Veille Informatique

La Cybersécurité des véhicules autonomes et connectées

-Vulnérabilités et attaques potentielles

1ère étape : Attaques

-**L'usurpation de messages ou de données (attaques utilisant l'ingénierie sociales)** (le message semble provenir d'une personne que vous connaissez, mais il s'agit en réalité d'un pirate). Manipulation du code interne et des données du véhicule.

-**Possibilité d'interférence au sein des réseaux de communication**, En résumé, l'intrusion décrite met en évidence la possibilité pour un attaquant de perturber la communication entre les serveurs distants et le système informatique embarqué dans le véhicule, ce qui peut avoir des conséquences graves en termes de sécurité et de fonctionnalité du véhicule.
"Lorsqu'un attaquant parvient à compromettre la sécurité de cette communication, il peut potentiellement accéder à des données sensibles échangées entre le véhicule et les serveurs, ou même modifier ces données pour causer des dommages ou des perturbations. Par exemple, un attaquant pourrait intercepter des mises à jour logicielles pour injecter des logiciels malveillants dans le système embarqué du véhicule, ou encore modifier les informations de navigation pour envoyer le véhicule sur un itinéraire différent."
(Man in the middle)

-Les attaques par entrée sans clé et par porte-clés représentent 50 % de tous les vols de véhicules. Il suffit que les voleurs soient à proximité de la télécommande pour qu'un hacker Black Hat puisse capter et reproduire son signal. "Des attaques DDoS contre les systèmes de transport intelligents (STI), qui pourraient saturer les canaux de communication des voitures connectées"

2ème Etape : Conséquences de cette intrusion :

-**Vols de voiture : "** À Oakville, au Canada, 124 vols de véhicules ont été signalés au cours du premier semestre 2021, dans une ville qui ne compte que 211 000 habitants. "

- ***Conséquence sur*** **les fonctionnalités du véhicule**, ”encore modifier les informations de navigation pour envoyer le véhicule sur un itinéraire différent”, **Mise en danger de la vie des passagers par la désactivation des freins : “***Les risques de cybersécurité dans les véhicules à conduite autonome peuvent avoir un impact direct sur la sécurité des passagers, des piétons, des autres véhicules et des infrastructures connexes “.*

-**Fuite de données sur le DARK net conséquences irréversibles :** “Il ne s’agit pas seulement de voitures. Deux grandes sociétés de transport public israéliennes ont récemment été frappées par des attaques de ransomware et ont vu leurs données fuir sur le Darknet. En plus des données volées, l’attaque a entraîné la fermeture des sites web des entreprises”

D’accéder à des informations critiques stockées dans le disque dur du véhicule.

-Usurpation d’identité par la saisie de toutes ces données personnels, altération de ces données.

-Exemple d’attaques : Une Tesla Model 3 s'est faite hachée... pour la bonne cause, dans le cadre d'un concours de sécurité informatique.

(Problème : l’intégration de l’IA rend plus complexe la protection du système informatique embarqué et des données plus ou moins sensibles qui y transitent)

Cause du Problème de sécurité

L'intégration de l'intelligence artificielle (IA) dans les véhicules autonomes peut rendre plus complexe la protection en termes de sécurité informatique pour plusieurs raisons :

Complexité des systèmes : Les systèmes IA dans les véhicules autonomes sont souvent complexes et comportent de nombreux composants interconnectés, ce qui augmente la surface d'attaque potentielle pour les cyberattaques. La sécurisation de ces systèmes exige une compréhension approfondie de leurs interactions et de leurs vulnérabilités.

Dépendance aux données : Les algorithmes d'IA dépendent fortement des données pour leur apprentissage et leur fonctionnement. Si ces données sont corrompues ou

manipulées par des attaquants, cela peut compromettre l'intégrité et la fiabilité des décisions prises par le système d'IA

Des failles de sécurité ont déjà été relevées par le passé

De manière plus générale, les auteurs constatent que « ***l'absence de connaissances et d'expertise suffisantes en matière de sécurité parmi les développeurs et les concepteurs*** *de systèmes sur la cybersécurité de l'IA est un obstacle majeur qui entrave l'intégration de la sécurité dans le secteur automobile* ».

Il conviendrait donc selon les chercheurs que les décideurs et les entreprises cherchent à développer une culture de la sécurité tout au long de la chaîne d'approvisionnement et notamment auprès des sous-traitants.

