요약본

자율주행차 보안모델

PART Ⅰ: 자율주행차 및 서비스

2021. 12

과학기술정보통신부
Ministry of Science and ICT

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

제1장

개요

제1장
개요

1.1 목적

자율주행차는 커넥티비티 기술 및 센서 기술의 발전과 함께 급격하게 성장하고 있다. 구글을 비롯하여 GM, Ford 등 글로벌 차량 제조사들이 활발하게 자율주행차를 개발하고 있고 현대자동차 또한 CES에서 자율주행차를 선보이는 등 자율주행차가 더 이상 먼 미래의 얘기가 아니라 우리 손에 쥐어진 현실의 기술이 되었다.

이에 따라, 무인 셔틀, 주차, 배송 등 자율주행차를 활용한 서비스 모델이 활발하게 개발되고 있는데, 이런 서비스들은 자동차, 인프라, 통신, 전자, ICT 등이 융합되어 시너지를 발휘하고 있다. 하지만, 이런 융합으로 인하여 기존 ICT 환경에서 발생했던 사이버 공격들이 자동차 환경으로 전이되고 있다. 자동차의 안전은 운전자와 승객 더 나아가 도로 위에 존재하는 모든 사물들의 안전과 직결되므로 자동차를 대상으로 수행되는 사이버 공격들에 대한 방어 태세를 완비해야 한다.

현재, 자율주행차 서비스들은 아직 성숙 단계에 들어서지 못하여 기술 개발에 치중하고 있어서 사이버 보안에 대한 대비가 미비하다. 따라서, 본 연구는 기 수행한 자율주행 서비스 조사 및 차량/인프라에 대한 취약점 분석 결과를 기반으로 자율주행차 보안 모델을 제시하고자 한다.

본 자율주행차 보안모델은 다음과 같은 항목을 고려한다.

- 자율주행차 및 관련 서비스의 구성도에 따라 보안위협과 공격 경로, 피해 자산 등을 도식화
- 자율주행차 보안위협 분석 결과를 바탕으로 보안 강화에 필요한 보안 기술과 솔루션 제시

1.2 범위

자율주행차 서비스 현황 조사를 통하여 총 9종의 서비스를 식별하였고, 각 서비스에 대한 Data Flow Diagram (DFD)를 통하여 attack surface를 확인하였다. 하지만, 공개된 자료를 통해서 각 서비스의 세부 구성을 알 수 없고, 각 서비스 provider들마다 구성을 다르게 가져가기 때문에 공통된 데이터 흐름이 존재하지 않는다. 따라서, 식별된 서비스 중 보안 컨설팅을 진행한 다음의 두 사례를 제외한 나머지 서비스들은 일반적인 수준의 간략한 DFD 및 그에 대한 위협을 식별하였다.

- 자율주행 셔틀
- 자율주행 서비스 제공을 위한 텔레매틱스 서비스

자율주행 서비스의 조사분석 내용, 보안위협과 보안요구사항에 따른 대응방안 등은 '자율주행차 보안모델 Part 1' 전체버전에서 다루고 있으며, 본 요약본에서는 자율주행차 보안요구사항을 다룬다.

제2장

자율주행차 보안 모델

제2장

자율주행차 보안모델

본 장에서는 자율주행차 서비스 관점에서 차량, 백엔드 인프라에 대한 보안 모델을 설명한다. 또한 법규 준수 관점의 사이버보안 관리 체계에 대한 간략한 설명을 제공한다.

자율주행차 보안 모델은 특성에 따라 크게 두 가지 관점으로 구분될 수 있다.

- 자율주행차 서비스 관점
  - 차량 내부 통신
  - 차량 외부 통신 (백엔드 인프라 포함)
- 법규 준수 관점 (사이버보안 관리 체계, CSMS)

그림 2는 앞서 언급한 두가지 관점에서의 자율주행차 보안모델 구성을 보여준다.

그림 2 자율주행차 보안모델 구성

자율주행차 서비스 관점은 자율주행차 서비스 이용자가 원하는 시점에 의도한 서비스를 제공받을 수 있도록 자율주행차 서비스에 발생할 수 있는 위협을 완화하기 위한 보안 모델이다.

자율주행차 서비스 이용자는 자율주행차 서비스를 제공하는 벡엔드 인프라를 통해 원하는 서비스를 요청하고, 백엔드 인프라는 서비스 제공을 위한 최적의 자율주행차를 선정 및 제어 명령을 통신 채널을 통해 자율주행차에 전송한 뒤 자율주행차는 서비스 이용자에게 서비스를 제공함과 동시에 주기적으로 서비스 제공 상태를 백엔드 인프라에 보고한다. 이러한 형태는 본 연구를 통해 확인된 자율주행차 서비스의 일반적인 운영방식이다. 따라서 자율주행차 서비스 관점의 보안 모델은 자율주행 서비스를 구성하는 3요소 (차량, 백엔드 인프라, 통신 채널)를 대상으로 하며, 요소 별 보안 대책을 제공한다.

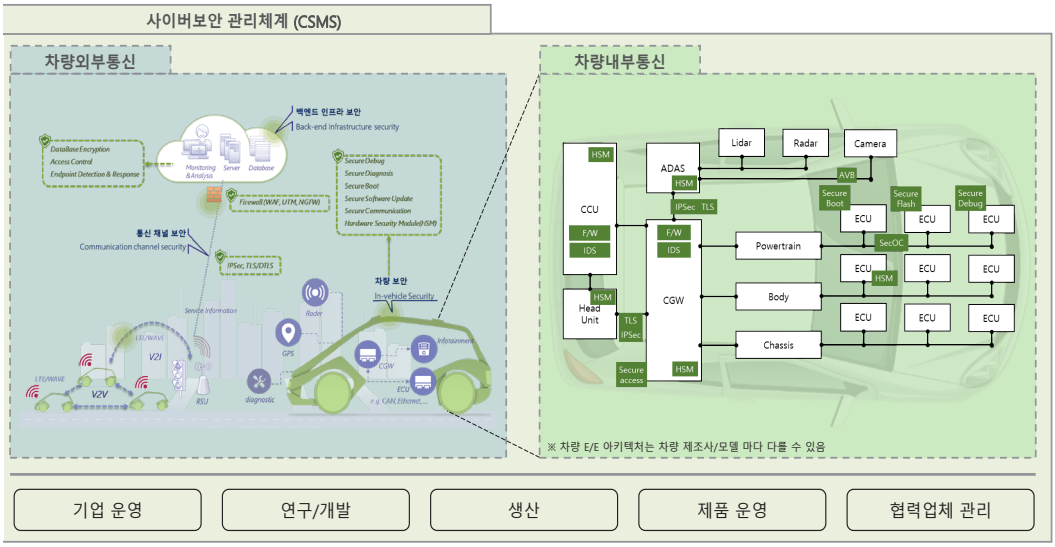
법규 준수 관점은 UN 차량 사이버보안 규정 (UN Regulation No.155)에 기반을 둔다. 법규 준수 관점은 자율주행 차량의 설계/개발/운영에 이르기까지 차량 라이프사이클 전반에 걸쳐 차량을 개발하는 조직에 필요한 정책, 프로세스 등을 모두 다룬다는 점에서 자율주행차 서비스 관점과는 차이를 가진다.

자율주행차 보안모델은 사이버 보안의 특수성을 고려하여 설계되었다. 사이버보안은 대상 서비스의 기능 및 구성, 시간의 흐름에 따른 기술의 발전에 영향을 받는다. 예를 들어 자율주행차 서비스가 제공되는 특정 시점에는 사이버보안이 보장되었다 할지라도 기술의 발전에 따라서 더 이상 안전하지 않을 수 있다. 따라서 지속적으로 자율주행차의 사이버보안을 보장하기 위해서는 두 가지 측면 (서비스 측면, 법규 준수 측면)을 모두 고려해야한다.

UN 차량 사이버보안 규정에서 언급된 것 처럼 차량에 대한 사이버보안의 총괄적 책임은 차량 제조사에 있다. 따라서 본 문서에서 도출된 자율주행차 보안모델의 적용 대상 또한 차량 제조사이다. 협력 업체는 차량 제조사의 요구 조건에 따라서 납품하는 시스템 또는 조직의 사이버보안을 관리 할 것이다. 이와 관련된 역할 및 책임 정의는 협력 업체와 차량 제조사간 협의에 따라 달라질 수 있다.

