Summary of Discussions on Vehicle Cybersecurity and Software Updates at the World Forum for Harmonization of Vehicle Regulations (WP.29)

Tetsuya Niikuni
UNECE WP.29 GRVA/CSTF Co-Chair
National Traffic Safety and Environment Laboratory

Hideo Himeno
Japan Automobile Standards Internationalization Center (JASIC)

1. Introduction

In December 2016, the United Nations World Forum for Harmonization of Vehicle Regulations (UNECE/WP.29) established the UN Task Force on Cyber security and OTA (Over-The-Air, i.e., wireless update) issues (abbreviated to TFCS) in order to identify security issues pertaining to vehicles. Currently (as of November 2018), discussions are being held to draft internationally harmonized regulations relating to vehicle cybersecurity and software updates. The results of these discussions have been compiled into a proposal document for the Working Party on Automated/Autonomous and Connected Vehicles (GRVA), which is the parent body of TFCS. This document presents an outline of the discussions in TFCS, focusing on the contents of this proposal document.

2. Proposal document on vehicle cyber security

The proposal document on vehicle cyber security covers two main topics.

- Guidance on vehicle cyber security
- A draft regulation for the application of cyber security to vehicles

These topics are discussed below.

2.1 Guidance on vehicle cyber security

The document offers guidance for vehicle manufacturers, and summarizes the measures and principles that they should adopt during vehicle development to ensure that data and information related to the control of vehicles cannot be misappropriated. Its contents are mainly concerned with security measures that are considered to be necessary for ensuring vehicle safety.

● Principles of cyber security

The principles of cyber security indicate the cyber security measures that vehicle manufacturers should systematically implement at each stage of the vehicle life cycle (development, design, manufacture, use, etc.).

Principles relating to organizational requirements:

- Ensure that security is ingrained into an organization by establishing a system where security is managed and promoted at the highest echelons (where decisions can be made that permeate through the entire organization)
- Create a system that can continuously monitor cyber security throughout the organization
- Create a mechanism that maintains security throughout the organization, including related suppliers and service providers

Principles relating to vehicles:

- In structures built to store and communicate data (e.g., in-vehicle network equipment), vehicle manufacturers must adopt designs such that improper operation of one component cannot affect the whole system or any other part thereof
- Consider software security over the life of the vehicle
- Consider the security aspects of data storage and transfer
- Vehicle manufacturers should evaluate security functionality by carrying out testing, etc.
- Vehicle manufacturers should design their vehicles to cope with unauthorized use of data, etc.
- Vehicle manufacturers should design vehicles that can detect and respond to unauthorized use of data

The above requirements constitute guidance that vehicle manufacturers should reflect as much as possible in the development of vehicles.

2.2 Draft regulation for the application of cyber security to vehicles

A characteristic of the proposal document is the proposal that an authorizing body should certify the extent to which vehicle manufacturers adhere to the requirements shown in the guidance presented in section 2.1. An overview of the draft provision

relating to this proposed regulation is presented below.

Envisaged applications and scope of the proposed regulation:

The concept of a Cyber Security Management System (CSMS) is defined for activities related to vehicles and their development. Instead of regulating the manufactured products (vehicles, components and systems) themselves, a CSMS consists of rules to guide the actions of vehicle manufacturers and other organizations, and mechanisms whereby these rules are implemented. The organizations targeted by a CSMS include not only vehicle manufacturers but also other organizations in their supply chain.

Structure of the proposed regulation:

The authorizing body issues approvals after confirming that the cyber security requirements indicated in the proposed draft regulation have been properly implemented by the vehicle manufacturing organization in question. For this reason, vehicle types are only approved after the vehicle manufacturer has obtained a certificate demonstrating that CSMS certification has been achieved.

Vehicle type certification:

To obtain approval for a vehicle type, the vehicle manufacturer must first demonstrate to the authorizing body that the requirements certified by a valid CSMS certificate have been applied to the vehicle type requiring certification.