-Manque de mise à jour, donc traitement des vulnérabilités

-Communication sans fil non sécurisée : *Les communications sans fil utilisées dans les véhicules connectés, telles que le Wi-Fi, le Bluetooth et les réseaux cellulaires, peuvent être vulnérables aux interceptions et aux attaques de type "man-in-the-middle" si elles ne sont pas correctement sécurisées.*

En résumé, les cyberattaques sur les véhicules connectés peuvent être causées par divers facteurs, y compris des vulnérabilités logicielles, le manque de mises à jour, l'interconnexion avec d'autres systèmes, les communications sans fil non sécurisées et les techniques d'ingénierie sociale. Il est essentiel pour les fabricants de véhicules et les utilisateurs de prendre des mesures pour identifier et atténuer ces risques afin de garantir la sécurité des véhicules connectés et de leurs occupants.

- Solutions et contre-mesures :

L'ENISA recommande également aux parties prenantes de simuler divers scenarii d'attaque et de **mettre en place des équipes de traitement** et de **réponse aux incidents de cybersécurité.**

Les acteurs de l'automobile devront donc par exemple mettre en place **des mesures de sécurité renforcées** ainsi **que des mécanismes de détection** et de **protection aptes à prévenir d'éventuelles atteintes évolutives**, à **limiter les intrusion**s, à **protéger les données des individus,** et à **répondre avec célérité aux failles de sécurité**.

Pour cela, **les outils d'intelligence artificielle utilisés devront être régulièrement évalués et mis-à-jour** afin de s'assurer que le véhicule sera en mesure de faire face à des situations inattendues voire malveillantes.

Mettre en place des technologies de sécurité adaptées intégrant notamment **le pare-feu**, **le chiffrement**, **le contrôle des appareils**, **la sécurité des applications**, **le scan de vulnérabilités**, **la signature de code**, **l'IDS (Intrusion Detection System) pour CAN (Controller Area Networks)** et l'antivirus pour l'unité principale.

La **Blockchain** peut également jouer un rôle dans la sécurisation des transactions effectuées sur les réseaux automobiles.

D'autres technologies déjà connues, comme **l'utilisation de mots de passe forts**, **le chiffrement des données** et **l'authentification multifacteur**, peuvent également contribuer à améliorer la résilience de l'industrie automobile face à la cybercriminalité.

Mais avant toute chose, **la prévention de la cybercriminalité** dans l'industrie automobile et les autres secteurs exige une mobilisation des ressources humaines **pour former les employés à l'importance de la sécurité numérique**. Cette démarche de formation est indispensable pour permettre à chacun de mesurer l'importance de la cybersécurité et contribuer à limiter les cyberattaques.

Trend Micro et **Global sign** fournit des solutions logicielles informatique dédiés à la protection des cyberattaques.

De nombreux experts estiment que c'est **le facteur humain** qui constitue le maillon faible en matière de cyber-attaques sur les véhicules autonomes et connectés. **Le comportement des utilisateurs** est véritablement la clé du problème : **mauvaise utilisation des systèmes électroniques, influence des communications externes, altération des équipements ou encore négligence en termes de mises à jour des logiciels de sécurité. Sensibiliser** les utilisateurs aux bons gestes, rééquilibrer notre connaissance des technologies de pointe et nos interactions avec elles sont deux prérequis absolument nécessaires si vous voulons garantir l'assurabilité des véhicules autonomes et connectés.

-Réglementation et gouvernance :

Réglementation et gouvernance : Analysez les initiatives réglementaires et les normes de l'industrie visant à promouvoir la sécurité des véhicules autonomes. Explorez les exigences de conformité, les directives de sécurité recommandées et les mécanismes de gouvernance pour assurer la conformité et la responsabilité en matière de cybersécurité dans le développement et l'utilisation des véhicules autonomes.

Règlement général sur la protection des données (RGPD) de l'Union européenne

Le RGPD impose **des normes strictes de protection des données personnelles, y compris celles collectées par les véhicules autonomes**. Les fabricants de véhicules doivent s'assurer que la collecte, le stockage et le traitement des données des conducteurs et des passagers **respectent les principes de protection des données énoncés dans le RGPD.**

Dans le cadre de sa démarche d'accompagnement sectoriel, la CNIL a récemment lancé **un « *club conformité* »** dédié aux acteurs du véhicule connecté et de la mobilité.

Le pack conformité rappelait enfin que la sécurité est **un élément essentiel dans le déploiement de véhicules connectés et implique**, sinon l'anonymisation, en tous cas des mesures de chiffrement des canaux de transfert des données extraites du véhicule, des mesures de gestion des accès et authentification, ou encore un fort cloisonnement des données selon les fonctionnalités qui les utilisent (fonctions vitales du véhicule, fonctions de communication, données susceptibles de révéler des infractions, etc.).

