[SSR]자동차 소프트웨어 해킹과 보안

김보현

1.서론

얼마 전 드라마 <지금 거신 전화는> 에서 여주인공이 탄 차가 해킹당해 멋대로 라디오가 틀어지고 문이 열리지 않고 의도하지 않았는데 자동차의 속도가 올라가는 장면을 본 적이 있는데 자동차가 해킹을 당할 수 있다는 사실을 처음 알게되어 충격이었다. 그 이후 우연히 자동차 해킹을 정보보호 기술을 통해 방지하고 막을 수 있다는 사실을 알게되었고 그때부터 자동차 해킹과 보안에 관심이 생겼다.

입학 후, 진로탐색세미나를 통해 정보보호학부에서 진출할 수 있는 여러분야에 대해 알게되었는데 그 중 '시큐어 소프트웨어 시스템 아키텍트'에 대한 내용을 접하게되었고 소프트웨어 개발자가 되어 정보보호 지식을 활용해 소프트웨어를 안전하게 개발해보고 싶다는 생각을 하게 되었다. 소프트웨어와 보안을 접목할 수 있는 많은 분야가 있지만 먼저 가장 관심 있는 자동차 소프트웨어 보안에 대해 더 공부해보고싶어 이 주제를 선정하였다. 이번 SSR에서는 드라마 속에서 어떻게 지동차가 해킹이 된 것인지 여러가지 해킹 경로들에 대해 알아보고 추정해보려고한다.

또 자동차 소프트웨어를 보안한다고 할 때 어떤식으로 자동차 소프트웨어에 보안 기술을 접목할 수 있는지 알아보려고한다.

또한 최근 현대차그룹에서 주최한 'Pleos25'에 방문했었는데, 그곳에서 알게 된 최근 자동차 업계의 동향, 그리고 앞으로 보안과 관련해서 발생할 수 있는 문제점을 간단하게 다루어보려고 한다.

2.본론

1)드라마 속 자동차 해킹과 SDV

<드라마 속, 해킹한 범인의 핸드폰 화면>

드라마에서 자동차 해킹의 과정을 자세히 다루지는 않았지만 실제로 이러한 해킹은 소프트웨어 정의 차량(SDV(Software-Defined Vehicle))이라면 충분히 일어날 수 있다. 소프트웨어 정의 차량이란 하드웨어보다 소프트웨어가 중심이 되는 차량설계방식이다. SDV는 차량의 기능과 성능이 주로 기계적 부품과 전자 장치에 의해 결정되던 전통적 방식과 다르게 차량의 주요 기능이 소프트웨어로 정의되고 제어된다. 또한 무선 소프트웨어 업데이트(OTA업데이트)를 통해 새로운 기능 추가나 기존 기능을 개선할 수 있다. SDV의 가장 중요한 특징 중 하나는 중앙 집중형 제어방식이다.중앙 컴퓨터가 차량의 다양한 기능을 총괄적으로 제어하고 소프트웨어 중심 업데이트로 신속한 기능 추가와 성능 개선이 가능하게 된 것이다. 하지만 중앙 집중형은 사이버 공격에 취약하다는 단점이 있다.

위의 드라마 속 장면을 참고하면, 해커가 스마트폰 한 대로 차량 내부 제어 시스템에 침투해 차량 위치를 추적하고, 심지어 속도와 방향까지 바꾸는 모습을 확인할 수 있다. 그렇다면 어떻게 스마트폰 한 대로 차량 내부 제어 시스템에 침투할 수 있었던 것일까?

2)자동차 해킹 경로

자동차가 해킹당할 수 있는 원인 중 하나는 '스마트 키'이다.

스마트키는 운전자가 키를 꺼내지 않고도 차량의 문을 열고 시동을 걸 수 있는 무선 기술로, 차량 근처에 가면 자동으로 문이 열리고 일정 거리 이상 멀어지면 자동으로 문이 잠기며 원격 시동 및 공조기 작동이 가능하다. 이러한 특징을 가진 스마트 키를 해킹할 수 있는 방식은 여러가지가 있는데 그 중 첫번째는 '**리레이 공격**'이다. 리레이 공격은 해커가 두 개의 중계기를 사용해 스마트키와 차량 간의 신호를 가로채고 확장하는 방식으로, 차량 근처에 키가 없어도 신호를 확장해 문을 열고 시동을 걸 수 있다.

두 번째 방식은 '**무차별 대입 공격**'으로 스마트키의 암호화가 취약할 경우, 해커가 여러가지 키 값을 무작위로 입력해 올바른 코드 조합을 찾아내는 방식이다.

