http://dx.doi.org/10.16960/jhlr.24.3.202309.1

사이버 공격으로부터 첨단 교통 시스템 보호*

- 관련 입법례를 중심으로 -

류 병 운
(홍익대학교 법과대학 교수)

【초 록】

첨단 교통 차량이 점점 더 자동화되고 상호 연결성이 심화되는 것에 비례하여 그에 따른 사이버 침해 위험도 증가한다. 만일 해커 등이 첨단차량의 사이버 보안 취약성을 악용하는 경우 야기될 수 있는 위험은 탑승자의 불편이나 사소한 주행 방해에서부터 탑승자와 차량 외부인에 대한 생명의 위협까지 다양할 수 있다. 특히 해커가 차량의 가속, 감속, 제동장치, 조향장치를 무력화하거나 차량의 조향과 속도를 제어할 수 있는 능력을 가로챌 때 심각한 도로교통 위험을 초래할 수 있고 심지어는 차량을 테러 수단으로 악용할 수도 있다.

이 논문은 첨단 교통수단의 운행과 교통관리의 효율성 확보와 함께 사이버 위협에 대한 효과적 대응을 뒷받침하기 위하여 첨단 교통 차량과 그 시스템의 사이버 취약성과 사이버 위협 사례를 검토하고 국제규칙과 국제표준, EU, 미국 등의 입법 상황을 참조하여 바람직한 한국의 법 제도의 방향과 원칙을 모색하고자 한다.

주제어 : 자율주행자동차, 도심 항공 교통수단, 첨단교통 시스템, 사이버 위협, 해킹

* 이 논문은 2022학년도 홍익대학교 학술연구진흥비에 의하여 지원되었음.

【차 례】

Ⅰ. 서론

현재 개발과 산업화 과정에 있는 대표적 첨단 교통수단으로 자율주행자동차(Autonomous Vehicles: AV)와 도심 항공 교통수단(Urban Air Mobility: UAM)을 들 수 있다. AV는 "운전자 또는 승객의 조작 없이 자동차 스스로 운행이 가능한 자동차"[1]를 말한다. AV는 대체로 자동차 자체에 인공지능(Artificial Intelligence: AI) 기반의 '자동 운전 장치(Automated Driving System: ADS)'가 탑재되는 형태이다. ADS는 차량의 '첨단 운전자 보조시스템(Advanced Driver Assistance System: ADAS)[2]'를 통합하는 것은 물론 이전의 '내

1) 한국 「자동차관리법」 제2조 제1의3호. 좀 더 구체적으로 완전 자율주행차는 전혀 운전자의 개입 없이 주변 환경을 인식하고 주행 상황을 판단해 차량을 제어함으로써 스스로 운행하는 자동차를 말한다: 류병운, "자율주행자동차 사고의 법적 책임", 홍익법학 제19권 제1호 (2018) 33-34면.

2) ADAS는 예컨대 '충돌 회피 장치(Collision Avoidance System: CAS),' '주행 조향보조 시스템(Lane Keep Assist System: LKAS)', '첨단 스마트 크루즈 컨트롤(Advanced Smart Cruise Control: ASCC)', '후측방 충돌 회피 지원 시스템(Active Blind Spot Detection: ABSD)', 원격 주차 보조 시스템(Remote Smart Parking Assist: RSPA) 등 그 종류와 기능이 다양하다: G. Dimitrakopoulos, Current Technologies in Vehicular Communications, 63-96 (2017); Felipe Jiménez & José Eugenio Naranjo & José Javier Anaya & Fernando García & Aurelio Ponz & José María Armingol, "Advanced Driver Assistance System for road environments to improve safety and efficiency," 14 Transportation Research Procedia 2245, 2246-253 (2016) 참조.

재적(self-contained)' 방식을 벗어나 다른 차량, 도로와 교통 시설 등과 데이터를 주고받는 '상호 연결성(interconnected)'으로 교통상황을 판단 주행하는 방식으로 진화하였다.[3]

UAM은 "대도시 지역의 교통을 혁신하는 승객과 화물을 위한 안전하고 효율적이며 편리하고 저렴하며 지속 가능한 항공 운송 시스템"으로 "소포 배달 소형 드론으로부터 인구 밀집 지역 상공을 운항하는 여객 운송, 에어택시에 이르기까지 모든 것"[4] "고도로 자동화된 비행 차량을 사용하여 도시 및 교외 지역 내 낮은 고도에서 승객이나 화물을 운송하는 안전하고 효율적인 항공 운송 시스템"[5]으로 '첨단 항공 교통수단(Advanced Air Mobility: AAM)'의 한 종류이다.[6]

이러한 첨단 교통수단 기술은 경제적 및 환경적 이점과 함께 교통안전과 편의성을 획기적으로 증가시킨다.[7] 그러나 첨단 교통 차량이 점점 더 자동화되고 상호 연결성이 심화되는 것에 비례하여 그에 따른 사이버 침해 위험도 증가한다.[8] 만일 해커 등이 첨단차량의 사이버 보안 취약성(cybersecurity vulnerabilities)을 악용하는 경우 야기될 수 있는 위험은 탑승자의 불편이나 사소한 주행 방해에서부터 탑승자와 차량 외부인에 대한 생명의 위협까지 다양할 수 있다. 데이터의 오류에 따른 시스템의 오작동과 시스템의 무결성(無缺性)에 대한 위협, 특히 해커가 차량의 가속, 감속, 제동장치, 조향장치를 무력화하거나 차량의 조

---

3) Dorothy J. Glancy, Privacy in Autonomous Vehicles, 52 Santa Clara L. Rev. 1171, 1174-1177 (2012).

4) UAM Vision Concept of Operations (ConOps) UAM Maturity Level (UML) 4, Version 1.0, NASA 76 (2020).

5) FAA, Urban Air Mobility and Advanced Air Mobility (2020) at https://www. faa.gov/uas/advanced_operations/urban_air_mobility/, 08.10.2020.

6) Adam Cohen & Susan Shaheen, "Urban Air Mobility: Opportunities and Obstacles", International Encyclopedia of Transportation, 702, 702-703 (2021); David P. Thipphavong et al., "Urban Air Mobility Airspace Integration Concepts and Considerations," NASA 1-2 (2018). AAM은 '개인 비행차량(Personal Air Vehicle: PAV)' 또는 플라잉카(flying car)와 UAM 등을 포괄하는 보다 넓은 개념이다: id. UAM은 UAM 비행차량, 운항에 필요한 인프라, 운항 관리 시스템을 포괄한다: id.

7) Asma Zubedi et al, "Sustaining Low-Carbon Emission Development: An Energy Efficient Transportation Plan for CPEC",14(2) J. Inf. Process. Syst., 322, 336-340 (April 2018). 미국에서 AV가 전면적 상용화되는 경우, 차량 충돌 등 교통사고의 예방과 감소, 이동 시간의 단축, 특히 교통취약자의 편의성 제고, 교통 체증의 축소, 연비(에너지 효율성 증가) 등에 따른 사회적 이익만 연간 7,500억 USD로 예측되고, 장애인 일자리 440만 개 증가(미국 전역 총 일자리 920만 개), 미국 GDP 8,670억 USD증가(3.8% 증가), 미국 생산량 1조 6000억 USD 증가(5.7% 증가), 연방 세수 930억 USD증가(1.8% 증가)가 예상되고 있다: National Disability Institute : Economic Impacts of Removing Transportation Barriers to Employment for Individuals with Disabilities Through Autonomous Vehicle Adoption (2022) at https://www.nationaldisabilityinstitute.org/reports/autonomous-vehicle-adoption.

8) ENISA & JRC. Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous 31 (2021).

향과 속도를 제어할 수 있는 능력을 가로챌 때 심각한 도로교통 위험을 초래할 수 있고 심지어는 차량을 테러 수단으로[9] 악용할 수도 있다.

이 논문은 첨단 교통수단의 운행과 교통관리의 효율성 확보와 함께 사이버 위협에 대한 효과적 대응을 뒷받침하기 위하여 관련 첨단 교통 차량과 시스템의 사이버 취약성과 사이버 위협 사례를 검토하고 국제규칙, 미국, 유럽연합(European Union: EU) 등의 입법 상황을 참조하여 바람직한 한국의 법 제도의 방향과 골격을 모색하고자 한다.

Ⅱ. 첨단 교통 차량의 상호 연결성과 사이버 취약성

1. 상호 연결성

첨단 교통수단 산업을 선도하는 혁신적 기술 분야는 상호 연결성의 획기적 개선, 새로운 통신 채널 구축 및 액세스 포인트의 확산이라 할 수 있다. <그림 1>은 예시적으로 첨단 교통수단에서 확대되어 가는 통신 영역 및 액세스 포인트와 그 상호간의 연결성을 보여준다.

