TTA Standard

정보통신단체표준(국문표준)

TTAx.xx-xx.xxxx/R1 제정일: 2018년 12월 xx일

클라우드 커넥티드 자동차 보안 요구사항

Security Requirements for Cloud Connected Vehicle

표준초안 검토 위원회 응용보안/평가인증 프로젝트그룹(PG504)

표준안 심의 위원회 정보보호 기술위원회(TC5)

	성명	소 속	직위	위원회 및 직위	표준번호
표준(과제) 제안	권혁찬	한국전자통신연구원	책임연구원	PG505 위원	
표준 초안 작성자	이석준	한국전자통신연구원	책임연구원	PG505 위원	
	권혁찬	한국전자통신연구원	책임연구원	PG505 위원	
사무국 담당	김재웅	TTA	단장		
	문서연	TTA	전임		

본 표준 발간 이전에 접수된 지식재산권 확약서 정보는 본 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 2018.12
Tel : 02-3454-1901, Fax : 02-3454-1902

서 문

1 표준의 목적

이 표준은 클라우드와 자동차간 연계를 위해 표준 기반으로 또는 자체적으로 서비스 개발 시 고려해야할 보안 위협과 이에 대응하기 위한 보안 요구사항을 정의한다.

2 주요 내용 요약

이 표준은 클라우드 연계 자동차의 구조를 소개하고, 보안 위협 및 이에 대응하기 위한 보안요구사항을 정의한다. 보안 요구사항은 인증, 플랫폼(온보드/오프보드 장치 및 클라우드) 보안, 네트워크 보안 및 침해대응, 개인정보보호, 감사 및 보안관리 요구사항으로 분류하여 정의한다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

해당 사항 없음

3.2 인용 표준과 본 표준의 비교표

해당 사항 없음

Preface

1 Purpose

Recently, international standards for providing cloud-based automotive services have been developed in ISO TC22 SC31, 3GPP and GENIVI alliances. This standard defines security threats and requirements to consider when developing cloud-based automotive service.

2 Summary

This standard introduces the structure of cloud-connected vehicle, and analyzes the security threats and security requirements to counter them. Security requirements are defined for authentication, platform security, network security & intrusion prevention, auditing & security management and privacy protection.

3 Relationship to Reference Standards

None

목 차

클라우드 커넥티드 자동차 보안 요구사항
(Security Requirements for Cloud Connected Vehicle)

1 적용 범위

이 표준은 클라우드 커넥티드 자동차 서비스를 위한 보안 요구사항을 정의한다. 클라우드 커넥티드 자동차는 클라우드와 연계하여 서비스를 제공하는 자동차를 말한다. 현재, ISO TC22(도로 차량) SC31(데이터 통신) WG6(워킹그룹 6), 3GPP, GENIVI 등에서 클라우드 기반 자동차 서비스를 위해 차량데이터의 클라우드 전송을 위한 표준이 개발되고 있다. 이 표준은 상기의 클라우드 차량 연계 표준을 적용하거나 또는 자체적인 서비스 개발시 보안 요구사항 도출을 위한 목적으로 활용이 가능하다.

이 표준은 커넥티드 자동차와 클라우드 연계 과정에서의 보안 위협과 요구사항 도출을 대상으로 하며 일반적인 클라우드 서비스 및 도로·교통 인프라와 관련된 위협 및 요구사항은 포함하지 않는다.

이 표준은 C-ITS, 자율주행, 차량 위협탐지/대응, 카쉐어링 등 클라우드 기반의 다양한 형태의 자동차 서비스 등 다양한 서비스 분야에 적용이 가능하다.

2 인용 표준

해당사항 없음

3 용어 정의

3.1 지능형 교통 체계 (ITS, Intelligent Transport Systems)

교통수단 및 교통 시설에 전자·제어 및 통신 등 첨단 기술을 접목하여 교통 정보 및 서비스를 제공하고 이를 활용함으로써 교통 체계의 운영 및 관리를 과학화·자동화하고, 교통의 효율성과 안전성을 향상시키는 교통 체계. 버스 정류장의 버스 도착 안내 시스템, 교차로에서 교통량에 따라 자동으로 차량 신호가 바뀌는 시스템, 내비게이션의 실시간 교통 정보, 하이패스 등이 ITS 서비스이다. ITS국가교통정보센터는 ITS 서비스 분야를 교통 관리, 대중 교통, 전자 지불, 교통 정보 유통, 여행 정보 제공, 지능형 차량·도로, 화물 운송 7개 분야로 나누어 개발한다. ITS 이용으로, 물류비, 시설 유지 관리, 에너지 등을 절감하여 경제력이 강화되고, 교통 혼잡과 사고를 예방하여 교통안전이 개선된다.

