권두언

스마트 카와 교통시대의 과제

홍만표 한국정보보호학회 회장
아주대학교 사이버보안학과 교수

오늘날 4차 산업혁명이라는 기치 아래 정보통신과 타산업의 융합이 곳곳에서 일어나고 있는 것을 볼 수 있다. 특히 교통과 자동차 산업의 경우 네트워크에 연결되어 통신이 가능한 커넥티드 카(혹은 스마트 카) 등장과 함께 교통의 효율성 증대와 운전자의 안전성을 포함하여 다양한 교통서비스를 제공할 수 있는 스마트교통이 현실화되고 있다.

커넥티드 카 시장은 무선이동통신, IoT기술의 발전과 더불어 빠르게 성장하고 있고, IT융합의 가장 선도적인 산업으로 발전될 것으로 예견된다. 이는 BI 인텔리전스와 가트너(Gatner)에 따르면 2020년에 생산되는 자동차의 75%가 커넥티드 카일 것이고, 관련 산업의 매출액은 1,600억 불에 이를 것으로 예상하고 있다.

특히 미래 성장동력의 원천이 될 커넥티드 카에 대형 IT 플랫폼 업체인 애플(Apple)이나 구글(Goole) 등도 발 빠르게 진입하고 있어서, 자신들의 운영체제 기반의 인포테인먼트(Infotainment) 플랫폼인 Carplay와 Cadriod Auto에 다양한 콘텐츠와 운전자 맞춤형의 서비스를 장착할 수 있는 환경을 제공하고 있다.

앞으로는 단일 차량의 발전을 넘어서 자동차와 자동차(V2V, Vehicle to Vehicle) 통신과 V2I(Vehicle to Infra) 및 나아가 V2X(Vehicle to everything)를 통하여 자율협력차가 현실화될 것이다. 이러한 발전을 통한 스마트 카 서비스는 운전자의 편의성과 교통의 효율성을 극대화할 수 있을 것으로 기대되지만, 스마트 카와 교통 서비스에서 사이버 공격에 의한 침해사고가 발생할 경우 인명피해는 물론 전체 교통시스템의 혼란과 같은 치명적인 재앙으로 발생할 수 있다.

이러한 우려는 미래가 아니라 이미 현실화되어서, 2015년 미국 라스베가스에서 열렸던 블랙햇 컨퍼런스에서 보안전문가들인 찰리 밀러와 크리스 발라세크가 지프 체로키(Jeep Cherokee)와 피아트 크라이슬러(Fiat Chrysler) 자동차를 원격 해킹하는 것

을 시연해보였다. 이들은 자동차 펌웨어와 내부통신용 CAN 프로토콜을 리버스 엔지니어링(reverse engineering)하여 인포테인먼트 시스템을 해킹한 후, 브레이크와 운전대 및 기타 중요한 시스템을 마음대로 조작하는데 성공했다. 그 결과 크라이슬러는 문제점을 수정하기 위해 차량 140만 대를 리콜해야 했다.

우리나라에서도 2017년 4월, 현대자동차의 차량 제어 애플리케이션인 블루링크(BlueLink)가 해킹될 수 있다는 언론보도가 나왔다. 보안전문기업인 Rapid7은 블루링크의 보안 취약점으로 해커가 차량을 제어할 수 있다고 발표를 했다. 블루링크 앱에서 개인정보를 현대차에 전송하는 과정에서 사용자 이름과 암호, 개인식별번호(PIN)를 해커가 추출할 수 있었고, 나아가 원격으로 자동차 잠금 해제한 다음 시동을 걸 수 있는 치명적인 문제점이 노출된 것이다. 현대차는 해당 문제를 해결하기 위한 보안 패치를 발표, 공급했던 사례가 있다.

이와 같은 스마트교통에 대한 보안인식을 바탕으로 미국, 유럽, 일본 등 각 나라에서 스마트카 및 교통에 관련된 보안정책과 요구사항들을 제시하고 있다. 미국 도로교통안전국(NHTSA)은 2016년 9월에 자율주행자동차의 15가지 안전성 평가 기준의 내용을 담은 Federal Automated Vehicles Policy를 발표하고 10월에는 사이버안전 강화에 관한 7가지의 지침 내용을 담은 Cybersecurity Best Practices for Modern Vehicles를 발표하였다. 또한, 미국자동차기술학회(SAE)는 2016년 1월에 J3061 - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems를 발표하여 자동차 사이버보안을 위한 개발 프로세스와 보안성 점검을 위한 취약점 테스트기법 등을 제시하였다. 유럽네트워크정보보호원(ENISA)은 2016년 12월에 스마트카를 보호하기 위한 주요 보안위협, 위협시나리오 및 업계가 고려해야 하는 보안 조치에 관한 Cyber Security and Resilience of smart cars를 발표하였다. 일본의 정보처리추진기구(IPA)는 2017년 3월에 자동차 시스템의 생명주기의 단계별 기능과 보안위협 및 대응방안을 담고 있는 자동차 정보보안에 대한 가이드 개정판을 공개하였다. 범국제적인 활동으로 UNECE WP.29 산하 ITS/AD는 2017년 11월 사이버보안(Cyber Security) 및 데이터보호(Data Protection) 가이드라인을 개발하여 2017년 3월 WP.29총회에 상정하였으며, 통합지침서(R.E.3)의 부속서로 추가하였다.

스마트교통의 사이버보안에 관한 국제적 활동에 비해 국내 자동차・교통 산업계의 보안의식 수준이 낮고, 교통 시스템에 대한 체계적인 분류와 지침이 부족한 형편이다. 최근 인터넷진흥원에서는 스마트교통 산업에 필요한 기본적인 보안항목 및 대응방안을 제시하기위하여 스마트교통과 관련된 제품 및 서비스를 설계・제조하는 IT업체 및 운용업체와 이용자를 대상으로 보안인식 제고와 보안 내재화 촉진을 목적으로 스마트교통 사이버보안가이드를 발표하였다.

나아가 기존의 자동차 검사의 경우 주로 물리적인 기능이나 배출가스와 같은 환경적인 검사위주로 이루어졌다면, 앞으로 스마트 카의 경우에는 기존의 검사 항목 외에 사이버보안에 대한 취약성 점검이 필수적으로 추가되어야한다. 사이버보안 항목 검사를 위해서 검사의 방법과 기준에 대한 명확한 근거가 있어야할 것이고, 아울러 국제적인 표준화에 적극적인 개입과 협력이 무엇보다 시급한 과제이다. 그러므로 이에 필요한 기술적・제도적인 연구와 국제적인 동향에 대한 실시간 모니터링과 우리의 목소리를 전달할 체계적인 준비를 정부, 기업, 대학 등의 정보보호 전문가 집단들이 긴밀하게 협력하여 할 시점이다. 그런 점에서 최근 국토교통부 중심으로 자율협력주행 산업발전협의회를 구성하여 보안분과를 두어서 위 사항들에 대한 점검과 협의를 시작했다는 점에서 앞으로의 활동이 기대된다.