한국컴퓨터정보학회 하계학술대회 논문집 제25권 제2호 (2017. 7)

자율주행자동차의 취약점 및 보안 고려사항에 대한 연구

김예지[O], 이영숙[*]
[O*]호원대학교 사이버수사경찰학부
e-mail: foforh717@gmail.com[O], ysooklee@howon.ac.kr[*]

A Study on the Vulnerability and Security Considerations of Autonomous Vehicles

YeaJi Kim[O], YoungSook Lee[*]
[O*]Department of Cyber Security, Howon University

● 요 약 ●

자율주행자동차는 운전자의 개입 없이 스스로 목적지까지 도착할 수 있는 차량으로 세계 여러나라의 자동차 업체 뿐만 아니라 IT분야에서도 개발중에 있다. 일반 자동차와는 달리 차량에 카메라와 GPS, 각종 센서 등 IT 기술들이 도입되어 운전자와 차량 간에 소통이 이루어지면서 편리함을 가져다 준다. 그러나 자율주행자동차는 하나의 스마트폰이 탑재되었다고 볼 수 있을 만큼 지능적이고 다양한 기술이 적용되어 있기 때문에 취약점과 위협 요소가 존재한다. 본 논문에서는 자율주행자동차의 운행으로 인해 야기될 수 있는 취약점을 분석하고 적용 가능한 보안 고려사항을 제시한다.

키워드: 자율주행자동차(Autonomous Vehicle), 소통(Communication)

I. 서론

최근 가장 많이 주목받고 있는 자율주행기술은 자동차업계와 IT업계의 합작이라고 말할 수 있다. 자율주행자동차는 운전자의 관여 없이 자동차 스스로가 운전할 수 있다는 것이다. 일반 자동차는 사람이 직접 페달을 밟아야 하고 핸들을 잡고 주변 환경에 집중하며 운전해야 하지만 자율주행자동차는 사람이 원하는 목적지까지 알아서 도착할 수 있다. 자율주행 기술은 여러 단계로 구분되는데, 완벽한 자율주행기술을 보유한 자동차는 2020년 이후에 상용화 될 것으로 전망된다. 하지만 IT 기술이 합쳐지면서 자율주행자동차를 운행하는데 취약점과 보안 위협이 존재한다. 미국의 최고 기업인 구글이 개발한 자율주행자동차가 여러 번 시험 운행 중 사고가 났었고, 중국의 Tencent security research team Keen Security Lab에서 자율주행자동차인 테슬라 모델 S를 해킹하여 자동차의 선루프나 와이퍼를 저절로 작동시키는 등의 악의적인 행동을 공개했다. 게다가, 자동차 운행 중 브레이크가 급제동되는 위험한 상황이 연출 되었다. 자동차 운행 중 누군가의 해킹으로 인해 갑작스런 사고가 발생한다면 탑승한 운전자의 안전이 위협 받을 수 있다. 또한, 자율주행자동차 운행 시 개인정보 유출도 빈번해 질 수 있다는 것이다. 그러므로 자율주행 기술을 개발하는 모든 업체에서는 정보보안 취약점을 알아내고 그에 대한 보안고려사항을 준수해야 한다.

본 논문의 구성은 다음과 같다. 논문의 2장에서는 자율주행자동차의 개념, 국내·외 시장동향과 자동차 업체현황에 대해서 알아본다. 3장에서는 자율주행자동차의 기술단계와 자율주행에 쓰이는 기술과 그에 따른 법에 대한 내용을 분석하였고 법적으로 운행자의 책임이 어떻게 되는지에 대해서 서술하였다. 마지막으로 4장에서는 자율주행자동차의 취약점과 적용 가능한 보안 고려사항에 대해 소개한다.

II. 자율주행자동차의 개요

2.1 자율주행자동차의 개념

자율주행자동차는 주변 상황을 파악하고 위험을 감지하며 운전자의 개입 없이도 차량 스스로 정해진 목적지까지 주행하는 자동차이다. 내부에는 카메라, 라이더(lidar), HMI 기술 등이 있으며 여러 가지 센서와 명령을 내리는 중앙제어장치, 명령에 의해서 동작을 취하는 엑추에이터 등으로 구성되어 있다. 사람이 운전하지 않고 컴퓨터 등 첨단장치로 운전을 하기 때문에 사람으로 인해 발생하는 교통사고를 줄일 수 있고 몸이 불편해서 운전하기 힘든 시각장애인과 같은 사람들에게 운전할 수 있는 기회가 주어진다. 또한 고령화시대를 대비해서 고령 운전자들을 위해 대신 운전해주거나 범죄가 발생 가능한 주차장이나 대리운전, 택시운전을 해줄 수 있어서 여성 운전자들에게 많은 도움을 줄 수 있다. 자율주행자동차는 무인자동차(Driverless Car)와 비슷한 개념의 용어로 사용되고 있는데, 자율주행자동차는 운전자가 차를 직접 다루기보다는 차량이 완전하게 독립적으로 스스로 판단해서 주행하는 자율주행기술에 초점을 둔 것이다.