3.2 협력·지능형 교통 체계 (C-ITS, Cooperative Intelligent Transport Systems)

차량과 차량, 차량과 인프라 등 유무선 통신을 통하여 정보를 주고 받는 차량·사물 통신(V2X: Vehicle to Everything) 기술을 이용하여 서로 협력하는 지능형 교통 체계(ITS). C-ITS는 V2X 기술을 기반으로 하여 도로, 차량, 운전자 간의 관련성이 보다 긴밀해진다. 차량은 주행 중 다른 차량에서 직접 정보를 수신하거나 노변의 기지국이나 CCTV를 통해 주변 교통 상황, 급정거, 낙하물 등 정보를 실시간으로 확인할 수 있다. C-ITS는 2009년부터 유럽에서 사용된 용어이며, 미국에서는 커넥티드 비히클(connected vehicle), 일본에서는 아이티에스 스폿(ITS spot)이라 불리기도 한다.

[출처(3.1~3.2)] TTA 정보통신용어사전

3.3 텔레매틱스 제어 유닛 (TCU, Telematics Control Unit)

텔레매틱스 서비스를 제공하기 위해 GPS, 와이파이, 블루투스, 셀룰러 등의 통신 모듈이 탑재된 임베디드 장치

3.4 ITS Station

차량에 탑재되는 차량 간 통신용 모듈. OBU와 동일한 용어

3.5 IVI (In-Vehicle Infotainment, 차량용 인포테인먼트)

차량용 엔터테인먼트, 네비게이션, 유무선 연결 장치(와이파이, 블루투스, USB 등)을 포함한 자동차의 헤드유닛 장치

3.6 OBD (On-Board Diagnostics)

자동차의 온보드 진단 및 보고 기능을 나타내는 용어. 최신의 OBD는 표준화된 디지털 통신 포트를 사용하여 표준화된 진단 문제 코드 및 실시간 데이터를 제공

3.7 OBU (On-Board Unit)

차량에 탑재되는 차량 간 통신용 모듈. ITS Station과 동일한 용어

3.8 RSU (Road Side Unit)

노변에 설치되는 차량 간 통신을 위한 기지국

[출처(3.7~3.8)] TTAK.KO-12.0238, 차량 간 통신 보안 요구 사항

3.9 V2X (Vehicle-to-everything, 차량·사물 통신)

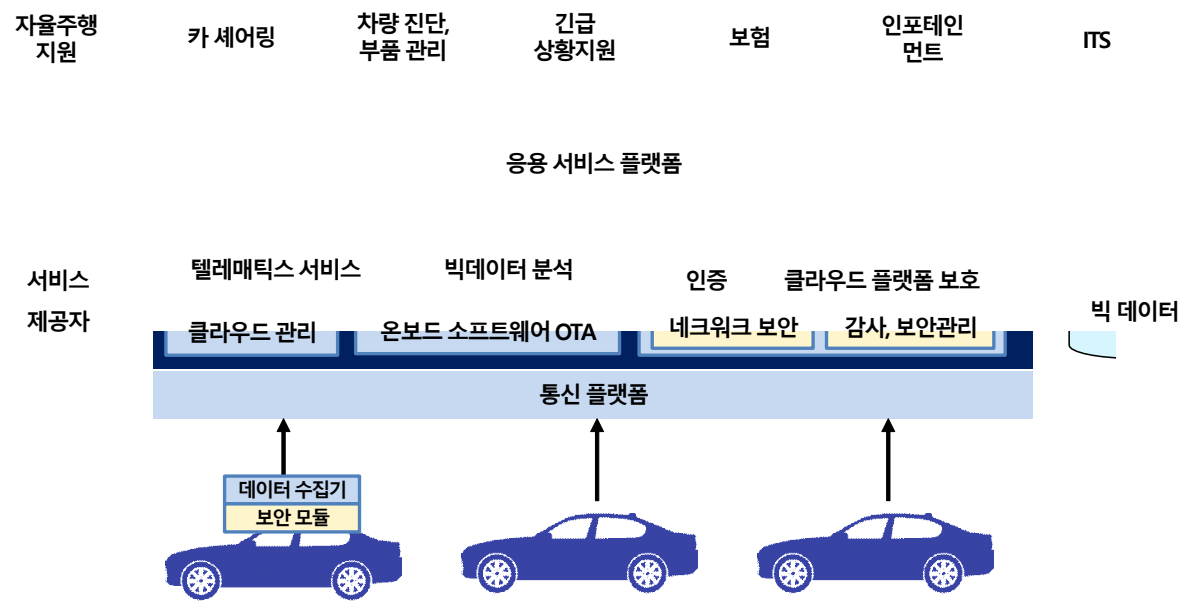
자동차를 중심으로 통신망을 이용하여 통신을 하는 기술. 자동차와 자동차 사이의 무선 통신, 자동차와 인프라 간의 무선 통신 등이 포함됨

