage est aujourd'hui principalement le Cloud.

Comme l'ajout de connectivité dans les véhicules permet la mise en place de services à destination du constructeur, des équipementiers ou autres organismes, le conducteur n'est plus le destinataire du résultat de certains traitements des données issues des capteurs de son propre véhicule. Par exemple, un capteur sonore peut permettre d'identifier l'état de la chaussée pour ainsi avertir les services d'entretien des tronçons à remettre à neuf en priorité. Dans un tout autre contexte, la collecte des données entraîne la constitution d'une boîte noire, qui peut s'avérer intéressante dans le cas d'un accident survenu à proximité du véhicule du conducteur, pour déterminer les responsabilités. Encore faut-il que les organismes d'assurance ou étatiques n'en abusent pas.

Au centre des véhicules connectés se situent donc les données collectées et les différents acteurs qui cherchent à en dégager de la valeur. Or un conducteur peut estimer que ses données peuvent relever de la vie privée, et il peut être en droit de choisir si ses données sont transmises et à qui. Malgré tout, certaines situations exceptionnelles peuvent nécessiter que des données considérées privées par le conducteur doivent être transmises à un organisme précis. Aujourd'hui, la réglementation joue en faveur du conducteur et un cadre juridique est en cours d'instanciation [3]. Toutefois, il existe un fossé entre un texte juridique et une réalisation technique. De plus, les solutions actuelles ne mettent pas le conducteur dans la boucle.

Il est donc nécessaire d'identifier des mécanismes de protection qui doivent tenir compte des contraintes suivantes : 1) stockage des données dans le Cloud sachant que le fournisseur Cloud ne doit pas pouvoir accéder aux données en clair ; 2) possibilité pour le conducteur d'associer des droits d'accès au cas par cas, à chaque acteur ou groupe d'acteurs ; 3) la gestion de situation exceptionnelle, permettant à un acteur précis (i.e., organisme *assermenté*) d'outrepasser ces restrictions, temporairement. Dans ce contexte, le chiffrement est une piste incontournable et le chiffrement par attributs possède selon nous les propriétés adaptées à la mise en place d'une telle politique. Ainsi, cet article propose une politique de contrôle d'accès aux données collectées, qui se veut dynamique, à grains fins, basée sur le chiffrement par attributs.

La section suivante présente plus en détail les différents acteurs concernés. Dans la section III, la proposition de cet article est positionnée par rapport à l'état de l'art. La section IV présente le chiffrement par attributs et la description de notre proposition et la section V conclut avec les pistes envisagées et les verrous à lever.

II. Acteurs

De la chaîne de production à l'usage, un véhicule connecté implique plusieurs acteurs différents.

Le **conducteur** est la première personne concernée par la production de données. Son trajet et ses habitudes sont révélateurs de nombreux aspects de son comportement. Par exemple, la vitesse de son véhicule peut être utilisée pour identifier d'éventuels délits et ses arrêts peuvent révéler ses lieux

de prédilection. Il est important de préserver sa souveraineté sur ses données personnelles, dans la mesure du possible.

Le **constructeur** fabrique et vend ou loue le véhicule au conducteur mais profite également des remontées de données pour mieux gérer son parc automobile. Il est aussi susceptible de valoriser ces données en les proposant à divers organismes. Certaines données sont par contre indispensables pour lui permettre de mener des études sur le bon fonctionnement des véhicules.

Les **équipementiers** ont en charge la conception d'un ou plusieurs systèmes embarqués dans le véhicule. Ils peuvent collecter des données au travers de leurs systèmes. L'accès aux données par ce type de société est moins évident aux yeux du conducteur. À l'instar du constructeur, ils peuvent avoir besoin de données pour étudier le bon fonctionnement de leurs systèmes.

Étant donné la quantité de données à stocker, un dépôt dans le Cloud est indispensable. Un **fournisseur Cloud** est donc également un acteur à considérer. Son rôle doit à priori se cantonner au stockage voire au traitement des données. Toutefois, la curiosité peut éventuellement l'amener à consulter les données à l'insu des conducteurs.

Les **partenaires commerciaux** constituent les acteurs auprès desquels la valorisation des données prend son sens. Par exemple, une société spécialisée en météorologie peut souhaiter disposer des remontées des capteurs de température et un cabinet d'étude de marché peut s'intéresser aux différents relevés de géolocalisation pour identifier un emplacement commercial idéal. Ils sont donc à priori consommateurs de données. Un conducteur doit pouvoir accepter qu'une certaine catégorie de partenaires commerciaux aient accès à certaines de ses données tout en refusant l'accès à d'autres.

Une **société d'assurance** peut être intéressée par l'accès à certaines données en cas d'accident notamment. Cependant, un conducteur doit pouvoir refuser de lui envoyer des données de façon continue de crainte que leur traitement serve à ajuster son contrat. La société ne doit donc avoir accès aux données qu'en cas d'accrochage ou autres accidents, et uniquement aux données émises dans une fenêtre temporelle précise.