Ce pack conformité, bien qu'antérieur au RGPD, demeure pertinent dans beaucoup de domaines, **en particulier pour répertorier les finalités des traitements qu'il est possible de mettre en place sur les données collectées via l'utilisation d'un véhicule connecté**. Ce sont cependant, désormais, les

Lignes Directrices du CEPD du 9 mars 2021 qui constituent la doctrine actuelle des autorités de protection.

L'Organisation internationale de normalisation (ISO) et la Society of Automotive Engineers International (SAE International) ont récemment publié leur norme précisant la réglementation et les exigences en matière de cybersécurité pour les véhicules automobiles :

La norme **ISO/SAE 21434** est une norme internationale qui définit les exigences de sécurité pour le développement de systèmes de cybersécurité dans les véhicules automobiles. Elle a été publiée conjointement par l'Organisation internationale de normalisation (ISO) et la Society of Automotive Engineers (SAE) pour répondre aux défis croissants posés par les cybermenaces dans les véhicules connectés et autonomes.

Thématiques de cette norme :

Gestion de la sécurité : La norme définit les processus et les activités à mettre en place pour gérer la sécurité tout au long du cycle de vie des systèmes de cybersécurité dans les véhicules.

Exigences de sécurité : La norme spécifie les exigences de sécurité à respecter lors de la conception, du développement et de la validation des systèmes de cybersécurité pour les véhicules automobiles. Cela comprend des exigences de conception sécurisée, de cryptographie, de détection d'intrusion, de gestion des clés, etc.

Intégration de la sécurité : La norme aborde l'intégration de la sécurité dans l'ensemble du processus de développement des véhicules automobiles, en s'assurant que les systèmes de cybersécurité sont intégrés de manière transparente avec les autres systèmes du véhicule et qu'ils fonctionnent de manière fiable dans un environnement opérationnel.

Validation et vérification : La norme définit les processus de validation et de vérification à appliquer pour s'assurer que les systèmes de cybersécurité répondent aux exigences de sécurité spécifiées. Cela inclut des tests fonctionnels, des tests de robustesse

Documentation et traçabilité : La norme exige une documentation détaillée de toutes les activités liées à la sécurité, ainsi que la traçabilité des décisions prises et des mesures prises pour garantir la sécurité des systèmes

La Directive sur la sécurité des réseaux et des systèmes d'information (NIS) ne spécifie pas de normes spécifiques à suivre, mais elle établit plutôt des obligations générales pour les États membres de l'UE afin de renforcer la sécurité des réseaux et des systèmes d'information dans divers secteurs, y compris les transports.

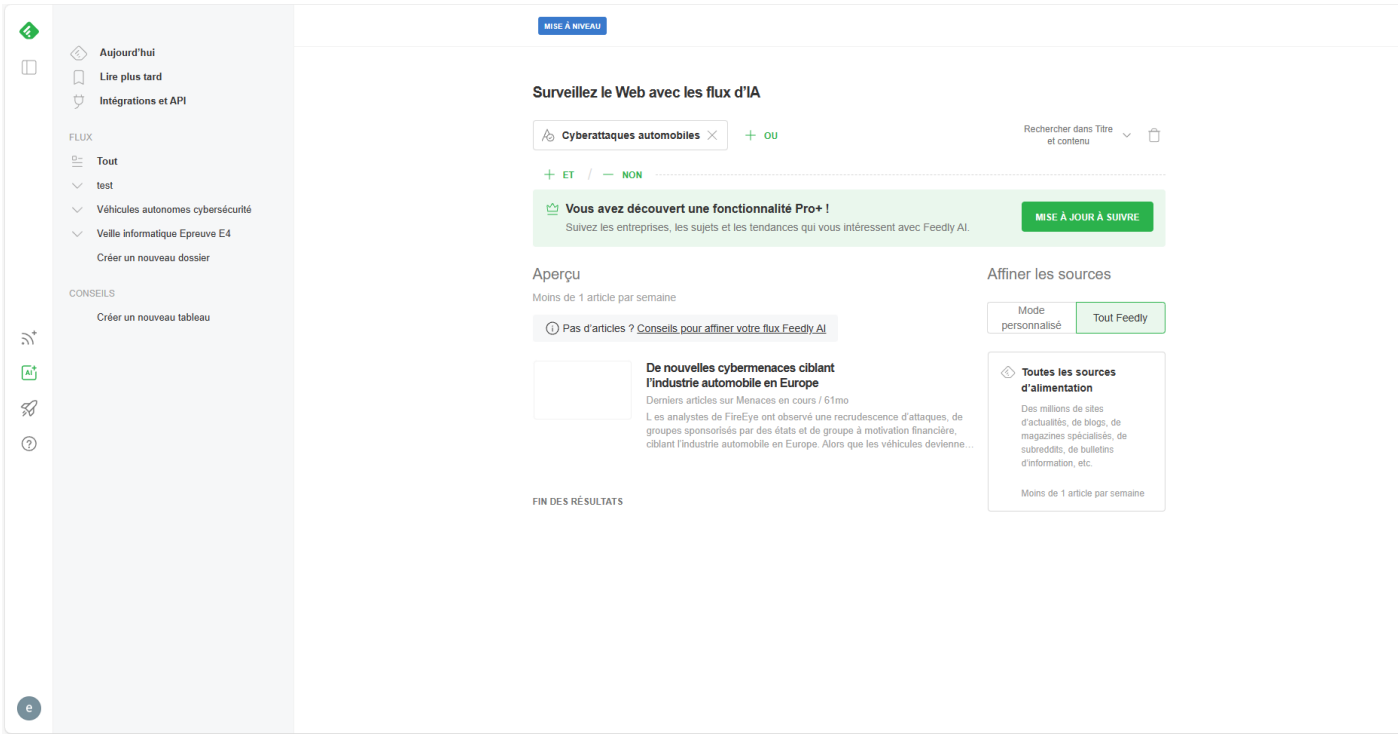
Cependant, une norme souvent citée dans le contexte de la NIS est la **norme ISO/IEC 27001** sur le management de la sécurité de l'information. Bien qu'elle ne soit pas spécifique aux systèmes de transport, elle fournit un cadre de gestion de la sécurité de l'information

