UN Regulation 155

20210638 최무송

UN Regulation 155

- Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

- 사이버 보안 및 사이버 보안 관리 시스템과 관련된 차량 승인에 관한 통일된 규정

- 12 Paragraph and 5 Annex

대상

UNECE WP.29 R155, R156 규제를 적용 받는 국가에 차량을 판매하는 제조사

적용 국가

EU 27개 회원국, 영국, EFTA 국가(스위스, 노르웨이,아이슬랜드,리히텐슈타인) 등

정의

정부 인증 기관(TAA)이 지정한 공식 기술 서비스 기관 (TS)

역할

R155/R156 인증 심사 활동, VTA 인증 평가 활동

특징

인증에 필요한 모든 심사 및 평가를 수행한 후 그 결과를 TAA에 보고

대상

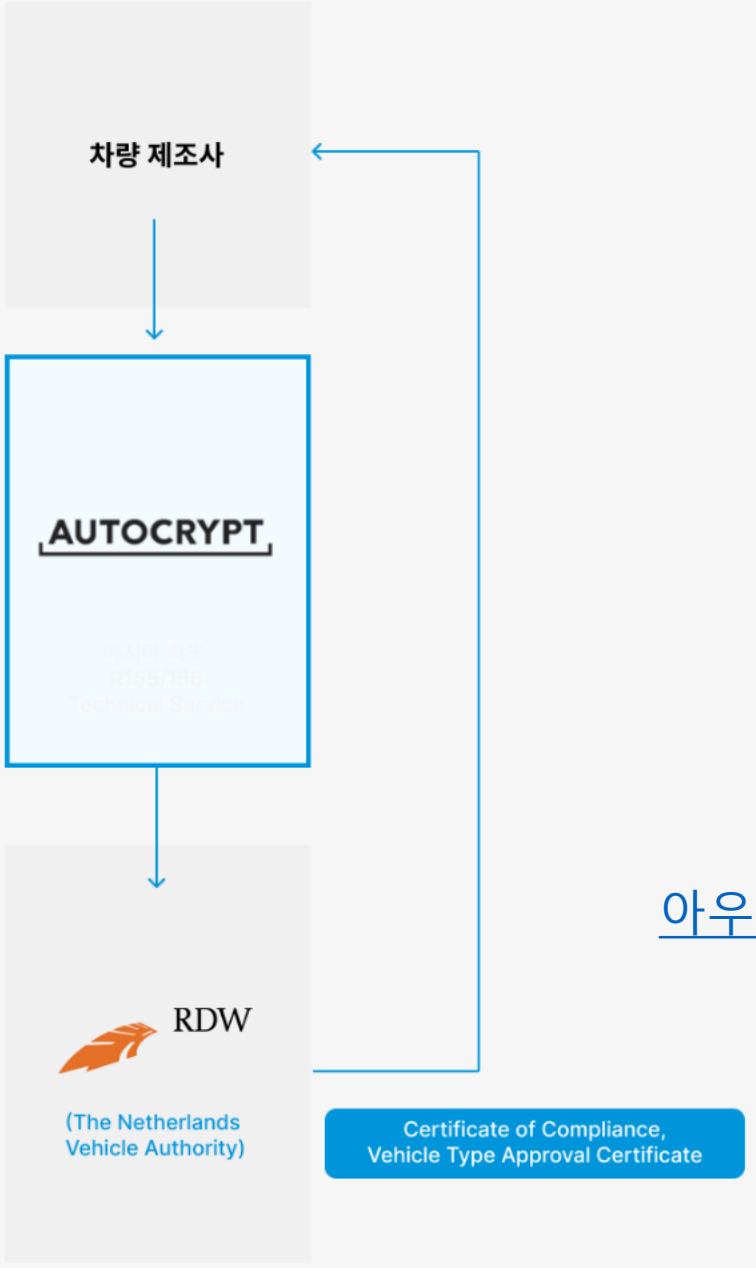
UNECE WP.29 R155, R156 규제를 적용 받는 국가에 차량을 판매하는 제조사

역할

R155/R156 인증서 발행, VTA 인증서 발행

특징

정부기관으로서 공신력이 있는 인증서 발행



[아우토크립트 | UN R155/R156]

Key points

- Cyber Security Management System

- 7.3 Requirements for vehicle types

- Annex 5 Table A

Defininion of CSMS (2.3)

- "Cyber Security Management System (CSMS)" means a systematic risk-based approach defining organisational processes, responsibilities and governance to treat risk associated with cyber threats to vehicles and protect them from cyber attacks.

- "사이버 보안 관리 시스템(CSMS)"은 차량에 대한 사이버 위협과 관련된 위험을 처리하고 사이버 공격으로부터 이를 보호하기 위한 조직적 프로세스, 책임 및 거버넌스를 정의하는 체계적인 위험 기반 접근 방식을 의미합니다.

