자율주행자동차 해킹 사례 분석

지도교수 : 한상훈
연 구 자 : 김승한

< 목 차 >

요 약

자율자동차 보안의 해킹은 소프트웨어 취약점 및 치명타 버그 및 해킹까지 이슈 사례가 많다. 자율자동차가 컴퓨터가 조종하기 때문에 보안이 뚫린다면 목적지, 소프트웨어, 공격 해킹으로 바꿔버릴 수 있다. 본 연구에서는 언론이나 인터넷을 통하여 발표되는 자율 자동차 해킹 관련 기사들을 조사하여 사례들을 찾아보는 것이 주된 목표이다.

자율자동차에서 발생하는 보안 문제 및 해킹 사례들을 살펴봄으로써 미래 자동차에 대한 문제점들을 생각해 보고자 한다.

주요어 : 자율주행자동차, 보안, 차량 해킹, 테슬라 해킹

1. 서론

1.1 주제를 정하기

- 얼마 전에 해외뉴스에 자율자동차 보안의 해킹 사고가 많이 등장했다. 문제는 보안의 해킹 때문이다. 왜 발생하는지 이유를 잘 모르겠다. “어떻게 해킹이 간단히 쉽게 뚫어버렸지?”라고 고민했다. 인터넷 사례를 살펴보니 자동차 사이버 공격 주요 경로 1위는 무선도어 잠금장치이다. 2위는 제작사 서버이다. 2010년부터 첫 사례가 발생하여 약 5건이다. 1년 만에 약 2.5배 이상 늘어났다. 그래서 자율자동차 보안의 해킹 분석으로 주제를 결정했다.

1.2 보안 및 해킹 발생한다.

- AI 기반 자율주행차량은 개방형 및 모바일 네트워크를 사용하여 컴퓨터 플랫폼에 인공지능을 기반으로 ICT 기술에 의한 자율주행차량을 개발하고 있었지만, 자율주행차량의 전자제어 시스템에 대한 해킹 공격이 가능해짐에 따라 차량 제어 시스템 공격, 원격제어 공격 등 여러 가지 해킹 사례가 많이 발생하고 있다. 이러한 해킹 공격 사고사례는 내부, 외부 공격자에 의한 해킹 위협이 증가하고 있으며, 자율주행차량이 대중화되면 해킹 피해 사례가 더욱 많이 발생한다.

1.3 자율주행 자동차 단계

- 사람의 조작 없이 자동차 스스로 달리는 자율주행 기술 현실 가능성을 놓고 회의론이 부쩍 늘어난다. 정보 기술 업계가 눈앞의 미래인 것처럼 장밋빛 청사진을 제시했지만 실제로 기술 구현까진 갈 길이 한참 멀다는 이야기다.

[사진 1] 자율주행 자동차 단계

1.4 자율주행 자동차가 어떻게 해킹될 수 있을까?

- 우선 자율주행 자동차에서 보안 측면에서 문제가 될 수 있는 부분은 크게 세 가지를 꼽을 수 있다. 컴퓨터 조정 장치(CCU), 전자 제어 장치(ECU), 보안 프로세스 그 자체 세 가지로 분류할 수 있는데, 우선 컴퓨터 조정 장치(CCU)의 경우 컴퓨터나 웹 같은 부분에 취약점이 있는 경우 해킹의 문제로 이어질 수 있다. 특히 이러한 장치를 이용하여 차량을 실시간으로 통신하는 것을 돕기 때문에 취약점이 있다면 통신하는 과정에서

해킹이 발생할 수 있다. 이때, CCU를 이용해 주행 정보를 교환하는 등의 행위를 하므로 해킹이 발생한다면 위치정보 등의 정보 유출과 같은 상황에 마주할 수 있다. 두 번째로 ECU(Engine Control Unit)의 경우 엔진 제어 장치로 센서나 액추에이터를 위해 만들어진 제어 모듈이다. 센서나 액추에이터를 담당하기 때문에 취약점이 드러나게 된다면 공격자는 이를 이용해서 사용자가 의도하지 않은 동작을 하게끔 하여 사고로 이어지게끔 만들 수 있다. 마지막으로 보안프로세스 그 자체가 부족한 경우에는 자동차가 겪는 해킹 상황에 대해서 여러 가지 보안 프로세스를 준비해두어야 하며, 보안 프로세스를 준비해 두지 않을 시에는 해커에 의해 악의적인 제어가 가능해질 수도 있다.

