Date: 19.04.2024

bulletin.ch

electrosuisse

Bulletin.ch / electrosuisse
8320 Fehraltorf
044/ 956 11 11
https://www.bulletin.ch/de/

Genre de média: Médias imprimés
Type de média: Presse spécialisée
Tirage: 6'612
Parution: 8x/année

Page: 46
Surface: 211'119 mm²

Hes·so

Ordre: 1073023
N° de thème: 375.009

Référence: 91652154
Coupure Page: 1/6

Vers une mobilité connectée et sécurisée

Assurer la fiabilité des communications entre véhicules et infrastructure | À l'avenir, les véhicules intelligents interagissant avec une infrastructure connectée deviendront la norme, assurant ainsi une amélioration de la sécurité routière ainsi qu'une utilisation plus efficace des ressources. Pour y parvenir, une communication fiable et sécurisée entre les véhicules et l'infrastructure est toutefois indispensable.

MICHAEL MÄDER, GABRIEL PYTHON, DENIS ROSSET

Date: 19.04.2024

bulletin.ch

electrosuisse

Bulletin.ch / electrosuisse
8320 Fehraltorf
044/ 956 11 11
https://www.bulletin.ch/de/

Genre de média: Médias imprimés
Type de média: Presse spécialisée
Tirage: 6'612
Parution: 8x/année

Hes·so

Page: 46
Surface: 211'119 mm²

Ordre: 1073023
N° de thème: 375.009

Référence: 91652154
Coupure Page: 2/6

La numérisation avance à pas de géant dans de multiples secteurs, et notamment dans celui de la mobilité. Cette évolution implique une transformation non seulement des véhicules tels que les voitures et les camions, mais aussi des infrastructures comme les feux de signalisation et les panneaux dans les tunnels, qui deviennent de plus en plus interconnectés. Cette transition vers le numérique et l'interconnexion apporte divers avantages, notamment une amélioration de la sécurité dans l'écosystème de la mobilité ainsi qu'une utilisation plus efficace des ressources telles que la capacité des routes et l'énergie. À l'avenir, les véhicules intelligents en symbiose avec une infrastructure connectée deviendront la norme à l'échelle internationale, introduisant ainsi de nouveaux défis.

Grâce à une multitude de capteurs et à une communication avec l'infrastructure intelligente, par exemple avec les feux de signalisation, les véhicules intelligents seront capables d'anticiper des situations et d'éviter des dangers potentiels. Ensemble, ces véhicules et les infrastructures formeront un système complexe échangeant continuellement des données, s'adaptant aux conditions en temps réel et améliorant constamment leurs performances ainsi que la sécurité. Pour y parvenir, une communication fiable et sécurisée entre les véhicules et l'infrastructure (Vehicle-to-Infrastructure, V2I) est indispensable, car la confiance des utilisateurs dans cette nouvelle technologie dépendra de cette fiabilité.

De nouvelles réglementations telles que le règlement UNECE R155 [1] relatif à la cybersécurité pour les véhicules exigent un niveau de sécurité accru dans la communication V2I. Cette dernière s'est donc trouvée au cœur du projet de recherche SecV2IComm – mené à la Haute école d'ingénierie et d'architecture de Fribourg (HEIA-FR) ainsi qu'au sein de son centre de compétences Rosas – ayant pour objectif la vérification de la fiabilité la communication V2I dans des conditions de laboratoire et réelles. Cette analyse s'est basée sur la norme ISO 21434 Véhicules routiers – ingénierie de la cybersécurité [2].

Le projet en bref

Dans le cadre du projet SecV2IComm, une plateforme de test a été mise en place au centre de compétences Rosas, impliquant un véhicule automatisé et téléopéré – développé précédemment au cours du projet de recherche NPR Téléopération [3] – et un feu de signalisation prototype élaboré lors de ce projet **(figure de titre)**.

Ces deux éléments constituent l'écosystème de mobilité en question, communiquant entre eux via une connexion réseau de données (V2I) à évaluer. Le véhicule est équipé d'une OBU (On-Board Unit) pouvant recevoir des paquets de données d'autres composants tels que des véhicules ou des infrastructures. Ces paquets peuvent, par exemple, contenir des informations sur l'état des feux de signalisation à proximité. De leur côté, les feux de signalisation sont connectés à une RSU (Road Side Unit) permettant la transmission de l'état et de la localisation du feu aux véhicules connectés environnants.