Les mécanismes de protection que nous proposons dans cet article doit nécessairement prendre en compte l'ensemble de ces acteurs et l'attribution de droits d'accès adaptés. Avant de présenter cette proposition, nous présentons un bref état de l'art dans la section suivante.

III. État de l'art

L'European Telecommunications Standards Institute (ETSI) a standardisé l'architecture et la gestion de la sécurité afin de sécuriser les communications dans les systèmes de transport intelligents [4], [5]. Ces standards imposent l'usage de certificats qui étendent les certificats usuels avec l'ajout d'informations spécifiant les types de messages qu'un véhicule peut envoyer et les permissions associées qui tiennent compte des positions géographiques et de l'heure. Chaque véhicule se voit attribuer un certificat et l'utilise pour signer les messages envoyés. L'entité qui reçoit le message doit consulter le certificat pour savoir si le contenu du message est valide. Cependant cette approche n'empêche nullement les acteurs curieux de consulter le message lui-même.

D'autres travaux utilisent une blockchain [6], [7], pour garantir l'intégrité et la disponibilité des données. Renault expérimente l'utilisation d'une blockchain afin de stocker le carnet d'entretien du véhicule et maintenir son intégrité [8]. Cependant, dans ces projets, le conducteur n'a aucun contrôle sur les données alors que le constructeur voire les équipementiers ont un droit de regard sur ces données.

Dans tous les cas, la cryptographie est un mécanisme indispensable à la réalisation d'une politique fine de contrôle d'accès. Les approches usuelles, basées sur les infrastructures à clé publique, sont construites pour sécuriser l'échange vers un unique interlocuteur. Or les services Cloud associés aux véhicules connectés sont fondamentalement multi-prestataires, en opposition aux mécanismes classiques point-à-point. Il en résulte une explosion du nombre de clés et certificats à gérer, complexifiant d'autant plus la mise en place de ces services. Un premier élément de réponse à cette problématique est le chiffrement de groupe [9], dans lequel un schéma de groupe associe à une clé publique un ensemble de clés privées. Toutefois, ce schéma ne prend pas aisément en compte la dynamicité, i.e., l'arrivée de nouveaux interlocuteurs dans un groupe, et impose la création d'autant de groupes que d'acteurs et le conducteur doit chiffrer éventuellement une donnée pour plusieurs groupes. Une solution qui nous semble plus pertinente est le chiffrement par attributs [10], ce schéma possède les propriétés nécessaires à la réalisation d'une politique fine de contrôle d'accès aux données. La section suivante est dédiée à cette solution.

IV. Politique de contrôle d'accès à grains fins

A. Objectifs

La politique que nous proposons doit tenir compte des différents acteurs, du type des données, de la date de génération des données ainsi que du lieu et du contexte. À la différence des politiques usuelles définies par l'administrateur du système, la définition de la politique doit se faire conjointement avec le conducteur. Le conducteur peut décider de sacrifier une partie de sa vie privée au profit d'un service supplémentaire. Cela doit être fait volontairement et réalisé en toute conscience. Le choix de restreindre l'accès à une donnée par un conducteur peut être discuté par les autres acteurs, comme par exemple la consigne de température de l'habitacle qui, pourtant à priori ne révèle pas d'information à caractère personnel. Dans tous les cas, le conducteur doit pouvoir faire un choix et ce choix doit être respecté sans être remis en cause.

B. Modèle d'adversaire

L'adversaire que nous considérons possède un profil curieux, il peut être extérieur au système ou être un acteur du système et chercher à accéder à des données pour lesquelles il n'a aucun droit. Si l'adversaire est extérieur, il ne doit avoir accès à aucune donnée, si c'est un acteur, il a accès

uniquement aux données consenties par la politique. Dans le cadre de ce travail, nous considérons que cet adversaire est passif et ne fait que lire le contenu du cloud.

C. Chiffrement par attributs

Le chiffrement par attributs est un schéma de chiffrement asymétrique permettant d'associer aux données chiffrées une politique de contrôle d'accès. L'intérêt majeur de ce schéma est que l'on peut faire varier la politique de contrôle d'accès, autrement dit, le nombre d'acteurs capables de déchiffrer le message, sans avoir à générer de nouvelles clés de sécurité. Dans la pratique, chaque acteur se voit attribuer une clé privée avec un jeu d'attributs associés. Lors du chiffrement d'une donnée avec l'unique clé publique, l'émetteur crée une politique de contrôle d'accès qui est fonction des attributs. Un récepteur peut alors déchiffrer la donnée uniquement si les attributs contenus dans sa clé sont compatibles avec la politique de contrôle d'accès associée à la donnée. L'utilisateur est alors capable de définir la portée de sa donnée, en associant une politique restrictive pour des données sensibles, et plus souples pour des données plus communes. Une **autorité de confiance**, disposant d'une clé dite maître, est responsable de l'attribution des attributs à chaque acteur. Il existe également une autre construction, fonctionnant inversement, dans laquelle des attributs sont chiffrés dans les messages et une formule de contrôle d'accès est chiffrée dans la clé.