그림 3은 자율주행 서비스 관점과 법규 준수 관점을 모두 고려하여 최종 도출한 자율주행차 보안모델을 보여준다. 해당 보안 모델은 자율주행차 서비스를 제공하기 위해 필요한 차량 내/외부의 기술적인 측면과 안전한 자율주행차 서비스 개발, 생산, 운영을 위해 필요한 거버넌스 측면을 모두 다루고 있다.

그림 3 자율주행차 보안모델 구성 (상세)



자율주행차 보안모델은 자율주행차 대표 서비스 9종에 대한 분석과 UN 차량 사이버보안 규정에 대한 해석을 통해 도출되었다. ‘2.1 자율주행차 및 서비스’ 절에서는 자율주행차 서비스별 공통 구성요소를 식별하고, 자율주행차 서비스 구성도 간략하게 도식화 되었지만, 서비스 유형 및 구성은 서비스 제공자의 설계, 자율주행차 기술 및 ICT 응용 서비스의 발달에 따라 변경 될 수 있다. 또한 자율주행차 내부의 전기/전자 아키텍처도 차량 제조사 및 차량 형식에 따라 각기 달라질 수 있음에 유의해야 한다.

2.1 자율주행차 및 서비스

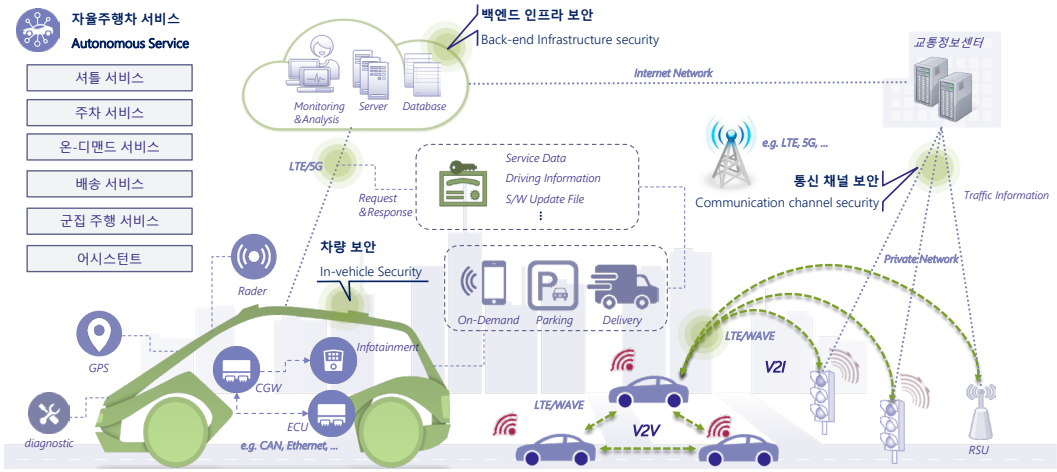
자율주행차 보안모델을 개발하기위해 먼저 대상이 되는 자율주행차 서비스를 조사하여 각 서비스 유형에 대한 데이터 흐름을 분석하였다. 이를 통해 자율주행차 서비스의 공통적인 구성요소를 식별하였고, 공통 구성요소의 대표서비스에 대한 데이터 흐름을 분석하였다.

그림4에서 보는 바와 같이 차량은 V2X 통신을 위하여 차량 간 셀룰러 통신(C-V2X), WAVE 통신 등을 하는데, 이 때 보안을 위하여 서명 및 서명 검증을 수행한다. 서명 및 서명 검증에 사용할 인증서를 발급받고, 이상 행위를 보고하기 위하여 차량은 또한, RSU를 통하여 인프라와 통신을 수행한다.

셔틀 서비스나 온-디맨드 서비스, 배송 서비스 등은 차량의 각종 정보를 백엔드 인프라로 전송하고, 필요 정보를 수신하여 관련 서비스를 제공한다. 또한, 군집 주행 및 어시스턴트 서비스는 차량 간 정보를 공유하며, 이동통신 기술을 기반으로 차량 상태를 확인하여 원격 제어, 안전, 편의 기능을 제공한다. C-ITS 서비스는 주행 중에 필요한 교통 상황과 도로정보를 실시간으로 제공하여 자율주행 시 발생할 수 있는 사고를 예방한다.

이와 같은 자율주행차 서비스는 차량을 기반으로 다양한 통신 채널을 통해 백엔드 인프라, 교통정보센터에 교통, 안전, 편의, 차량 관리 등 정보를 전달하고, 사용자는 해당 정보를 백엔드 인프라나 차량과의 통신을 통해 전달 받아, 서비스를 이용할 수 있게 된다. 그림4에서는 자율주행차 대표 서비스 9종을 도출하여 서비스별로 공통 구성요소로 서비스 구성도를 간략하게 도식화하였으나, 자율주행차 기술과 ICT 응용 서비스의 발달에 따라, 서비스 유형과 구성은 변경될수 있다.

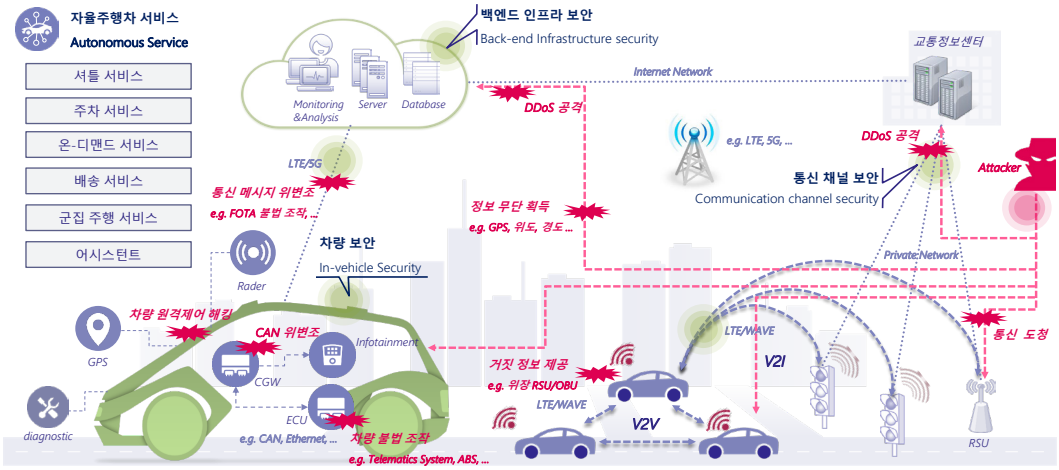
그림 4 자율주행차 서비스 구성도



이런 통신 환경에 대한 서비스 유형별 보안위협은 STRIDE 위협 모델링 방법론을 통해 도출하여 기술한다. 또한 UNECE 및 ISO/SAE 21434 표준 기반으로 개발한 점검 체크리스트를 기준으로 취약점 점검을 수행하였으며, 이 과정을 통해 도출한 보안위협을 기술하였다.

다음 그림은 자율주행차 서비스 유형에서 발생할 수 있는 위협요소를 보여준다. 차량과 백엔드 인프라가 통신할 때 공격자는 도청 및 데이터 변조를 수행할 수 있고, 백엔드 인프라에 대하여 DoS와 같은 직접적인 공격을 수행할 수 있다. 차량에 대해서는 차량 제어기의 인터페이스를 통하여 송수신되는 데이터 또는 저장된 데이터를 도청, 변조하거나 업데이트 패키지를 위변조하여 공격을 수행할 수도 있다.