Dans la configuration de test retenue, l'OBU et le RSU communiquent via le protocole ITS-G5. Afin de jouer le rôle du pirate, le concept inclut également un équipement réseau, communément appelé « hacking box », capable de gérer la communication via le protocole ITS-G5, permettant ainsi l'écoute, la modification et l'envoi de paquets de données. Cette hacking box n'est rien d'autre qu'un mini-ordinateur équipé d'une carte réseau.

À la clôture du projet, un concept de validation de la communication V2I conforme aux normes actuelles a été élaboré, permettant une validation avec des éléments réels tels que des véhicules et des feux de signalisation.

Communication V2I: le protocole ITS-G5

La sécurité de la communication est d'une importance capitale, car des intrusions de pirates informatiques peuvent entraîner des actions indésirables et dangereuses au niveau des véhicules ou des infrastructures, mettant ainsi en péril la sécurité des individus et des installations. Par exemple, la modification des informations concernant l'état d'un feu de signalisation peut créer un écart entre l'état réel et celui reçu, entraînant un comportement inattendu du véhicule.

Pour évaluer la sécurité de la communication V2I, le protocole standardisé ITS-G5 (IEEE 802.11p) a été sélectionné en premier lieu parmi les protocoles disponibles et en partie déjà utilisés. Ce protocole est similaire au protocole WLAN (IEEE 802.11a) bien connu, avec quelques ajustements (de la bande de fréquence de 5,85 à 5,925 GHz, par exemple). Deux types de messages ont été examinés plus en détail: les messages Spatem (Signal, Phase and Timing Extended Message), qui transmettent l'état d'un feu de signalisation (par exemple rouge, orange ou vert), et les messages Mapem (Map Extended Message), qui décrivent l'emplacement géographique du composant d'infrastructure **(figure 1)**.

Date: 19.04.2024

bulletin.ch

electrosuisse

Bulletin.ch / electrosuisse
8320 Fehraltorf
044/ 956 11 11
https://www.bulletin.ch/de/

Genre de média: Médias imprimés
Type de média: Presse spécialisée
Tirage: 6'612
Parution: 8x/année

Page: 46
Surface: 211'119 mm²

Ordre: 1073023
N° de thème: 375.009

Référence: 91652154
Coupure Page: 3/6

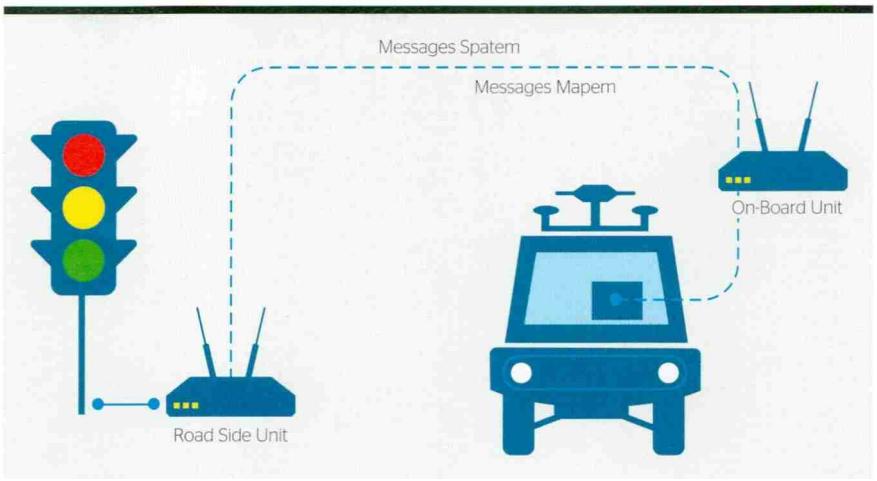

Figure 1 L'écosystème ITS-G5 : la RSU (Road Side Unit) reliée au feu de signalisation transmet des messages Spatem, relatifs à l'état du feu, et Mapem, relatifs à sa localisation, à l'OBU (On-Board Unit) embarquée dans le véhicule.

Figure 2 Feu de signalisation équipé de la RSU (boîte grise derrière le feu).