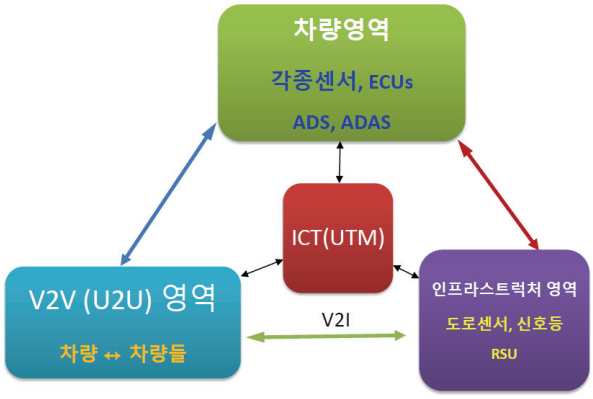
AV와 UAM은 차량과 차량, 차량과 교통 인프라스트럭처, 차량과 교통 (관제) 시스템 상호 연결된다. AV에 장착되는 ADS는 ①차량과 무선연결(Wifi, 블루투스, 5G 이동통신), ②차량-사물간 통신(Vehicle to Everything communication: V2X or U2X) 기술, ③ C-V2X알고리즘 개발, 정밀한 위치측정, 3D 고화질(HD) 맵핑(maping)},[10] ④ V2X의 데이터 축적하여 AV가 주행 환경을 완벽하게 파악하게 하는 드라이브 데이터 플랫폼(Drive Data Platform: DDP)과 차량이 환경변화 등 사례와 경험을 학습하는 딥러닝(deep learning), 기계학습(Machine Learning: ML), AI의 통합적 기능, ⑤계속 진화하는 ADAS[11] 등을 통합한다.[12]

---

9) 예컨대, 여러 대의 차량을 해킹하여 공급망과 응급구조 서비스를 차단할 수 있다: Nynke E. Vellinga, "Connected and vulnerable: cybersecurity in vehicles," 36(2) International Review of Law, Computers & Technology 161, 163 (2022).

10) 또한 이와 같은 시스템과 정보를 전문적으로 관리 해주는 '교통 통신 회사(Transportation Networking Companies: TNCs)'의 등장도 예상된다: Daniel A. Crane & Kyle D. Logue, Bryce C. Pilz, "A Survey of Legal Issues Arising From the Deployment of Autonomous and Connected Vehicles" 23 Mich. Telecomm. & Tech. L. Rev. 191 202 (Spring, 2017).

11) ADS를 개발하는 방향은 ①기존의 ADAS를 통합하고 자동화 수준을 향상시키는 진화적 방향과 ②처음부터 완전 자율주행 시스템 개발로 직행하는 혁명적 방향이 있다: Ching-Yao Chan, "Advancements, prospects, and impacts of automated driving systems," 6 International Journal



<그림 1> 첨단 교통수단의 주요 통신 영역과 상호 연결성

V2X는 '차량과 차량 사이의 무선 통신(Vehicle to Vehicle: V2V)',[13] '차량과 교통 인프라스트럭처 사이의 무선 통신(Vehicle to Infrastructure: V2I)' 등으로 구성된다. AV는 다양한 V2X 무선 통신으로 다른 차량, 시설, 주변 환경으로부터 획득한 데이터를 판단하여 스스로 위험 상황에 대처하면서 '자율 협력 주행'을 한다.[14] 이러한 상호 연결성에 초점을 맞추어 AV를 커넥티드 자율자동차(Connected Autonomous Vehicles: CAV)라고 부르기도 한다.

V2I 통신은 차량과 도로 인프라 간의 데이터를 무선으로 교환하는 것이다. 사물 인터넷(Internet of Things: IoT) 기반의 신호등, 차선표시, 도로표지판, 도로 카메라, 속도센서, 차벽 설치(dynamic and intelligent road barriers), 통행료 징수, 기상 관측 등의 하드웨어와 소프트웨어, 펌웨어로 구현되는 V2I 통신은 무선 및 양방향으로 차량과 정보를 주고받는다. V2I는 교통기반시설 간(infrastructure to infrastructure: I2I) 통신으로 확대된다. V2I 통신을 통하여 차량에서 도로변 장치(Roadside Units: RSUs)에 전송되는 데이터는 이동 출발지,

---

of Transportation Science and Technology 208, 210-211 (2017).

12) 류병운, supra note 1, at 34-36. UAM 비행차량도, AV와 유사하게, 배터리, 모터, 전자제어칩과 (UAM Vehicle to Everything communication: U2X)을 포함한 센서, ML과 강력한 클라우드 기반 컴퓨팅 플랫폼, 첨단기술과 빅데이터, AI가 적용된다: Sandeep Kulkarni & Renju Panicker & Murali Kadeppagari & Imtiaz Elahi, "Next-Gen Maintenance Framework for Urban Air Mobility Vehicles," SAE Technical Paper 2022-26-0008, (2022) at 6; 류병운. "UAM의 도입 및 산업화를 위한 법·제도의 설계", 홍익법학 제23권 제2호 (2022) 9-10면.

13) 현재 V2V 통신은 약 300미터 이내의 다른 차량들과의 통신이다: NHTSA V2V Fact Sheet (2017) at http://www.safercar.gov/v2v/index.html.

14) Federal Motor Vehicle Safety Standards: Vehicle-to-Vehicle (V2V) Communications, 79 Fed. Reg. 49,270 (Aug. 20, 2014); V2I Safety Applications: An Overview of Concepts and Operational Scenarios, U. S. Dep't of Transp, (Dec. 14, 2012).

차량의 과거 궤적, 목적지와 선호하는 이동 경로 등인데 RSU는 다른 RSU간의 I2I 통신을 통하여 차량에 실시간 교통 흐름 정보 데이터 등을 제공할 수 있다.[15]

CAV, V2V, V2I, I2I는 지능형 교통 시스템(Intelligent Transportation Systems, ITS)으로 관리된다. ITS는 사람의 안전, 시간과 비용의 절약, 환경 보호를 위하여 교통관리에 첨단기술을 적용한 것이다. [16] ITS의 목적에는 차량과 교통 시스템의 사이버 보안도 당연히 포함된다.[17] ITS의 정의에는 지상 및 철도에서 해상 및 항공 여행에 이르기까지 모든 교통수단이 포함된다. 예컨대, 자율 기동성, 편의성, 이동성 및 통신, 데이터 처리 및 저장 등 UAM의 특징적 기능으로 인해 UAM은 필연적으로 ITS의 핵심 구성 요소이다.[18]

AV나 UAM 비행차량에는 개별 차량의 사고 방지나 편의성 향상 등의 안전한 주행, 교통 혼잡 완화 등 전체적 교통관리를 위하여 중앙 교통 네트워크 시스템을 통해 상호 연결되는 최대 150개의 전자 제어 장치(Electronic Control Units: ECUs)들이 장착되어 있다. 비록 AV가 아니더라도 오늘날 새로 개발되는 차량에는 사물 IoT 기능이 추가된 각종 차량 센서, LIDAR, RADAR, 입체 카메라, GPS로 불리는 위성항법장치(Global Navigation Satellite System: GNSS), 일기 예보, 주차 장소 감지, 교통 체증, 통행료 결제 등 다양한 목적을 위한 다양한 장치가 장착되고 다양한 기술 수준의 무선통신 기능이 탑재되며, 인터넷에 연결되어 주행, 안전, 엔터테인먼트 시스템의 업데이트를 할 수 있다. 또한 탑승자는 휴대전화로 차량의 엔터테인먼트 시스템과 연결되고 차량 내비게이션에는 GNSS 위치 입력 등의 작업도 가능하다.

2. 사이버 보안 취약성

첨단 교통수단의 지능성과 V2X 등 상호 연결성의 급증으로 해킹 등 사이버 보안 위협은 더욱 심각해졌다. 시스템 요구 사항과 복잡성의 증가와 함께 인포테인먼트 연결부터 무선

15) T.S. Abraham & K. Narayanan, “Cooperative communication for vehicular networks” in EEE International Conference on Advanced Communications, Control and Computing Technologies 1163 - 1167 (2014).

16) Intelligent Transportation Systems Society of Canada, ITS Canada. “Intelligent Transportation.” (2012) at https://www.itscanada.ca/it.

17) T. Mecheva & N. Kakanakov, “Cybersecurity in Intelligent Transportation Systems,”. 9(4) Computers 83, 84-87 (2020).

18) Leilei Wang, et al., “A review of Urban Air Mobility-enabled Intelligent Transportation Systems: Mechanisms, applications and challenges”, 141 Journal of Systems Architecture 102902 (2023) at 2-3.