그림 5 자율주행차 서비스 보안위협



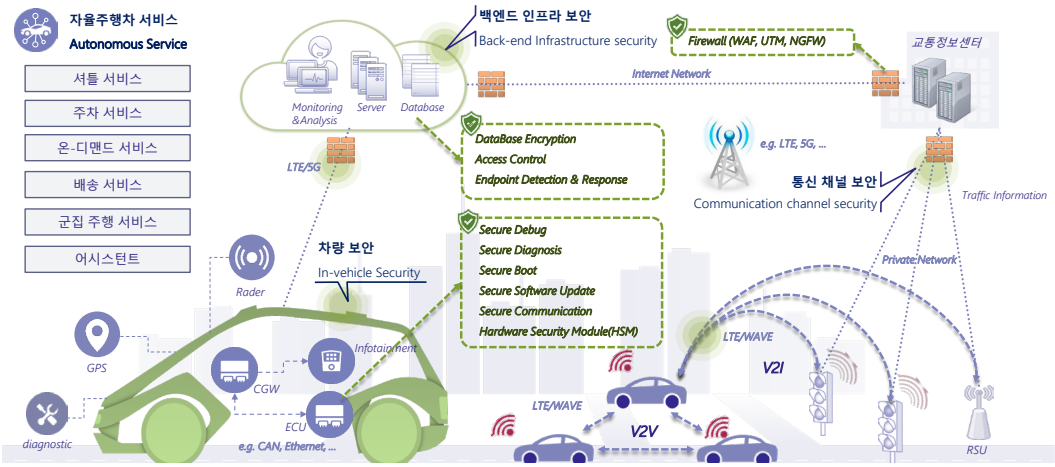
차량, 통신채널, 백엔드 인프라 영역에서 발생할 수 있는 보안위협을 간략하게 정리하면 다음 표와 같다. 통신채널의 경우 커넥티비티 기술로 인해 서비스 유형에 따라 다양한 구간이 존재하며, 그에 따라 사이버 공격 벡터도 늘어나고 있다.

표 2 자율주행차 서비스 구간별 보안위협

영역	구간	보안위협
차량	N/A	펌웨어 변조, 차량 원격제어 해킹, CAN 위변조, 차량 불법 조작, 서비스 거부(DoS)
통신채널	차량 – 차량	통신도청, 통신메시지 위변조, 정보 무단 획득, 거짓 정보 제공, 부인
	차량 – 백엔드 인프라	
	차량 – 노변인프라	
	백엔드 인프라 – 노변인프라	
	백엔드인프라 –백엔드 인프라	
백엔드 인프라	N/A	정보 유출, 권한 상승, 서비스 거부(DoS)

차량에서는 ‘HPSE(HSM)’, ‘Secure Boot’, ‘Secure Debug’, ‘Secure Diagnosis’, ‘Secure Flash’, ‘Secure Access’, ‘Secure Software Update’ 와 같은 보안기술을 적용하여 차량을 안전하게 보호할 수 있다. 또한 백엔드 인프라에서는 보안서비스(‘기밀성’, ‘무결성/가용성’, ‘권한관리’, ‘식별/인증’, ‘로깅/감사추적’, ‘보안관리’, ‘접근통제’ 분야)에 따른 대응방안을 제시한다. 데이터, 시스템, 단말 영역에서 Firewall, DataBase Encryption, Access Control, Endpoint Detection & Response와 같은 보안기술 및 솔루션을 적용하여 안전하게 보호할 수 있다.

그림 6 자율주행차 서비스 보안기술 및 솔루션



각 영역별 보안위협에 적용할 수 있는 보안기술을 요약하면 다음 표와 같다. 개별 보안 기능 성공적인 공격의 난이도를 높이기에 충분하지 않기 때문에 모든 사이버 보안은 전체론적인 접근 방식 (Holistic approach)을 통해서만 보장될 수 있다.

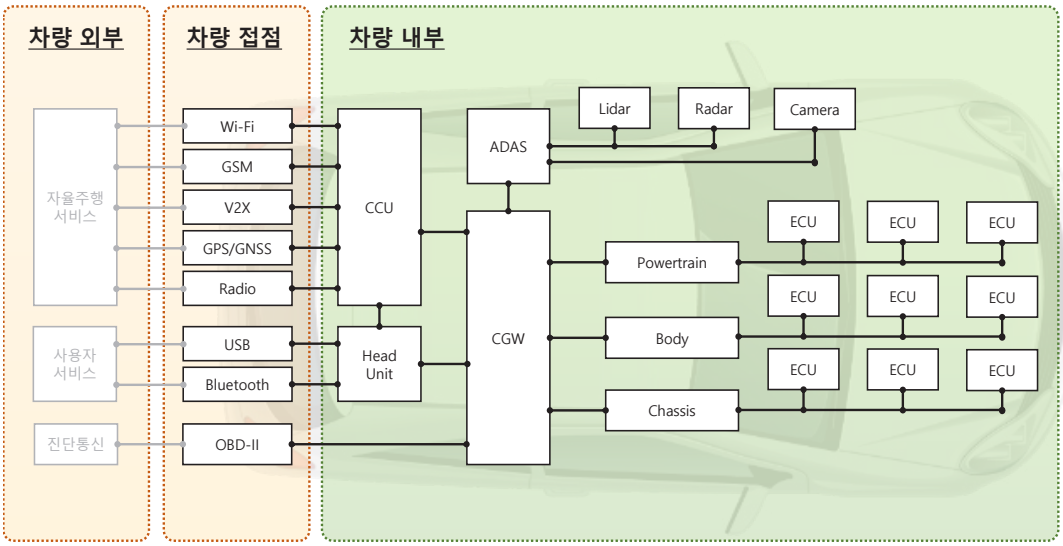
표 3 보안위협별 대응 보안기술

영역	보안위협	보안기술
차량	펌웨어 변조	HPSE(HSM), Secure Boot, Secure Debug, Secure Diagnosis, Secure Flash, Secure Software Update
	차량 원격제어 해킹	Secure Access, Secure Diagnosis, IDS, SecOC
	CAN 위변조	IDS, SecOC, Secure Software Update
	차량 불법조작	Secure Access, Secure Diagnosis
	서비스 거부(DoS)	IDS
통신채널	통신도청	IPSec, TLS/DTLS, WAVE 통신 보안 기술
	통신메시지 위변조	
	정보 무단 획득	
	거짓 정보 제공	
	부인	
백엔드 인프라	정보 유출	Firewall(WAF, UTM, NGFW), DataBase Encryption, Access Control, Endpoint Detection & Response
	권한 상승	Access Control
	서비스 거부 (DoS)	Firewall(WAF, UTM, NGFW)

차량 내부 영역은 차량 제조사 및 차종 마다 탑재된 기능 및 인터페이스가 다르지만, 현재 시판중인 차량을 기준으로 다음과 같이 구분할 수 있다.

- 차량 외부
- 차량 접점
- 차량 내부

그림 7 자율주행차의 일반적인 구성



차량 외부는 차량과 통신을 주고 받는 개체 또는 서비스로, 백엔드 인프라, 정비 진단기 등을 의미하고,차량 접점은 차량 외부와 차량 내부가 통신을 수행할 수 있도록 하는 데이터의 송수신 통로이다. 원격에서 자동차를 공격하는 대부분의 공격은 차량 접점을 통하여 이루어지므로 해당 부분에 대한 보안 대책이 중요하다. 차량 내부는 외부에서 수신한 데이터를 기반으로 서비스가 적용될 수 있도록 제어기, 센서 및 엑추에이터로 구성된 네트워크를 말한다. 예를 들어, ITS 서비스를 제공하는 시나리오에서는 서비스 제공자로부터 V2X (WAVE or DSRC) 통신 매체를 통하여 데이터가 제공되면 차량의 CCU에 탑재된 V2X 모뎀을 통하여 해당 데이터를 수신한 후 게이트웨이를 통하여 관련 장치로 전송된다.

차량 내부 통신간에는 아래 그림과 같은 위협이 존재할 수 있다. 예를 들어, 공격자는 변조된 펌웨어를 진단기나 OTA 기능을 이용하여 자동차에 주입하려 할 수 있다. 펌웨어가 변조되면 차량 외부에서 메시지를 해당 펌웨어로 전송하여 차량을 제어하게 된다.