Date: 19.04.2024

bulletin.ch

electrosuisse

Bulletin.ch / electrosuisse
8320 Fehraltorf
044/ 956 11 11
https://www.bulletin.ch/de/

Genre de média: Médias imprimés
Type de média: Presse spécialisée
Tirage: 6'612
Parution: 8x/année

Hes·so

Page: 46
Surface: 211'119 mm²

Ordre: 1073023
N° de thème: 375.009

Référence: 91652154
Coupure Page: 4/6

La diffusion de ces messages est assurée par la RSU reliée dans le cadre de ce projet à un feu de signalisation, permettant ainsi à tous les véhicules dotés d'une OBU et se trouvant à proximité de les recevoir. Cependant, cette diffusion non chiffrée et non signée laisse la voie libre à toute entité compatible ITS-G5 d'intercepter et potentiellement d'altérer ces messages. Par conséquent, un dispositif malveillant se faisant passer pour une RSU (hacking box) pourrait diffuser de fausses informations telles que des états de feux de signalisation incorrects (Spatem) ou de fausses informations géographiques (Mapem), induisant ainsi en erreur les véhicules et mettant en danger la sécurité routière.

L'environnement de test

La théorie a été mise en pratique afin de vérifier si les « craintes » en matière de sécurité pouvaient réellement se réaliser. Trois composants principaux constituent l'environnement de test: le véhicule intelligent avec son OBU, qui peut soit rouler de manière autonome, soit être commandé par téléopération, un feu de signalisation classique équipé d'une RSU **(figure 2)**, qui passe périodiquement du vert au rouge et inversement, et enfin, la hacking box, qui permet d'écouter la communication V2I et d'envoyer des messages, jouant ainsi le rôle d'une deuxième RSU.

Manipulation de la communication V2I

L'attaque au moyen de la hacking box comprend plusieurs étapes. Tout d'abord, la communication entre l'OBU et la RSU a été analysée. Pour ce faire, les paquets de données ont été enregistrés dans le but de les retransmettre ultérieurement grâce à la hacking box. Ces messages provenant de la hacking box ont été acceptés sans problème par l'OBU et ont permis de réécrire l'état du feu de signalisation dans le système du véhicule.

Il a ainsi été possible d'envoyer un statut erroné au véhicule. En d'autres termes, lorsque le feu était rouge, le boîtier de piratage envoyait à un intervalle beaucoup plus court un grand nombre de messages Spatem décrivant le feu comme étant vert **(figure 3)**. L'OBU du véhicule reçoit tous les messages et réagit en conséquence: le véhicule poursuit son chemin, mettant potentiellement en danger les autres usagers de la route.

Prévention des attaques par rejeu grâce à la cryptographie

La configuration de base de l'infrastructure utilisée (OBU et RSU) ne comporte l'activation d'aucun paramètre de sécurité spécifique. En conséquence, les mêmes messages peuvent être retransmis autant de fois que désiré, et sont toujours considérés comme valides et traités en conséquence. Pour prévenir la simple rediffusion, une contre-mesure consiste à utiliser un compteur générant un chiffre lors de l'envoi du message, qui ne peut être considéré comme valide qu'une seule fois. Afin d'éviter qu'un pirate informatique n'incrémente lui-même le compteur avant d'envoyer les messages falsifiés, tous les messages doivent être signés de manière cryptographique.

La signature cryptographique implique la création d'une valeur de hachage unique pour chaque message envoyé. Pour ce faire, une paire de clés composée de la clé privée et de la clé publique est utilisée. La signature est ensuite chiffrée avec la clé privée et envoyée avec le message. Cette paire de clés devrait être générée uniquement par des services officiels tels que l'Office fédéral des routes (OFROU).

Pour vérifier l'authenticité du message, l'autre partie (l'OBU) peut également calculer la valeur de hachage du message et la comparer avec le hachage chiffré envoyé avec le message. Si les deux valeurs de hachage correspondent, la signature est authentique et le message est considéré comme valide. Dans le cas contraire, le message est rejeté comme non valide.