(over-the-air: OTA) 소프트웨어 업데이트까지 디지털 혁신이 유입되면서 첨단교통 차량은 데이터 교환소가 되었다. 무선통신으로 소프트웨어 업데이트는 악성코드를 심는 기회가 될 수 있다. 탑승자를 위한 다양한 차량 앱과 온라인 서비스, 특히 고객이 온라인으로 운송서비스를 구매하고 잠금을 해제할 수 있는 차량 기능도 존재한다. 그런데 첨단 교통 차량의 수많은 센서들이 생성하는 엄청난 양의 매우 다양한 데이터, 특히 암호화되지 않는 IoT 장치 생성 프로토콜 데이터의 적절한 관리와 보안은 상당히 어렵다. 데이터의 막대한 양과 다양성, 특히 '장치 신호의 비일관성(inconsistency of device signal)'은 개별 차량 자체 시스템에 대한 사이버 위협을 가하는 애드웨어, 맬웨어 등 악성코드의 탐색을 어렵게 한다. 이러한 취약성을 악용하여 해커 등 네트워크 침입자들은 차량 내 중요 ECUs와 생성 또는 축적 데이터에 접근하여 차량의 안전 기능과 탑승자 등 개인데이터를 침해할 수 있다. 현재 차량내 네트워크(In Vehicle Networking: IVN) 프로토콜에는 충돌 해결을 위한 ID 기반 중재 시스템의 보안 취약성과 메시지 인증이나 암호화 부족의 문제가 있다.[19] 이것은 해커 등 네트워크 침입자가 입력 데이터를 임의로 변경하여 차량의 주행을 방해하거나 연결 통신을 차단할 수 있는 것을 의미한다.[20] 이와 같은 데이터 변경을 즉시 시정하여 차량의 시스템을 안전하게 보호할수 있는 보정 기능도 갖추고 있지 않다.[21] 또한, 해커는 연결 통신을 방해하기 위해 과도한 양의 트래픽으로 장치에 과부하를 주는 DoS 공격을 가할 수도 있다.[22]

만일 해커가 일단 차량 시스템에 대한 액세스 권한을 획득한다면 주행과 통신에 영향을 미칠 수 있는 거의 모든 형태의 조작이 가능하다.[23]

이러한 데이터는 IVN에서는 물론 외부로 전송되는 과정에서도 사이버 위협에 노출될 수 있다.[24] 그런데 차량은 외부의 교통 시스템, 다른 차량, 시설과 다양하고 무수한 구성요소와 수많은 라인의 소프트웨어 코드로 연결된 특성으로 말미암아 가능성이 다양한 사이버 공격과 위협을 파악하여 대처하기 어렵다. 해커는 몇 줄의 악성코드만으로 차량 통제

19) M. Iorio et al., "Securing SOME/IP for in-vehicle service protection," 69(11), IEEE Trans. Veh. Technol. 13450, 13454-3465 (2020).
20) A. Taeihagh & H. Si Min Lim, "Governing Autonomous Vehicles: Emerging Responses for Safety, Liability, Privacy, Cybersecurity, and Industry Risks." 39 (1) Transport Reviews 103, 115 - 117 (2019).
21) Nynke E. Vellinga, supra note 9, at 63.
22) M. Iorio et al., supra note 19, at 13465.
23) D. P. F. Möller & R. E. Haas, Guide to Automotive Connectivity and Cybersecurity: Trends, Technologies, Innovations and Applications. 367 - 369 (2019).
24) F. W. Alsaade & M. H. Al-Adhaileh, "Cyber Attack Detection for Self-Driving Vehicle Networks Using Deep Autoencoder Algorithms." 23(8) Sensors 4086, 4088 (2023).

와 관련된 SIM 카드를 침해할 수 있다. 해커는 리버스 엔지니어링 방식으로 IoT 장치의 데이터 생성 및 통신 기술을 파악하여 악의적인 데이터를 연결 네트워크에 주입하는 '침입 기반 공격(intrusion-based attacks)'을 감행할 수 있다. 인터넷, Wi-Fi 또는 블루투스와 인포테인먼트(infotainment) 시스템을 통해 차량에 대한 사이버 공격이 가능하다.[25] 차량 데이터의 보안 취약성과 함께, 특히 가로채어 악의적인 목적으로 악용될 수 있는 무선통신 기반의 차량 상호 연결성의 확대는 교통안전과 차량 기능에 대한 위험을 증가시키고 개인 프라이버시 침해 가능성도 심각해졌다.[26] 연결망은 해킹이나 버그의 생성으로 그 시스템의 파괴, 오작동, 불안정을 초래할 수 있다. 예컨대, V2I 시스템 공격자는 커넥티드 교통시설을 악용하여 차량이나 탑승자 등에 피해를 일으킬 수 있다. 교통 시스템 통신망에 기능적 장애를 일으키면 도로교통의 위험과 체증이 발생하게 된다.

국민이 첨단 교통수단을 선택하고 이용을 결정하는 수용성(受容性)은 그 교통수단의 안전과 편의성에 대한 신뢰에 달려있다.[27] 첨단 교통수단의 사이버 보안 취약성을 극복하지 않고는 그 신뢰성을 확보할 수 없다. 사이버 보안은 차량 내 시스템의 디지털화, 소프트웨어 확산, 나아가 새로운 완전 디지털 모빌리티 서비스 창출의 필요조건이라고 할 수 있다.

Ⅲ. 사이버 공격 사례

1. 차량관련 사례

커넥티드 자동차에 대한 초기 사이버 공격 사례는 2002년 아우디, 폭스바겐, 포르쉐, 포드 자동차에 대하여 발생하였다.[28] 2005년 BMW와 Nissan 자동차도 해킹당했다.[29]

---

25) P. H. Phung & D. K. Nilsson, "A model for safe and secure execution of downloaded vehicle applications". in Road transport information and control conference and the ITS United Kingdom members' conference (RTIC 2010)-better trans- port through technology, IET. 1 - 6 (2010).

26) W Choi et al., "Identifying ecus using inimitable characteristics of signals in controller area networks" 67 IEEE Trans. Veh. Technol. 4757, 4761 (2018).

27) 류병운. supra note 12. at 4.

28) Jonathan Fahey, "How to Hack Your Car" (Jul 8, 2002) at https://www.forbes.com/forbes/2002/0708/148.html?sh=40999b236b49.

29) Id.

2015년형 시속 70마일로 주행중이던 Jeep Cherokee가 사이버 보안 전문가인 Miller와 Valasek의 해킹으로 손상되었다.[30] 이 해킹은 차량의 인터넷 연결을 통해 15km 이상 떨어진 곳에서 원격으로 이뤄졌다.[31] 해커들은 IP 주소에 액세스를 허용하는 취약성을 가진 Uconnect 기능을 악용하여 차량의 인포테인먼트 시스템에 원격으로 액세스할 수 있었다. 다음 해커는 와이어 시스템을 통해 운전할 수 있는 권한을 얻었고 시동을 켜고, 엔진 속도를 낮추고, 갑자기 브레이크를 작동하거나 브레이크를 비활성화할 수 있었다. 또한 그들은 Jeep의 GNSS(GPS) 및 IMU(관성 이동 장치)에 액세스하여 속도, 온도, 거리, 방향을 측정할 수 있었다. 이 해킹으로 자동 가속, 브레이크 작동, AC 장치 온도의 변경, 조명 변경, 라디오 방송 채널 변경과 전원 버튼 부작동, 앞유리 와이퍼의 작동, 차량 도어 잠김 등 현상이 발생하였다.[32] 2015년 Jeep Cherokee 해킹 사건은 해커가 일단 차량에 대한 액세스 권한을 얻은 후에는 그 주행이나 운전에 무한정으로 개입할 수 있다는 것을 보여준다.[33]

2016년형 Mitsubishi Outlander PHEV 모델이 PenTestPartners의해 해킹되어 원격으로 제어되었다.[34] 이 모델은 연결 서비스 통신으로 Wi-Fi를 사용한다.[35] Wi-Fi는 GSM 모듈 대신 액세스 포인트가 한정됨으로써 원격 액세스 범위가 크게 제한되는 반면 특수한 원격 연결 방법을 악용하는 공격에는 더 취약할 수 있다. PenTestPartners는 Wi-Fi의 사전 공유키(Pre Shared Key: PSK)를 크래킹하여 이를 이용하고 차량에 인증된 전화에 연결 시에만 그 차량에 액세스할 수 있도록 하여 알람을 비활성화하고 차량 잠금을 해제할 수 있었다.[36]

2016년 호주의 한 연구자는 영국에 있는 Nissan Leaf에 침투하여 차량 온도 조정과 모든 주행 기록 열람이 가능함을 보여 주었다.[37] 이 모델이 사용하는 'NissanConnect' 소프트웨

30) A. Greenberg, "Hackers Remotely Kill a Jeep on the Highway - With Me in It," Wired, (21 July 2015). at https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway. 이전에 Miller와 Valasek은 OBD(On Board Diagnostics)-II 연결을 통해 Ford Escape를 해킹한 바 있다: id.

31) Id.

32) Id. 몇 줄의 코드로 차량의 센서들을 기만하여 기압, 조명, 온도, 차량 데이터 다운로드, 음악 재생 또는 통화, 도어 제어, 브레이크 및 가속기와 같은 차량 모니터링 시스템을 제어하거나 훼손할 수 있다: id.

33) D. P. F. Möller & R. E. Haas, supra note 23. at 368-369.

34) D. Lodge, "Hacking the Mitsubishi Outland PHEV hybrid," PenTestPartners, (June 5 2016) at https://www.pentestpartners.com/security-blog/hacking-the-mitsubishi-outlander-phev-hybrid-suv.