2. 본론

2.1 미국서 “차량 해킹”

- 미국에서 '차량 해킹', 즉 차량에 장치된 인터넷 접속 가능 단말기를 통해 차량의 기능을 외부에서 제어하는 데 성공한 사례가 또 나타났다. 11일(현지 시각) 와이어드 등 정보기술(IT) 전문 매체들에 따르면 샌디에이고 캘리포니아대(UCSD)의 스테판 새비지 교수가 이끄는 연구진이 차량정보수집 단말기(OBD2)가 장착된 '콜벳' 승용차의 제어장치를 해킹하는 데 성공했다. 이런 단말기는 보험회사나 차량 리스회사에서 차량 운행정보를 파악하는 데 주로 쓰이지만, 연구진은 이 단말기를 외부에서 조작해 휴대전화로 차량의 브레이크를 작동할 수 있도록 만들었다. 차량에 여러 전자제어장비는 물론 인터넷 접속이 가능한 다양한 정보단말기가 장착되면서 '차량 해킹'에 대한 우려 또한 제기돼 왔다. 지난달에는 정보보안 전문가들이 노트북PC로 '지프' 승용차의 가속페달과 브레이크를 작동시키는 시범을 보였다. 이때도 차량에는 인터넷 접속 기능이 포함된 제어장치가 장착돼 있었다. 이에 대해 '지프' 차량 제조업체인 피아트크라이슬러는 일부 제어장치에 국한되는 현상이고 취약점을 개선했다는 입장을 보였다. 하지만, 차량 간 정보통신기능을 포함해 차량 내 컴퓨터가 외부 통신망과 접속해야 하는 다양한 부가기능들이 속속 개발되고 있는 만큼 차량 해킹에 대한 우려 또한 이어질 전망이다.

