V2X 환경에서의 차량 보안 위협에 관한 연구

김찬민[1], 이준택[1], 서지원[2]
[1]한국자동차연구원
[2]단국대학교 사이버보안학과
cmkim@katech.re.kr, jtlee@katech.re.kr jwseo@dankook.ac.kr

A Study on Vehicle Security Threats in V2X Environment

Chan-Min Kim[1], Jun-Taek Lee[1], Ji-Won Seo[2]
[1]Korea Automotive Technology Institute
[2]Dept. of Cyber Security, Dankook University

요 약

과거 자동차 내부 네트워크는 폐쇄적이었으나, 오늘날 블루투스,WiFi, 셀룰러 등 다양한 인터페이스를 통해 외부와 연결되며 안전과 편의성을 제공하기 위해 커넥티드카 혹은 스마트카로 변화하고 있다. 그러나, 외부와의 연결성이 제공됨으로써 기존에 존재하지 않았던 보안 위협이 꾸준히 증가하고 있다. 특히 커넥티드카는 V2X(Vehicle to Everything) 통신을 통해, 다양한 보안 취약점이 발생할 수 있게 되었다. 따라서 본 논문에서는 커넥티드카에서 발생할 수 있는 보안 위협 시나리오들에 대해 제안하고자 한다.

1. 서론

오늘날 자동차와 인터넷의 연결성이 증가함에 따라 사이버 공격 경로가 더 많아지고, 이에 따른 위협 가능성도 증가하고 있다[1]. 이러한 위협에는 자동차를 원격으로 조작하는 사이버 공격이 포함되며, 이를 통해 자동차를 무기로 이용한 공격도 가능하다. 지능형 자동차 인프라에 대한 사이버 공격은 ITS 센터의 해킹, 교통 신호 제어기의 물리적 접근 해킹, V2X 통신 주파수 간섭 등 다양한 형태로 이뤄질 수 있습니다. 이러한 공격으로 인해 국가의 주요 기반 시설인 교통 시스템 등이 마비될 경우 사회와 경제에 큰 손실을 초래할 수 있다. C-ITS(Cooperative-Intelligent Transport Systems)는 교통사고를 예방하는 중요한 기능을 수행하므로, 지능형 교통 시스템의 안전한 보안 체계가 더욱 필요하다는 점이 점점 더 중요해지고 있습니다.

이러한 위협에 대응하기 위해, UNECE(유럽경제위원회)의 산하 차량 법규를 위한 세계 포럼 작업반인 WP.29는 2020년 6월 차량 사이버보안 관련 법규를 채택하였다[2], [3]. 구체적으로 R155 (UN Regulation No. 155)은 CSMS(Cybersecurity Management System)에 대한 법규로, 제조사 및 협력사가 차량 사이버보안 위협 대응을 위하여 CSMS을 구축해야 함을 명시하고 있다. 즉, 사이버보안 조건이 충족하지 않을 경우 유럽으로의 차량 혹은 전장부품을 수출할 수 없도록 강제한다.

커넥티드카 보안에 대한 중요성이 커지고 있으나, 기존 전장부품 업체는 보안성 평가를 위한 장비 구축 혹은 솔루션 개발에 대한 비용 부담이 크다. 따라서 커넥티드카 보안 규제에 대응하기 위해 최소한의 보안 솔루션 구축도 어려운 실상이므로, 여전히 많은 취약점을 가지고 있다. 특히, 커넥티드카의 통신 서비스인 V2X (Vehicle to Everything) 통신 [4]에서 보안 위협이 발생한다면, 차량 운전자의 개인정보 뿐 아니라 생명에도 위협을 가할 수 있기 때문에 치명적인 위협 수준을 가지고 있다. 구체적으로, 자동차 해킹을 통해 운전 중 시동 해제, 핸들 오작동, 제동기 오작동, 과속, GPS 조작 등과 같은 자동차 보안 사고 발생이 가능하다.

본 논문에서는 C-ITS 환경에서 차량 통신 시 발생할 수 있는 보안 위협 시나리오에 대해 소개하고자 한다. 이러한 보안 시나리오들은 국제 사이버보안 법규 대응을 위해 수행해야 하는 보안성 평가에 적용될 수 있을 것이라 기대한다.