35) 반면 보다 많은 신차들은 GSM(Global System for Mobile Communications) 모듈을 사용하므로 소유자는 차량에서 멀리 떨어져 있어도 모바일 통신으로 위치 추적, 냉난방 설정, 창문 열기를 할 수 있다. GSM 휴대폰 및 태블릿 등 모바일 장치에서 사용되는 900MHz의 주파수를 사용하는 디지털 통신 표준으로 ETSI(European Telecommunications Standards Institute)에서 개발하였다.

36) D. Lodge, supra note 34.

37) R. Hull, "Nissan disables Leaf electric car app after revelation that hackers can switch on the

어는 사용자가 앱에 차대번호(VIN)를 입력을 하면 차량에 액세스할 수 있도록 하여 사이버 공격에 매우 취약하였다.[38]

2018년에는 BMW의 3개 모델에서 사이버 취약점의 존재가 발견되었다. 해커는 OBD 연결을 통해 잘못된 메시지로 차량 시스템에 과부하를 주어 차량을 정지시킬 수 있었다.[39]

2018년 해커가 로컬 네트워크를 통해 Tesla차량에 통신 방해 메시지를 전달하였다.[40]

기술보고서에서만 사이버 취약성이 드러난 경우로서 2020년형 폭스바겐 폴로(Volkswagen Polo)의 인포테인먼트 시스템을 해커가 악용한다면 트랙션 컨트롤을 전환하고 운전자의 개인 데이터를 검토할 수 있는 액세스 권한을 확보할 수 있는 가능성이 드러났다.[41]

2. 관리 및 지원 시스템관련 사례

2017년 Tesla 플리트 중앙 서버가 해킹당했다.[42] 'Mothership'은 Tesla의 홈 서버 이름으로, 이를 통해 전체 자동차와 통신한다. Teslas는 개별 차량이 자율주행 중 얻은 데이터를 'Mothership'에 전송하면 이를 서버에 업로드 하여 모든 차량이 액세스하여 이전에 탐색한 적이 없는 환경에서 자율 주행을 할 수 있도록 한다. 즉, 한 차량이 무언가를 배우면 전체 차량이 그것을 배우게 된다. 그런데 'Mothership에' 대한 액세스 권한을 얻으면 전체 Tesla 플리트 차량들을 상당한 정도로 제어할 수 있게 된다. 다만, 이러한 Tesla 사(社) 중앙 관리 지원을 받기 위해서는 Tesla 플리트 중앙 서버가 실행 중이고 호스트에 액세스할 수 있어야

---

heater to drain the battery," This is Money.co.uk, (Feb 26 2016) at https://www.thisismoney.co.uk/money/cars/article-3465459/Nissan-disables-Leaf-electric-car-app-hacker-revelation.html.

38) 사실 많은 차량에서 VIN은 앞유리 등에 찍혀 있어 파악하기 쉽고 제조업체 코드, 모델 코드, 국가 코드가 공통 있으므로 사이버 공격자는 차량마다 달라지는 5자리 코트를 크래킹하거나 추정하면 된다: id.

39) "New Vehicle Security Research by KeenLab: Experimental Security Assessment of BMW Cars," Keen Security Lab , (May 22 2018) at https://keenlab.tencent.com/en/2018/05/22/New-CarHacking-Research-by-KeenLab-Experimental-Security-Assessment-of-BMW-Cars.

40) A. Chowdhury et al., "Attacks on Self-Driving Cars and Their Countermesasures: A Survey," IEEE Access, vol. 8, 35 (2020).

41) L. Barber, "Popular connected cars from Ford and Volkswagen could put your security, privacy and safety at risk, Which? finds," Which?, (April 9, 2020) at https://press.which.co.uk/whichpressreleases/popular-connected-cars-from-ford-and-volkswagen-could-put-your-security-privacy-and-safety-at-risk-which-finds.

42) F. Lambert, "The Big Tesla Hack: A hacker gained control over the entire fleet, but fortunately he's a good guy," Electrek, (Aug. 27 2020) at https://electrek.co/2020/08/27/tesla-hack-control-over-entire-fleet.

한다. 이 사례에서 해커는 자신 차량의 VPN을 사용하여 Tesla 개발자 네트워크에 연결이 가능해지자 마치 모선에서 함대에 명령을 보내는 것처럼 플리트 전 차량들의 일부 기능의 제어와 위치 정보, 배터리 상태 등 여러 데이터에 대한 액세스 권한을 확보할 수 있었으며 Tesla사(社)의 명령 전달을 가장할 수 있었다.[43]

2017년 4월 9일 오후 11시 40분경 해커들에 의하여 미국 텍사스 댈러스에서 156개 모든 비상 사이렌이 울렸다.[44] 비상 사이렌은 관제센터와 사이렌 장치 간에 인터넷 연결이 없는 무선통신만 사용했으나 해커들은 먼저 보안을 풀어 시스템 제어 권한을 획득하고 사이렌을 작동시키기 위해 무선통신을 조작하였다. 이것이 ITS 인프라에 대한 직접적 사이버 공격은 아니나 놀란 주민들의 911 문의전화 폭주 등으로 사실상 긴급 구난 시스템 마비 상황을 초래하였다.[45]

2017년 독일 뒤셀도르프의 대중 교통 회사인 Rheinbahn 사(社)의 노선 및 일정 관리시스템의 업그레이드가 잘못되어 80개의 노선에서 총 832대의 버스와 기차의 연착, 지연, 운행 취소의 사태가 발생하였다. 이 사건은, ITS 사이버 공격으로 발생한 것은 아니지만, 사이버 공격으로 같은 상황이 얼마든지 발생할 수 있음을 보여준다.[46]

2016년 11월 미국 샌프란시스코 도시교통국(San Francisco Municipal Transportation Agency: Muni) 시스템이 크립토 랜섬웨어 공격을 당했다.[47] 이 공격으로 Muni 전철역의 요금기에 고장 안내가 표시되다 보니 Muni는 무료로 경전철을 운행할 수밖에 없었다.[48] 이 사례는 자동차 등 여타 교통수단의 관리시스템에 대한 사이버 공격 가능성을 보여준다.

---

43) Id.

44) Samira Said, “Hacker sets off emergency alarms, frightening Dallas residents.”. (9 April 2017) athttp://www.cnn.com/2017/04/08/us/dallas-alarm-hack/index.html.

45) Lily Hay Newman, “That Dallas Siren Hack Wasn’t Novel – It Was Just Really Loud.” Wired, (10 April 2017) athttps://www.wired.com/2017/04/dallas-siren-hack-wasnt-novel-just-really-loud.

46) Alessa Brings and Stefani Geilhausen, “Wie Hightech am Donnerstag die Rheinbahn lahm legte.” RP Online (21 April 2017)at http://www.rp-online.de/nrw/staedte/duesseldorf/wie-hightech-am-donnerstag-die-rheinbahn-lahm-legte-aid-1.6768928.

47) 당시 악성 코드 변종 공격에 연결된 이메일 주소가 HDDCryptor이었다: Stephen Hilt and Fernando Mercês, “HDDCryptor: Subtle Updates, Still a Credible Threat,” (November 30, 2016) at http://blog.trendmicro.com/trendlabs-security-intelligence/hddcryptor-updates-still-credible-threat.

48) Sean Gallagher “Ransomware locks up San Francisco public transportation ticket machines,”Ars Technica (November 29, 2016). at https://arstechnica.com/information-technology/2016/11/san-francisco-muni-hit-by-black-friday-ransomware-attack; Joe Fitzgerald Rodriguez. “‘You Hacked’ appears at Muni stations as far payment system crashes.” San Francisco Examiner (November 26 2016) at http://www.sfexaminer.com/hacked-appears-muni-stations-fare-payment-system-crashes.

3. 교통시설관련 사례

2017년 워싱턴대, 미시간대, 스토니브룩대, UC 버클리 연구원 그룹은 도로 표지판에 스티커를 붙여 도로 표지판을 시각적으로 조작하는 방식으로 자율주행 차량을 해킹할 수 있었다.[49] 연구원들은 차량의 이미지 분류 알고리즘을 분석한 다음, 예컨대, STOP 표지판을 45MPH표지판으로 착각하도록 기계학습을 속이기 위해 스티커를 사용하여 도로 표지판을 시각적으로 조작했다.[50] 이러한 공격의 결과는 이미 (부분적) 자율주행이 이루어지는 현실 세계에서, 특히 V2I 통신이 활성화되는 경우 매우 치명적일 수 있다.

2016년 미국 텍사스 달라스 고속도로 교통(안내) 표지판이 해킹으로 교통정보 대신 "Drive Crazy Yall"라는 말이 표시되었다.[51] 비슷한 시기에 해킹으로 달라스의 교통(안내) 표지판에 엉뚱한 내용들이 표시되었다.[52] 2017년 캘리포니아의 고속도로 교통안내 전자 게시판이 해킹되어 혐오 내용이 게시되는 사건이 여러 건 발생하였다.[53] 처음 사건이 발생한 후 전자 게시판 관리소는 접근 암호를 설정하였으나 해커는 여전히 암호를 우회하여 다른 메시지를 게시하였다. 이러한 행위는 운전자의 주의를 분산시켜 안전을 위태롭게 할 수 있고 또한 향후 첨단 교통수단을 위한 교통시설에 대한 해킹 위협을 드러낸다.[54]

4. 기타 사례

---

49) John Beltz Snyder, “Researchers hack a self-driving car by putting stickers on street signs.” Autoblog (August 4 2017) at https://www.autoblog.com/2017/08/04/self-driving-car-sign-hack-stickers.