세 번째 방식은 '**무선 신호 재전송 공격**'으로 차량과 스마트키가 주고받는 신호를 해커가 저장한 후 나중에 재전송하여 차량을 제어하는 방식이다. 보안이 강화된 최신 스마트키는 일회성 코드를 사용해 이를 방지하지만 구형 모델은 여전히 위험에 노출되어있다.

자동차가 해킹될 수 있는 또 다른 원인으로는 **무선 업데이트(OTA)를 통한 해킹**이다. 무선 연결은 와이파이나 셀룰러 연결을 통해 이루어지는데 이러한 무선 환경에서는 해커가 전용 소프트웨어를 통해 자동차로 진입할 수 있다. 또한 무선주파수로도 해킹을 할 수 있는데 블루투스 NFC , RFID와 같은 근거리 통신 정보도 해킹에 취약하기 때문이다.

이 외에도 최근 진행된 버그바운티 해킹 경연대회 '폰투오운(Pwn2Own)' 에서는 SDV 적용 자동차와 차내 인포테인먼트 시스템 등 다양한 분야에서 총 49개 취약점이 발견되기도 했다고 한다.

3) 전기차, 자율주행 자동차와 관련된 자동차 해킹 위험

이번 'pleos25'에 참석했을 때 가장 핵심이 되고 있는 주제는 소프트웨어 정의 차량과 자율주행이었다. 하지만 자율주행 자동차는 일반 자동차에 비해 해커의 표적이 될 가능성이 높고, 실제로도 보안에 상대적으로 취약하다고 한다.

첫 번째 문제점은 자율주행 자동차의 핵심 기술인 '차량-사물 간 통신(V2X)'이다.

이 기술이 도입되면 자동차는 상시적으로 정보통신망에 연결된 상태가 되며,

스마트폰 애플리케이션을 통해서도 자동차를 조작하고 통제할 수 있게 된다.

하지만 그렇게 되면 해커가 시스템을 조작해 문을 잠그거나 열고, 시동을 켜고 끌 수 있게 된다. 만약 차가 정차해 있다면 이러한 공격은 단순히 도난으로 그칠 수 있지만 만약 차를 운행 중이라면 운전자와 차량에 치명적일 수 있다.

두 번째 문제점은 차량용 인포테인먼트 시스템이다. 아직 자율주행 자동차가 보편화되지 않았음에도 불구하고 벌써 자동차가 자율주행을 하는 동안 사용자가 차 안에서 각종 OTT를 이용할 수 있게 기반을 마련하고 있고 실제로도 그러한 기술들이 도입되고 있다. 하지만 이렇게 되면 차량에 연결되어있는 OTT서비스를 통해 사용자의 개인정보가 유출될 가능성이 있다. 또한 만약 사용자가 차량 내에서 중요한 화상 회의나 통화를 하고있다면 그 내용을 해커가 엿들을 수도 있으며 심지어는 차량 내부에 있는 핸드폰이나 노트북을 블루투스, 와이파이 등 무선 통신망을 이용해 해킹할 가능성도 충분하다.

요즘 화제가 되고 있는 전기차와 관련한 보안상의 문제점도 제기되고 있다.

전기차 특성상 무수히 많은 컴퓨터 전력과 온라인 서비스에 연결되어있기 때문이다.

이러한 전기차를 해킹할 수 있는 경로는 다양한데 자동차 제조사가 제작한 차량과의 소통 경로에 접근하거나 운전자가 충전소 플러그와 차량을 연결할 때 차량 접근 권한을 손에 넣는 것이 그 예이다. 혹은 공공 충전 시설의 셀룰러 네트워크 및 인터넷 연결이 차량 시스템의 접근 경로가 될 수도 있다.

현재 전기차 충전 시스템의 가장 심각한 피해 사례로는 배터리가 실제 소프트웨어에

표시된 것보다 과도한 수준으로 전력을 충전해 밤마다 차량이 과열된 것이라고 한다. 해커가 충전 시스템을 장악해 차량을 의도적으로 손상한 사례인 것이다.

4) 자동차 소프트웨어 보안 방안

첫번째로는 **엔드 투 엔드 암호화(E2EE)**가 있다.

E2EE란 전송자와 수신자 사이의 커뮤니케이션을 암호화하는 방법이며,

이들은 해당 데이터를 해독할 수 있는 유일한 당사자들이다. 현재까지 E2EE는

메시지 플랫폼에서 이용되고 있다.