그림 8 자율주행차의 위협 예시

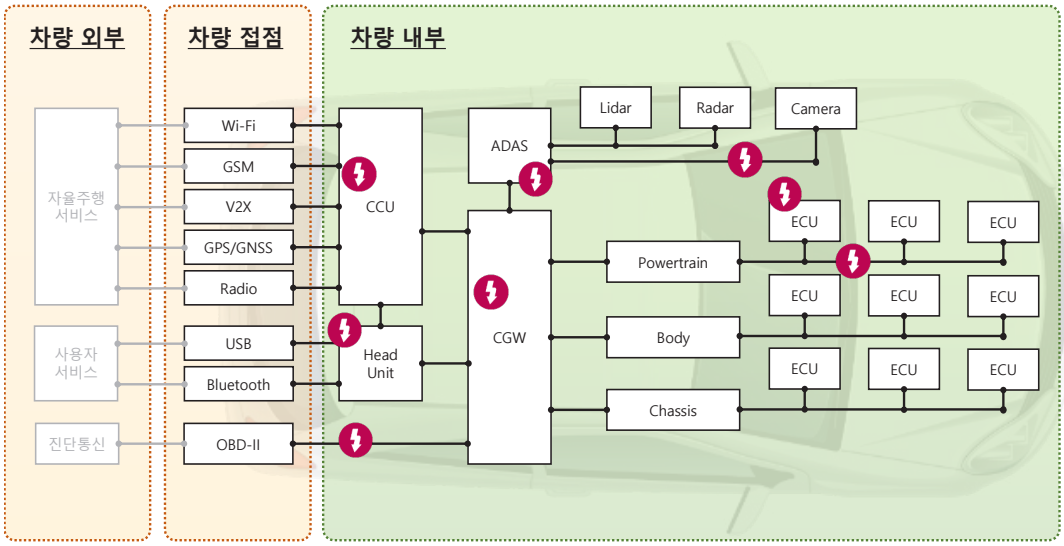


표 4 자율주행차 레이어별 보안위협

영역	보안위협
제어기	펌웨어 변조, 펌웨어 분석, 메모리 덤프 등
내부통신	CAN 메시지 위변조, Replay attack, 서비스 거부 등
외부통신	강제제어, 변조된 펌웨어 주입 등

차량 내부에서 상기와 같은 위협을 완화하기 위한 보안 기술 및 솔루션은 다음과 같다. 예를 들어, 공격자가 특정 제어기의 펌웨어를 변조하여 차량을 제어하려 할 경우, 다음의 단계를 거치게 된다.

① 제어기에 접근하여 펌웨어를 분석
② 분석 내용을 기반으로 펌웨어 변조
③ 변조된 펌웨어 주입
④ 주입된 펌웨어 실행
⑤ 자동차 제어

이 때 공격자는 펌웨어 분석을 위하여 제어기에 접근하여야 하는데, 인가되지 않은 개체가 제어기에 접근할 수 없도록 하는 secure debug를 통하여 효과적으로 차단할 수 있다. 또한, 변조된 펌웨어가 유효한 효과를 발휘하기 위하여 차량에 주입해야 하는데, 펌웨어는 다음의 두 가지 방법으로 주입될 수 있다.

- OTA
- 진단기 접속

OTA는 UN Regulation No. 156에 따라 잘 관리되어야 하며, 차량과 업데이트 백엔드 사이의 암호화 통신, 차량 내부에서의 서명 검증 등 여러 보안 기능을 포함하고 있는 시스템이어야 한다.

진단기 접속의 경우, Secure access를 통하여 인가된 사용자만 접근할 수 있도록 강제하여야 한다. 만약, 위의 기능들이 무력화되어 공격자에 의하여 변조된 펌웨어가 주입되었다 하더라도 이 펌웨어가 실행되는 단계에서 Secure boot 기능을 통하여 위협을 완화시킬 수 있다. 마지막으로 공격자에 의하여 변조된 펌웨어가 주입되어 실행된다 하더라도 정상적이지 않은 거동을 보이는 경우, IDS 등을 통하여 효과적으로 공격을 탐지하여 위험이 실체화 되기 전에 차단할 수 있다.

그림 9 자율주행차의 보안 기술 및 보안 솔루션

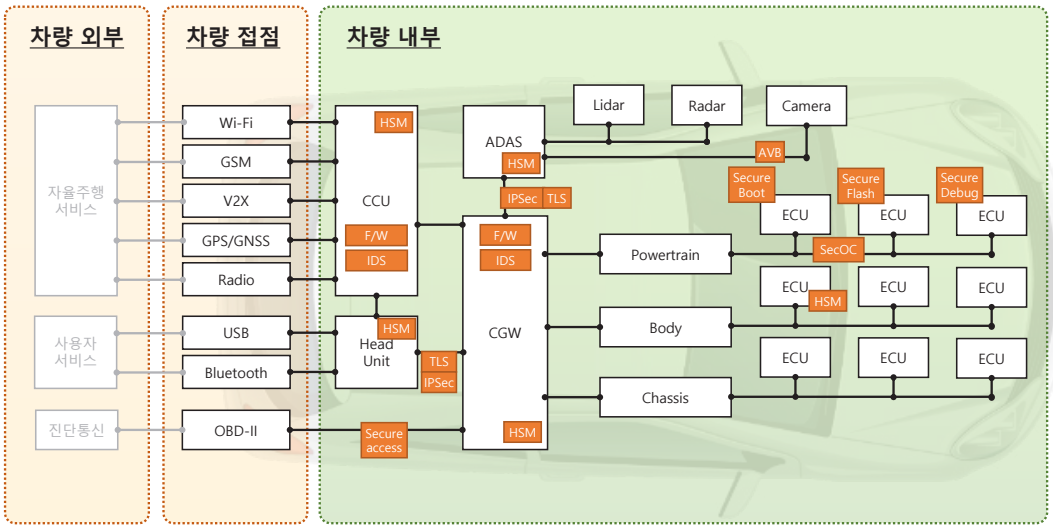


표 5 자율주행차 레이어별 보안기술 및 솔루션

영역	보안 기술 및 솔루션
제어기	Secure boot, Secure Flash, Secure Debug, HSM
내부통신	AutoSAR SecOC, IPSec/TLS , AVB, IDS, HSM
외부통신	OTA, Secure access, IDS, FW, HSM

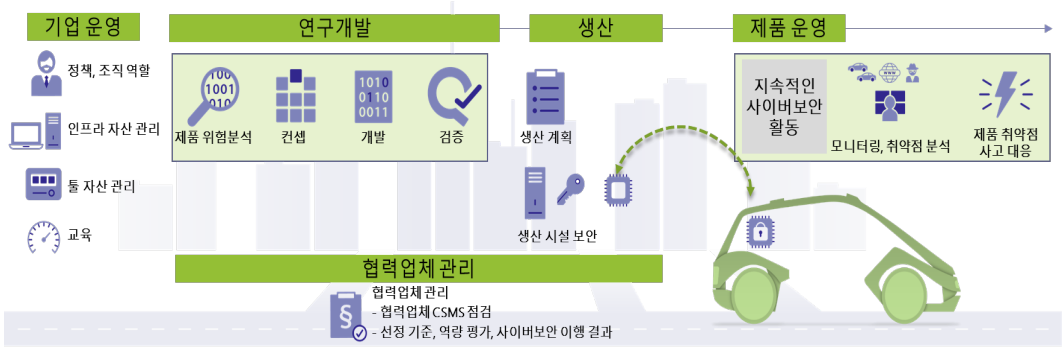
2.2 사이버보안 관리체계

사이버보안 관리 체계는 차량 제조사가 차량 전체 라이프사이클에 걸쳐 사이버보안을 고려할 수 있도록 하기 위한 것으로 차량 제조사가 사이버보안을 고려하기 위한 정책, 조직, 프로세스 등이 포함된다. 차량 제조사는 사이버보안에 관한 연구개발, 협력업체 관리 및 생산에 그치지 않고, 차량이 고객에게 판매 된 이후에도 차량에 발생하는 사이버보안을 지속적으로 고려해야 한다. 이를 위해 차량 제조사는 프로젝트 팀 단위가 아닌 전사 차원의 사이버보안 정책, 전담/협력 조직 그리고 관련자들에 대한 사이버보안 인식 교육, 관련 툴 관리에 이르기 까지 기업 운영 차원의 고려가 필요하다.

차량 제조사가 사이버보안 관리체계 구축을 위해 고려해야 할 내용을 차량 라이프사이클 특성 별로 구분하면 다음과 같다.