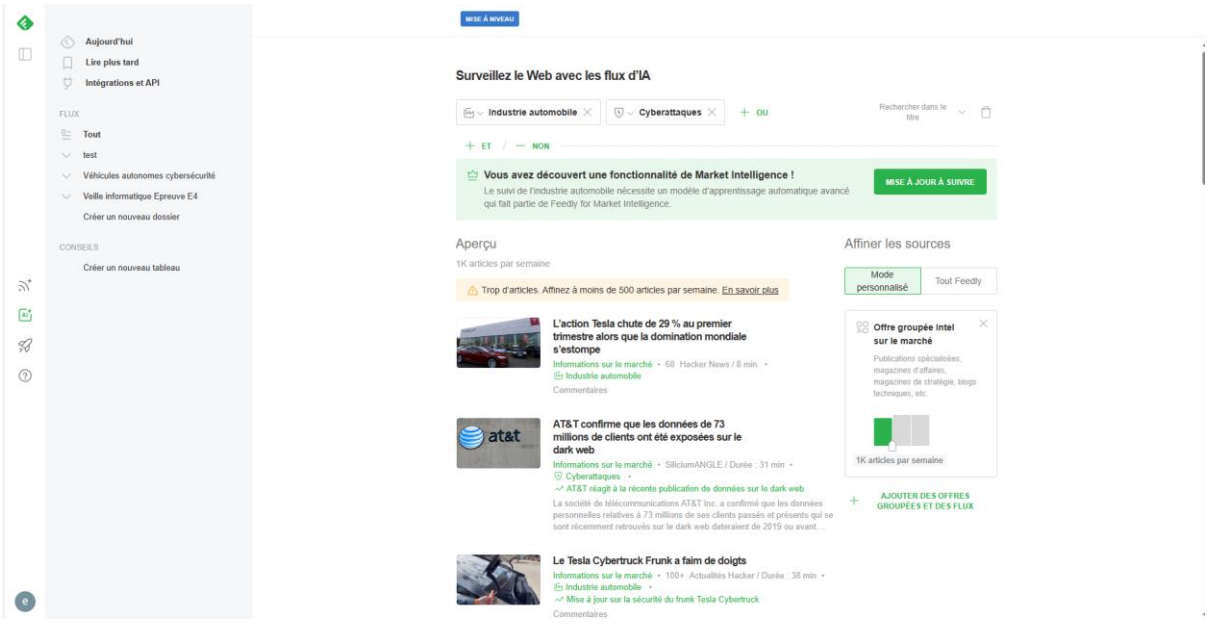
Cette norme **aide les organisations à établir, mettre en œuvre, maintenir et améliorer un système de management de la sécurité de l'information.**

Cette norme peut être utilisée pour promouvoir la sécurité des systèmes de transport contre les cybermenaces **en fournissant un cadre de bonnes pratiques pour la gestion de la sécurité de l'information dans ces domaines.**

En résumé, **bien que la norme ISO/IEC 27001 ne soit pas obligatoire en soi**, elle peut être rendue obligatoire par des réglementations spécifiques ou des exigences contractuelles dans certains cas, et elle est souvent utilisée comme un cadre de bonnes pratiques pour la gestion de la sécurité de l'information dans de nombreux secteurs et industries.

Mise en place de ma Veille :





FLIPBOARD, GOOGLE ACTUALITES, FEEDLY