4 약어

AVN	Audio, Video and Navigation
DDoS	Distributed Denial of Service
HSM	Hardware Security Module
ITS	Intelligent Transport Systems
IVI	In-Vehicle Infotainment
IVN	In-Vehicle Network
OBD	On-Board Diagnostics
OBU	On-Board Unit
OTA	Over-The-Air
RSU	Road Side Unit
TCU	Telematics Control Unit
V2X	Vehicle to Everything
WAVE	Wireless Access in Vehicular Environments
WPA2	Wi-Fi Protected Access 2

5 클라우드 커넥티드 자동차

5.1 클라우드 커넥티드 자동차 개요



(그림 5-1) 클라우드 커넥티드 자동차 구조 (예)

클라우드 커넥티드 자동차 구조의 예는 (그림 5-1)과 같다. 자동차의 데이터를 클라우드로 전송하기 위해 사용하는 통신 프로토콜, 구조 및 방식은 5.2절에 기술된다.

일반적으로 자동차용 클라우드 서버는 자동차의 데이터를 수집 및 분석하고 그 결과를 다양한 서비스에 활용 가능한 응용 서비스 플랫폼, 다수의 차량과의 통신을 지원하는 통신 플랫폼 및 보안 플랫폼을 제공한다. 클라우드에 탑재되는 기본 기능으로는 일반적으로 빅데이터 분석, 클라우드 관리, 텔레매틱스, 온보드 소프트웨어 원격 업데이트 등과 보안 기능으로 인증, 클라우드 플랫폼 보호, 감사 및 보안관리, 네트워크 보안 및 침해대응 등이 있다.

자동차는 데이터를 수집하는 장치와 수집한 데이터를 보호하고 클라우드로 안전하게 전송하기 위한 보안 모듈이 탑재된다. 클라우드 전송과정에는 다양한 온보드, 오프보드 장치가 사용될 수 있으며 상세 내용은 5.2절에 기술되어 있다.

자동차 클라우드를 통한 서비스로는 자율주행 지원, 자동차의 부품 진단/관리, 긴급 상황지원, 운전성향 분석 등을 통한 보험 서비스, 오디오/비디오 등 멀티미디어 서비스, 카쉐어링 등 다양하다. 그 외에 지능형 교통 서비스(ITS) 제공을 위해 자동차의 정보 외에 자동차간 통신 정보를 수집 분석하는 서비스도 가능하다.

5.2 자동차-클라우드 연결 구조

이 절에서는 자동차와 클라우드 연결 방식을 표준 어댑터 기반 연결(그림 5-2의 ①~③), 온보드 장치 및 애플리케이션 기반 연결(그림 5-2의 ④~⑧) 및 표준 서버 인터페이스 기반 연결(그림 5-2의 ⑨) 방식으로 분류하여 정의한다.