E2EE는 암호화 알고리즘을 사용하여 중요한 데이터를 암호화하는 것으로 시작한다. 이 알고리즘은 복잡한 수학 함수를 사용하여 데이터를 읽을 수 없는 형식, 즉 암호 텍스트로 스크램블한다. 암호 해독 키라고 하는 비밀 키를 가진 인증된 사용자만 메시지를 읽을 수 있다. E2EE는 두 개의 서로 다른 키를 사용하여 데이터를 암호화하고 해독하는 비대칭 암호화 체계 또는 암호화 및 해독에 단일 공유 키를 사용하는 대칭 암호화 체계를 사용할 수 있다. 다음으로 전송 단계에서는 암호화된 데이터(암호 텍스트)는 인터넷이나 기타 네트워크와 같은 통신 채널을 통해 이동한다. 메시지는 목적지로 이동할 때 애플리케이션 서버, 인터넷 서비스 공급자(ISP), 해커 또는 기타 엔터티가 읽을 수 없는 상태로 유지된다.

다음으로 암호 해독이 이루어지는데 수신자의 디바이스에 도달하면 수신자의 개인 키(비대칭 암호화의 경우) 또는 공유 키(대칭 암호화의 경우)를 사용하여 암호 텍스트가 해독된다. 데이터를 해독하는 데 필요한 개인 키는 수신자만 소유한다.

여기서 대칭 암호화란 암호화와 해독 모두에 하나의 공유 키를 사용하여 속도와 효율성을 높이지만 안전한 키 관리가 필요한 방식이다. 키가 손상되면 데이터가 위험에 노출되기 때문이다. 반면 비대칭 암호화란 두 개의 암호화 키, 즉 암호화를 위한 공개 키와 암호 해독을 위한 개인 키를 사용한다. 이 방법을 사용하면 보안 키 교환이 필요하지 않지만 처리 속도가 느려지는 경우가 많다.

마지막은 인증 단계인데, 해독된 데이터는 무결성과 신뢰성을 보장하기 위해 검증되는 것이다. 이 단계에는 전송 중에 누구도 데이터를 변조하지 않았음을 확인하기 위해 발신자의 디지털 서명이나 기타 자격 증명을 검증하는 것이 포함될 수 있다.

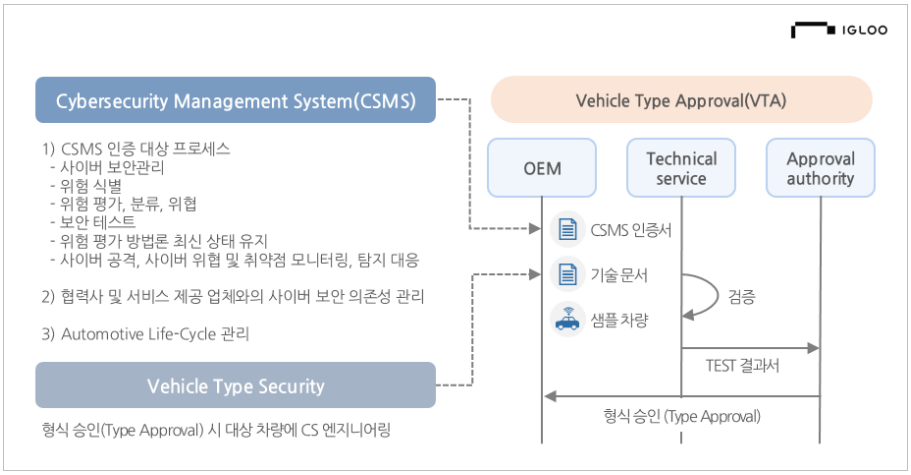
두 번째로는 **방화벽**으로, 최신 차량에 사용되고 있는 기술이다.
방화벽은 해커나 크래커의 불법 침입을 차단하여 정보 유출, 시스템 파괴 등의 보안 문제를 사전에 방지하는 소프트웨어, 혹은 그 소프트웨어가 탑재된 하드웨어로 통용된다. 네트워크 방화벽은 일반적으로 네트워크 구조의 최상단에 위치하며 인터넷과 같은 외부망으로부터 들어오는 접근 시도를 1차로 제어·통제(허용/거부)함으로써 내부 네트워크를 보호하는 역할을 한다.

세 번째로는 **침입 탐지 시스템**으로 , 역시 최신 차량에 사용되고 있다.
침입 탐지 시스템은 일반적으로 시스템에 대한 원치 않는 조작을 탐지하여 준다.
침입 탐지 시스템은 전통적인 방화벽이 탐지할 수 없는 모든 종류의 악의적인 네트워크 트래픽 및 컴퓨터 사용을 탐지하기 위해 필요하다. 이것은 취약한 서비스에 대한 네트워크 공격과 애플리케이션에서의 데이터 처리 공격(data driven attack), 그리고 권한 확대(privilege escalation) 및 침입자 로그인 / 침입자에 의한 주요 파일 접근/ 악성 소프트웨어(컴퓨터 바이러스, 트로이 목마, 웜)와 같은 호스트 기반 공격을 포함한다.