[사진 2] 차량 해킹 예시

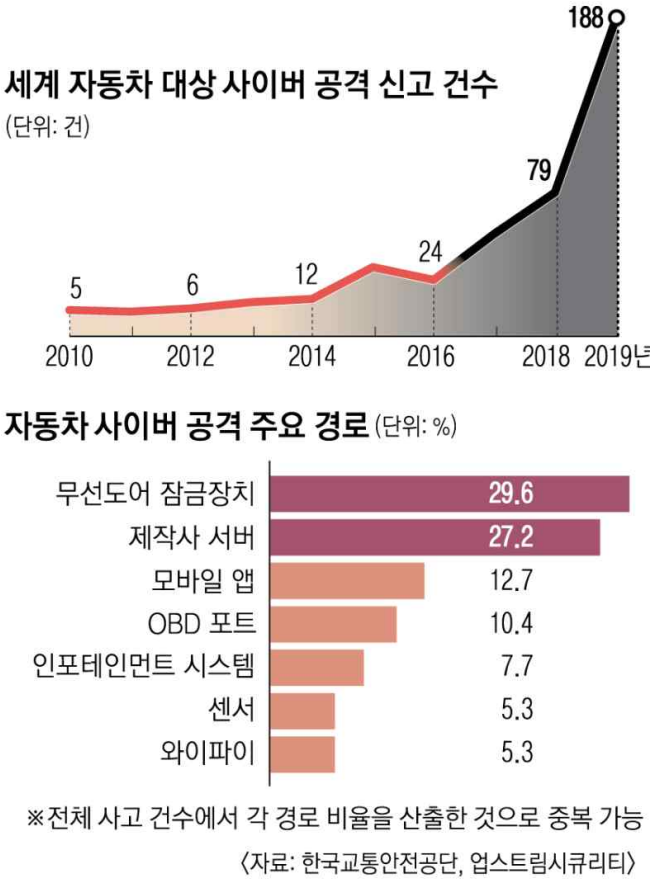
2.2 해커들의 새로운 먹잇감

- 2015년 두 명의 보안 연구원들이 노트북을 이용해 지프 체로키 차량을 해킹했다. 이들은 차량과 16km 떨어진 곳에서 차량 내부 시스템에 접속해 라디오 방송 채널을 바꾸고 앞 유리 와이퍼를 마음대로 조작했다. 심지어 차량의 전원을 차단하거나, 본인들의 사진을 차량 내비게이션 화면에 띄우기도 했다. 보안 취약점이 만천하에 드러나자 지프 모회사인 FCA는 무려 140만 대의 차량을 리콜해야 했다. 그 후 6년이 지나는 동안 자동차의 기능은 급속도로 발전했다. 뉴욕타임스는 지난 18일(현지 시각) "소비자들은 자동차의 편의 기능을 좋아하지만, 해커들은 더 좋아할 수 있다"면서 "전 세계 자동차 업계 관계자들은 교통 시스템에 일어날 수 있는 혼란을 막기 위해 밤잠을 설치고 있다"고 보도했다. 자동차는 운전자는 물론 주변 차량이나 스마트폰, 위성, 제조사, 방송국 등과 끊임없이 소통하며 점차 더 많은 기능을 탑재하고 있다. 삼성전자와 LG전자 등 IT 업체들은 자동차 운전석과 조수석 앞쪽의 차량 편의 기능 장치를 디지털화한 '디지털 콕핏'을 앞다투어 선보이고 있다. 또 통신업체들은 더 빠르고 지연이 거의 없는 자동차 통신 기술 개발 경쟁을 펼치고 있다. 자동차가 단순히 교통수단이 아닌 엔터테인먼트 기기이자 새로운 생활공간으로 영역을 확장하고 있는 것이다. 하지만 이런 기능들은 자동차와 운전자를 위험에 노출시키는 약점이 되기도 한다. 차량 통신망이나 블루투스(근거리 통신)를 이용해 침투한 해커가 차량에서 정보를 수집하고 마음대로 조종할 수도 있기 때문이다. 폭로 전문 웹사이트 위키리크스는 미국 중앙정보국(CIA)이 자동차에 악성 코드를 심어 감청을 해왔다는 문건을 공개하기도 했다. 포브스는 "현재의 자동차에는 해커가 돌을 던져서 깨고 싶은 유리창이 너무 많다"고 했다. 이스라엘 보안업체 업스트림에 따르면 2016년부터 차량 해킹 시도는 매년 2배씩 증가하고 있다. 진정한 재앙은 따로 있다. 해커가 차량의 전자 컨트롤 시스템에 접근하면 차량의 속도를 갑자기 올리거나, 브레이크가 작동하지 않도록 할 수도 있다. 뉴욕타임스는 "해커가 자동차 한 대의 방향을 난폭하게 틀게 하면 대형 사고를 일으킬 수 있고, 전기차의 전원을 완전히 차단하는 것도 가능하다는 것이 입증돼 있다"면서 "세계 주요 자동차 브랜드 대부분이 해킹에 노출됐던 경험이 있다"고 전했다.

[사진 3] 첨단 자동차를 위협하는 해킹

2.3 스마트카 해킹 사례

- 2018년 9월 미국 텍사스주 와코에서 21세 청년이 자동차 절도 혐의로 경찰에 체포됐다. 이 청년은 렌터카 업체로부터 전기차인 테슬라 '모델S'를 훔쳐 도주하다 사흘 만에 붙잡혔다. 용의자는 테슬라의 스마트폰 애플리케이션을 해킹해 자동차 문을 열고, 위성항법시스템(GPS)을 무력화시켜 이동경로 추적을 피했던 것으로 드러났다. 자동차의 전자제어 방식 장치가 늘어나고, 차량에 무선 이동통신 네트워크를 연결한 '커넥티드카'(스마트카)가 등장하면서 자동차 사이버 보안이 시급한 과제로 떠올랐다. 국내에선 아직 표면화되지 않았지만 미국 등에서는 스마트폰을 이용해 커넥티드카 기술이 적용된 자동차에 불법 침입하는 사례가 늘고 있다.



[사진 4] 스마트카 해킹 사례

21일 한국교통안전공단에 따르면 이스라엘 보안업체 '업스트림 시큐리티'가 전 세계 자동차의 사이버 공격을 집계한 결과 2010년엔 5건이었으나, 2015년 32건, 2018년 79건, 지난해 188건으로 급격히 늘고 있다. 특히 지난해는 1년 만에 두 배 이상 늘었다. 업스트림 시큐리티는 글로벌 자동차업체들이 보안 취약성이 드러나는 걸 꺼려 한다는 점에서 실제로는 이보다 더 많을 것으로 예측했다. 사이버 공격은 자동차의 전자 잠금 장치를 해킹해 차량 자체를 훔치는 것부터 고객의 정보를 대량으로 빼내는 등 다양한 형태로 이뤄진다. 자동차 회사들이 진단용으로 사용하는 블루투스, 온보드 차량점검(OBD) 포

트 등을 통해서도 해킹할 수 있다는 지적이 나온다. 사이버 공격 경로로는 차 키를 이용하지 않고도 차 문을 여닫을 수 있는 무선도어 잠금장치(키리스 엔트리 시스템)를 통한 공격이 29.6%로 가장 많았다. 자동차 제작사의 서버(27.2%), 모바일 앱(12.7%), OBD 포트(10.4%)도 보안에 취약했다. 키리스 엔트리 시스템을 공격하는 데 성공하면 차를 직접 훔칠 수 있다. 제작사 서버를 공격하면 한 번에 수많은 차량에 영향을 줄 수 있다.