	온보드 장치	네트워크 I/F	오프보드 장치			9 표준 IF	클라우드	
				3rd party 서버				
1	OBD 컨트롤러	OBD 포트	OBD 동글	Bluetooth	모바일 단말 (G/W)		Cellular, Wi-Fi	사용자
2	OBD 컨트롤러	OBD 포트	OBD 동글	Wi-Fi	모바일 단말 (G/W)		Cellular	
3	OBU 장치 (ITS Station)	USB 포트 등	ITS 커넥터				Cellular	
4	텔레매틱스 제어 유닛 (TCU)	이동통신 모듈					Cellular	
5	IVI (헤드유닛 /AVN)	이동통신 모듈 와이파이 모듈					Cellular, Wi-Fi	
6	IVI (헤드유닛 /AVN)	와이파이 모듈		Wi-Fi	모바일 단말		Cellular	
7	OBU 장치 (ITS Station)	WAVE 모듈		WAVE	도로기지국 (RSU) (G/W)		Wired	
8	OBU 장치 (ITS Station)	이동통신 모듈					Cellular	

(그림 5-2) 자동차-클라우드 연결 구조

5.2.1 표준 어댑터 기반 연결 구조

표준 어댑터 기반 연결구조(그림 5-2의 ①~③)는 OBD 컨트롤러, OBU 등 차량의 온보드 장치에 표준화된 어댑터(OBD 동글, ITS 커넥터 등)를 장착하여 차량의 데이터를 클라우드로 전송하는 구조이다.

가. (그림 5-2의 ①) 차량의 OBD 포트에 블루투스 통신 모듈이 장착된 어댑터/커넥터(예: OBD 동글)를 연결하여 차량의 데이터를 클라우드로 전송하는 구조이다. 수집한 자동차의 데이터를 클라우드로 전송하기 위해 사용자 단말(스마트폰, 랩톱 등)이 게이트웨이 역할을 수행한다. 어댑터와 사용자 단말 구간은 블루투스 통신으로 데이터를 전송하고, 사용자 단말과 클라우드 간에는 와이파이 또는 이동통신망을 이용하여

데이터를 송수신한다.

나. (그림 5-2의 ②) 차량의 OBD 포트에 와이파이 통신 모듈이 장착된 어댑터/커넥터(예: OBD 동글)를 연결하여 차량의 데이터를 클라우드로 전송하는 구조이다. 수집한 자동차의 데이터를 클라우드로 전송하기 위해 사용자 단말(스마트폰, 랩톱 등)이 게이트웨이 역할을 수행한다. 어댑터와 사용자 단말 구간은 와이파이 통신으로 데이터를 전송하고, 사용자 단말과 클라우드 간에는 와이파이 또는 이동통신망을 이용하여 데이터를 송수신하는 구조이다. 어댑터와 사용자 단말간의 와이파이 통신을 위한 일반적으로 사용자 단말의 테더링 기능을 사용한다.

다. (그림 5-2의 ③) V2X 통신을 위한 OBU 단말에 셀룰러 통신 모듈이 장착된 어댑터/커넥터(예: ITS 커넥터)를 장착하여 차량의 데이터를 클라우드로 전송하는 구조이다.

5.2.2 온보드 장치 및 애플리케이션 기반 연결

온보드 장치 및 애플리케이션 기반 연결 구조(그림 5-2의 ④~⑧)는 차량에 탑재된 온보드 장치 및 클라우드 연동 애플리케이션을 통해 차량의 데이터를 클라우드로 전송하는 방식이다. 이 구조에서 온보드 장치는 IVI 장치(헤드유닛, AVN, 인포테인먼트 시스템 등), V2X 통신을 위한 OBU 등이 포함된다.

가. (그림 5-2의 ④) 자동차의 텔레매틱스 제어 유닛(TCU)이 수집한 자동차 데이터를 셀룰러 통신을 이용하여 클라우드로 직접 전송하는 방식이다. 이 경우 텔레매틱스 제어 유닛은 클라우드 연동을 위한 애플리케이션이 탑재되어 있어야 한다.

나. (그림 5-2의 ⑤) 자동차의 IVI 장치가 셀룰러 또는 와이파이 통신을 이용하여 수집한 자동차 데이터를 클라우드로 직접 전송하는 방식이다. 이 경우 IVI장치에는 클라우드 연동을 위한 애플리케이션이 탑재되어 있어야 한다.

다. (그림 5-2의 ⑥) 사용자 단말(스마트폰, 랩톱 등)이 자동차의 IVI 장치와 클라우드 사이의 게이트웨이 역할을 하는 구조이다. IVI 장치는 자동차의 데이터를 사용자 단말로 와이파이 등을 이용하여 전송하고, 사용자 단말은 이동통신망을 이용하여 그 데이터를 클라우드로 전달하는 방식이다.