하지만 요즘은 둘의 용어가 혼용되어 사용되고 있다. 그리고 무인자동차와 같이 거론되는 용어가 있는데 바로 커넥티드카(Connected Car)이다. 커넥티드카는 자동차와 IT기술이 합쳐져 인터넷 서비스가 가능하고 다른 자동차와도 상호 통신이 가능한 차량이다[1].

2.2 자율주행자동차의 국·내외 시장동향

자율주행자동차 시장의 규모가 꾸준히 성장해 상승세를 이어갈 것으로 예측되며, 많은 전문가들은 자율주행자동차를 미래 자동차 산업의 신성장동력 으로 언급했다. 자율주행자동차의 세계시장규모는 2020년에는 1,890억 달러, 2035년에는 1조 1,520억 달러까지 성장할 것으로 보여진다. 특히 자율주행자동차는 ICT 기술에 대한 필요성이 요구됨으로써 글로벌 업체들 중 완성차 업체뿐만 아니라 ICT 업체들의 개발 전망이 높을 것이다[2].

III. 자율주행차량의 핵심기술 동향 및 법·제도 동향

3.1 자율주행자동차 기술단계

도로교통안전국(NHTSA)은 자율주행자동차를 운전자의 개입의 여부와 정도에 따라서 총 5단계로 나누었다. 먼저 0단계는 자율주행기술을 전혀 갖추고 있지 않은 단계로 우리가 주위에서 많이 볼 수 있는 대다수의 자동차가 이 단계에 속해있다. 그러므로 운전자는 운전의 모든 권한을 가져야 한다. 1단계는 자율주행기술이 일부 적용된 자동차가 포함된 단계로서 운전을 보조하는 기술이 들어가 있다. 차선유지시스템이나 크루즈컨트롤 같은 운전자 보조 시스템을 갖추고 있어서 운전자가 일반적으로 운전하거나 다른 차량과의 충돌하기 바로 전 상황에서의 일부 기능을 제외한 자동차 제어권을 가진다. 2단계에서는 그 전 단계인 1단계의 기술이 탑재된 상태에서 제어기능이 결합하여 운전자를 보조하는 역할을 한다. 대표적인 것으로는 차선유지 기능과 결합한 적응형 순항제어(ACC: Adaptive Cruise Control)를 꼽을 수 있다. 2단계에서는 운전자가 핸들과 페달을 자유롭게 다룰 수 있지만, 1단계와 마찬가지로 운전자는 주변을 주시 해야한다. 3단계는 제한된 자율주행 단계로 운전자가 운행주도권을 자동차에게 완전히 넘겨줄 수 있는 단계로, 이 때는 운전자가 조작 및 감시를 하지 않아도 된다. 하지만 자동차는 자율주행이 불가능한 상황이 오면 스스로 이를 판단하여 운전자에게 운행권을 넘겨준다. 즉 3단계는 자동차와 운전자가 서로 운전할 수 있는 상황을 변환시킬 수 있는 단계라고 말할 수 있다. 마지막으로 4단계는 완전 자율주행 단계라고도 불리며, 운전자의 개입이 없어도 되는 단계이다. 운전자가 정해준 목적지까지 스스로 갈 수 있으며 자동차가 전적으로 모든 상황을 책임지게 된다[3].

Table 1. 자율주행의 기술단계에 따른 변화

단계	운전자 개입	제어주체	책임주체
Level 0	필요	운전자	운전자
Level 1	필요	운전자 또는 자동차	운전자
Level 2	필요	자동차	운전자
Level 3	필요	자동차	운전자 또는 자동차
Level 4	필요없음	자동차	자동차

3.2 자율주행자동차 주요기술

자율주행기술은 출발지와 목적지를 입력하면 최적의 경로를 탐색하여 스스로 목적지까지 도착할 수 있게 하는 기술로 V2X 기술, ADAS 기술, 시스루 기술, 라이다 기술, 고정밀 지도 등이 있다.