2.4 200억 년 걸리면 해킹 가능하다?

- 지난 2016년 미국 전기차 업체 테슬라의 모델S 차량은 주행 중 갑자기 트렁크가 열리고 사이드미러가 접혔다. 심지어는 차량의 창문이 열리거나 좌석이 움직이며 급제동되기도 했다. 아무도 타지 않는 그 차량이 이상한 움직임을 보인 건 바로 중국 연구진의 해킹에 뚫렸기 때문이다. 중국 '킨 보안연구소'의 연구진은 테슬라 차량을 원격으로 해킹한 뒤 근처에서 노트북으로 조작하며 차를 마음대로 움직이게 했다. 만약 도로 위의 차들이 시스템으로 상호 연결된 자율주행차 시대가 열릴 경우 차량 몇 대만 해킹해도 도심지 도로 전체를 마비시킬 수 있다. 자율주행차뿐만 아니라 사물인터넷(IoT) 시대가 다가오면서 사이버 보안에 대한 우려가 더욱 커지고 있다. 이미 IoT 기기들에 대한 해킹 사례가 빈번히 보고되면서 이를 안전하게 사용할 수 있는 보안 대책이 요구되고 있다. 그런데 가장 뛰어난 해커들조차도 도저히 뚫을 수 없는 독특한 보안 기술이 최근에 개발돼 주목을 끈다. 미국 오하이오 주립대학의 물리학과 연구진은 자신들이 개발한 이 보안 시스템을 풀기 위해선 우주의 수명보다 더 오랜 시간이 걸릴 것이라고 주장했다. 연구진이 개발한 것은 컴퓨터 칩에 내장된 '물리적 복제 방지 기능(PUF)' 기술의 새로운 버전이다. PUF(physical unclonable function)란 동일한 제조공정에서 생산되는 반도체의 미세 구조 차이를 이용해 보안키를 생성하는 기술이다.

[사진 5] 이해를 돕기 위한 첨부사진

2.5 자율주행 전기차 해킹

- 테슬라의 자율주행 전기차가 누군가에 의해 원격조종을 당하는 일이 벌어질 수 있을까? 테슬라 자율주행차의 소프트웨어가 해킹당했다. 중국의 인터넷기업 텐센트의 한 부서인 '킨보안연구소'가 테슬라의 S모델 시리즈를 원격조종하는 모습을 유튜브에 올렸

다고 IT전문매체 버지 등이 20일(현지시간) 보도했다. 테슬라는 관련 소프트웨어의 문제점을 보완해 무선 업데이트했다고 밝혔지만 잇따른 자율주행차의 결함 사례가 보고되면서 소비자들의 불안감은 가시지 않고 있다. 킨보안연구소의 연구원들은 원격조종으로 주행 중인 차를 급제동시키는 모습을 선보였다. 이들은 모델 S85D 차량을 19㎞ 떨어진 곳에서 노트북으로 조작해 브레이크를 걸었다. 차선 변경 때 백미러를 접거나 방향지시등을 켜고 트렁크를 열기도 했다. 연구원들은 또 신형 모델인 S75D를 주차모드에서 조종해 문을 열거나 좌석을 앞뒤로 움직이는가 하면, 차량에 탑재된 인터넷 브라우저의 터치스크린을 무용지물로 만들었다. 테슬라는 원격조종 확률은 극히 낮다고 주장한다. 차의 인터넷 브라우저가 작동 중이고 악성 와이파이 핫스팟에 연결되어야만 하는 등 제한적인 조건에서만 가능하다는 것이다. 테슬라는 성명을 내고 현실적인 해킹 가능성은 매우 낮지만 신속하게 대응해 나가겠다고 밝혔다. 잠재적인 시스템의 취약점을 보완할 수 있도록 해킹 대응 전문가인 화이트 해커 및 보안연구 업체와 교류하고 있다고 강조했다. 테슬라는 연구를 장려하기 위해 이번에 해킹을 시도한 연구팀을 포상할 계획이다. 킨연구소는 대중에게 테슬라의 오류를 공개하기 전 테슬라에 시스템 결함을 먼저 통보했다. 연구소는 “테슬라가 전향적으로 사전대책을 강구하겠다고 했다”며 “다른 회사였다면 복잡한 절차 때문에 더 많은 시간이 걸렸을 텐데 테슬라가 10일 안에 문제를 해결했다는 사실이 대단하다”고 밝혔다. 자율주행차가 결함으로 사고를 낼 수 있고 해킹까지 가능하다는 사실이 알려지면서 소비자들의 불안감은 더욱 커질 것으로 보인다.