- 기업 운영
- 연구개발
- 생산
- 제품 운영
- 협력업체 관리

그림 10 자율주행차의 보안 기술 및 보안 솔루션



차량 제조사는 기업 운영 차원에서 경영진의 책임'을 포함한 전사적 사이버보안 정책과 이를 준수하기 위한 기업 내 업무 프로세스를 갖춰야 한다. 사이버보안 정책은 차량 사이버보안에 대한 기업의 목표 및 방향을 제시하는 최상위 정책 문서를 의미하며, 일반적으로 규정과 지침으로

구성된다. 업무 프로세스는 규정, 지침을 준수하기 위한 구체적이고 세부적인 상세 내용을 설명한 문서를 의미한다. 여기에는 TARA 방법론, 정보 공유, 사이버보안 모니터링, 사이버보안 사고 대응을 포함하여 사이버보안 컨셉, 제품 개발, 생산, 운영, 유지보수 및 단종까지 모든 영역을 포함해야 한다.

연구 개발 단계에서 차량 제조사는 개발하려는 컨셉 단계에서부터 사이버보안 위험을 식별하여 이에 대한 처리 방안을 결정한다. 결정된 처리 방안을 사이버보안 목표로 명시하고, 이를 검증(validation) 단계에서 확인하게 된다. 또한 사이버보안 목표를 준수하기 위한 사이버보안 컨셉을 만들고, 이를 기반으로 각 시스템 및 컴포넌트를 구현해야한다. 구현된 결과물은 각 단계별로 기능 및 통합 검증(verification)을 수행하여 의도한대로 동작함을 증명하게 된다.

생산 단계에서 차량 제조사는 생산 시 고려해야 할 사이버보안 요구사항을 수립 및 점검하기 위한 생산 관리 계획을 작성해야 한다. 생산 관리 계획에는 사이버 보안에 관련된 일련의 생산 절차, 생산에 필요 시 되는 도구 및 의도한 대로 생산되었는지 확인하기 위한 방법 등이 포함되어야 한다. 사이버 보안은 보안 대책 적용만으로는 충분하지 않다. 사이버보안에서는 신뢰의 근간(Root of trust)이라고 할 수 있는 키(Key)의 관리가 매우 중요한데, 생산 단계에서 키가 주입된다. 따라서 생산 관리 계획에는 암호학적 연산에 사용되는 키를 언제, 어떻게, 무슨 장비를 통해 제품에 주입하고, 정상 주입 여부를 판단할지를 작성해야 한다. 이것이 생산 단계의 사이버보안 요구사항이 된다.

제품 운영은 지속적으로 수행되어지는 활동으로 생산 이후 사이버보안 관점의 모니터링 체계와 사고 대응이 요구된다. 차량 제조사는 제품 운영 단계에서 잠재적인 위협 및 취약점에 대한 내부 및 외부 소스 모니터링을 통해 수집된 사이버보안 이벤트를 분석하여 아이템에 영향을 미치는지 여부를 판단해야 한다.

차량 사이버보안을 보장하기 위해서는 차량 제조사의 노력뿐만 아니라 모든 협력 업체의 노력이 필요하다. 따라서 차량 제조사는 협력 업체에 대한 사이버보안 역량 입증 및 평가가 요구되며, 사이버보안 협정서 (Cybersecurity Interface Agreement, CIA)를 통해 프로젝트 수행 시 협력 업체와의 역할 정의가 요구된다.

사이버보안 관리 체계에 대한 자세한 내용은 자율주행차 보안모델 Part 2에서 설명한다.

제3장

자율주행차 보안요구사항

제3장

자율주행차 보안요구사항

3.1 차량 보안요구사항

본 장에서는 차량, 특히 CCU의 유즈케이스, 자산, 보안요구사항을 설명한다.

3.1.1 Use Cases

차량 영역에서의 유즈케이스는 다음과 같다.

표 73 차량 영역의 Use Case

ID	Use Case	설명
UC01	Over-the-air update	차량 ECU 소프트웨어의 원격 업데이트
UC02	Telematics	차량 제어, 사고 정보, IDS 데이터 등 차량 데이터 전송
UC03	V2X	C-ITS 서비스 관련 정보 송수신
UC04	Autonomous shuttle service	배차정보, 승객 승하차 정보 등 자율주행버스 정보 전송
UC05	Data logging	차량에 문제 발생 시 분석을 위한 데이터 수집 후 저장
UC06	Remote vehicle control	외부에서 차량 원격 제어
UC07	e-Call	비상 상황 자동 알림 서비스
UC08	Vehicle status monitoring	차량 소유주가 차량의 상태를 원격에서 확인
UC09	Infortainment services	차량의 인포테인먼트 서비스

3.1.2 보안 자산 식별

보안자산(Security Asset)은 보호해야 하는 분석 대상 (차량 – CCU)의 데이터, 기능 및 자원을 말한다. 시스템 모델 및 Use Case로부터 다음과 같은 자산이 식별될 수 있다.

보안속성(Security Objectives)은 무결성(Integrity), 기밀성(Confidentiality), 진본성(Authenticity), 가용성(Availability), 최신성(Freshness) 으로 나뉘며, 각 자산에 존재할 수 있는 보안속성을 식별한다.

표 74 차량의 자산식별

보안자산	설명	보안 속성
CCU Configuration Data	CCU 설정정보–관제 센터 IP, Port 정보, 서비스 정보 등	Integrity
CCU firmware	CCU에서 동작하는 컴파일된 코드 (펌웨어)	Confidentiality
		Integrity
OTA package	바이너리 코드, 스크립트, 설정파일 등 업데이트 관련 정보를 포함하고 있는 데이터 패키지	Confidentiality
		Authenticity
		Freshness
Telematics data	EDR/DSSAD 정보, IDS 로그, 차량 원격제어 정보 등의 서비스를 수행하기 위한 정보	Integrity
Communication w/backend	관제센터와 통신을 위해 송수신되는 데이터	Confidentiality
		Authenticity
		Freshness
		Availability
Cryptographic materials	암복호화에 사용되는 키 또는 인증서 등의 정보	Confidentiality
		Integrity
V2X traffic	다른 차량 및 인프라와 V2X 통신을 수행하기 위해 송수신되는 데이터	Authenticity
		Freshness
		Availability
Logging Data	IDS, F/W log	Integrity
Diagnostic trouble code	원격 진단 시 전송되는 진단 오류 코드 (SAE J2012)	Integrity
Vehicle Control Data	원격 시동, 공조장치 On/Off 등의 원격 제어 데이터	Integrity
SOS Data	위급 상황 시 전송되는 알림 데이터	Integrity
GPS Data	차량 위치 파악을 위한 위치정보 데이터	Integrity
Vehicle Status Data	차량 원격 제어를 위한 상태 정보	Integrity
Infortainment Service Data	인포테인먼트를 위한 데이터 – 날씨, 음악 등의 서비스 및 음성인식 Home IoT등 서비스 제어를 위한 데이터	Confidentiality
		Integrity

3.1.3 보안요구사항 도출

보안자산의 보안속성을 통해 보안요구사항을 도출하면 다음과 같다.

표 75 차량 보안요구사항 도출

보안요구사항ID	보안요구사항 설명	관련 보안위협ID
SRV01	CCU 설정정보가 변조되지 않도록 무결성을 확보해야 한다.	ST02, ST04
SRV02	CCU firmware가 외부에 유출되지 않도록 기밀성을 확보해야 한다.	ST01, ST05, ST13
SRV03	CCU firmware가 변조되지 않도록 무결성을 확보해야 한다.	ST03
SRV04	OTA package가 변조되지 않도록 무결성을 확보해야 한다.	ST01, ST08, ST09
SRV05	OTA package의 진본성을 확보해야 한다.	ST11
SRV06	OTA package의 최신성을 확보해야 한다.	ST12
SRV07	Telematics data가 변조되지 않도록 무결성을 확보해야 한다.	ST02, ST14
SRV08	Communication w/backend가 변조되지 않도록 무결성을 확보해야 한다.	ST01, ST10
SRV09	Communication w/backend의 진본성을 확보해야 한다.	ST11
SRV10	Communication w/backend의 최신성	ST12
SRV11	Communication w/backend의 서비스 제공이 중단되지 않도록 가용성을 확보해야 한다.	ST04, ST15
SRV12	Cryptographic materials가 외부에 유출되지 않도록 기밀성을 확보해야 한다.	ST06, ST07, ST13
SRV13	Cryptographic materials가 변조되지 않도록 무결성을 확보해야 한다.	ST02
SRV14	V2X traffic의 진본성을 확보해야 한다.	ST11
SRV15	V2X traffic의 최신성을 확보해야 한다.	ST12
SRV16	V2X traffic의 서비스 제공이 중단되지 않도록 가용성을 확보해야 한다.	ST04, ST15
SRV17	Logging Data가 변조되지 않도록 무결성을 확보해야 한다.	ST16
SRV18	DTC가 변조되지 않도록 무결성을 확보해야 한다.	ST16
SRV19	Vehicle Control Data가 변조되지 않도록 무결성을 확보해야 한다.	ST16
SRV20	SOS Data가 변조되지 않도록 무결성을 확보해야 한다.	ST11, ST14
SRV21	GPS Data가 변조되지 않도록 무결성을 확보해야 한다.	ST11, ST14, ST15
SRV22	Vehicle Status Data가 변조되지 않도록 무결성을 확보해야 한다.	ST16
SRV23	Infortainment Service Data가 외부에 유출되지 않도록 기밀성을 확보해야 한다.	ST17
SRV24	Infortainment Service Data가 변조되지 않도록 무결성을 확보해야 한다.	ST16

3.2 백엔드 인프라 보안요구사항

백엔드 인프라 영역은 정보보호관리체계(ISMS) 및 ISO 27001표준에 의거하여 서버(35), 네트워크장비(30), DBMS(26) 분야로 구분하여 91개의 보안요구사항을 정의한다.