라. (그림 5-2의 ⑦) V2X 통신을 위한 OBU 단말(ITS station)이 웨이브(WAVE) 통신을 이용하여 RSU로 자동차의 데이터를 전송하고, RSU가 게이트웨이 역할을 하여 클라우드로 데이터를 전달하는 방식이다. 이 경우 OBU 장치에는 클라우드 연동을 위한 애플리케이션이 탑재되어 있어야 한다.

마. (그림 5-2의 ⑧) 셀룰러 모뎀이 장착된 V2X OBU 단말이 이동통신망을 이용하여 자

동차의 데이터를 직접 클라우드로 전송하는 방식이다. 이 경우 OBU 장치에는 클라우드 연동을 위한 애플리케이션이 탑재되어 있어야 한다.

5.2.3 표준 서버 인터페이스 기반 연결

표준 서버 인터페이스 기반 연결 구조에서는 자동차의 데이터를 수집하여 관리하는 백엔드 서버는 자동차 제작사 등에서 관리하고 제3의 기관에서 차량의 데이터를 분석할 수 있도록 표준화된 인터페이스를 제공하는 구조이다. 예를 들어 자동차 제작사에서 차량 진단 서비스를 제공하는 제3의 기관에게는 진단용 데이터만을 공유하며, 보안 위협 분석 기관에게는 위협 분석에 필요한 데이터만을 공유하는 방식이다. ISO TC22 SC31의 확장형 자동차(Extended vehicle) 표준에서 개발하고 있는 인터페이스 표준이 이 구조에 적용 가능하다. 확장형 자동차 표준의 경우, 자동차 제작사의 백엔드 서버와 외부 클라우드 간에는 웹 인터페이스형태의 API를 제공하는 구조를 갖는다. 차량 데이터의 프라이버시 및 소유권을 중요하게 여기는 자동차 제작사 입장에서 상대적으로 선호하는 구조이다.

가. (그림 5-2의 ⑨) 자동차 데이터를 수집/관리하는 1차 클라우드 서버에서 제공하는 표준화된 서버 인터페이스를 통해 제3의 기관의 2차 클라우드로 데이터를 공유하는 방식이다. 자동차에서 1차 클라우드까지의 데이터 전송방식은 그림 5-2의 ①~⑧번 구조가 모두 가능하다. 1차 클라우드에서는 2차 클라우드의 목적(진단, 위험 분석, 보험서비스 등)에 따라 필요한 데이터만 공유할 수 있다. 예를 들어 확장형 자동차(Extended vehicle) 표준에서 정의한 표준화된 웹 API를 열어주는 등의 방식이 가능하다.

6 클라우드 커넥티드 자동차 보안 위협

이 장에서는 클라우드 커넥티드 자동차에 대한 보안 위협을 정의한다. <표 6-1>의 대상군은 온보드 장치, 게이트웨이 장치, 클라우드로 구분하여 정의한다. 온보드 장치에는 OBD 컨트롤러, OBU, 텔레매틱스 제어 유닛, IVI가 포함되며, 게이트웨이 장치는 클라우드와의 게이트웨이 역할을 하는 모바일 단말이 포함된다.

