Proposition d'un sujet de thèse dans l'axe2 de la chaire C3S

Partage et traitement distribué de données privées de voitures connectées

Directeurs de thèse : Duong Hieu Phan, Houda Labiod (Télécom Paris)
Co-encadrant : Aurélien Dupin (Thalès)

Chaire C3S, https://chairec3s.wp.imt.fr/

1. Contexte et motivation

Les véhicules connectés autonomes feront partie de systèmes de transport intelligents coopératifs qui dépendront d'une grande masse de données provenant de nombreuses sources. Par exemple, les véhicules autonomes seront connectés à différentes unités de contrôle de la circulation, qui leur permettront d'ajuster leur vitesse en fonction des feux de circulation et de trouver l'itinéraire le moins congestionné. En plus du confort offert aux conducteurs, le système pourra optimiser les flux du trafic sur les routes ainsi qu'aux intersections diminuant ainsi la pollution et les accidents. Le véhicule connecté autonome de demain sera doté d'un système de perception coopératif très sophistiqué capable de faire de la fusion de données provenant de plusieurs sources internes et externes (capteurs embarqués, caméras, communications V2X,…).
La sécurisation de l'échange de ces données est primordiale y compris les données à caractère personnel (position du véhicule, position de la destination, …). Les passagers d'une voiture autonome peuvent ne pas vouloir révéler leurs escales ou leur destination à d'autres parties. Par conséquent, l'enjeu est de faire des manipulations de ces données privées, tout en évitant toute fuite ou divulgation d'informations.

Le « calcul multipartites » (MPC) sécurisé est un type de protocoles cryptographiques qui permettent à un ensemble de parties de calculer une fonction de chacune de leurs entrées individuelles, sans qu'elles aient à révéler leur entrée. Le calcul MPC sécurisé prend également en compte le fait que des adversaires peuvent tenter d'attaquer ces protocoles. Ces adversaires peuvent être honnêtes mais curieux, ou même actifs. Il serait intéressant d'explorer l'utilisation de cette approche dans le cadre du véhicule connecté autonome pour créer des protocoles préservant la privacy et l'intégrité, et assurer des communications sécurisées dans un contexte fortement distribué.

D'un côté, le MPC est aujourd'hui à maturité. Voir par exemple l'article [2] pour une application au partage anonyme de voitures (ou les travaux de Matthieu Rambaud [CRX19; KMR19]). Il existe même des implémentations open source qui fonctionnent pour un grand nombre de parties.

D'un autre côté, dans le contexte de la voiture connectée, nous devrons définir de nouvelles notions de sécurité plus fortes car les informations des utilisateurs sont non seulement stockées dans des bases de données, mais aussi utilisées dans de nombreuses applications. Ensuite, pour déployer le MPC en situation réelle, des sujets importants tels que la complexité en temps réel des complications et des calculs doivent être pris en compte.

2. Objectifs

Le premier objectif de cette thèse est d'acquérir une compréhension très pointue du paradigme MPC sécurisé et de maitriser les méthodes associées. Le deuxième objectif est d'exploiter ces connaissances pour créer des protocoles MPC sécurisés pour effectuer divers calculs sur des données privées d'un véhicule connecté autonome et d'évaluer les performances de cette approche vis-à-vis de l'existant basé sur les standards de sécurité ETSI, IEEE et ISO.
Nous appliquerons cette approche dans deux cas d'usage identifiés pour atteindre les objectifs suivants:

- Sécurité et vitesse des communications intra-véhicule et/ou avec l'extérieur

Nous considèrerons un cas d'usage qui fait appel à des communications intra-véhiculaire et/ou extra-véhiculaire V2X (V2V, V2I, V2Cloud, V2server). L'enjeu est de définir des solutions de cryptographie adaptées en prenant en compte les ressources limitées du véhicule connecté autonome. On pourra notamment réfléchir à des solutions qui optimisent la performance en temps réel, au prix de calculs et d'échanges préliminaires "hors ligne". Les travaux effectués sur ce volet pourront interagir avec les travaux effectués au sein de l'axe2.

- Partage et traitement anonyme de l'information en temps réel et de façon distribuée

Dans l'axe 4, on souhaite détecter des comportements anormaux, possiblement sur l'ensemble du réseau de voitures et en temps réel (par exemple pour détecter une cyberattaque, ou juste pour localiser un accident). En première approche on peut faire remonter toute l'information à un point central, qui l'analyse. Ce n'est pas satisfaisant car cela pourrait introduire un point de faiblesse (et de ralentissement) unique, qui traite en outre de l'information privée qu'il n'est pas censé voir. Une solution naïve à base d'anonymisation telle que [1] est facilement attaquable car on peut reconstituer le trajet d'un véhicule, et donc remonter à l'identité de son propriétaire. L'approche MPC est pertinente à être utilisée car elle permet de traiter des données privées de façon décentralisée.

Références

[1] Virendra Kumar, William Whyte, Abhishek Jain, Connected Vehicle Communication With Improved Misbehavior Processing United States Patent Application 20190245705, 2018.

[2] I. Symeonidis et al., SePCAR: A Secure and Privacy-enhancing Protocol for Car Access, Computer Security – ESORICS 2017 pp 475-493.

[Cho+18] Jérémy Chotard et al. “Decentralized Multi-Client Functional Encryption for Inner Product”. In: Advances in Cryptology - ASIACRYPT ’18. Ed. by Thomas Peyrin and Steven D. Galbraith. Vol. 11273. Lecture Notes in Computer Science. Springer, 2018, pp. 703–732.

[Cra+18] Ronald Cramer et al. “SPDZ2k : Efficient MPC mod 2k for Dishonest Majority”. In: Lecture Notes in Computer Science (2018).

[CRX19] Ronald Cramer, Matthieu Rambaud, and Chaoping Xing. Asymptotically-Good Arithmetic Secret Sharing over Z=p`Z with Strong Multiplication and Its Applications to Efficient MPC. submitted. 2019.

[Dam+19] Ivan Damgård et al. “New Primitives for Actively-Secure MPC mod 2k with Applications to Private Machine Learning”. In: IEEE Security and Privacy 2019. Springer Berlin Heidelberg, 2019.

[Esc+20] Daniel Escudero et al. “Improved Primitives for MPC over Mixed Arithmetic-Binary Circuits”. In: IACR Cryptol. ePrint Arch. 2020 (2020), p. 338. url: https://eprint.iacr.org/2020/338.

[GGV20] Sanjam Garg, Shafi Goldwasser, and Prashant Nalini Vasudevan. “Formalizing Data Deletion in the Context of the Right to be Forgotten”. In: EUROCRYPT ’20. https://eprint.iacr.org/2020/254. 2020.

[KMR19] Katarzyna Kapusta, Gérard Memmi, and Matthieu Rambaud. “Circular All-Or-Nothing: Revisiting Data Protection Against Key Exposure”. In: CoRR abs/1901.08083 (2019). to appear in AsiaCCS 020. url: http://arxiv.org/abs/1901.08083.