Dans le contexte des véhicules connectés, le chiffrement par attributs permet, avec un jeu limité de clés de sécurité, de gérer l'évolution dynamique des acteurs, tout en permettant à l'utilisateur d'avoir une vraie maîtrise de la portée des données qu'il chiffre. De plus, contrairement aux solutions usuelles de contrôle d'accès demandant une autorisation préalable d'accès à la donnée, le chiffrement par attributs permet de s'affranchir de cette étape réduisant d'autant le nombre d'échanges nécessaires au niveau des protocoles. Enfin, lors d'une situation exceptionnelle, l'autorité de confiance permet à un acteur légal précis, d'outrepasser temporairement ces restrictions. Elle pourra accorder temporairement plus de droits à l'acteur afin qu'il puisse déchiffrer certaines données qu'il ne pouvait pas déchiffrer initialement.

L'élaboration de la politique de contrôle d'accès nécessite donc la définition d'acteurs, de règles, et d'une autorité de confiance. Les acteurs devront être authentifiés et posséder des attributs chiffrés dans leur clé. La spécification des règles de la politique se fera en fonction des acteurs mais également en fonction de la nature des données. Il doit être possible d'accorder l'accès aux données en fonction de certaines caractéristiques des données elles-mêmes, pour cela, il est nécessaire de les typer. On peut par exemple envisager les caractéristiques suivantes :

- le niveau de criticité associé à la donnée (par exemple, message de défaillance d'un calculateur et durée de réaction de l'airbag qui sont critiques, etc.);
- l'origine de la donnée (capteur mécanique : moteur, boîte de vitesse, freins, etc.; capteur environnemental : caméra, localisation, température, etc.);
- la capacité d'inférence à partir de la donnée;
- le type de remontée : obligatoire ou facultative;
- l'ensemble minimal des acteurs qui doivent y avoir accès.

Le rôle de typer les données revient à l'autorité de confiance et ce travail sort du périmètre de cet article. L'autorité de confiance a également une portée d'ordre juridique, elle sera la garante de la bonne attribution des rôles et de la classification des données en fonction de leur niveau.

V. Perspectives

Dans cet article nous avons présenté le problème de la perte du contrôle des données des conducteurs dans une situation de communication entre un véhicule connecté et un Cloud. Nous avons proposé une politique fine de contrôle d'accès aux données respectueuse de la vie privée basée sur le chiffrement par attributs afin de répondre à ce problème.

L'utilisation du chiffrement par attributs nécessite d'étudier sa mise en pratique. Il est important de s'assurer que ce schéma n'entraîne pas un coût trop important en temps de calcul lors des opérations de chiffrement et déchiffrement ainsi qu'une augmentation trop importante des besoins en stockage et en réseau. Par ailleurs, l'utilisation de clés entraîne le besoin d'un mécanisme de révocation des clés, ce mécanisme sera également à l'étude dans nos travaux futurs.

References

[1] "Immatriculations de voitures particulières neuves en novembre 2018", Ministère de la transition écologique et solidaire, Commissariat général au Développement durable, Observation et statistiques, http://www.statistiques.developpement-durable.gouv.fr/publicationweb/149, Dernier accès : 21 janvier 2019.

[2] Recherche de véhicules dans les bases de l'INSEE, Institut national de la statistique et des études économiques, https://www.insee.fr/fr/recherche/recherche-statistiques?q=v%C3%A9hicules, Dernier accès : 21 janvier 2019.

[3] "Règlement général sur la protection des données du 27 avril 2016", Journal officiel de l'Union européenne, https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR, Dernier accès : 28 janvier 2019.

[4] "ITS communications security architecture and security management", European Telecommunications Standards Institute, 2018, https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.03.01_60/ts_102940v010301p.pdf, Dernier accès : 28 janvier 2019.

[5] "Security Services and Architecture", European Telecommunications Standards Institute, 2010, https://www.etsi.org/deliver/etsi_ts/102700_102799/102731/01.01.01_60/ts_102731v010101p.pdf, Dernier accès : 28 janvier 2019.

[6] E. Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri and V. Sassone, "Blockchain-based database to ensure data integrity in cloud computing environments", 2017.

[7] I. Zikratov, A. Kuzmin, V. Akimenko, V. Niculichev, and L. Yalansky, "Ensuring data integrity using Blockchain technology", In Open Innovations Association (FRUCT), 2017 20th Conference of IEEE (pp. 534-539).

[8] Jamal El Hassani, "La blockchain, le secret de Renault et PSA contre la fraude automobile", 2017, https://www.journaldunet.com/economie/automobile/1204234-blockchain-renault-psa-fraude-automobile/, Dernier accès : 30 janvier 2019.

[9] A. Kiayias, Y. Tsiounis and M. Yung, "Group encryption", In International Conference on the Theory and Application of Cryptology and Information Security (pp. 181-199), Springer, Berlin, Heidelberg, December 2007.

[10] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data", In Proceedings of the 13th ACM conference on Computer and communications security (pp. 89-98), October 2006.