<표 6-1> 클라우드 커넥티드 자동차 보안 위협

위협	내용	대상
데이터 노출	- 클라우드 서비스 제공자와의 데이터 송수신 과정에서 정보노출 - 자동차 데이터의 클라우드 전송에 사용되는 온보드 및 오프보드 장치(헤드유닛, 클라우드 커넥터, OBU, 스마트폰 등)에 대한 해킹을 통해 개인 및 차량 정보의 불법 수집, 유출 및 공유 가능 - 차량과 외부와의 유무선 통신 프로토콜(이더넷, 와이파이, 블루투스, 셀룰러 등) 해킹 등을 통한 개인 및 차량 정보의 불법 수집, 유출 및 공유 가능 - 클라우드 서버에 불법 접근 및 권한 상승 등을 통해 클라우드에 저장된 개인 및 차량 데이터의 불법 수집, 유출 및 공유 가능	온보드 장치 게이트웨이 클라우드
위장 공격	- 중간자 공격을 통한 클라우드 접근 권한 획득 가능 - 무선 프로토콜의 특성(취약점)을 이용한 공격을 통한 불법적인 무선 접속 후 중간자공격, 프로토콜 분석 등을 통한 제어 데이터 정보 습득 및 공격에 활용 가능	클라우드
인증 우회	- 클라우드 접속 및 통신 중 인증 ID 탈취 - 클라우드 서버 불법 접근 및 권한 상승을 통한 접근 권한 획득	클라우드
데이터 위변조	- 재전송 공격 등을 통해 클라우드 연동을 위한 제어데이터를 악의적으로 변경하는 공격 가능	클라우드
가용성 침해	- 해킹된 차량들의 DDoS 공격 등을 통해 RSU 및 클라우드의 서비스 가용성 침해 - 클라우드에 연결된 자동차의 수의 급속한 증가, 자동차의 잦은 데이터 처리, 대량의 데이터 송수신 등에 따라 클라우드의 가용성 침해 가능	게이트웨이 클라우드
차량 내부 불법 침투	- 클라우드 연동을 위한 온보드/오프보드 장치 및 장치에 탑재된 소프트웨어, 펌웨어 등을 해킹하여 차량 내부 불법 침투를 위한 경로로 사용 가능 - 자동차 데이터의 클라우드 전송에 사용되는 온보드 및 오프보드 장치의 포트 스캐닝, 메모리 공격 등을 통해 접근권한 획득 후 차량 내부에 악의적인 데이터 주입 가능	온보드 장치 게이트웨이 클라우드
악성코드 감염	- 클라우드 기반으로 제공되는 콘텐츠(원격 업데이트되는 자동차용 애플리케이션/펌웨어, 비디오, 오디오 등)의 악성코드 감염 가능	온보드 장치 게이트웨이 클라우드

7 클라우드 커넥티드 자동차 보안 요구사항

이 장에서는 클라우드 커넥티드 자동차 보안 요구사항을 인증, 플랫폼(온보드/오프보드 장치 및 클라우드) 보안, 네트워크 보안 및 침해대응, 개인정보보호, 감사 및 보안관리 요구사항으로 분류하여 정의한다. 각 요구사항에 명시된 M은 필수(Mandatory), O는 선택(Optional)을 구분한 것이다.

7.1 인증 요구사항

이 절에서는 클라우드 연동을 위한 접속기기 및 앱 인증을 위한 요구사항을 정의한다.

[SR-1] (인증) 클라우드와 자동차간 통신시 중간자 공격, 위장공격, 인증 우회를 방지하기 위해 클라우드 연결에 사용되는 온보드 장치, 오프보드 장치, 표준 어댑터 등에 대한 안전한 인증 메커니즘을 제공해야 한다. (M)

[SR-2] (인증) 클라우드 연결을 위한 게이트웨이 역할을 하는 스마트 폰에 탑재된 클라우드 연동 앱에 대한 인증 기능을 제공해야 한다. (M)

[SR-3] (인증) 클라우드 연결을 위한 게이트웨이 역할을 하는 스마트 폰에 탑재된 클라우드 연동 앱은, 공식적으로 인가된 사이트에서 서명한 신뢰할 수 있는 앱의 경우에만 클라우드 접속이 가능해야 한다. (M)

[SR-4] (인증) 클라우드에 저장, 분석, 가공된 데이터를 사용자에게 제공하는 경우, 제공받는 사용자에 대한 인증 메커니즘이 제공되어야 한다. (M)

[SR-5] (키관리) 클라우드 및 자동차에서 키의 노출을 방지하기 위해 비밀키를 안전하게 저장하고 세션키를 안전하게 생성, 발급 관리하기 위한 구조 및 메커니즘(HSM 등)이 제공되어야 한다. (M)

[SR-6] (키관리) 자동차의 개인 키 및 인증서에 대한 비인가적 접근이 불가능해야 한다. (M)

7.2 클라우드 연계 플랫폼(온보드, 오프보드 장치 및 클라우드) 보안 요구사항

이 절에서는 클라우드 연계에 사용되는 온보드 및 오프보드 장치 플랫폼에 대한 보안 요구사항을 정의한다.