50) Id.

51) 이 사건 Geoffrey Eltgroth가 피의자 체포되어 기소되었다: Tom Steele. “Central Texas man says he changed highway sign to ‘Drive Crazy Yall’ for a laugh.” Dallas News (May 23 2016) at https://www.dallasnews.com/news/crime/2016/05/23/central-texas-man-says-he-changed-highway-sign-to-drive-crazy-yall-for-a-laugh.

52) Katie Mettler, “Somebody keeps hacking these Dallas road signs with messages about Donald Trump, Bernie Sanders and Harambe the gorilla.” The Washington Post (June 6 2016) at https://www.washingtonpost.com/news/morning-mix/wp/2016/06/06/somebody-keeps-hacking-these-dallas-road-signs-with-messages-about-donald-trump-bernie-sanders-and-harambe-the-gorilla/?utm_term=.d396ae2a8d66.

53) 예컨대, "트럼프에 헤르페스가 있습니다", "향후 무료 매춘", "아시아인 운전자 주의"등이 고속도로 교통안내 게시판에 표시되었다: Carla Herreria,“California Traffic Sign Hacked To Warn People Of ‘Asian Drivers’,” HuffPost (August 7 2017) at http://www.huffingtonpost.ca/entry/caution-asian-drivers-napa-traffic-sign_us_595ef341e4b0d5b458e9678e

54) Jessica Morgan “California road sign hacked to read ‘Trump Has Herpes’.”Evening Standard (August 4 2017) at https://www.standard.co.uk/news/world/california-road-sign-hacked-to-read-trump-has- herpes-a3603821.html;

2017년 보안전문회사인 Whitescope사(社) 연구원들이 인터넷에 연결된 드라이브 스루 세차장에서 해커가 원격으로 세차기(PDQ 레이저워시) 관리 권한을 확보하여 차량과 탑승자 등을 물리적으로 공격할 수 있는 취약점을 발견했다.[55] 세차를 하는 사람은 세차장 진입 전에 터치스크린으로 세차 방식을 선택할 수 있다. 그런데 PDQ 시스템에 접속하려면 사용자 이름과 패스워드가 필요하지만, IoT 기기들이나 CCTV 카메라 등에서 흔히 사용하는 디폴트 패스워드는 어렵지 않게 추정할 수 있다.[56] 또한 인증 프로세스 중에도 취약점이 있어 우회할 수도 있다.[57] 이와 같은 세차시설은 ITS에 통합될 가능성이 없고 해킹이 발견되기 전에 현실적으로 제한적인 피해만 야기할 수 있으나, 손상된 인터넷 연결 시스템으로 인해 차량과 운전자의 안전이 위험에 처할 수 있는 추가 사이버 공격이 가능하다.[58]

Ⅳ. 첨단 교통의 사이버 안보를 위한 입법례

1. UN 규칙 No. 155와 No. 156

자동차의 전자제어와 커넥티드 장치의 장착 및 관련 통신시스템의 구축으로 불법 자동차 제어, 제어 방해, 프라이버시 침해 등 사이버 취약점과 위협이 증가함에 따라 '국제연합 유럽 경제 위원회(United Nations Economic Commission for Europe: UNECE)'[59] WP.29

55) PDQ 레이저워시 드라이브 스루 타입 세차기 입구와 출구의 문을 잠궈 탑승자의 감금은 물론 차량과 승무원에게 부상을 입힐 수도 있다: "Warning over internet connected car washes as hackers show they can 'go rogue' and be remotely controlled to trap motorists and damage cars," (July 27 2017) at https://www.dailymail.co.uk/sciencetech/article-4737298/Car-wash-hacks-trap-motorists-smash-cars.html.

56) Id.

57) Id.

58) Kim Zetter, "Car Wash Hack Can Strike Vehicle, Trap Passengers, Douse Them With Water."Vice Motherboard (July 26 2017) at https://motherboard.vice.com/en_us/article/bjxe33/car-wash-hack-can-smash-vehicle-trap-passengers-douse-them-with-water.

59) UNECE는 ① 당사국간 자동차 승인 및 상호 인증을 위하여 규칙(기준)을 통일하기 위한 1958년 협정{Agreement concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations, Revision 3, E/ECE/TRANS/505/Rev.3 (20 October 2017)}; ② UN 글로벌 기술 규칙(Global Technical Regulations: GTR)을 위한 1998년 협정{Agreement on UN Global Technical Regulations, ECE/TRANS/132, (25 JUNE 1998)} ③ 자

(자동차기준국제조화협의회)는 자동차 사이버보안에 관한 UN 규칙 No. 155[60]와 No. 156[61]을 채택하였다.

UN 규칙 No. 155는 UNECE 당사국들의 국내 기준으로 채택되는 신차의 형식승인(Vehicle Type Approval: VTA)을 위한 사이버 보안과 사이버 보안 관리 통일 기준이다. 동 규칙의 적용 대상 자동차는 승용차, 승합차, 화물차, 전자제어 장치가 장착된 트레일러, 자율주행 기능이 장착된 초소형차 등이다.[62] UN 규칙 No. 155에 따라 UNECE 당사국 내 제작사들은 신규 생산 차량에 대한 사이버 보안 관리를 위한 체계(Cyber Security Management System: CSMS)를 구축하여 형식승인을 받아야 한다. 따라서 형식승인을 신청하는 제작사는 CSMS 인증서를 제출해야 한다.[63] CSMS는 "차량에 대한 사이버 위협과 관련된 위험을 처리하고 사이버 공격으로부터 보호하기 위해 조직 프로세스, 책임 및 거버넌스를 정의하는 체계적인 위험 기반 접근 방식"[64] 이다. 제작사가 갖추었음을 증명해야 하는 CSMS 프로세스에는 차량 유형에 대한 위험을 식별, 평가, 분류, 관리를 위한 프로세스[65]와 차량 유형의 사이버 보안성 시험에 사용되는 프로세스[66]가 포함된다. CSMS 사이버 보안을 위하여 "무단 접근을 방지하고 탐지하기 위한 조치를 취해야"[67]하는 제작사의 의무 외에 다양한 사이버 위험의 완화를 위한 구체적 프로세스가 동 규칙 부록 5에 나열되어 있다. 신청된 VTA 처리를 위하여 기술 서비스 기관(Technical Service)이 제작사가 신청한 차량 형식에 대해 기능 안전과 동시에 사이버 보안을 심사하게 된다.

UN 규칙 No. 156은 차량의 소프트웨어 업데이트 방법에 대한 요구 사항을 규정한다.

동차 검사 규칙을 위한 1997년 협정{Amendments to the 1997 Agreement on Periodic Technical Inspection of wheeled vehicle ECE/TRANS/WP.29/2020/38 (9 January 2020)}의 채택을 주관하였다. 이 협정들은 UNECE 세계 포럼(WP.29) 세션에 참석하는 당사국이 자동차 및 관련 규칙, 규제 수단을 채택할 수 있는 법적 틀을 제공한다.

60) Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system, UN Regulation No. 155, ECE/TRANS/WP.29/2020/79 (as amended by ECE/TRANS/WP.29/2020/94 and ECE/TRANS/WP.29/2020/97)[이하 "UN 규칙 No.155"].

61) Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system, UN Regulation No. 156, ECE/TRANS/WP.29/2020/80 [이하 "UN 규칙 No.156"]. .

62) UN 규칙 No.155 para. 1, Consolidated Resolution on the Construction of Vehicles (R.E.3.), document ECE/TRANS/WP.29/78/Rev.6, para. 2.

63) UN 규칙 No.155 para. 7.2.1.

64) Id. para. 2.3.

65) Id. para. 7.2.2.2.(b).

66) Id. para. 7.2.2.2.(e).

67) Id. para. 9.1.

VTA를 신청하는 제작사는 '소프트웨어 업데이트 관리시스템(Software Update Management System: SUMS)'인증서를 제출해야 한다.[68] SUMS는 UN 규칙 No. 156의 소프트웨어 업데이트 제공 요구 사항을 준수하기 위한 조직적 프로세스 및 절차를 정의하는 체계적 접근 방식이다.[69] SUMS 준수 인증서를 얻기 위해 제작사는 업데이트 프로세스가 소프트웨어의 손상 방지를 위한 것[70]과 운전 중에 무선 업데이트 진행이 안전에 영향을 미치지 않는다는 것을 평가하기 위해 사용할 프로세스와 절차를 증명해야 하고[71] 업데이트된 시스템과 다른 시스템의 상호 의존성을 식별할 수 있는 프로세스[72] 및 업데이트와 대상 차량 구성의 호환성을 설정하는 프로세스[73] 등 다양한 조직 프로세스를 갖춰야 한다. 이와 같이 제작사는 SUMS를 통하여 악성코드 설치를 회피해야 한다.