An outline of the proposal document including the draft cyber security regulation proposed by TFCS has been described above. A characteristic of this proposal document is that instead of the requirements shown in the guidance in their own right, it proposes a draft regulation that includes rules for checks by the authorizing body as to whether vehicle manufacturers are complying with the requirements. This makes it unnecessary to make frequent alternations to the regulation in order to keep up with rapid advances in information technology. Also, since it does not specify any specific technology (e.g., a specific encryption algorithm) as a regulation, it does not expose any attack targets.

3. Proposal document on vehicle software updates

Like the proposal document on vehicle cyber security, the proposal document on software updates covers two main topics.

- Guidance on vehicle software updates
- A draft regulation for implementing vehicle software updates

These topics are discussed below.

3.1 Guidance on vehicle software updates

The following requirements have mainly been proposed for vehicle safety.

- If a software download is interrupted (e.g., due to a break in communication), it should still be possible to start the system in the state it was in before the transfer started.
- Before installing the downloaded software, the driver should be notified about what has been updated.
- If the process of installing an update places restrictions on the operation of functions controlled by the software, especially functions related to vehicle safety, then the vehicle must be made inoperable during this installation process.
- The vehicle manufacturer must inform the user about the success or failure of the update, and must also ensure that the details of any functional changes caused by the update are notified to the user and reflected in the instruction manual (the manner in which instruction manuals are to be updated is not specified in this proposal).

About OTA updates (over-the-air wireless updates):

OTA updates must comply with the following requirements.

- For updates that require additional actions by the user (e.g., tasks that requires an operation other than driving), the running of OTA updates while driving must be prohibited.
- If the completion of an OTA update requires any work to be carried out by an engineer with specialist knowledge (that an ordinary vehicle user does not have), then the vehicle manufacturer must ensure that the OTA update is completed by a suitably skilled engineer.

3.2 Draft regulation for implementing vehicle software updates

Like the proposed regulation on vehicle cyber security, this document proposes a mechanism whereby the vehicle manufacturer's systematic software update process is implemented by a mechanism that can be checked by a certifying authority. An overview of the draft provision relating to this proposed regulation is as follows.

Envisaged applications and scope of the proposed regulation:

The concept of a software update management system

(SUMS) is defined with respect to the software update mechanism for vehicles. SUMS itself does not specify manufactured products (vehicles, parts or systems), but represents a set of rules that apply to actions performed by a vehicle manufacturer or other organization for software updates and a mechanism for implementing these rules. The organizations targeted by a SUMS include not only vehicle manufacturers but also other organizations in their supply chains and the like. A vehicle manufacturer must demonstrate how it has configured SUMS in order to implement the guidelines shown in section 3.1. In the draft regulation proposed by TFCS, SUMS certification is essential for approval of a vehicle type.

Vehicle type certification:

To gain approval for a vehicle type, the vehicle manufacturer must first demonstrate to the authorizing body that the requirements certified by a valid SUMS certificate have been applied to the vehicle type in question. In particular, the manufacturer must demonstrate to the authorizing body that the vehicle will be developed, designed and produced based on the manufacturer's SUMS, and that compatibility with this SUMS can be maintained during the use phase.

4. Definition of software reference number

To make the software update process transparent, TFCS studied a method that matches the software installed in vehicles with approvals issued by the authorizing body. This study proposes the idea of defining a RxSWIN (Regulation x Software Identification Number) as number that aggregates the version information of software installed on the in-vehicle systems of approved vehicle types (including multiple software packages when a system comprises multiple units, each with its own software). Operational rules such as version control of software to be updated using RxSWIN can be set by individual vehicle manufacturers for each system.

5. Conclusion

An outline of the proposed regulation for vehicle security and software updates (including OTA) was presented at the United Nations World Forum for Harmonization of Vehicle Regulations (UNECE/WP. 29). As of October 2018, GRVA member countries are reviewing this proposal, and its contents will be discussed at the second GRVA meeting scheduled to be held in January 2019.

Cover Art

Bijinga (Picture of beautiful women).

Utagawa Toyokuni (1769-1825)

Collection of the Art Research Center (ARC)
Ritsumeikan University
Object number: arcUP0029