[SR-7] (클라우드 연계 장치의 플랫폼 보호) 클라우드 연결에 관련된 온보드 장치, 오프보드 장치 플랫폼에 대해 시스템 레벨의 보안 기능(예: 시큐어 부팅, 시스템 접근제어, 애플리케이션 샌드박스 등)을 제공해야 한다. (O)

[SR-8] (클라우드 연계 장치의 플랫폼 보호) 클라우드 연계에 관련된 온보드 장치, 오프보드 장치 플랫폼을 악성코드로부터 보호하기 위한 메커니즘(차량용 백신 등)이 제공되어야 한다. (M)

[SR-9] (안전한 API) 클라우드 및 차량 애플리케이션의 경우, 업계에서 수용하는 표준, 법, 법령, 규정 등을 준수한 안전한 API를 설계하여 개발 적용해야 한다. (O)

[SR-10] (안전 업데이트) 클라우드 연동을 위한 소프트웨어의 취약점이 발견된 경우, 이에 대응하기 위한 원격 소프트웨어 업데이트 메커니즘을 제공해야 한다. (O)

7.3 네트워크 보안 및 침해대응 요구사항

이 절에서는 자동차 데이터의 클라우드 전송을 위한 네트워크 및 접속기기 인증을 위한 요구사항을 정의한다.

[SR-11] (전송 데이터 무결성) 클라우드와의 송수신 데이터에 대한 위변조 방지를 위해 안전한 세션키를 이용한 무결성 검증 기능을 제공해야 한다. (M)

[SR-12] (전송 데이터 기밀성) 클라우드와의 송수신 데이터는 불법적인 도청 방지를 위해 안전한 세션키를 이용하여 암호화된 형태로 전송되어야 한다. (M)

[SR-13] (전송 데이터 신뢰성) 클라우드 및 자동차에서 비정상적인(anomalous) 외부 유입 데이터 및 트래픽을 탐지하여 대응할 수 있어야 한다. (O)

[SR-14] (무선 프로토콜 보안) 클라우드 데이터 전송을 위해 사용되는 무선 프로토콜 취약점을 이용한 공격에 대응하기 위해 표준 기반의 무선 보안 프로토콜(예: WPA2) 등의 기술적 대책이 제공되어야 한다. (M)

[SR-15] (이상징후 탐지) 자동차 데이터의 클라우드 전송에 사용되는 온보드 및 오프보드 장치가 해킹 되어 비정상 동작하는 경우, 이를 시스템 또는 네트워크 레벨에서 모니터링하여 탐지 및 대응하는 기능을 제공해야 한다. (O)

[SR-16] (클라우드 침입탐지) 클라우드의 외부 또는 내부의 트래픽 폭증을 발생하는 DDoS 등의 공격을 사전에 탐지 및 차단하여 클라우드 서버의 가용성을 높일 수 있어야 한다. (O)

[SR-17] (IVN 접근제어) 클라우드와 연계된 온보드 장치(헤드유닛, OBU, OBD 컨트롤러 등)를 통한 차량 내부네트워크(IVN) 불법 접근 경로를 차단하기 위해 방화벽, 접근제

어 등의 보안 기능이 제공되어야 한다. (M)

[SR-18] (IVN 접근제어) 클라우드와 연계되면서 차량 IVN과도 연결된 헤드유닛, OBU 등의 온보드 장치가 해킹 및 악성코드에 감염된 경우, 그 피해 범위를 제한하고 내부 네트워크로의 전파를 방지하기 위해 하이퍼바이저, 애플리케이션 샌드박스 등 플랫폼 가상화 및 분리(isolation) 기능을 제공해야 한다. 특히 IVN과 연결된 모듈의 경우는 별도의 강력한 접근제어 기능이 제공되어야 한다. (O)

7.4 개인정보보호 요구사항

이 절에서는 클라우드 연계과정에서의 개인정보보호를 위한 요구사항을 정의한다.

[SR-19] (개인정보보호) 클라우드에 저장된 사용자 및 자동차 데이터를 보호하기 위해 암호화 저장, 접근제어 등의 기능이 제공되어야 한다. (M)

[SR-20] (개인정보보호) 사용자 및 자동차 데이터에 대한 접근, 공유에 대한 엄격한 제어 및 데이터 관리 프로세스를 제공해야 한다. (M)

[SR-21] (개인정보보호) 클라우드에서 관리하는 개인 또는 자동차 정보가 포함된 자원에 대한 접근제어 정책 관리 기능이 제공되어야 한다. (M)

7.5 감사 및 보안관리 요구사항

이 절에서는 보안 준수 여부에 대한 감사 및 보안관리에 대한 요구사항을 정의한다.