- cf. SUMS - Software update management system (UN Regulation 156)

What to implement (7.3.7)

- The vehicle manufacturer shall implement measures for the vehicle type to:
  - (a) Detect and prevent cyber-attacks against vehicles of the vehicle type;
  - (b) Support the monitoring capability of the vehicle manufacturer with regards to detecting threats, vulnerabilities and cyber-attacks relevant to the vehicle type;
  - (c) Provide data forensic capability to enable analysis of attempted or successful cyber-attacks.

Exhaustive risk assessment (7.3.3)

- The vehicle manufacturer shall identify the critical elements of the vehicle type and perform an exhaustive risk assessment for the vehicle type and shall treat/manage the identified risks appropriately. The risk assessment shall consider the individual elements of the vehicle type and their interactions. The risk assessment shall further consider interactions with any external systems. While assessing the risks, the vehicle manufacturer shall consider the risks related to all the threats referred to in Annex 5, Part A, as well as any other relevant risk.

Mitigations (7.3.4)

- The vehicle manufacturer shall protect the vehicle type against risks identified in the vehicle manufacturer's risk assessment. Proportionate mitigations shall be implemented to protect the vehicle type. The mitigations implemented shall include all mitigations referred to in Annex 5, Part B and C which are relevant for the risks identified. However, if a mitigation referred to in Annex 5, Part B or C, is not relevant or not sufficient for the risk identified, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented.

Annex 5 Table A

- High level descriptions of threats and relating vulnerability or attack method are listed.

- Ex) Spoofing of messages or data received by the vehicle → Spoofing of messages, Sybil attack

Annex 5 Table B/C

- Mitigations to the threats intended for vehicles are listed in Table B.
- Mitigations to the threats outside of vehicles are listed in Table C.
- Comprehensive expressions are used rather than explicitly suggesting a solution.

Threats regarding back-end servers related to vehicles in the field

Back-end servers used as a means to attack a vehicle or extract data	Abuse of privileges by staff (insider attack)
	Unauthorized internet access to the server (backdoors, unpatched system software vulnerabilities, SQL attacks or other means)
	Unauthorized physical access to the server (USB sticks or other media connecting to the server)
Services from back-end server being disrupted, affecting the operation of a vehicle	Attack on back-end server stops it functioning, for example it prevents it from interacting with vehicles and providing services they rely on
Vehicle related data held on back-end servers being lost or compromised ("data breach")	Abuse of privileges by staff (insider attack)
	Loss of information in the cloud. Sensitive data may be lost due to attacks or accidents when data is stored by third-party cloud service providers
	Unauthorized internet access to the server (backdoors, unpatched system software vulnerabilities, SQL attacks or other means)
	Unauthorized physical access to the server (USB sticks or other media connecting to the server)
	Information breach by unintended sharing of data (e.g. admin errors)

Threats to vehicles regarding their communication channels

Spoofing of messages or data received by the vehicle	**Spoofing of messages** by impersonation (e.g. 802.11p V2X during platooning, GNSS messages, etc.)
	Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road)
Communication channels used to conduct unauthorized manipulation, deletion or other amendments to vehicle held code/data	Communications channels permit **code injection**, for example tampered software binary might be injected into the communication stream
	Communications channels permit **manipulate/overwrite/erasure** of vehicle held data/code
	Communications channels permit introduction of data/code to the vehicle (write data code)
Communication channels permit untrusted/unreliable messages to be accepted or are vulnerable to session hijacking/replay attacks	Accepting information from an **unreliable or untrusted source**
	Man in the middle attack/ session hijacking
	Replay attack, for example an attack against a communication gateway allows the attacker to downgrade software of an ECU or firmware of the gateway
Information can be readily disclosed. For example, through eavesdropping on communications or through allowing unauthorized access to sensitive files or folders	**Interception of information** / interfering radiations / monitoring communications
	Gaining **unauthorized access** to files or data

Threats to vehicles regarding their communication channels

Denial of service attacks via communication channels to disrupt vehicle functions	**Sending** a large number of garbage **data** to vehicle information system, **so that it is unable to provide services** in the normal manner
	Black hole attack, in order to disrupt communication between vehicles the attacker is able to block messages between the vehicles
An unprivileged user is able to gain privileged access to vehicle systems	An unprivileged user is able to **gain privileged access**, for example root access
Viruses embedded in communication media are able to infect vehicle systems	**Virus** embedded in communication media infects vehicle systems
Messages received by the vehicle (for example X2V or diagnostic messages), or transmitted within it, contain malicious content	**Malicious** internal (e.g. CAN) **messages**
	Malicious **V2X messages**, e.g. infrastructure to vehicle or vehicle-vehicle messages (e.g. CAM, DENM)
	Malicious diagnostic messages
	Malicious **proprietary messages** (e.g. those normally sent from OEM or component/system/function supplier)