2. 커넥티드카 용어

C-ITS는 협력 지능형 교통 시스템으로, 교통 시

스템에서 차량, 도로 인프라 및 운전자 간의 상호작용을 강화하여 교통 흐름을 최적화하고 안전성을 향상시키는 기술과 서비스다. C-ITS에서는 차량 간 통신(V2V), 차량과 인프라 간 통신(V2I), 차량과 네트워크간 통신(V2N)을 포함하여 다양한 통신 기술을 활용한다. 이러한 통신을 통해 차량은 서로간 정보를 공유하고 도로 인프라와 상호작용하며 교통 상황을 전반적으로 파악하며 예방 조치를 취하는 것이 가능해진다. 이러한 C-ITS의 목표는 교통 체계를 보다 지능적이고 안전하며 효율적으로 만드는 것이다. 이를 통해 교통 혼잡을 감소시키고 사고 발생률을 낮추며, 에너지 소비를 최적화하는 것이다. 또한, 운전자에게는 실시간으로 교통 정보를 제공하여 주행하는데 있어 도움을 주며, 도로 안전에 관한 경고 메시지를 제공함으로써 운전자의 안전 역시 증진시킬 수 있다.

V2X는 차량간, 차량과 인프라, 차량과 보행자 간에 정보를 교환하는 기술을 의미한다. SAE(Society of Automotive Engineering)에서 정의한 SAE J2735 표준[5]을 활용하여 정보를 교환하며 주로 사용하는 메시지 중 가장 대표적으로는 BSM 메시지가 있다. BSM 메시지는 전달하고자는 내용에 따라 Part1/Part2로 구분되며, 차량 식별 번호, 위도, 경도, 속도 등과 같은 정보를 포함하는 메시지다.

3. C-ITS 대상 공격 시나리오 생성 연구

C-ITS에는 차량, 신호등, RSU 등 인프라 노드 및 차량 노드와 이들을 관리하기 위한 ITS Center가 존재한다고 가정한다. C-ITS의 구성 요소들은 V2X 표준 메시지를 사용하며, ITS Center는 일반 IT처럼 네트워크에 연결되어 있다고 가정한다. ITS Center는 C-ITS에 대한 모니터링을 수행하고 RSU(Road-Side Unit)에게 경고 메시지를 전송한다. RSU는 ITS Center로부터 전송받은 정보를 바탕으로 V2I(Vehicle-to-Infra) 메시지를 생성하여 자신의 관할 구역에 해당 메시지를 전송하는 역할을 수행한다.

먼저, ITS Center의 경우 외부 네트워크와의 연결점이 많아 공격자 유입이 유리하므로 RSU 및 OBU(Onboard Unit) 대비 공격자의 타겟이 될 확률이 높다. 따라서, ITS Center를 활용한 공격 시나리오로는 ITS Center를 공격하여 침투에 성공한 후, RSU로 악성 메시지를 전송하여 주변 차량을 공격하는 시나리오다. 즉, ITS Center를 통해 RSU에 악성 V2X 메시지를 전송하면, RSU는 해당 메시지가 ITS Center로부터 왔기 때문에 전송받은 메시지를 정상적인 메시지라 판단하며 해당 메시지를 주변 차량 및 노드들에 전송하게 된다.

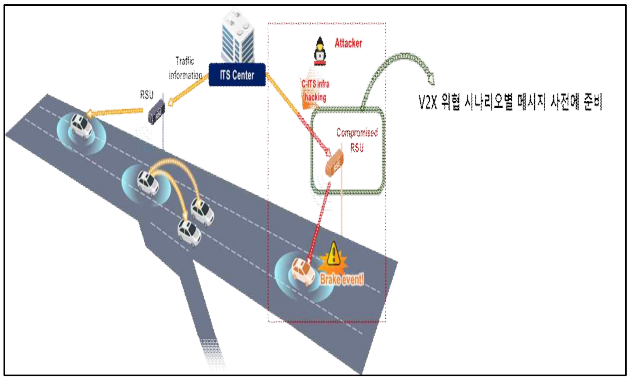

그림 1 V2X 보안 위협 시나리오 예시

그림 1은 ITS Center에 공격자가 침투하여 취약한 RSU에 악의적인 메시지를 전송하는 과정을 보여준다. 취약한 RSU는 해당 메시지에 대한 어떠한 보안성 평가를 거치지 않고, 주변 관할 차량에게 메시지를 송신하고 있다. 이로 인하여 주변 차량이 급브레이크를 할 수 있음을 나타내고 있다.