[SR-22] (감사) 제3의 기관(또는 서비스 제공자)을 통해 보안 정책에 따른 서비스 제공 여부, 개인 및 차량 데이터의 위·변조 및 불법 유출 위협에 대한 안전성 여부 등에 대한 감사 기능을 제공해야 한다. (M)

[SR-23] (관리) 감사, 대응, 분석을 위한 보안 이벤트 로그 관리 기능을 제공해야 한다. (O)

[SR-24] (환경설정) 사용자에게 자신의 데이터(개인, 자동차)의 접근, 공유, 관리를 위한 환경 설정 또는 동의 기능을 제공해야 한다. 특히 자동차 제작사에서 보유한 클라우드 데이터를 제3의 기관에 제공하여 분석 및 서비스를 제공하는 경우 사용자의 동의를 받아야 한다. (M)

[SR-25] (보고) 클라우드 커넥티드 자동차의 보안상태 및 개인정보보호 수준에 대한 정

보를 사용자에게 제공해야 한다. (예: 자동차 대시보드, 사용자 스마트폰 등) (O)

[SR-26] (클라우드 정보 제공) 원활한 클라우드 서비스를 제공하기 위해 서비스 제공상태, 오류, 리소스 현황 등에 대한 모니터링 및 알림 기능을 제공할 수 있어야 한다. (O)

7.6 보안 위협과 요구사항 매핑

이 절에서는 6장에서 도출한 보안 위협과 이 장에서 정의한 보안 요구사항과의 관련성을 기술한다. <표 7-1>은 클라우드 커넥티드 자동차 보안 위협과 요구사항을 매핑한 테이블이다. <표 7-1>의 M은 필수(Mandatory), O는 선택(Optional) 요구사항을 의미한다.

<표 7-1> 클라우드 기반 커넥티드 자동차 보안 위협과 요구사항 매핑

보안 위협	보안 요구사항
데이터 노출	(M) SR-5, SR-6, SR-8, SR-12, SR-13, SR-14, SR-19, SR-20, SR-21 (O) SR-7, SR-9, SR-10
위장 공격	(M) SR-1, SR-2, SR-3, SR-4
인증 우회	(M) SR-1, SR-2, SR-3, SR-4
데이터 위변조	(M) SR-11, SR-12, SR-14 (O) SR-13
가용성 침해	(M) SR-8, SR-14 (O) SR-7, SR-9, SR-15, SR-16
차량 내부 불법 침투	(M) SR-14, SR-17 (O) SR-15, SR-16, SR-18
악성코드 감염	(M) SR-8 (O) SR-7, SR-9, SR-10
공통	(M) SR-22, SR-24 (O) SR-10, SR-23, SR-25, SR-26

부 록 Ⅰ-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

지식재산권 확약서 정보

Ⅰ-1.1 지식재산권 확약서(1)

해당사항 없음

Ⅰ-1.2 지식재산권 확약서(2)

해당사항 없음

부 록 Ⅰ-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

시험인증 관련 사항

Ⅰ-2.1 시험인증 대상 여부

해당사항 없음

Ⅰ-2.2 시험표준 제정 현황

해당사항 없음

부 록 Ⅰ-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

본 표준의 연계(family) 표준

해당사항 없음

부 록 Ⅰ-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

참고 문헌

[1] ISO, 20077-1:2017, Road Vehicles-Extended vehicle (ExVe) methodology, Part 1: General information

[2] ISO, 20077-2:2018, Road Vehicles-Extended vehicle (ExVe) methodology, Part 2: Methodology for designing the extended vehicle

[3] ISO/FDIS 20078-1, Road vehicles-Extended vehicle (ExVe) 'web services', Part 1: ExVe content

[4] ISO/FDIS 20078-2, Road vehicles-Extended vehicle (ExVe) 'web services', Part 2: ExVe access

[5] ISO/DIS 20078-3, Road vehicles-Extended vehicle (ExVe) 'web services', Part 3: ExVe security

[6] ISO/DIS 20078-4, Road vehicles-Extended vehicle (ExVe) 'web services', Part 4: ExVe control

[7] GENIVI Alliance, Remote Vehicle Interaction, Networking Expert Group

[8] 3GPP, LTE release 14, 2016

부 록 Ⅰ-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

영문표준 해설서

해당사항 없음

부 록 Ⅰ-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

표준의 이력

판수	채택일	표준번호	내용	담당 위원회
제1판	2018.12.12	제정 TTAx.xx-xx.xxxx	클라우드 커넥티드 자동차 보안 요구사항	PG504