3.2.1 Server

표 76 Server 보안요구사항

ID	보안 서비스	보안요구사항	설명	관련 위협ID
SRS01	권한관리	사용자 계정 생성 원칙 준수	- 계정ID는 계정 생성자와 관련된 정보를 포함하지 말아야 함 - 관리자 권한 계정명의 경우, root/admin/ master 등의 문구를 포함하지 말아야 함	STS01
SRS02	권한관리	기본 계정 사용 제한	- 불필요한 기본 계정/비밀번호는 삭제 또는 접근 금지 시켜야 함	STS02
SRS03	권한관리	사용자 계정 공동 사용 제한	- 사용자 계정을 공동으로 사용하는 것을 금지하고 부득이 하게 사용할 경우 최소 권한 및 개인별 사용 기록을 관리해야 함	STS03
SRS04	권한관리	계정 현행화	- 유효하지 않는 계정ID로 시스템에 접속할 수 없어야 하며, 계정정보는 현행화해야 함 - 개발자 계정 등 임시 계정 제거	STS04
SRS05	권한관리	권한 부여 원칙 준수	- 최소 권한 부여, 알 필요(Need to Know)에 의한 최소 인원에게, 업무에 필요한 최소 권한만 부여해야 함 - 등급에 따른 차등 권한 부여, 권한 부여 시 시스템 접근 자격등급에 따라 권한을 차등 부여해야 함 - 사용자 업무별로 접근권한 통제 수행	STS05
SRS06	권한관리	특수권한 할당 및 사용 제한	- 정보시스템(Server, Network 장비, DBMS 등)을 제어할 수 있는 특수권한 할당 및 사용을 제한해야 함 - 시스템 사용자의 권한에 따라 사용할 수 있는 명령어를 최소한으로 제한해야 함	STS06
SRS07	권한관리	시스템 파일 접근 권한 제한	- 시스템의 중요 파일은 최소 권한으로 접근 실행되어야 함	STS07
SRS08	기밀성	비밀번호 암호화	- 비밀번호는 안전한 일방향 암호화 함수를 적용하여 저장해야 함 - 전송 시, 일방향 암호화가 권고되나(표준), 업무적 불가피성에 의한 양방향 암호화는 허용됨 (컴플라이언스 허용 수준)	STS08
SRS09	기밀성	암호키 관리	- 암호화 키는 안전하게 관리해야 함	STS09

ID	보안 서비스	보안요구사항	설명	관련 위협ID
SRS10	로깅/ 감사추적	접속시도 오류 기록 및 알람	- 로그인 시도 성공/실패, 잠김 계정의 로그인 시도, 로그오프에 대해 로깅해야 함 - 연속된 접속시도의 오류가 발생한 경우 감사 기록뿐 아니라 경보 발생 등을 통해 시스템 관리자에게 통보해야 함 (로컬 로그인 시도 포함) - 해당 로그는 정기 점검/확인 감독해야 함	STS10
SRS11	로깅/ 감사추적	최종 접속시간 표시	- 로그인 성공 후, 가장 최근의 로그인 시간 및 접속 위치(IP)를 표시하도록 함	STS11
SRS12	로깅/ 감사추적	시스템 가동 기록 로깅	- 시스템 가동기록은 자동 기록되어야 함 (접속기록, DB접근 로깅 등 포함)	STS12
SRS13	로깅/ 감사추적	계정 권한관리 내역 로깅	- 계정, 권한에 대한 부여/변경/말소 이력을 로깅해야 함	STS13
SRS14	로깅/ 감사추적	특수권한 사용자 수행 내역 기록	- 정보시스템은 운영자/관리자 등 특수 권한을 가진 계정 접근 기록, 명령어 사용내역 등을 기록해야 함 - 주요 업무 관련 행위는 책임자가 이중확인 및 모니터링해야 함	STS14
SRS15	로깅/ 감사추적	시간 동기화	- 네트워크에 연결된 모든 시스템은 감사 추적성 (Audit Trail) 확보를 위해 시스템상의 시간이 일치되도록 설정해야 함	STS15
SRS16	로깅/ 감사추적	로깅 정보 위/변조 방지	- 주요 로그는 관리자 이외에 접근이 불가하도록 제한해야 하며, 로그 기록의 변경/삭제를 방지해야 함	STS16
SRS17	무결성/ 가용성	파일/프로그램 배포 시스템 점검	- 배포 시스템에서 배포파일 대상으로 무결성 검증 수행 및 시스템 보호대책 적용	STS17
SRS18	무결성/ 가용성	주요 시스템 구성 파일 무결성 체크	- OS, Web/WAS 등의 주요 구성파일은 주기적으로 임의 변경에 대한 무결성 점검을 할 수 있음	STS18
SRS19	무결성/ 가용성	정보보호시스템 정기점검	- 정보보호시스템 작동 상태를 주기적으로 점검할 것	STS19
SRS20	무결성/ 가용성	장비 이중화 구성	- 시스템은 가용성이 확보되는 구성을 유지해야 함	STS20
SRS21	무결성/ 가용성	백업 및 소산관리	- 주요정보시스템의 안정적인 서비스를 위해 주기적으로 백업해야 함	STS21
SRS22	무결성/ 가용성	재해복구 대응	- 시스템 오류, 자연재해등 본 전산센터의 기능 상실에 대비하여 재해복구센터를 구축/운영하여 무지속성을 확보해야 함 - 재해복구 전환 훈련을 실시해야 함 - 핵심업무 복구목표시간을 설정해야 함 - 핵심 정보보호시스템은 재해대응센터 내 구축해야 함	STS22
SRS23	무결성/ 가용성	시스템 가용성 확보, 비상대책 수립 및 시행	- 적정 용량 산정 및 확보 - 운영 및 개발 매뉴얼 작성 - 위기대응행동매뉴얼 수립 및 보고 - 비상대응훈련 실시 및 보고 - 침해사고 대응 및 복구 훈련 실시	STS23

