Communiqué de presse

Avec le projet TAM, SystemX poursuit ses travaux en matière de cybersécurité et de protection de la vie privée des systèmes de mobilité autonomes, connectés et coopératifs.

S'inscrivant dans la lignée du projet SCA qui vient de s'achever, le projet Trusted Autonomous Mobility (TAM) ambitionne de lever d'importants verrous de cybersécurité des communications des systèmes de mobilité autonomes, connectés et coopératifs. Il adressera de nouveaux cas d'usage liés à la voiture et à la navette autonomes. Le projet s'attachera notamment à garantir la confiance dans les données échangées entre véhicules dans une démarche de perception collective, et étudiera l'impact de la cybersécurité sur la sûreté de fonctionnement et la prise de décision du véhicule autonome.

Palaiseau, le 1er avril 2021 – L'Institut de Recherche Technologique (IRT) SystemX lance le projet de R&D *Trusted Autonomous Mobiilty* (TAM) centré sur la cybersécurité de bout en bout et la protection de la vie privée dans les Systèmes de Transport Intelligents Coopératifs (C-ITS), pour une mobilité connectée, coopérative et autonome. D'une durée de 36 mois, TAM fédère 7 partenaires industriels (Atos-IDnomic, Navya, Oppida, Renault, Stellantis*, Trialog et Yogoko) et 1 partenaire académique (Institut Mines-Télécom). Il bénéficie également du soutien de deux partenaires institutionnels, l'ANSSI et la Plateforme Automobile française (PFA).

Le projet TAM qui s'inscrit dans la lignée du projet SCA achevé en novembre 2020, traite des cas d'usages liés au transport intelligent, autonome, connecté et coopératif et adresse 5 nouveaux défis :

- **Garantir la sécurité de bout-en-bout, dans un contexte d'acteurs/opérateurs différents et de connectivité multiple et sans fil**

L'arrivée de technologies de communication émergentes (LTE-V2X ou la 5G) favorise le déploiement de nouveaux cas d'usages des C-ITS dont les besoins en ressources ne peuvent être satisfaits par les technologies actuelles. L'hybridité des communications étant un vecteur supplémentaire de risques d'attaques, les solutions de cybersécurité déployées doivent être interopérables et répondre aux exigences de sécurité des applications C-ITS quelles que soient les technologies utilisées. De plus, les pertes de connectivité dues à l'environnement sans fil et à la forte mobilité sont également un vecteur de risque. Les protocoles de cybersécurité déployés doivent être robustes face à ces déconnexions et permettre un retour de connectivité fiable et sécurisé sur un autre réseau (redondance).

Ces verrous seront adressés à travers des cas d'usage du véhicule personnel autonome et connecté (enjeu de perception collective : comment valider la confiance dans les données qui proviennent des capteurs d'autres véhicules et détecter si elles sont erronées de manière intentionnelle ou non ?) et de la navette autonome et connectée (en cas de perte de connectivité, comment rétablir la sécurité des communications entre la navette et le centre d'assistance à distance ? comment favoriser les interventions à distance avec du transfert de voix ou de vidéo en cas de situation bloquée ou à risque ?).

Le projet TAM en quelques mots

Durée : 36 mois
ETP : 20
8 partenaires industriels et académiques
Secteurs applicatifs : mobilité et transport autonome, défense et sécurité

Enjeux / défis :

- Etudier de nouveaux cas d'usage de la voiture et de la navette autonomes, connectés et coopératifs
- Maintenir un haut niveau de sécurité tout au long du cycle de vie de la voiture et de la navette autonomes
- Faire évoluer la solution de Misbehavior Detection développée dans le projet SCA et l'étendre à de nouveaux cas d'usage
- Définir une vision commune de la protection de la vie privée des ITS coopératifs
- Etudier et évaluer l'impact de la cybersécurité sur la sûreté de fonctionnement

- **Maintenir le Système de Transport Intelligent Coopératif en conditions de sécurité tout au long du cycle de vie du véhicule**

Alors que la durée de vie d'un véhicule est d'une quinzaine d'année en moyenne, les technologies utilisées par les C-ITS évoluent rapidement, aussi bien en termes de matériel que de logiciel. Motivé aussi par la règlementation UN R155, il est essentiel que les solutions de cybersécurité déployées dans les C-ITS puissent être maintenues à jour tout au long de la vie du véhicule et soient agiles, c'est-à-dire capables de s'adapter aux changements. A cet effet, le projet TAM s'attachera à spécifier des protocoles et une architecture crypto-agile, à les implémenter et à les tester.

Dans TAM, les partenaires étudieront également des solutions de cybersécurité plus amont comme les algorithmes post-quantum. Ces travaux de recherche s'attacheront à identifier les solutions existantes dans l'IT et à voir comment les adapter pour les C-ITS.

Enfin, la gestion des identités numériques associées à un véhicule tout au long de son cycle de vie est également une problématique aujourd'hui non résolue. Plusieurs problématiques seront étudiées dans TAM : comment supprimer les identités numériques du véhicule lors de sa vente à un tiers ? Comment réinsérer un véhicule qui aurait été désactivé/éjecté du système suite à un comportement malveillant ?