La signature cryptographique empêche toute personne qui n'est pas en possession de la clé privée de créer et de signer des messages. Les clés privées sont gérées par les bureaux de l'Office fédéral des routes qui mettent en service les feux de signalisation (ou d'autres éléments de l'infrastructure) et doivent s'assurer qu'aucun « faux » élément de l'infrastructure ne puisse avoir accès à ces clés. Chaque paire de clés créée par un organisme officiel doit donc divulguer la clé publique et s'assurer qu'elles sont connues des OBU. Dans le cas contraire, la signature décrite ne peut pas être vérifiée.

Conclusions et perspectives

Les réglementations actuelles doivent être considérablement renforcées en matière de cybersécurité. La signature des messages doit devenir un élément obligatoire de la chaîne de communication V2I. De plus, tous les composants doivent être certifiés pour garantir la vérification des signatures, empêchant ainsi tout message invalide d'être accepté et traité. Une configuration par défaut sécurisée des fabricants doit être activée.

À l'avenir, la structure de test du centre de recherche Rosas sera utilisée pour évaluer la sécurité des systèmes de communication ITS-G5, indépendamment du fabricant ou du type (OBU et RSU) des composants. De nouveaux essais et scénarios d'attaque seront mis en place pour élargir l'environnement de test. Ce projet a également permis de créer un service fournissant une plateforme d'essai (ITS-G5 ou autre) pour

Date: 19.04.2024

bulletin.ch

electrosuisse

Bulletin.ch / electrosuisse
8320 Fehraltorf
044/ 956 11 11
https://www.bulletin.ch/de/

Genre de média: Médias imprimés
Type de média: Presse spécialisée
Tirage: 6'612
Parution: 8x/année

Hes·so

Page: 46
Surface: 211'119 mm²

Ordre: 1073023
N° de thème: 375.009

Référence: 91652154
Coupure Page: 5/6

valider et présenter les résultats et améliorations d'un point de vue technique ainsi que pour garantir la conformité aux normes ISO d'une communication V2I sécurisée.

En outre, des recommandations seront élaborées sur la base des recherches technologiques menées pour assurer une communication V2I sécurisée. Ces résultats seront également intégrés à d'autres projets de recherche (MB4 de l'OFROU, SwissMoves, etc.) visant à promouvoir une mobilité future intelligente, numérique et prédictive.

Liens

- → Vidéo du projet SecV2IComm : youtube.com/watch?v=FCz1XCS4G7Y
- → Filière ISC de la Haute école d'ingénierie et d'architecture de Fribourg : heia-fr.ch/fr/formation/bachelor/informatique-et-systemes-de-communication
- → Centre de compétences Rosas : rosas.center/fr

Références

[1] UNECE UN Regulation No. 155 Cyber security and cyber security management system. unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security
[2] ISO Standards, ISO/SAE 21434:2021 Road vehicles – cybersecurity engineering. iso.org/standard/70918.html
[3] Nouvelle politique régionale (NPR), projet Téléopération. innosquare.com/fr/projets-realises/projets-collaboratifs-npr-2020-2023/teleoperation/

Auteurs

Michael Mäder est professeur à la Haute école d'ingénierie et d'architecture de Fribourg (HEIA-FR).
→ HEIA-FR, 1700 Fribourg
→ michael.maeder@hefr.ch

Gabriel Python est adjoint scientifique au sein du centre de compétences Rosas de la HEIA-FR.
→ Rosas, 1700 Fribourg
→ gabriel.python@hefr.ch

Denis Rosset est collaborateur scientifique au sein du centre de compétences Rosas de la HEIA-FR.
→ denis.rosset@hefr.ch