ID	보안 서비스	보안요구사항	설명	관련 위협ID
SRS24	보안관리	바이러스 백신 설치	- 정보시스템에 상용 백신 프로그램을 설치하고, 최신 업데이트하여 사용해야 함	STS24
SRS25	보안관리	불필요한 서비스 불용 처리	- 시스템 운영상 불필요 서비스는 불용 처리해야 함	STS25
SRS26	보안관리	이동저장매체 통제	- 이동형 저장매체(USB메모리, SD메모리, CD/DVD RW 등) 사용을 제한해야 함 - 보조기억매체는 주기적인 보유 현황 등 관리실태 점검 후 책임자 승인을 득해야 함	STS26
SRS27	보안관리	보안설정 가이드 준수	- 정보시스템 도입 시 보안설정 가이드를 적용해야 함	STS27
SRS28	식별/인증	중복 로그인, 다중 연결세션 제한	- 시스템 접속시 하나의 계정 ID로 여러 세션을 연결할 수 없도록 제한해야 함	STS28
SRS29	식별/인증	단순 비밀번호 제한	- 로그인 비밀번호를 반드시 설정해야 함 - 비밀번호 복잡도 법규 요건 준수 필요 계정ID에 대해 단순 비밀번호 사용을 제한 하는 비밀번호 규칙을 적용해야 함	STS29
SRS30	식별/인증	비밀번호의 주기적인 변경	- 비밀번호를 주기적으로 변경 관리해야 함	STS30
SRS31	식별/인증	비밀번호 연속 오류 대응	- 일정 횟수 이상 로그인 실패 시 경우 즉시 해당 비밀번호를 이용하는 계정을 잠금 조치하고 접속을 차단해야 함 - 계정잠금/접속차단 계정은 본인 확인 절차를 거쳐 비밀번호를 재부여하거나 초기화해야 함	STS31
SRS32	식별/인증	정보시스템 접속 단말 인증 강화	- 인가된 단말기만 중요 정보시스템에 접근 가능해야하며, 사용자가 시스템에 접속할 때 계정/PW 방식 외 추가 인증 등 강화된 보호대책을 적용해야 함 ※ 강화된 인증방식 : FIDO, 모바일 OTP, 사설 인증서 등	STS32
SRS33	접근통제	세션 아이들 타임아웃 적용	- 시스템 접속 후 일정 시간 거래/입력이 없을 경우, 세션 유지를 제한해야 함	STS33
SRS34	접근통제	외부에서 접속 시 접근통제	- 외부에서 내부망으로 접근을 원칙적으로 금지함 - 업무적 필요시 암호통신, 이중화된 인증, 책임자 승인 등을 통하여 보완해야 함	STS34
SRS35	접근통제	정보시스템 접속 단말기 제한	- 시스템에 접근하려고 하는 단말기의 접속 여부의 적절성을 판단하여 필터링하는 기능 적용 및 설정 강제 ※ 시스템 : 정보시스템/정보처리시스템을 일컫는 일반적인 용어이며, 단말기 / 네트워크 장비 / 서버 / APP / DBMS / 보안설비 등을 통칭함	STS35

3.2.2 Network 장비

표 77 Network장비 보안요구사항

ID	보안 서비스	보안요구사항	설명	관련 위협ID
SRN01	권한관리	기본 계정 사용 제한	- 불필요한 기본 계정/비밀번호는 삭제 또는 접근 금지 시켜야 함	STN01
SRN02	권한관리	사용자 계정 공동 사용 제한	- 사용자 계정을 공동으로 사용하는 것을 금지하고 부득이 하게 사용할 경우 최소 권한 및 개인별 사용기록을 관리해야 함	STN02
SRN03	권한관리	계정 현행화	- 유효하지 않는 계정ID로 시스템에 접속할 수 없어야 하며, 계정정보는 현행화해야 함	STN03
SRN04	권한관리	권한 부여 원칙 준수	- 최소 권한 부여, 알 필요(Need to Know)에 의한 최소 인원에게, 업무에 필요한 최소 권한만 부여해야 함 - 등급에 따른 차등 권한 부여, 권한 부여 시 시스템 접근 자격 등급에 따라 권한을 차등 부여해야 함 - 사용자 업무별로 접근권한 통제 수행	STN04
SRN05	권한관리	특수권한 할당 및 사용 제한	- 정보시스템(Server, Network 장비, DBMS 등)을 제어할 수 있는 특수권한에 대한 할당 및 사용을 제한해야 함 - 시스템 사용자의 권한에 따라 사용할 수 있는 명령어를 최소한으로 제한해야 함	STN05
SRN06	기밀성	비밀번호 암호화	- 비밀번호는 안전한 일방향 암호화 함수를 적용하여 저장해야 함 - 전송 시, 일방향 암호화가 권고되나(표준), 업무적 불가피성에 의한 양방향 암호화는 허용됨(컴플라이언스 허용 수준)	STN06
SRN07	기밀성	전송구간 암호화	- 암호화 대상 정보는 정보통신망을 통해 송수신할 경우, 암호화해야 함	STN07
SRN08	로깅/ 감사추적	접속시도 오류 기록 및 알람	- 연속된 접속시도의 오류가 발생한 경우 감사 기록뿐 아니라 경보 발생 등을 통해 시스템 관리자에게 통보해야 함 (로컬 로그인 시도 포함) - 접속기록은 정기적인 점검/확인감독해야 함	STN08
SRN09	로깅/ 감사추적	최종 접속시간 표시	- 로그인 성공 후, 가장 최근의 로그인 시간 및 접속 위치(IP)를 표시하도록 함	STN09
SRN10	로깅/ 감사추적	시스템 가동 기록 로깅	- 시스템 가동기록은 자동 기록되어야 함	STN10
SRN11	로깅/ 감사추적	계정 권한관리 내역 로깅	- 계정, 권한에 대한 부여/변경/말소 이력을 로깅해야 함	STN11

ID	보안 서비스	보안요구사항	설명	관련 위협ID
SRN12	로깅/ 감사추적	특수권한 사용자 수행 내역 기록	- 정보시스템은 운영자/관리자 등 특수 권한을 가진 계정 접근 기록, 명령어 사용 내역 등을 기록해야 함 - 주요 업무 관련 행위는 책임자가 이중 확인 및 모니터링해야 함	STN12
SRN13	로깅/ 감사추적	시간 동기화	- 네트워크에 연결된 모든 시스템은 감사 추적성(Audit Trail) 확보를 위해 시스템 상의 시간이 일치되도록 설정해야 함	STN13
SRN14	로깅/ 감사추적	로깅 정보 위/변조 방지	- 주요 로그는 관리자 이외에 접근이 불가 하도록 제한해야 하며, 로그 기록의 변경/삭제를 방지해야 함	STN14
SRN15	보안관리	불필요한 서비스 불용 처리	- 시스템 운영상 불필요 서비스는 불용 처리 해야 함	STN15
SRN16	보안관리	유해트래픽 차단	- 웜이나 DoS/DDoS 에 대한 대응 및 유해 트래픽/불법적 접근을 차단해야 함	STN16
SRN17	보안관리	실시간 감시 및 대응	- 해킹 등 전자적 침해행위로 인한 사고를 방지하기 위한 실시간 감시/대응 시스템을 설치·운영하여야 함	STN17
SRN18	보안관리	보안설정 가이드 준수	- 정보시스템 도입 시 보안설정 가이드를 적용해야 함	STN18
SRN19	식별/인증	단순 비밀번호 제한	- 로그인 비밀번호를 반드시 설정해야 함 - 비밀번호 복잡도 법규 요건 준수 필요 계정ID에 대해 단순 비밀번호 사용을 제한 하는 비밀번호 규칙을 적용해야 함	STN19
SRN20	식별/인증	비밀번호의 주기적인 변경	- 비밀번호를 주기적으로 변경 관리해야 함	STN20
SRN21	식별/인증	비밀번호 연속 오류 대응	- 일정 횟수 이상 로그인 실패 시 경우 즉시 해당 비밀번호를 이용하는 계정을 잠금 조치하고 접속을 차단해야 함 - 계정잠금/접속차단 계정은 본인 확인 절차를 거쳐 비밀번호를 재부여하거나 초기화해야 함	STN21
SRN22	식별/인증	정보시스템 접속 단말 인증 강화	- 인가된 단말기만 중요 정보시스템에 접근 가능해야하며, 사용자가 시스템에 접속할 때 계정/PW 방식 외 추가 인증 등 강화된 보호대책을 적용해야 함 ※ 강화된 인증방식 : FIDO, 모바일 OTP, 사설 인증서 등	STN22
SRN23	접근통제	세션 아이들(Idle) 타임아웃 적용	- 시스템 접속 후 일정 시간 거래/입력이 없을 경우, 세션 유지를 제한해야 함	STN23
SRN24	접근통제	중복 로그인, 다중 연결세션 제한	- 시스템 접속시 하나의 계정 ID로 여러 세션을 연결할 수 없도록 제한해야 함	STN24