2. 국제 기술 표준

자동차 사이버 보안에 대한 대표적 국제 기술 표준으로는 국제 표준화 기구(International Organization for Standardization: ISO)와 자동차공학회(Society of Automotive Engineers: SAE)가 공동으로 채택한 ISO/SAE 21434, 전기전자공학협회(Institute of Electrical and Electronics Engineers: IEEE)의 802.11p 등을 들 수 있다.

UN 규칙 No. 155는 VTA승인 당국과 그 기술 서비스는 예컨대, ISO/SAE 21434와 같은 적절한 사이버 보안 기술과 특정 자동차 위험평가 지식을 갖춘 유능한 인력을 갖추어야 한다고 규정하고 있다.[74] 이것은 ISO/SAE 21434에 따라 CSMS를 입증과 전반적인 사이버 보안관리에 대한 평가가 이루어질 수 있다는 것을 의미한다.

3. EU

EU 자동차 일반 안전 규칙[75] [이하 "EU 규칙 2019/2144"]은 "차량의 연결성과 자동화

68) UN 규칙 No. 156 para. 6.2.
69) Id. para. 2.5.
70) Id. para. 7.1.3.2.
71) Id. para. 7.1.4.1.
72) Id. para. 7.1.1.5.
73) Id. para. 7.1.1.7.
74) UN 규칙 No. 155 para. 5.3.1.(a)
75) Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November, 2019 PE/82/2019/REV/1, OJ L 325/1.

로 인해 차량 내 데이터에 대한 무단 원격 액세스와 무선 소프트웨어의 불법 수정 가능성이 높아졌다."[76]라는 인식 아래 "이러한 위험을 고려하기 위해서는 사이버 보안에 관한 UN 규칙이나 기타 규제법이 발효된 후 가능한 한 빨리 의무적으로 적용되어야 한다."[77]라고 하면서 EU VTA 프로세스에 UN 규칙 No. 155과 No. 156을 편입시켰다.[78] 따라서 2022년 7월 6일부터 모든 새로운 유형의 차량은 UN 규칙 No. 155과 No. 156의 요구 사항을 충족해야 한다.[79] EU 규칙 2019/2144는 사고 데이터 기록장치(Event Data Recorder: EDR)의 장착을 의무화하였다.[80] 이 EDR은 '중요한 충돌 관련 매개변수 및 정보'를 기록하고 저장해야 한다.[81] EDR은 차량 시스템 및 안전성 검토에 중요한 장치이자 그 정보는 해커의 표적이 될 수 있다.

EU 자동차 승인 및 시장 감시 규칙[82][이하 "EU 규칙 2018/858"]은 VTA 승인기관이 차량이나 시스템이 심각한 위험을 초래하거나 규칙을 준수하지 않는 것으로 의심되는 경우 승인 재검토, 승인 철회 등의 조치를 해야 한다고 규정한다.[83] EU 규칙 2018/858은 '심각한 위험'을 정의(定義)하지 않은 채 오작동으로 인해 차량 시스템의 기능에 심각한 위험을 초래할 수 있는 시정조치 대상 목록[84]만을 제공한다. 그런데 동 규칙의 위임에 따라 EU 집행위원회가 그 목록을 최신 내용으로 수정할 수 있어[85] 차량에 대한 사이버 위협이 '심각한 위험'에 포함될 여지가 생겼다.[86]

EU의 ① VTA이외의 다른 제품 승인에 적용되는 EU 사이버 보안규칙,[87] ② '높은 공통 수준의 사이버 보안 조치에 대한 지침[이하 "NIS 2"][88], ③ EU의 '일반적 데이터 보호 규칙'[89] [이하, "GDPR"] 와 같은 입법들도 차량과 교통 시스템에 대한 사이버 보안성 제고에

76) Id. Recital 26.
77) Id.
78) Id. art. 19, Annex II (D4).
79) Id.
80) Id. art. 6(1)(g).
81) Id. art. 3(13).
82) Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018PE/73/2017/REV/1, OJ L 151/1.
83) Id. art. 7(4).
84) Id. Appendix VI.
85) Id. art. 55(4).
86) Nynke E. Vellinga, supra note 9, at 168.
87) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019, PE/86/2018/REV/1, OJ L 151/15.
88) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022PE/32/2022/REV/2, OJ L 333/80.
89) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 OJ

이바지할 수 있다. NIS 2는 ITS를 사이버 보안 필수 중요 시설로 규정한다.[90] GDPR은 정보 주체에게 열람권, 정정권, 삭제권, 처리 제한권, 기제공 정보에 대한 반환이나 개인 데이터를 본인이 제3자에게로 전송을 결정할 수 있는 정보 이전권(right to data portablility), 프로파일링 등에 대한 반대권과 프로파일링을 포함한 의사결정의 자동화에 대한 거부권 등 정보 주체의 데이터에 대한 권리와 보호를 대폭 강화하였다.[91]

4. 미국

모든 차량에 대한 사이버 보안 및 개인 정보 보호에 대한 통제를 강화하기 위하여 현재 미국 의회에는 스파이자동차법안(the SPY Car Study Act of 2019)이 상정되어 있다.[92] 이 법안은 미국 교통안전청(National Highway Traffic Safety Administration: NHTSA)에게 미국에서 판매용으로 제조된 자동차를 ECUs, 중요한 소프트웨어 시스템 또는 운전 데이터에 대한 무단 접근으로부터 보호하는 규칙을 수립하고, 개인의 사이버 보안 및 개인 정보 보호 수준을 소비자에게 알리기 위해 표준화된 그래픽이 포함된 사이버 대시보드를 표시하도록 하며, 모든 차량의 중요 소프트웨어 시스템과 중요하지 않은 소프트웨어 시스템은 분리해야 하고, 차량 전자 시스템에서 수집된 데이터가, 전송 중 또는 오프보드 저장소 보관되는 동안, 그 보안을 보장하기 위한 사양을 도입하는 규칙을 제정할 것을 요구한다.[93] 또한 NHTSA는 차량이 운전 데이터를 캡처하거나 차량을 제어하려는 시도를 즉시 감지, 중지 및 보고할 수 있어야 하며, AV가 소비자의 개인 정보 및 사이버 보안을 보호하는 정도를 AV에 표시되도록 해야 한다.[94]

미국 교통부는 커넥티드 차량의 통신 안보와 신뢰성을 확보하고 해킹에 대비하고 하기 위하여 V2V와 V2X의 단기 통신 인증을 담당하는 '안보 자격 관리 시스템(Security Credential Management System: SCMS)'의 설치 운용을 제안하고 있다.[95] 또한, 미국 교통

L119/1.

90) NIS 2 art. 3, Annex I.

91) Id. art. 15~18, 20~22.

92) 이 법안은 2017년에 하원에 상정되었었고 다시 2019년에 상원에 상정되어 있다: H.R.701-115th Congress; S. 2182－116th Congress at https://www.congress.gov/116/bills/s2182/BILLS-116s2182is.pdf.

93) Id.

94) Id.

95) U.S. Dep'T Transp., Vehicle-To-Vehicle Security Credential MGMT SYS.; Request for Info 1-17 (Oct. 2014). 미국 교통부는 현재 NHTSA로 하여금 SCMS 소유권과 주요 공공 인프라스트럭처 정책을 포함한 거버넌스 모델을 개발 중이다: U.S. Dep'T Transp.,National Security Credential

부는 IEEE 802.11p 표준을 채택하고 전용 단거리 통신(dedicated short-range communications: DSRC)을 기반으로 한 V2V 통신 확장의 의무를 위한 규칙안을 제안하였다.[96] 이 DSRC/802.11p 통신 확장 의무에 따라 제작사들은 V2V 기술 개발하고 발전시켜야 한다.[97]

아울러 NHTSA는 AV의 사이버 보안을 위한 다양한 권고적 표준(가이드라인, Best practices)을 발표하고 있다. 예컨대, 제조사와 소프트웨어 회사는 국가표준기술연구소(National Institute for Standards and Technology: NIST), NHTSA, SAE 및 자동차 제작사 연합 등이 발표한 표준과 같은 기존 국제 표준에 따라 AV 시스템을 설계할 것과[98] "강력한 사이버 사고 대응 계획"을 수립하고 설계 과정에서 차량 사이버 보안을 고려하고 조정된 취약성 보고/공개 정책을 채택하는 시스템 엔지니어링 접근 방식을 사용할 것을 권고한다.[99] 또한, 위험 기반 우선순위 식별 및 보호, 적시 감지 및 신속한 대응, 방법 및 조치 설계를 포함하여 계층화된 사이버 보안을 설계하기 위하여 포괄적이고 체계적인 접근 방식이 필요하다는 것을 지적한다.[100] 한편 NHTSA에는 잠재적인 사이버 취약성을 평가 및 모니터링을 하기 위해 새로운 전자 시스템 안전 연구 부서가 설립되었으며 전자 및 사이버 보안 연구에 관한 협력을 강화하기 위해 내부 기관 실무 그룹인 전자 협의회도 설립되었다.[101]

5. 영국

2017년 영국 교통부는 CAV 및 ITS 생태계와 공급망 전반에 걸쳐 적용할 수 있는 사이버 보안의 핵심 원칙[102]을 수립하였다. 그 원칙은 보안 위험의 적절하고 비례적인 관리 및 평

Management System (SCMS) Deployment Support: SCMS Baseline Summary Report, FHWA-JPO-18-688, 10-57 (January 12, 2018).