- **Etendre à de nouveaux cas d'usage le système de Misbehavior Detection développé dans le projet SCA**

Le système Misbehavior Detection mis au point dans le cadre du projet SCA vise à superviser les échanges entre véhicules autonomes et connectés pour détecter les comportements malveillants et réagir de manière adaptée. Dans le projet SCA, seules les données cinématiques (CAM = Coopérative Awareness Message) des véhicules avaient été prises en compte. Dans le projet TAM, d'autres messages seront adressés comme les CPM (Collective Perception Message), qui permettent l'échange de données capteurs entre véhicules et favorisent la perception collective.

Pour définir s'il s'agit d'un comportement anormal non intentionnel (défaillance) ou intentionnel (malveillance), des algorithmes de Machine Learning/Deep Learning sont utilisés. Ces algorithmes peuvent également être la cible d'attaques, ce qui peut biaiser le système. Le projet TAM visera à mettre en place des contre-mesures afin de rendre plus robustes ces algorithmes et ne pas en détourner l'usage.

Ces travaux contribueront à faire évoluer la solution de Misbehavior Detection développée dans le projet SCA et actuellement en cours de normalisation à l'ETSI, en y intégrant de nouveaux cas d'usage (perception collective notamment).

Une thèse sur le thème « Le Misbehavior Detection pour la perception collective » sera également menée et visera à mettre au point un algorithme capable de garantir le haut niveau de confiance requis au niveau des données échangées entre véhicules.

- **Garantir la protection de la vie privée des usagers et de leurs données**

Les données émises par les véhicules sont considérées comme privées. Bien qu'elles ne soient pas directement liées à l'identité du propriétaire, leur analyse permet de dresser des profils utilisateurs, voire de retrouver les lieux visités par ces usagers (domicile, lieu de travail, écoles, centres commerciaux, etc.). Cependant, ces données sont éphémères et ne doivent pas être traitées comme les données persistantes de l'internet.

Chaque acteur des C-ITS (constructeurs, équipementiers, gestionnaires de routes, opérateurs télécom, …) a un regard et une compréhension différente du respect de la vie privée. L'un des objectifs de TAM est d'arriver à faire converger l'ensemble des acteurs sur une vision commune du respect de la vie privée et de la protection des données dans les C-ITS, à travers notamment la définition de modèles de protection des données qui sont compréhensibles par tous (et notamment les utilisateurs finaux).

- **Etudier l'impact de la cybersécurité sur la sûreté de fonctionnement et la prise de décision du véhicule autonome**

Le projet TAM va s'intéresser à l'impact des attaques de cybersécurité sur la sûreté de fonctionnement. Par exemple, si une caméra est défectueuse, il sera compliqué de valider les données qui proviennent du véhicule voisin. A l'inverse, il sera également intéressant d'étudier l'impact des défaillances (sûreté de fonctionnement) sur la cybersécurité du système. L'objectif est de réaliser une analyse du système qui combine ces deux aspects.

Les partenaires du projet identifieront une solution existante dans l'état de l'art et l'évalueront sur un cas d'usage pour relever ce défi.

Un démonstrateur en environnement réel sera mis au point à l'issue du projet, pour évaluer et tester les performances des solutions proposées. Ces expérimentations pourront être enrichies par des évaluations par simulation, ce qui permettra notamment d'appréhender les performances des solutions à large échelle (échelle d'une ville par exemple). Le développement d'un cas d'usage spécifique lié aux événements internationaux de 2023-2024 (Coupe du monde de Rugby 2023, J.O. de Paris 2024) sur le démonstrateur est envisagé.

« *Le projet TAM va capitaliser sur tous les résultats du projet SCA, qui avait permis de lever de nombreux verrous scientifiques et technologiques liés à la cybersécurité des communications des C-ITS. La très grande majorité des partenaires a à nouveau répondu présent pour continuer à investiguer encore plus en profondeur ce sujet et d'autres sujets sous-jacents, complexes et mouvants que constituent les enjeux cyber et de protection de la vie privée liés à la mobilité autonome, connectée et coopérative* », explique Arnaud Kaiser, chef de projet TAM, SystemX.

* Stellantis : né de la fusion entre Groupe PSA et FCA Group.

À propos de l'IRT SystemX

SystemX est un institut de recherche technologique (IRT) expert en analyse, modélisation, simulation et aide à la décision appliqués aux systèmes complexes. Seul IRT dédié à l'ingénierie numérique des systèmes, il coordonne des projets de recherche partenariale, réunissant académiques et industriels dans une perspective multi-filière. Ensemble, ils s'appliquent à lever des verrous scientifiques et technologiques majeurs de 4 secteurs applicatifs prioritaires : Mobilité et Transport autonome, Industrie du futur, Défense et Sécurité, Environnement et Développement durable. Au travers de projets orientés cas d'usage, les ingénieurs-chercheurs de SystemX répondent aux grands enjeux de notre temps, sociétaux et technologiques, et contribuent ainsi à l'accélération de la transformation numérique des industries, des services et des territoires. Basé sur le plateau de Paris-Saclay, Lyon et Singapour, SystemX a lancé depuis sa création en 2012, 53 projets de recherche (dont 29 en cours), impliquant plus de 100 partenaires industriels et 55 laboratoires académiques, et compte actuellement 197 collaborateurs en équivalent temps plein (ETP) dont 134 ressources propres.
Pour en savoir plus : www.irt-systemx.fr | @IRTSystemX | LinkedIn | YouTube

Contacts presse
Marion Molina – Claire Flin
Tél. 06 29 11 52 08 / 06 95 41 95 90
marionmolinapro@gmail.com / clairefline@gmail.com