BlackBerry Intelligent Security. Everywhere.

Towards the Future of Vehicle Maintenance:

Safety and Security Considerations for Vehicle Software Updates

Panel - Cybersecurity in the Aftermarket Vehicle Sector
Transport Canada's Vehicle Cyber Security Conference
March. 24, 2022

Takashi Suzuki,
Senior Director, BlackBerry Standards

Agenda

- BlackBerry for Automotive Cybersecurity & Safety
- Regulations and Standards
- Challenges for Aftermarket Vehicle Software Updates
- Recommendations
- Conclusions

BlackBerry for Automotive Cybersecurity and Safety

- 40 years building safety-certified and secure embedded systems used in a variety of mission critical settings including automotive.

- Solid safety and security culture
  - Field-proven safety and security lifecycle management
    - Thorough safety and security analysis
    - Reliable software development and verification based on V-model

- Over 195 million vehicles powered by BlackBerry QNX
  - ASIL B/D pre-certified QNX OS and Hypervisor for Safety -- Micro-kernel & modular architecture design
  - Certicom Key Management Solutions for Automotive -- SW protection & verification by digital signature
  - BlackBerry Jarvis -- Binary composition analysis & security testing solution to uncover SW vulnerabilities
  - BlackBerry QNX OTA -- Customizable secure Over The Air software update solution

Regulations and Standards – Risk based & Lifecycle Approach

- Regulations and Guidance
  - Transport Canada's Vehicle Cyber Security Guidance, Vehicle Cyber Security Strategy, and VCAT
  - UNECE WP.29 GRVA (Working Party on Automated & Connected Vehicle)
    - Regulation 155 – Approval of vehicles with regard to cybersecurity & cybersecurity management system
    - Regulation 156 – Approval of vehicles wrt software update & software update management system
    - Recommendations for Automotive Cyber Security and Software Updates
      - Guidance for the 1998 Contracting Parties -- Technical requirements based on the two regulations above

- Standards
  - ISO/SAE 21434: 2021 -- Vehicle Cybersecurity Engineering Standard
    - Requirements for automotive cybersecurity management and activities to support vehicle lifecycle stages
  - ISO/DIS 24089 -- Vehicle Software Update Engineering Standard (to be published Nov. 2022)
    - Requirements for infrastructure & vehicle design for SW update, package development and update operations
  - ISO 26262:2018 – Road Vehicles - Functional Safety Standard
    - Part 6 defines requirements for safety software lifecycle (architecture, development, verification, integration).

Challenges for Aftermarket Vehicle Software Updates

- Context
  - Rapidly evolving cybersecurity threat landscape (attack tactics & techniques)
  - New vulnerabilities and weakness – can be latent in off-the-shelf components, e.g. open-source software, and your own code
  - Emerging needs for SW updates to prevent adversaries from exploiting them

- Challenges for updating vehicle software
  - Managing cybersecurity & safety risks introduced by software update functions
  - Agile and Reliable safety verification for timely patching of vulnerabilities
    - Safety impact assessment and verification can require time & resources, which can prevent OEMs from performing timely cybersecurity patching.

Recommendations for safe & secure software updates (SU)

- Practice up-to-date guidance and standards
  - Transport Canada's VCAT – Consider SU in each phases, e.g., Risk Assessment
  - WP.29 Recommendation – Section 2.2 (Requirements for SU), Annex Part A (Threats) & B (Mitigation)
  - ISO/SAE 21434 – Threat Analysis & Risk Assessment (Clause 15)
  - ISO 24089 - Manage safety & cybersecurity risks of software update life cycle.
    - Ensure a safe vehicle state at the start of and during the software update operation.
    - Verify the integrity & authenticity of the downloaded SU package before the activation.

- Build on solid foundation of cryptography & key management solutions
  - Trusted and flexible PKI management
  - Secure key and sensitive asset provisioning
  - Strong authentication and authorisation
  - Secure boot
  - Digitally signing and verifying SU packages

Recommendations for agile & reliable safety verification

- Use of tools to automate processes with human oversight
  - For example, safety (& Security) impact assessment, testing and artifact collection
  - ➔ Don't scale well without mature cybersecurity and safety lifecycle management

- Secure Design and Development Lifecycle to avoid future software update needs
  - Achieve secure architecture design robust against known and foreseeable threats.
    - Thorough Threat Analysis and Risk Assessment
    - Defence-in-depth approach – multiple layers of cybersecurity controls
  - Verify software including third party & open-source components to eliminate known weakness and vulnerabilities.
    - Follow a good software testing guidance, e.g., NISTIR 8397
    - Use binary SW composition analysis and detect latent vulnerabilities, leakage of secret and improper build configuration.
  - Prioritize vulnerabilities to patch using risk based approach

- Modular and independent architecture design to avoid software updates from affecting functional safety
  - Adopt modular design and isolate critical safety functions from cybersecurity & other functions
  - Establish bidirectional traceability btw requirements, design, implementation & verification for precise impact assessment
  - Continuous improvement -- monitor the effect of patches by collecting field data

Conclusions - for agile and reliable vehicle software maintenance

- Practice up-to-date global guidance and standards
- Security by design -- TARA and Defence-in-depth
- Safety by design -- Modular design and the isolation of safety & security
- Mature safety and secure life cycle management
- Automated tools and toolchain

Thank you

BlackBerry Intelligent Security. Everywhere.