96) Federal Motor Vehicle Safety Standards; V2V Communications. 82(8) FR 3854 (2017) at https://www.govinfo.gov/content/pkg/FR-2017-01-12/pdf/2016-31059.pdf.

97) Federal Motor Vehicle Safety Standards; V2V Communications. 82(8) FR 3854, 3857-3894 (2017) at https://www.govinfo.gov/content/pkg/FR-2017-01-12/pdf/2016-31059.pdf.

98) U.S. Dep'T Transp., Automated Driving Systems 2.0: A Vision for Safety 11 (2017).

99) U.S. Dep'T Transp., Automated Driving Systems 2.0: A Vision for Safety 11 (2017); U.S. Dep'T Transp., Preparing For The Future Of Transportation Automated Vehicles 3.0 17-18 (Oct. 2018)

100) U.S. Dep'T of Transp. NHTSA, Report No. Dot Hs 812.333, Cybersecurity Best Practices For Modern Vehicles 10-20 (2016).

101) U.S. Dep'T Transp., Preparing For The Future Of Transportation Automated Vehicles 3.0 18 (Oct. 2018).

102) UK Dep'T of Transp., The Key Principles of Cyber Securities for Connected and Automated Vehicles, (2017).

가해야 하고 시스템은 심층 방어 접근 방식을 통합해야 하며 안전한 업데이트를 통해 소프트웨어 보안을 위해 평생 제품 사후 관리를 권장한다.[103] 또한 데이터의 안전하고 통제된 전송 및 저장을 요구하고 사이버 공격에 대한 융통성 있는 대응과 방어에 실패하는 경우 비례적으로 대응을 주문하고 있다.[104]

2023년 영국 비즈니스혁신기술부(BIS) 연결되고 자동화된 차량이 더 넓은 운송 생태계 내에 존재할 것임을 인식 아래 CAV란 용어를 CAM(Connected and Automated Mobility) 수정하였다.[105]

Ⅴ. 사이버 보안 입법의 방향과 원칙

첨단 교통 차량과 시스템의 사이버 취약성과 예상되는 사이버 위협에 대응하기 위하여 국가들은 관련 사이버 보안법제를 도입하고 있다. AV와 UAM의 개발과 상용화를 목전에 두고 있는 한국의 경우, 첨단 교통사단 사이버 보안에 대한 입법수요에도 불구하고 현재까지 구체적 법규칙이 없다. 따라서 한국 정부는 여러 입법례와 국제 표준 그리고 다음과 같은 방향과 원칙을 참고하여 신속하게 관련 법제도를 마련하여야 한다.

1. 첨단 교통수단의 '사이버 보안'에 대한 명확한 정의(定義)

첨단 교통수단에 대한 사이버 위협에 대응하는 법과 정책을 수립하기 위해서는 먼저 그 '사이버 보안'에 대한 적절하고 명확한 정의가 필요하다.[106] 이러한 정의를 위해서는 먼저 첨단 교통수단과 관련하여 어떤 규제가 필요하고 그 규제의 대상과 행위를 파악해야 한다.

---

103) Id. at 5-9 10-13.

104) Id. at 14-17.

105) Connected and automated mobility-Vocabulary BSI Flex 1890 v5.0: 2023-04 at https://www.bsigroup.com/en-GB/CAV/cam-vocabulary. "자율주행차를 따로따로 보는 것이 아니다. 이 기술은 …다양한 미래 모빌리티 솔루션의 핵심이 될 것이다. 이들은 결합되어 우리의 교통 시스템을 보다 효율적으로 만들 수 있는 잠재력을 제공하여 보다 포괄적이고 지속 가능한 이동성을 제공할 수 있다…": id.

106) G. G. Fusterand & L. Jasmontaite. 2020. "Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights." in The Ethics of Cybersecurity: The International Library of Ethics, Law and Technology, vol. 21, 99 - 113 (M. Christen, B. Gordijn & M. Loi eds. 2020).

UN 규칙 No. 155 는 '사이버 보안'을 전기 또는 전자 부품에 대한 사이버 위협으로부터 도로 차량과 그 기능을 보호하는 조건으로 정의한다.[107] 여기서 영국 BSI가 CAV대신 CAM 용어를 사용하여 포섭되는 교통수단을 확대하였다는 점[108]과 미국 NHTSA의 계층화된 사이버 보안을 설계하기 위하여 포괄적이고 체계적인 접근 방식이 필요하다는 가이드라인[109]을 주목할 필요가 있다.

사이버 보안 대상을 확대하고 조건이 아닌 탑승자의 활동과 사이버 위협 행위에 보다 중점을 두고[110] 사이버 보안을 정의할 필요가 있다. 차량의 V2X 기능과 함께 차량시스템에 탑승자의 GNSS 등 정보 입력이나 휴대폰이 차량의 엔터테인먼트나 편의 시스템에 연결되어 데이터 공유가 이루어진다는 점을 고려해야 한다. 이러한 무선통신 연결은 가로채어져 악의적 목적으로 악용될 수 있고 업데이트 시에 악성코드를 심을 수 있으며 입력 데이터가 임의로 변경되어 차량의 주행을 방해하거나 연결 통신을 단절할 수 있다.[111]

2. 사이버 보안의 관점에서 AV와 UAM 통합 관리의 필요성

최근 첨단 교통수단 산업을 선도하는 혁신적 기술 분야는 상호 연결성의 획기적 개선, 새로운 통신 채널 구축 및 액세스 포인트의 확산이라 할 수 있다. 액세스 포인트의 확산 등에 의한 연결성의 향상은 더 크게 첨단 교통수단의 안전성과 이익을 제고시킬 것이다. 그러나 연결성의 확대는 곧 사이버 보안 위험의 증가를 의미한다. 요컨대, ①V2X 등액세스 포인트의 확산은 첨단 교통수단의 안전과 편의성을 증가시킨다. 반면, ②예컨대 TV 리모컨과 에어컨 리모컨 간의 간섭과 같이 V2V(U2U)의 네트워크는 AV와 UAM 비행차량간 간섭이나 주파수 변경을 통한 해킹의 통로가 될 가능성이 있다. 따라서 예컨대, AV의 통합 관제센터로서[112] ICT와 UAM에 대한 무인기 교통관리(Unmanned Aircraft System Traffic Management: UTM)에 대한 사이버 보안의 통합 관리시스템이 필요하다. CAV, UAM 비행

107) UN Regulation No. 155.
108) Connected and automated mobility-Vocabulary BSI Flex 1890 v5.0:2023-04 at https://www.bsigroup.com/en-GB/CAV/cam-vocabulary.
109) U.S. Dep'T of Transp. NHTSA Report No. Dot Hs 812 333, Cybersecurity Best Practices For Modern Vehicles 10-20 (2016).
110) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019, PE/86/2018/REV/1, OJ L 151/15. art. 2.
111) A. Taeihagh & H. Si Min Lim, supra note 20, at 115 - 117.
112) 金愉美, "自律走行車 商用化에 따른 安全性 改善事項 提言", 成均館大學校情報通信大學院, 碩士學位請求論文 (2020) 41-42면.

차량을 포함한 모든 첨단차량에서 사이버 보안을 확실하게 보장하려면 보다 계층적으로 조율되고 통합되는 입법이 필요하다.[113]

3. 차량과 그 시스템에 대한 무단 접근 차단

첨단 교통수단 사이버 보안의 핵심적 과제는 차량과 그 시스템에 대한 무단 접근 차단이다. 이것은 차량에 대한 직접적 접근뿐만 아니라 휴대폰과 연결 간접적 접근도 차단되어야 한다.[114] 사실 UN 규정 No. 155와 UN 규정 No. 156과 대부분의 입법례가 차량 시스템에 대한 접근을 방지하는 것을 목표로 한다.

V2X의 통신을 고려할 때 차량 시스템은 물론 RSU에 접근도 철저하게 차단되어야 한다. 아울러 ITC 시설과 시스템에 대한 보안도 확고하게 구축되어야 한다.

4. 즉각적 복원과 경고 시스템

무단 접속이 발생한 경우 사이버 보안 상태가 즉시 복원될 수 있어야 한다.[115] 침해나 취약점이 발견되면 소프트웨어 업데이트 등을 통해 이 문제를 패치(patch) 해야 한다. 새로운 사이버 위협이 발생할 때 그에 대한 경고 시스템도 필요하다. 따라서 이러한 복원 및 경고 시스템도 제작사 등의 의무로 규정되어야 한다.

5. 보안의 지속적 유지와 보수

차량의 사이버 보안은 한결같이 계속 지속되어야 한다. 이를 위해서는 제작사 등은 그 보안 상태를 지속적으로 모니터링하고 새로 발견된 취약점의 패치를 위하여 수시로 업데이트하는 것이 필요하다.