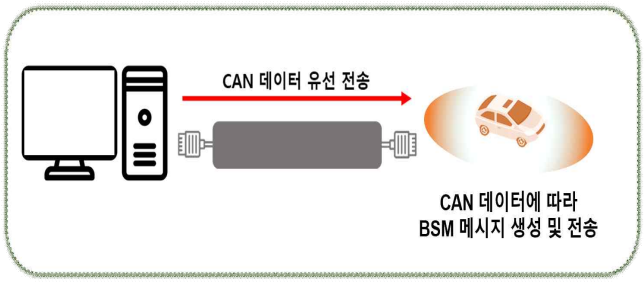

그림 2 V2X 메시지 생성 및 주입 방법

위와 같은 시나리오를 위해서는 실시간으로 메시지를 주입하거나 공격자는 취약한 RSU 내부에 사전에 악의적인 메시지를 주입해야 한다. 그림 2는 실시간으로 메시지 주입하는 방안을 보여준다. 먼저, 구상한 V2X 시나리오에 맞는 차량 데이터인 CAN 메시지를 단말기로 주입한다. CAN 메시지는 자동차 내부 전자 장치 간 데이터를 교환하기 위한 표준 통신 프로토콜로, CAN 버스를 통해 송수신되는 메시지로 주로 자동차의 엔진, 제동 시스템 등과 관련된 데이터를 포함한다. 이후 단말기는 이러한 CAN(Controller Area Network) 메시지 컨텐츠에 따라 차량

간 통신을 위한 표준 메시지 형식 중 하나인 BSM (Basic Safety Message) 메시지를 생성하여 전송하게 된다. BSM 메시지는 차량의 기본적인 운전 정보를 V2X 통신을 통해 다른 차량이나 인프라 시설에게 브로드캐스트 되기 때문에 큰 보안 위협을 야기할 수 있게 된다.

4. 결론

최근 자동차 기술의 발전으로 인하여 안전 및 편의성을 제공하기 위해 커넥티드 카는 다양한 외부 통신 인터페이스를 갖게 되었다. 그러나 이와 동시에 자동차 소프트웨어 복잡성으로 인하여 공격자가 침투할 수 있는 진입점이 증가하게 되어 사이버 공격의 가능성 및 위험성이 증가되고 있고, 사이버보안 위협 문제가 심각한 상태이다. 이러한 보안에 대한 중요성이 강조되어 UNECE WP.29 R155와 같은 국제 법규가 발표되어 보안성 평가를 통한 보안성 평가를 강조하고 있다. 본 논문에서는 이와 같은 평가에 활용될 수 있는 보안 시나리오를 제안하였다. 이러한 보안 위협 시나리오를 기반으로 향후 안전한 C-ITS를 위해 자동차 산업에 긍정적인 영향을 미칠 것이라 기대한다.

참고문헌

[1] TREND MICRO, “The Evolution of Conne cte d Cars as Defined by Threat Modeling UN R 155 -Listed Attack Vectors”, Sep 02. 2021, The Evolut ion of Connected Carsas Defined by Threat Model ing UN R 155-Listed Attack Vectors, 2021.

[2] Addendum 156 - UN Regulation No. 156, “Un iform provisions concerning the approval of vehicl es with regards to software update and software updates management system”, 2021.

[3] Addendum 155 - UN Regulation No. 155, “Un iform provisions concerning the approval of vehicl es with regards to cyber security and cyber secur ity management system”, 2021.

[4] M Ullmann, T Strubbe, C Wieschebrink. Misu se Capabilities of the V2V Communication to Har m the Privacy of Vehicles and Drivers. Internation al Journal on Advances in Networks and Services, 2017

[5] SAE International, SAE J2735 V2X Communic ations Message Set Dictionary: https://www.sae.or g/standards/content/j2735_202007/, 2020