가. V2X 기술

V2X (Vehicle to Everything communication)란 자율주행차의 핵심기술로써, 유·무선망을 통해서 외부 환경과 차량을 연결하는 기술을 말한다. V2X 기술에는 V2V (Vehicle to Vehicle), V2I (Vehicle to Infrastructure), V2N (Vehicle to Nomadic device)가 있다. V2V는 차량 간 통신기술로 차량 안전 서비스를 위한 자능형교통시스템이다. 한 차량이 외부의 다른 차량의 움직임을 사전에 파악할 수 있다면 예상치 못한 충돌과 차선 이탈 및 변경에 대해 대비 할 수 있으므로 사고를 감소시킬 수 있다. V2I는 차량과 노변 기지국 간의 통신기술로 인터넷 서비스를 지원한다. 도로의 상황정보를 차량에 제공하여 운전자는 공사구간이나 사고발생구간 등을 알 수 있다. V2N은 차량이 운전자의 모바일 기계와 연결되는 기술로 모바일 기기를 이용해서 차량 상태를 인지하고 관리 할 수 있다. 차량 내의 스마트폰이나 네비게이션 시스템과 연결하여 차량과 보행자가 가까워지게 된다면 양쪽 모두에게 경고음을 발생시켜서 교통사고를 방지할 수 있다. Fig. 1. 은 V2X에 대한 대략적인 개념 그림이다[4].

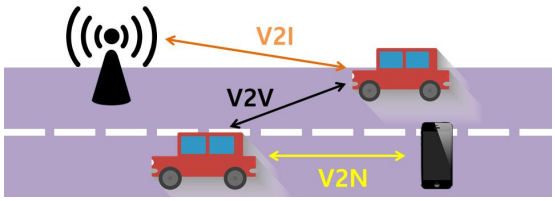

Fig. 1. V2X의 개념도

나. ADAS 기술

ADAS(Advanced Driver Assistance System)은 첨단 운전자 보조 시스템으로 차량에 설치되어 있는 각종 센서를 통해 운전자의 안전과 편의를 지원한다. 이 시스템은 인지, 판단, 제어로 3가지 구성요소를 가지고 있다. 인지의 단계에서는 차량 주변에 장애물이

있는지, 전방/후방 차량과의 간격은 어떠한지 현재의 주행 상황을 인식한다. 판단은 인지 단계에서 알아낸 상황을 판단하여 행동을 결정한다. 전해도 되는지, 제어는 판단에서 내린 결정을 수행하는 단계이다. 예를 들면 핸들을 얼마나 돌릴 것인지, 브레이크를 얼마나 밟을 것인지가 있다.

IV. 자율주행자동차의 취약점 및 분석

4.1 자율주행자동차의 취약점

자율주행자동차는 하나의 스마트폰이 차량에 탑재되었다고 볼 수 있을 만큼 자동적이고 다양한 ICT 기술들이 적용 되어있다. 그러므로 자동차에 대한 사이버 공격을 받을 수 있는 가능성이 존재한다. 자동차를 세가지로 분류해보면 물리적인 움직임을 담당하는 구동부와 자동차의 엔진이나 변속기를 제어하는 전자제어장치(Electronic Control Unit, ECU), 차 안에서 외부를 연결시켜주는 인포테인먼트(infotainment) 시스템으로 구분된다. ECU는 CAN(Controller Area Network)를 통해서 제어가 가능하다. 이로 인해서 공격자는 CAN을 이용하여 ECU 영역을 침범해 자동차를 급제동을 가능케 하거나 브레이크 페달을 무력화 시킬 수 있다. 인포테인먼트 부분에서는 자동차 내부의 네비게이션에 스마트폰 화면을 그대로 비춰주는 '미러링크' 기술이 취약점으로 발견되었다. AVN(Audio, Video, Navigation) 시스템에서도 CD 등을 통해 취약점 공격이 가능하고 GPS를 통한 해킹에도 취약하다. 또한 블루투스를 이용하여 외부로부터 전송된 파일들을 통해서 악성코드가 감염 될 수 있다. Table 2는 자율주행자동차를 이용하는데 있어 발생할 수 있는 취약점을 보여준다[5].