2.6 자율주행 전기차 해킹 사례

이 차는 이제 제껍니다. 마음대로 탈 수 있습니다. 해킹으로 자동차 훔치기 테슬라 뚫렸다.

- 2분 30초면 컴퓨터로 자동차를 훔칠 수 있다? 한 화이트해커가 미국 전기차업체 테슬라가 만든 프리미엄 SUV '모델X'를 해킹으로 훔치는 데 성공했다. 다행히 실제 범죄 상황은 아니다. 보안 시스템의 취약성을 찾기 위한 실험이었다. 가족으로 보이는 3명의 사람이 어두운 회색의 모델X를 주차하고 차에서 내린다. 나들이를 즐기는 사이, 검은색 후드티를 입은 해커가 나타나 컴퓨터 장치로 모델X 앞으로 다가간다. 장치를 몇 차례 조작하더니 모델X의 문이 열리고, 해커는 모델X를 운전해 유유히 어디론가 가버린다. 차량을 도난당한 것이다. 해킹의 주인공은 벨기에 뢰번가톨릭대학의 보안전문가 레너트 워터스이다. 워터스는 사이버 보안 시스템의 취약성을 찾아내 해당 기업에 알려주는 화이트해커이다. 워터스는 블루투스 해킹을 통해 모델X의 보안을 뚫었다. 블루투스로 자신의 노트북과 모델X 자동차 키를 연결해 잠금 해제 코드를 생성했고, 차 문을 열고 들어가 모델X와 복제한 키를 연동하는 데 성공한 것으로 보인다. 모델X 잠금장치를 푸는 데는 1분 30초, 모델X에 타 시동을 걸고 모는 데까지는 1분이 걸렸다고 한다.

[사진 6] 스마트카 해킹 예시

3. 결론

자율주행 자동차가 해킹에 노출되었다. 이 문제는 내, 외부 네트워크 통신을 통해 자동차 제어기 신호를 내, 외부 통신 사이에 집어넣어 오류를 발생할 수 있다. 차주 몰래 이물질을 집어넣어 차량 운행이 불가능하게 만드는 행위를 생각할 수 있다.

해커들이 자율주행 자동차를 해킹하고 있다. 해커들은 와이파이, 블루투스, 통신 등 해킹 공격을 하며 해킹이 되면 자율자동차 먹통, 시동을 켜거나 끄기, 문 열기, 이상한 제어, 개인정보 등의 문제가 발생한다.

내 생각은 자율자동차를 끄고 나가고, 소프트웨어도 보안(패키지) 업데이트가 필요하다는 것이다.

현재 테슬라는 해킹이 뚫렸고 안전하지 않다. 운전석의 자율자동차 시동을 켜놓고 자리를 비우면 해킹 가능성이 크다. 테슬라를 사지 않고 다음 몇 년 후에 소프트웨어의 보안을 최대한 노력한다. 보안을 믿지만 결정은 어렵다.

참고문헌

- 출처 -
1.3
URL : https://www.hani.co.kr/arti/economy/marketing/1000146.html
1.4
URL : https://blog.naver.com/with_msip/222492414870
2. 본론
2.1
URL : https://www.yna.co.kr/view/AKR20150812007600071
2.2
URL :
https://www.chosun.com/economy/tech_it/2021/03/25/KVIZYG43TBHUZNYMAJOKL5CJSI/
2.3
URL : https://www.seoul.co.kr/news/newsView.php?id=20200922010002
2.4
URL :
https://www.sciencetimes.co.kr/news/200%EC%96%B5%EB%85%84-%EA%B1%B8%EB%A0%A4%EC%95%BC-%ED%95%B4%ED%82%B9-%EA%B0%80%EB%8A%A5%ED%95%98%EB%8B%A4/
2.5
URL :
https://www.khan.co.kr/world/world-general/article/201609211731001#csidx0739bd943a990a3b377675cf4fa68d3
2.6
URL : https://news.kbs.co.kr/news/view.do?ncd=5055290