BlackBerry Intelligent Security. Everywhere.

Vers l'avenir de l'entretien des véhicules :

Aspects de sûreté et de sécurité pour les mises à jour logicielles des véhicules

Comité – La cybersécurité dans le secteur du marché secondaire des véhicules
Conférence sur la cybersécurité des véhicules de Transports Canada
24 mars 2022

Takashi Suzuki, directeur principal, Normes BlackBerry

Ordre du jour

- BlackBerry pour la cybersécurité et la sécurité automobile
- Règlements et normes
- Les défis posés par les mises à jour de logiciels des véhicules du marché secondaire
- Recommandations
- Conclusions

BlackBerry pour la cybersécurité et la sécurité automobile

- 40 ans d'expérience dans la fabrication de systèmes intégrés sécurisés et certifiés, utilisés dans une variété de contextes essentiels critiques, notamment dans l'industrie automobile.

- Une culture solide en matière de sécurité et sûreté
  - Gestion du cycle de vie de la sûreté et de la sécurité éprouvée sur le terrain
    - Analyse approfondie de la sûreté et de la sécurité
    - Développement et vérification de logiciels fiables selon le modèle cycle en V.

- Plus de 195 millions de véhicules équipés du système QNX de BlackBerry
  - Système d'exploitation QNX et hyperviseur précertifiés ASIL B/D pour la sécurité – Conception d'architecture modulaire et micro-noyau
  - Solutions de gestion clé de Certicom pour l'automobile – Protection et vérification des logiciels par signature numérique
  - Outil Jarvis de BlackBerry – Solution d'analyse de la composition binaire et de test de sécurité pour découvrir les vulnérabilités des logiciels
  - Technologie sur les ondes QNX de BlackBerry – Solution de mise à jour logicielle sur les ondes sécurisée et personnalisable

Règlements et normes – Approche axée sur le risque et le cycle de vie

- Règlements et lignes directrices
  - Lignes directrices sur la cybersécurité des véhicules, Stratégie de cybersécurité des véhicules et OECV de Transports Canada
  - WP.29 GRAVA de l'UNECE (Groupe de travail sur les véhicules automatisés et connectés)
    - Règlement 155 – Homologation des véhicules en ce qui concerne la cybersécurité et de leurs systèmes de gestion de la cybersécurité
    - Règlement 156 – Homologation des véhicules en ce qui concerne les mises à jour logicielles et le système de gestion des mises à jour logicielles
    - Recommandations pour la cybersécurité automobile et les mises à jour logicielles
      - Prescriptions pour les parties contractantes de 1998 – Exigences techniques fondées sur les deux règlements ci-dessus
- Normes
  - ISO/SAE 21434:2021 — Norme d'ingénierie de la cybersécurité des véhicules routiers
    - Exigences en matière de gestion et d'activités de cybersécurité automobile pour soutenir les étapes du cycle de vie des véhicules
  - ISO/DIS 24089 — Norme d'ingénierie de mise à jour du logiciel des véhicules routiers (à publier en novembre 2022)
    - Exigences en matière d'infrastructure et de conception de véhicules pour les mises à jour logicielles, le développement des progiciels et les opérations de mise à jour
  - ISO 26262:2018 – Véhicules routiers – Norme de sécurité fonctionnelle
    - La partie 6 définit les exigences relatives au cycle de vie des logiciels de sécurité (architecture, développement, vérification, intégration).

Défis liés aux mises à jour logicielles des véhicules du marché secondaire

- Contexte
  - Évolution rapide du contexte des cybermenaces (tactiques et techniques d'attaque)
  - Nouvelles vulnérabilités et faiblesses – elles peuvent être latentes dans les composantes de série, comme les logiciels libres, et dans votre propre code
  - Besoins émergents de mises à jour logicielles pour empêcher les adversaires de les exploiter

- Défis de la mise à jour des logiciels des véhicules
  - Gestion des risques de cybersécurité et de sécurité introduits par les fonctions de mise à jour logicielle
  - Vérification de la sécurité agile et fiable permettant de corriger les vulnérabilités ponctuellement
    - L'évaluation et la vérification de l'impact sur la sécurité exigent du temps et des ressources, ce qui peut empêcher les fabricants d'équipement d'origine d'effectuer les correctifs de cybersécurité en temps opportun.

Recommandations pour des mises à jour logicielles (MJL) sûres et sécurisées

- Mettre en pratique des directives et des normes actualisées
  - OECV de Transports Canada – Tenir compte de la MJL à chaque étape, comme l'évaluation des risques
  - Recommandation du WP.29 – Article 2.2 (Exigences an matière de MJL), Partie A (Menaces) et Partie B (Atténuation) de l'Annexe
  - ISO/SAE 21434 – Analyse des menaces et évaluation des risques (clause 15)
  - ISO 24089 – Gérer les risques de sécurité et de cybersécurité du cycle de vie des mises à jour logicielles.
    - Veiller à un bon fonctionnement du véhicule au début et pendant l'opération de mise à jour logicielle.
    - Vérifier l'intégrité et l'authenticité du progiciel de MJL téléchargé avant l'activation.

- S'appuyer sur une base solide de solutions de cryptographie et de gestion des clés
  - Gestion fiable et flexible de l'ICP
  - Provisionnement sécurisé des clés et des biens sensibles
  - Authentification et autorisation robustes
  - Démarrage sécurisé
  - Signature numérique et vérification des progiciels de MJL

Recommandations pour une vérification de la sécurité agile et fiable

- Recours à des outils d'automatisation des processus assortis d'une supervision humaine
  - Comme exemple, évaluation de l'impact sur la sûreté (et la sécurité), tests et collecte d'artéfacts

  ➔ Ils ne se prêtent pas à une application à grande échelle en l'absence d'une gestion bien établie de la cybersécurité et du cycle de vie de la sécurité

- Une conception et un cycle de vie de développement sécurisés pour éviter les besoins futurs de mise à jour logicielle
  - Réaliser une conception d'architecture sécurisée et robuste contre les menaces connues et prévisibles.
    - Évaluation approfondie des menaces et des risques
    - Principe de défense en profondeur – plusieurs niveaux de contrôles de cybersécurité
  - Vérifier les logiciels, y compris les composants tiers et ouverts, pour éliminer les faiblesses et les vulnérabilités connues.
    - Suivre de bonnes directives de vérification des logiciels, comme celles du NISTIR 8397
    - Utiliser une analyse de composition binaire des logiciels et détecter les vulnérabilités latentes, les fuites de données et les configurations de compilation inappropriées.
  - Prioriser les vulnérabilités à corriger en utilisant une approche fondée sur les risques

- Conception d'une architecture modulaire et indépendante pour éviter que les mises à jour logicielles nuisent à la sécurité fonctionnelle
  - Adopter une conception modulaire et isoler les fonctions critiques de sécurité de la cybersécurité et d'autres fonctions
  - Établir une traçabilité bidirectionnelle entre les exigences, la conception, la mise en œuvre et la vérification pour une évaluation précise de l'impact
  - Amélioration continue : surveiller l'effet des correctifs en recueillant des données sur le terrain

Conclusions – pour une maintenance agile et fiable des logiciels de véhicules

- Mettre en pratique des directives et des normes mondiales actualisées
- Sécurité dès la conception – Évaluation de la menace et des risques, et défense en profondeur
- Sûreté dès la conception – Conception modulaire et isolement de la sûreté et de la sécurité
- Gestion bien établie de la sûreté et de la sécurité du cycle de vie
- Outils automatisés et chaîne d'outils

Thank you

Intelligent Security. Everywhere.