마지막으로는 **보안 관련 규제**이다.
2018년 12월 UNECE(유엔 유럽 경제 위원회)에서는 급격하게 성장하고 있는 차량 산업의 보안 위협을 우려해 UNECE Cyber Security Regulation No.155를 수립했고 2020년 6월 WP.29(자동차 국제 기준 회의체)에서 해당 법규를 채택했다.
2021년 1월 UNECE CS 법규가 발효되어 2022년 7월부터 UNECE 산하 56개 국가의

신규 생산 차량은 제작업체(OEM)뿐 아니라 부품 공급 업체(Tier)는 차량 사이버보안 관리 체계(CSMS, CyberSecurity Management System)를 구축하여 인증을 받게 됐고, 2024년 7월까지는 업체의 모든 차량에 대한 인증이 의무화됐다.

UNECE에서는 기존 차량 안전성에 관한 국제 표준 ISO 26262가 아닌 ISO/SAE 21434를 참고하여 CSMS를 운영하도록 권장하고 있다. ISO/SAE 21434는 차량 기획 단계부터 시작해 생산 및 포스트 프로덕션(Post Production) 과정까지의 사이버보안 활동에 관한 프로세스를 정의하는 것을 목적으로 만들어진 국제 표준이다.



3.결론

SSR을 마무리하며 내가 본 드라마에서의 해킹 경로로 가장 유력한게 무엇일까 생각해 보았다. 드라마에서 여주인공이 스마트키를 이용했다는 점, 해킹범이 한 번도 아닌 두 번 여주인공의 차를 해킹했다는 점을 생각해보면 리레이 공격이나 무차별 대입 공격을 통해 스마트키를 이용해 여주인공의 차량의 소프트웨어에 접근하여 내부 제어 시스템에 침투한 것 같다는 결론을 내렸다.

이번 SSR을 통해 자동차 해킹 경로들을 다양하게 살펴보았고, 자동차 소프트웨어를 보안할 수 있는 여러 방안에 대해서 그 이론과 보안 과정들을 살펴보았다.

다음 SSR에는 이번에 조사하고 공부한 이론들을 토대로 세세하게 자동차 소프트웨어의 구조, 자동차 소프트웨어 보안에 관한 책이나 논문을 참고하여 더 깊고 전문적인 내용을 다뤄보고 싶다. 또 가능하다면 관련 실습도 진행해보려고한다.

[참고 문헌]

1. 스패로우/2025/드라마 <지금 거신 전화는>으로 보는 자동차 해킹&사이버 보안 규제 총정리/ https://blog.naver.com/sparrowast/223794248831
2. AB87/2024/소프트웨어 정의 차량(SDV):미래 자동차의 새로운 패러다임 /https://capitalists.tistory.com/435
3. 한국교통안전공단/2025/자동차에 보안이 중요해지고 있는 이유는?/ https://post.naver.com/viewer/postView.naver?volumeNo=53733016&memberNo=652228&vType=VERTICAL
4. A치/2025/스마트카 키 해킹, 당신의 차량도 안전할까? 내 차를 지키는 법 /https://blog.naver.com/jabdabg/223752593920
5. 고다솔 기자/2023/내 전기차, 알고보니 해커의 다음 공격 대상? 사이버 보안 전문가 경고 잇따라 /https://cwn.kr/article/179565185608436
6. 이상우 기자/2022/자동차도 해킹되는 시대,사이버보안 강화 시급하다 /https://www.ajunews.com/view/20220703080835330
7. 돈벌카/2024/차량 소프트웨어 해킹 사례와 보안 /https://youngeung2.tistory.com/entry/%EC%B0%A8%EB%9F%89-%EC%86%8C%ED%94%84%ED%8A%B8%EC%9B%A8%EC%96%B4-%ED%95%B4%ED%82%B9-%EC%82%AC%EB%A1%80%EC%99%80-%EB%B3%B4%EC%95%88
8. IBM/엔트투엔드 암호화(E2EE)란 무엇인가요?/ https://www.ibm.com/kr-ko/topics/end-to-end-encryption
9. 이글루/2022/CSMS(ISO/SAE 21434)인증으로 살펴보는 차량 보안의 현재와 미래 /https://www.igloo.co.kr/security-information/csmsiso-sae-21434%EC%9D%B8%EC%A6%9D%EC%9C%BC%EB%A1%9C-%EC%82%B4%ED%8E%B4%EB%B3%B4%EB%8A%94-%EC%B0%A8%EB%9F%89-%EB%B3%B4%EC%95%88%EC%9D%98-%ED%98%84%EC%9E%AC%EC%99%80-%EB%AF%B8%EB%9E%98/