EU의 AI 규칙 법안도 "고위험 AI 시스템은…그 의도된 목적에 비추어 적절한 수준의 정확성, 견고성, 안전성 및 사이버 보안을 달성하고 수명주기 전반에 걸쳐 …수행되어야 한다.…"[116]"시장에 출시되거나 서비스에 들어간 후에도 계속 학습하는 고위험 AI 시스템

113) U.S. Dep'T of Transp. NHTSA, Report No. Dot Hs 812 333, Cybersecurity Best Practices For Modern Vehicles 10-20 (2016).
114) Nynke E. Vellinga, supra note 9, at 163-164.
115) Id.
116) Artificial Intelligence Act, Amendments adopted by the European Parliament on 14 June 2023,

은 편향된 출력이 향후 입력에 영향을 미치는 것('피드백 루프')과 입력의 악의적인 조작을 합당하게 규명하고 적절한 완화 조치를 보장하는 방식으로 개발되어야 한다."[117]라고 생애 주기의 한결같은 보장을 규정하고 있다. 검사 승인기관은 사이버 보안의 지속적 유지와 보수 여부를 차량의 수명주기 전반에 걸쳐 모니터링을 해야 한다.

6. 산업계 기반 규칙의 채택

첨단 교통시스템과 그 사이버 보안에 대한 정부의 정보와 관련 데이터가 부족한 상황에서 신속하게 관련 법제도의 구축은 쉽지 않다. 이 경우 정부는 정부가 제시하는 핵심적 입법 목표에 따라 장치 및 소프트웨어 개발자, 보안 전문 업체, 차량 제조사 등 관련 산업계가 입안한 업계 기반 규칙(Community Based Rules: CBRs)의 입법방식을 채택하는 것이 필요하다. 이러한 CBRs 방식의 입법은 개발자, 제작사, 시스템 (운영)관리자 등 모두에게 마찰 없이 신속하게 적용할 수 있다.

Ⅵ. 결론

첨단 교통수단 개발자, 제조사와 각국 정부는 복잡하고 진화하는 사이버 보안 환경에 맞춰 잠재적인 사이버 위협이나 시스템의 취약성을 정확히 파악하고 그에 대응하는 적절한 프로세스와 보호 장치를 마련하여 첨단 교통수단 기술의 교통 안전성 제고의 효과를 최대한 실현해야 한다.

첨단교통 시스템에 대한 효과적 사이버 보안을 위해서는 각국 정부, 장치 및 소프트웨어 개발자, 차량 제조사가 함께 복잡하게 진화하는 사이버 환경에 맞추어 그 시스템의 취약성과 예상되는 사이버 위협을 정확히 파악하고 그에 적합한 기술적, 법 제도적 장치를 적시에 충분하게 확보해야 한다.

그러한 법 제도를 구축하기 위해서 이 논문은 여러 입법례, 국제 표준과 함께 사이버 보안 입법의 방향과 원칙으로서 ①첨단 교통수단의 '사이버 보안'에 대한 명확한 정의, ②사

P9_TA(2023)0236, art. 15 para 1.

117) Id. art. 15 para 3.

이버 보안의 관점에서 AV와 UAM의 계층적 통합적 관리, ③첨단차량과 시스템, RSU에 접근 차단과 ITC에 대한 확고한 보안, ④침해 시 즉각적 복원과 패칭, 위협 감지 시 경고 시스템의 구축, ⑤차량과 시스템의 생애주기에 걸친 보안의 지속적 유지와 보수, ⑥장치 및 소프트웨어 개발자, 보안 전문 업체, 차량 제조사 등이 주도적으로 참여하는 CBRs 방식의 채택을 제안한다.

■ 참고문헌

金愉美, "自律走行車 商用化에 따른 安全性 改善事項 提言", 成均館大學校情報通信大學院, 碩士學位 請求論文 (2020).

류병운, "자율주행자동차 사고의 법적 책임", 홍익법학 제19권 제1호 (2018).

류병운, "UAM의 도입 및 산업화를 위한 법·제도의 설계", 홍익법학 제23권 제2호 (2022).

A. Chowdhury et al., "Attacks on Self-Driving Cars and Their Countermesasures: A Survey," IEEE Access, vol. 8, (2020).

Adam Cohen & Susan Shaheen, "Urban Air Mobility: Opportunities and Obstacles", International Encyclopedia of Transportation, 702 (2021).

A. Taeihagh & H. Si Min Lim, "Governing Autonomous Vehicles: Emerging Responses for Safety, Liability, Privacy, Cybersecurity, and Industry Risks." 39 (1) Transport Reviews 103 (2019).

Asma Zubedi et al, "Sustaining Low-Carbon Emission Development: An Energy Efficient Transportation Plan for CPEC",14(2) J. Inf. Process. Syst., 322 (April 2018).

Ching-Yao Chan, "Advancements, prospects, and impacts of automated driving systems," 6 International Journal of Transportation Science and Technology 208 (2017).

Daniel A. Crane & Kyle D. Logue, Bryce C. Pilz, "A Survey of Legal Issues Arising From the Deployment of Autonomous and Connected Vehicles" 23 Mich. Telecomm. & Tech. L. Rev. 191(Spring, 2017).

D. P. F. Möller & R. E. Haas, Guide to Automotive Connectivity and Cybersecurity: Trends, Technologies, Innovations and Applications (2019).

David P. Thipphavong et al., "Urban Air Mobility Airspace Integration Concepts and Considerations," NASA (2018).

Dorothy J. Glancy, "Privacy in Autonomous Vehicles," 52 Santa Clara L. Rev. 1171, (2012).

F. W. Alsaade & M. H. Al-Adhaileh, "Cyber Attack Detection for Self-Driving Vehicle Networks Using Deep Autoencoder Algorithms." 23(8) Sensors 4086 (2023).

Felipe Jiménez & José Eugenio Naranjo & José Javier Anaya & Fernando García & Aurelio Ponz & José María Armingol, "Advanced Driver Assistance System for road environments to improve safety and efficiency" 14 Transportation Research Procedia 2245 (2016).

G. Dimitrakopoulos, Current Technologies in Vehicular Communications, (2017).

ENISA & JRC. Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous (2021).

G. G. Fusterand & L. Jasmontaite. 2020. "Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights." in The Ethics of Cybersecurity: The International Library of Ethics, Law and Technology, vol. 21 (M. Christen, B. Gordijn & M. Loi eds. 2020).

Leilei Wang, et al., "A review of Urban Air Mobility-enabled Intelligent Transportation Systems: Mechanisms, applications and challenges", 141 Journal of Systems Architecture 102902

(2023) at at https://doi.org/10.1016/j.sysarc.2023.102902.

M. Iorio et al., “Securing SOME/IP for in-vehicle service protection,” 69(11), IEEE Trans. Veh. Technol. 13450, 13454-3465 (2020).

Nynke E. Vellinga, “Connected and vulnerable: cybersecurity in vehicles,” 36(2) International Review of Law, Computers & Technology 161 (2022).

T. Mecheva & N. Kakanakov, “Cybersecurity in Intelligent Transportation Systems,” 9(4) Computers 83 (2020).

T.S. Abraham & K. Narayanan, “Cooperative communication for vehicular networks” in EEE International Conference on Advanced Communications, Control and Computing Technologies (2014).

Sandeep Kulkarni & Renju Panicker & Murali Kadeppagari & Imtiaz Elahi, “Next-Gen Maintenance Framework for Urban Air Mobility Vehicles,” SAE Technical Paper 2022-26-0008, (2022).

UAM Vision Concept of Operations (ConOps) UAM Maturity Level (UML) 4, Version 1.0, NASA (2020).

W Choi et al., “Identifying ecus using inimitable characteristics of signals in controller area networks” 67 IEEE Trans. Veh. Technol. 4757 (2018).

투고일자 2023. 08. 30 심사개시일자 2023. 09. 20 게재확정일자 2023. 09. 22

Hongik Law Review, Vol. 24. No. 3(2023)

【ABSTRACT】

Protection of Advanced Transportation Systems from Cyberattacks: Focusing on Relevant Legislative Examples*

Lyou, Byung-Woon**

As advanced transportation vehicles become increasingly automated and interconnected, the threat of cyberattacks and disruption increases accordingly. If hackers and cyber attackers exploit cybersecurity vulnerabilities in advanced vehicles, the risks they could pose could range from inconvenience to occupants or minor disruption to the life of passengers and those outside the vehicle. In particular, it can pose a serious road traffic risk when hackers disable a vehicle's acceleration, deceleration, braking, and steering systems, or hijack the ability to control a vehicle's steering and speed. This hacked vehicle could even be used as a means of terrorism. In short, an effective response to cyber threats is needed along with ensuring the operation of cutting-edge transportation and the efficiency of its traffic management. This paper seeks to find the direction and principles of the desirable Korean legal system by reviewing cases of cyber vulnerabilities and cyber threats of advanced transportation vehicles and systems, and referring to international rules and standards, and legislative situations in the EU and the United States.

Key words : Autonomous Vehicle, Self-Driving Cars, Urban Air Mobility, UAM, Advanced Transportation Systems, Cyber Threats, Hacking

---

* This work was supported by 2022 Hongik University Research Fund.
** Professor of Law, Hongik University