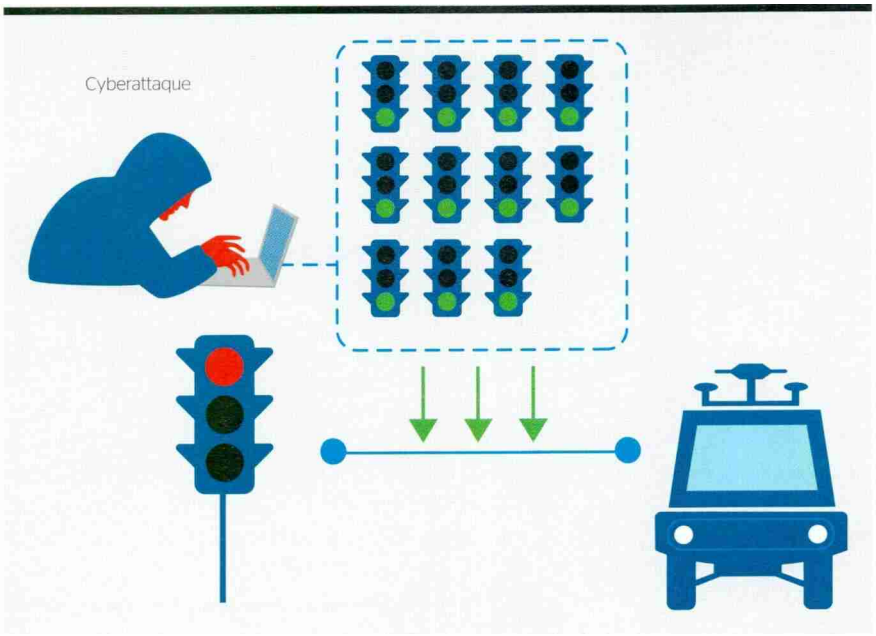

Figure 3 Attaque par rejeu (replay attack) à l'aide de la « hacking box ».

Date: 19.04.2024

bulletin.ch

electrosuisse

Bulletin.ch / electrosuisse
8320 Fehraltorf
044/ 956 11 11
https://www.bulletin.ch/de/

Genre de média: Médias imprimés
Type de média: Presse spécialisée
Tirage: 6'612
Parution: 8x/année

Page: 46
Surface: 211'119 mm²

Ordre: 1073023
N° de thème: 375.009

Référence: 91652154
Coupure Page: 6/6

Auf dem Weg zu einer vernetzten und sicheren Mobilität

Zuverlässige Kommunikation zwischen Fahrzeugen und Infrastruktur

IN KÜRZE

Künftig werden «intelligente» Fahrzeuge, die mit einer vernetzten Infrastruktur interagieren, zur Norm werden und so für mehr Sicherheit im Strassenverkehr sowie eine effizientere Nutzung der Strassenkapazität und Energie sorgen. Dazu braucht es aber eine zuverlässige und sichere Kommunikation zwischen Fahrzeugen und Infrastruktur (Vehicle-to-Infrastructure, V2I) sowie die entsprechende Regulierung.

Im Forschungsprojekt SecV2IComm der Hochschule für Technik und Architektur Freiburg (HEIA-FR) und ihrem Kompetenzzentrum Rosas wurde die Zuverlässigkeit der V2I-Kommunikation unter Labor- und realen Bedingungen getest. Dazu wurde eine Testplattform eingerichtet, die ein automatisiertes und ferngesteuertes Fahrzeug mit einer OBU (On-Board Unit), die Datenpakete empfangen kann, und eine Ampel mit einer RSU (Road Side Unit), die den Status und den Standort der Ampel an die umliegenden vernetzten Fahrzeuge übermitteln kann, umfasste. In der gewählten Testkonfiguration kommunizierten die OBU und die RSU über das ITS-G5-Protokoll, das mit einem herkömmlichen WLAN vergleichbar ist.

Im Projekt wurde gezeigt, dass es mit einem Minicomputer mit Netzwerkkarte (Hacking Box) möglich ist, die V2I-Kommunikation aufzuzeichnen und eine grosse Anzahl falscher Nachrichten an das Fahrzeug zu senden (Replay Attack), wodurch die Verkehrssicherheit gefährdet wird. Solche Angriffe lassen sich mit einem Zähler verhindern, der beim Senden der Nachricht eine Zahl erzeugt, die nur einmal als gültig betrachtet werden kann. Um zu verhindern, dass ein Hacker den Zähler selbst inkrementiert, bevor er die gefälschten Nachrichten versendet, müssen alle Nachrichten kryptografisch signiert werden.

Die bestehende Regulierung muss daher im Bereich der Cybersicherheit deutlich verschärft werden. Die Signatur von Nachrichten in der V2I-Kommunikationskette muss obligatorisch werden. Zudem müssen alle Komponenten zertifiziert sein, um die Verifizierung von Signaturen zu gewährleisten, und eine sichere Standardkonfiguration der Hersteller muss aktiviert sein.