Threats to vehicles regarding their update procedures

Misuse or compromise of update procedures	Compromise of over the air software update procedures. This includes fabricating the system update program or firmware
	Compromise of local/physical software update procedures. This includes fabricating the system update program or firmware
	The software is manipulated before the update process (and is therefore corrupted), although the update process is intact
	Compromise of cryptographic keys of the software provider to allow invalid update
It is possible to deny legitimate updates	Denial of Service attack against update server or network to prevent rollout of critical software updates and/or unlock of customer specific features

Threats to vehicles regarding unintended human actions facilitating a cyber attack

Legitimate actors are able to take actions that would unwittingly facilitate a cyber attack	Innocent victim (e.g. owner, operator or maintenance engineer) being tricked into taking an action to unintentionally load malware or enable an attack
	Defined security procedures are not followed

Threats to vehicles regarding their external connectivity and connections

Manipulation of the connectivity of vehicle functions enables a cyber attack, this can include telematics; systems that permit remote operations; and systems using short range wireless communications	Manipulation of **functions designed to remotely operate systems**, such as remote key, immobilizer, and charging pile
	Manipulation of vehicle telematics (e.g. manipulate temperature measurement of sensitive goods, remotely unlock cargo doors)
	Interference with **short range wireless systems** or sensors
Hosted 3rd party software, e.g. entertainment applications, used as a means to attack vehicle systems	**Corrupted applications**, or those with poor software security, used as a method to attack vehicle systems
Devices connected to external interfaces e.g. USB ports, OBD port, used as a means to attack vehicle systems	**External interfaces** such as USB or other ports used as a point of attack, for example through code injection
	Media infected with a **virus** connected to a vehicle system
	Diagnostic access (e.g. dongles in OBD port) used to facilitate an attack, e.g. manipulate vehicle parameters (directly or indirectly)

Threats to vehicle data/code

Extraction of vehicle data/code	Extraction of copyright or proprietary software from vehicle systems (product **piracy**)
	Unauthorized access to the **owner's privacy information** such as personal identity, payment account information, address book information, location information, vehicle's electronic ID, etc.
	Extraction of cryptographic keys
Manipulation of vehicle data/code	Illegal/unauthorized changes to **vehicle's electronic ID**
	Identity fraud. For example, if a user wants to display another identity when communicating with toll systems, manufacturer backend
	Action to **circumvent monitoring systems** (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs)
	Data manipulation to **falsify vehicle's driving data** (e.g. mileage, driving speed, driving directions, etc.)
	Unauthorized changes to **system diagnostic data**

Threats to vehicle data/code

Erasure of data/code	Unauthorized deletion/manipulation of **system event logs**
Introduction of malware	Introduce **malicious software** or malicious software activity
Introduction of new software or overwrite existing software	**Fabrication of software** of the vehicle control system or information system
Disruption of systems or operations	**Denial of service**, for example this may be triggered on the internal network by flooding a CAN bus, or by provoking faults on an ECU via a high rate of messaging
Manipulation of vehicle parameters	Unauthorized access of **falsify the configuration parameters** of vehicle's key functions, such as brake data, airbag deployed threshold, etc.
	Unauthorized access of **falsify the charging parameters**, such as charging voltage, charging power, battery temperature, etc.

Potential vulnerabilities that could be exploited if not sufficiently protected or hardened

Cryptographic technologies can be compromised or are insufficiently applied	Combination of short **encryption keys** and long period of validity enables attacker to break encryption
	Insufficient use of cryptographic algorithms to protect sensitive systems
	Using already or soon to be deprecated **cryptographic algorithms**
Parts or supplies could be compromised to permit vehicles to be attacked	**Hardware or software, engineered to enable an attack** or fails to meet design criteria to stop an attack
Software or hardware development permits vulnerabilities	**Software bugs**. The presence of software bugs can be a basis for potential exploitable vulnerabilities. This is particularly true if software has not been tested to verify that known bad code/bugs is not present and reduce the risk of unknown bad code/bugs being present
	Using remainders from development (e.g. debug ports, JTAG ports, microprocessors, development certificates, developer passwords, …) can permit access to ECUs or permit attackers to gain higher privileges
Network design introduces vulnerabilities	**Superfluous internet ports** left open, providing access to network systems
	Circumvent **network separation** to gain control. Specific example is the use of unprotected gateways, or access points (such as truck-trailer gateways), to circumvent protections and gain access to other network segments to perform malicious acts, such as sending arbitrary CAN bus messages
Unintended transfer of data can occur	Information breach. Personal data may be leaked when the **car changes user** (e.g. is sold or is used as hire vehicle with new hirers)
Physical manipulation of systems can enable an attack	**Manipulation of electronic hardware**, e.g. unauthorized electronic hardware added to a vehicle to enable "man-in-the-middle" attack **Replacement of authorized electronic hardware** (e.g., sensors) with unauthorized electronic hardware **Manipulation of the information** collected by a sensor (for example, using a magnet to tamper with the Hall effect sensor connected to the gearbox)