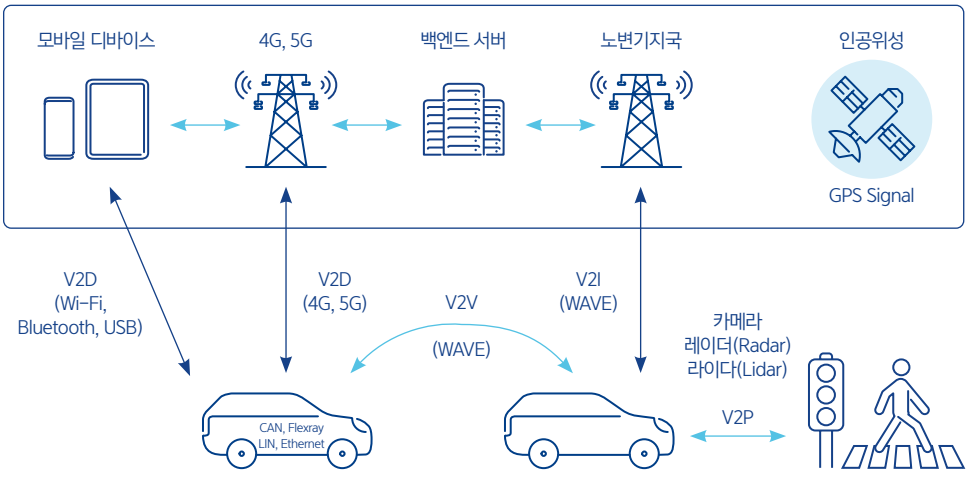
AhnLab
스마트교통 보안 컨설팅

Cyber Security Consulting for Smart Transportation

스마트카 전장 시스템 및 스마트카 서비스 인프라인 네트워크, 백엔드 서버 등에 대한 사이버 보안성을 평가하고 발생할 수 있는 위험을 사전 도출하여 대응 방안을 제시합니다.

서비스 개요

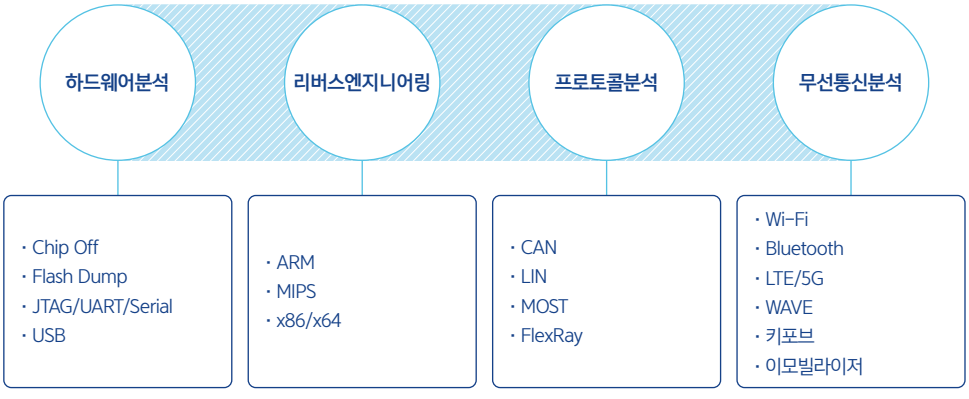
스마트교통의 핵심인 스마트카를 비롯한 유·무선 네트워크 기반으로 연결된 인프라, 백-엔드 서버에 대한 보안성을 평가하여 스마트교통 서비스 전반에 대한 위협을 식별하고 시나리오 기반의 모의해킹을 통해 스마트교통 서비스의 설정 오류 및 실체적 위험을 진단하고 대응 방안을 제시합니다.



[스마트교통 서비스 구성 – KISA 스마트교통 사이버보안 가이드(2019년 12월)]

특징

HW 및 유·무선 통신 환경 분석을 포함한 스마트카와 관련 인프라가 가진 전반적인 특성을 점검합니다.



점검항목

스마트교통에 대한 가용성 손상, 데이터 손실, 중간자 공격, 부적절한 암호 사용, 부적절한 접근 통제, 부적절한 물리적 통제, 악의적인 프로그램 실행, 잘못된 설계 구현, 미흡한 사용자 권한 관리, 부적절한 행위 등에 대해 안전성을 점검합니다

가용성 손상	· 통신 장애 및 센서 인식 방해를 통한 차량 마비
데이터 손실	· 통신 메시지 변조 및 공격을 통한 데이터 변조, 삽입, 삭제 유발
중간자 공격	· 사용자와 서비스 사이 통신의 중간에서 메시지를 도청 및 변조하거나, 해당 사용자 세션 탈취
부적절한 암호 사용	· 부적절한 관리로 인해 암호키가 노출되거나 취약한 암호 사용으로 쉽게 복호화
부적절한 접근 통제	· 백도어를 통한 접근이나 부적절한 보안 정책으로 인한 접근
부적절한 물리적 통제	· 디버그 포트(USB, JTAG, UART) 및 ODB-II 등의 포트를 통한 정보 유출
악의적인 프로그램 실행	· 바이러스 감염 및 펌웨어 변조를 통한 악의적인 프로그램 실행
잘못된 설계 구현	· 부적절한 업데이트 및 키 관리 프로세스, 불필요한 서비스, 소프트웨어 버그 등
미흡한 사용자 권한 관리	· 안전한 인증방법을 제공하지 않아 권한이 없는 사용자가 차량에 접근하여 권한 탈취
부적절한 행위	· 소유자 또는 설치/수리/유지보수 엔지니어의 잘못된 장비 구성으로 의도하지 않은 취약성 및 위협 발생

수행절차

스마트홈을 구성하는 인프라, 클라우드, 디바이스의 취약점 및 위협을 기반으로 시나리오를 작성하고 침투 시험을 수행하여 실제적 위험을 가시화하고, 발견된 취약점 및 위협 시나리오별로 대응 방안을 제시합니다.

AhnLab
경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901