ID	보안 서비스	보안요구사항	설명	관련 위협ID
SRN25	접근통제	단말기의 비인가 네트워크 접속 제한	- 정보처리시스템 접속 단말기는 외부망으로부터 물리적 분리해야 함 - 단말기의 접속 권한이 없는 망 접속 제한	STN25
SRN26	접근통제	개발망/ 테스트망/운영망 분리	- 개발망과 운영망 분리 - 외주 전산설비 등은 내무 업무망과 분리해야 함 - 개발/테스트(검증계)/운영 설비 분리 (기반시설 요건)	STN26
SRN27	접근통제	내부 업무용시스템 네트워크 접속 제한	- 내부망과 연결된 내부 업무용시스템은 인터넷 등 외부통신망과 분리·차단 및 접속 금지해야 함 - 주요 서버팜 구성을 통해 적절한 권한의 접근 통제를 적용해야 함 - 내부 통신망은 다른 기관 내부 통신망과 분리하여 사용해야 함	STN27
SRN28	접근통제	외부에서 접속 시 접근통제	- 외부에서 내부망으로 접근을 원칙적으로 금지함 - 업무적 필요시 암호통신, 추가 인증, 책임자 승인 등을 통하여 보완해야 함	STN28
SRN29	접근통제	무선네트워크 통제	- 허가되지 않은 무선망 통제	STN29
SRN30	접근통제	정보시스템 접속 단말기 제한	- 시스템에 접근하려고 하는 단말기의 접속 여부의 적절성을 판단하여 필터링하는 기능 적용 및 설정 강제	STN30

3.2.3 DBMS

표 78 DBMS 보안요구사항

ID	보안서비스	보안요구사항	설명	관련 위협ID
SRD01	권한관리	기본 계정 사용 제한	- 불필요한 기본 계정/비밀번호는 삭제 또는 접근 금지 시켜야 함	STD01
SRD02	권한관리	사용자 계정 공동 사용 제한	- 사용자 계정을 공동으로 사용하는 것을 금지하고 부득이 하게 사용할 경우 최소 권한 및 개인별 사용기록을 관리해야 함	STD02
SRD03	권한관리	계정 현행화	- 유효하지 않는 계정ID로 시스템에 접속할 수 없어야 하며, 계정정보는 현행화해야 함 - 개발자 계정 등 임시 계정 제거	STD03
SRD04	권한관리	권한 부여 원칙 준수	- 최소 권한 부여, 알 필요(Need to Know)에 의한 최소 인원에게, 업무에 필요한 최소 권한만 부여해야 함 - 등급에 따른 차등 권한 부여, 권한 부여 시 시스템 접근 자격 등급에 따라 권한을 차등 부여해야 함 - 사용자 업무별로 접근권한 통제 수행	STD04

ID	보안서비스	보안요구사항	설명	관련 위협ID
SRD05	권한관리	특수권한 할당 및 사용 제한	- 정보시스템(Server, Network 장비, DBMS 등)을 제어할 수 있는 특수권한에 대한 할당 및 사용을 제한해야 함 - 시스템 사용자의 권한에 따라 사용할 수 있는 명령어를 최소한으로 제한해야 함	STD05
SRD06	권한관리	시스템 파일 접근 권한 제한	- 시스템의 중요 파일은 최소 권한으로 접근 실행되어야 함	STD06
SRD07	권한관리	DB 접근권한 통제	- 개인/신용정보 DB에 대한 사용자 접근을 제한해야 함	STD07
SRD08	기밀성	표준 암호화 준수	- 암호화 적용 시, 공인기관이 권고하는 안전한 알고리즘 적용해야 함 · 공인기관: 국OOO원, 금융감독원, TTA, KISA, NIST 등 · 키 길이에 따른 유효기간이 설정됨 (대칭키 암호화 알고리즘의 경우, 128bit 키 길이를 갖으면 2030년까지 유효한 것으로 명기되어 있음) - 암호 프로그램을 안전하게 관리하여 부당 유포/사용을 방지해야 함	STD08
SRD09	기밀성	비밀번호 암호화	- 비밀번호는 안전한 일방향 암호화 함수를 적용하여 저장해야 함 - 전송 시, 일방향 암호화가 권고되나(표준), 업무적 불가피성에 의한 양방향 암호화는 허용됨 (컴플라이언스 허용 수준)	STD09
SRD10	기밀성	이용자 데이터 사용 제한	- 이용자의 데이터를 테스트 데이터로 사용 해야 할 경우 변환해서 사용해야 함	STD10
SRD11	로깅/감사추적	접속시도 오류 기록 및 알람	- 연속된 접속시도의 오류가 발생한 경우 감사 기록뿐 아니라 경보 발생 등을 통해 시스템 관리자에게 통보해야 함 (로컬 로그인 시도 포함) - 접속기록은 정기적인 점검/확인감독해야 함	STD11
SRD12	로깅/감사추적	최종 접속시간 표시	- 로그인 성공 후, 가장 최근의 로그인 시간 및 접속위치(IP)를 표시하도록 함	STD12
SRD13	로깅/감사추적	시스템 가동 기록 로깅	- 시스템 가동기록은 자동 기록되어야 함	STD13
SRD14	로깅/감사추적	계정 권한관리 내역 로깅	- 계정, 권한에 대한 부여/변경/말소 이력을 로깅해야 함	STD14
SRD15	로깅/감사추적	특수권한 사용자 수행 내역 기록	- 정보시스템은 운영자/관리자 등 특수 권한을 가진 계정 접근 기록, 명령어 사용 내역 등을 기록해야 함 - 주요 업무 관련 행위는 책임자가 이중 확인 및 모니터링해야 함	STD15

ID	보안서비스	보안요구사항	설명	관련 위협ID
SRD16	로깅/ 감사추적	로깅 정보 위/변조 방지	- 주요 로그는 관리자 이외에 접근이 불가 하도록 제한해야 하며, 로그 기록의 변경/삭제를 방지해야 함	STD16
SRD17	무결성/ 가용성	전산자료 유출 방지	- 전산자료의 유출방지를 위해 접근통제, 반출입 통제 등의 통제를 적용해야 함	STD17
SRD18	보안관리	보안설정 가이드 준수	- 정보시스템 도입 시 보안설정 가이드를 적용해야 함	STD18
SRD19	식별/인증	중복 로그인, 다중 연결세션 제한	- 시스템 접속시 하나의 계정 ID로 여러 세션을 연결할 수 없도록 제한해야 함	STD19
SRD20	식별/인증	단순 비밀번호 제한	- 로그인 비밀번호를 반드시 설정해야 함 - 비밀번호 복잡도 법규 요건 준수 필요 계정ID에 대해 단순 비밀번호 사용을 제한 하는 비밀번호 규칙을 적용해야 함	STD20
SRD21	식별/인증	비밀번호의 주기적인 변경	- 비밀번호를 주기적으로 변경 관리해야 함	STD21
SRD22	식별/인증	비밀번호 연속 오류 대응	- 일정 횟수 이상 로그인 실패 시 경우 즉시 해당 비밀번호를 이용하는 계정을 잠금 조치하고 접속을 차단해야 함 - 계정잠금/접속차단 계정은 본인 확인 절차를 거쳐 비밀번호를 재부여하거나 초기화해야 함	STD22
SRD23	식별/인증	정보시스템 접속 단말 인증 강화	- 인가된 단말기만 중요 정보시스템에 접근 가능해야하며, 사용자가 시스템에 접속할 때 계정/PW 방식 외 추가 인증 등 강화된 보호대책을 적용해야 함 ※ 강화된 인증방식 : FIDO, 모바일 OTP, 사설 인증서 등	STD23
SRD24	접근통제	세션 아이들 타임아웃 적용	- 시스템 접속 후 일정 시간 거래/입력이 없을 경우, 세션 유지를 제한해야 함	STD24
SRD25	접근통제	외부에서 접속 시 접근통제	- 외부에서 내부망으로 접근을 원칙적으로 금지함 - 업무적 필요시 암호통신, 이중화된 인증, 책임자 승인 등을 통하여 보완해야 함	STD25
SRD26	접근통제	정보시스템 접속 단말기 제한	- 시스템에 접근하려고 하는 단말기의 접속 여부의 적절성을 판단하여 필터링하는 기능 적용 및 설정 강제	STD26

자율주행차 서비스 보안모델 Part 1(요약본)

자율주행차 보안모델 Part 1(요약본)은 자율주행차 보안모델 전체 내용 중 일부 항목을 별도 편집한 것으로, 본 요약본에서 언급된 서비스 분석, 보안위협, 대응방안 등 세부 내용은 보안모델 전체본을 참고하시기 바랍니다.

문 의 : 한국인터넷진흥원 융합보안정책팀 061-820-1287, slivinglab@kisa.or.kr