Table 2. 자율주행자동차의 취약점

취약점	설 명
ECU	· TPMS(타이어 공압 모니터 시스템) 해킹으로 ECU에 전달 그로 인한 무선 통신 가능 · 자동차 접근 시스템 · 회전 및 브레이크 접근 · 조명 시스템 접근 · 차량자가진단장치(OBD Ⅱ)로 ECU에 접근 가능
인포테인먼트	· 미러링크 활성화하여 접근 통제 가능 · V2X를 통한 차량의 내부 시스템에 접근
AVN 시스템	· CD 등을 통한 펌웨어 취약점 공격 가능
블루투스	· 블루투스를 통해 다운받는 파일들로 인한 악성코드 설치

4.2 자율주행자동차의 보안 위협 분석

자율주행자동차의 보안 취약점이 증가하면서, 취약점을 이용한 다양한 보안 위협이 발생할 수 있다. Table 3은 취약점을 통한 위협 분석을 보여준다.

Table 3. 취약점을 통한 위협 분석

위협	설 명
정보유출	· 차량과 모바일 기기를 통신시켜주는 인포테인먼트 시스템을 통해 내부시스템에 접근하여 정보 유출
브레이크, 변속기 등 제어	· CAN에 진입하여 변조된 메시지 전송해 핵심부품 제어
악성코드 설치	· 블루투스를 통해서 스마트폰의 앱으로 받은 파일로 인한 악성코드 설치

4.3 자율주행자동차의 보안 고려사항

완전 자율주행자동차의 상용화를 위해 위에서 언급했던 취약점들을 보완하기 위한 보안 고려사항들이 꼭 필요하다. Table 4는 자율주행자동차 보안 위협에 대해 적용 가능한 보안 고려사항을 나타낸다.

Table 4. 자율주행자동차의 보안 고려사항

보안 대책	설 명
프라이버시 보호 인증	· PKI를 이용하여 차량용 인증서를 발급, 운영 및 관리로 운전자의 정보 보호 · CSR 인증서 · 익명 인증서
자동차 물리보안	· OBD 포트를 통한 물리적 접근을 막기 위해 통제
펌웨어 업데이트	· 주기적으로 펌웨어 업데이트를 통해 보안 강화

1) 프라이버시 보호 인증

PKI(Public Key Infrastructure)를 기반으로 한 차량용 인증서를 자동차가 출고될 때부터 발급받고 관리함으로써 운전자의 정보 유출을 막을 수 있다. 또한, 차량을 식별할 수 있는 CSR(Certificate Signing Request) 인증서와 차량 간 통신 시 신뢰성 여부를 확인하기 위해 사용되는 익명 인증서를 통해 중요정보 유출을 방지할 수 있다[6].

2) 자동차 물리보안

가장 큰 위협이 되는 부분은 자동차 자체이다. 자동차 내부의 취약한 'OBD(On-board Diagnostics)' 단자에 자동차용 AFW(Application Firewall)를 이용한 보안 솔루션을 적용하면서 차량 외부로부터 들어오는 비인가적인 통신과 공격자의 접근을 차단하도록 해야 한다[7].

3) 펌웨어 업데이트

블루투스나 CD, Wi-Fi 등을 통해 악성코드 감염이 가능하고 오디오 파일을 통해 차량에 비정상적인 CAN 패킷 전송이 우려된다. 그러므로 주기적인 펌웨어 업데이트와 백신 프로그램을 통해 취약점에 대한 대비가 필요하다[7].

Ⅴ. 결론

자율주행자동차는 운전자의 별다른 조작 없이 스스로 목적지에 도착하는 자동차로 앞으로 미래에 더 다가갈수록 우리의 생활에 편리함을 가져올 것이고 그만큼 보안고려사항은 아주 중요한 요소가 될 것이다. 자율주행기술이 포함하고 있는 보안 취약점으로 인해 인명사고나 개인정보 또는 사생활 유출 등 많은 위험이 생길 것으로 예측된다. 그러므로 본 논문에서 소개한 자율주행기술 취약점 분석을 알아두고 그에 대한 보안고려사항을 꼭 지켜줘야 한다.

REFERENCES

[1] Hwangsu-Jeon, and Sunju-Go, “Driver gives freedom to the driver, Traffic accidents are Zero,” pp.3, May 2015.

[2] “A Feasibility Study on Driving Technologies for Dedicated Freeway Construction,” KISTEP, pp.154, May 2016.

[3] “European Driving Technologies and policies in Europe,” Global Tech Korea(GT).

[4] Taeuk-Hwang, “Trends in Development of IT fusion Technologies for IT Convergence.

[5] Security Issues. http://www.igloosec.co.kr

[6] Sanggyu-Sim, and Duksoo-Kim, and Yoosik-Lee, “Security Technologies for V2X Communication,” April 2014.

[7] Dongjae-Lee, “Security response measures to be considered when developing cars,” MDS technology, pp.4~7