차량 OTA 업데이트 및 클라우드 보안

서지원 (단국대학교 사이버보안학과)

1. 서 론

커넥티드카는 디지털 기술과 자동차의 결합을 통해 다양한 기능과 서비스를 제공한다. 이 기술의 핵심은 차량과 외부 네트워크 간의 상호작용을 통해 실시간 데이터를 송수신하고, 이를 통해 사용자에게 더 나은 경험을 제공하는 것이다. 커넥티드카는 엔터테인먼트, 내비게이션, 원격 진단, 차량 상태 모니터링 등 다양한 서비스를 가능하게 하며, 차량 운전의 편의성과 안전성을 크게 향상시킨다.

특히, OTA(Over the Air) 업데이트는 커넥티드카의 중요한 기능 중 하나로, 차량 소프트웨어를 원격으로 업데이트할 수 있게 한다. 과거에는 차량 소프트웨어 업데이트를 위해 서비스 센터를 방문해야 했으나, 이제는 인터넷을 통해 원격으로 간편하게 업데이트를 수행할 수 있다. 이는 소프트웨어 버그 수정, 기능 개선, 새로운 서비스 추가 등을 신속하게 적용할 수 있게 하여 차량의 성능과 안전성을 지속적으로 향상시킨다.

그러나 이러한 기술적 진보는 동시에 새로운 보안 문제를 야기할 수 있다. OTA 업데이트와 클라우드 서비스는 본질적으로 네트워크를 통해 데이터를 주고받기 때문에, 해커의 공격에 취약할 수 있다 [1-3]. 해커가 악의적으로 차량 시스템에 접근할 경우, 소프트웨어를 변조하거나 민감한 데이터를 탈취할 수 있으며, 이는 운전자와 탑승자의 안전을 심각하게 위협할 수 있다. 또한, 커넥티드카의 데이터를 저장하고 처리하는 데 중요한 역할을 하는 클라우드 서버 역시 사이버 공격의 주요 타겟이 될 수 있다. OTA 업데이트 패키지뿐만 아니라 차량에서 생성되는 대량의 데이터는 클라우드 서버에 저장되어 분석된다. 이를 통해 실시간으로 다양한 서비스를 제공하는데, 데이터 유출, 네트워크 공격, 인증 문제 등 다양한 보안 위협이 존재하며, 이는 커넥티드카의 신뢰성을 저하시킬 수 있다.

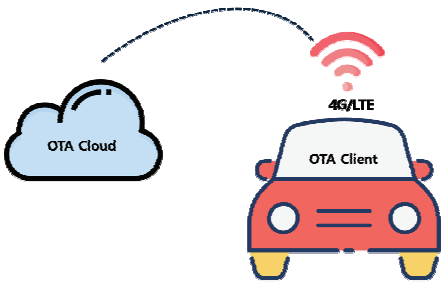
이와 관련하여 국제 사회는 커넥티드카의 보안을 강화하기 위해 여러 규제를 도입하고 있다. 대표적으로 UNECE WP.29(유럽 경제 위원회 세계 차량 규제 조정 포럼)의 UNR156 법규와 ISO 24089 표준[4]이 있다. UNR156은 차량의 사이버 보안을 규제하는 국제 표준으로, 차량 제조사에게 소프트웨어 업데이트 관리 시스템(SUMS)을 구축하고 운영할 것을 요구한다. 이는 차량의 라이프사이클 전반에 걸쳐 보안 위협을 관리하고 대응할 수 있도록 한다. ISO 24089는 차량의 소프트웨어 업데이트 절차에 대한 표준으로, OTA 업데이트 과정에서 발생할 수 있는 보안 문제를 방지하기 위한 지침을 제공한다. 이 표준은 업데이트의 무결성, 신뢰성, 인증 절차 등을 포함하며, 차량 소프트웨어의 안전하고 신뢰할 수 있는 관리를 보장한다.

본 연구에서는 커넥티드카의 OTA 업데이트와 클라우드 서비스에서 발생할 수 있는 보안 문제를 상세히 분석하고, 이를 해결하기 위한 방안을 제시하고자 한다. 또한 UNECE WP.29 UNR156 법규와 ISO 24089 표준의 내용을 포함하여, 커넥티드카 보안을 위한 국제적인 규제와 표준이 어떻게 적용되고 있는지 살펴볼 것이다. 이를 통해 커넥티드카의 안전성과 신뢰성을 확보하고, 사용자가 안심하고 이용할 수 있는 환경을 구축하는 데 기여하고자 한다.

2. 차량 OTA 업데이트 개념 논의

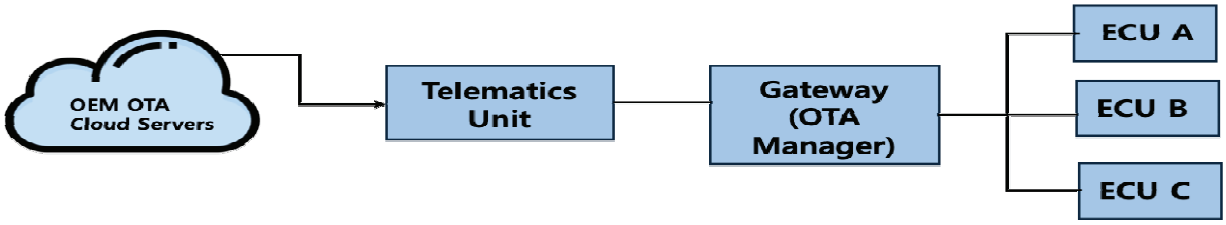
2.1 OTA(Over the Air) 업데이트

OTA(Over the Air) 업데이트는 차량 소프트웨어를 무선 통신을 통해 원격으로 업데이트하는 기술을 의미한다. 이 기술은 모바일 기기에서 시작되어 현재는 자동차 산업에서도 널리 사용되고 있다. OTA 업데이트는 차량의 전반적인 성능을 개선하고, 새로운 기능을 추가하며, 보안 취약점을 신속하게 수정할 수 있는 중요한 수단으로 자리 잡고 있다.



〈그림 1〉 차량 OTA 업데이트

OTA 업데이트는 여러 구성 요소로 이루어져 있다. 구체적으로, OTA 업데이트는 업데이트 서버, 차량 내부 시스템, 통신 네트워크, 보안 프로토콜, 그리고 클라우드 서비스로 구성되어 있다. 업데이트 서버는 차량 제조사나 소프트웨어 제공자가 운영하는 중앙 서버로 소프트웨어 업데이트 패키지가 준비되고 관리된다. 차량 내부 시스템은 차량 내



〈그림 2〉 OTA 업데이트 동작 원리

에서 업데이트를 수신하고 적용하는 시스템으로 차량의 ECU(Electronic Control Unit)들이 소프트웨어를 무선 통신을 통해 업데이트를 수행한다. 통신 네트워크란 차량과 업데이트 서버 간의 데이터를 전송하는 네트워크로, 셀룰러 네트워크(4G, 5G)나 Wi-Fi를 사용할 수 있다. 이 과정에서 보안을 유지하기 위한 암호와와 인증 메커니즘도 포함되어 있고, 클라우드 서비스는 업데이트 데이터를 저장하고 관리하는데 사용되는 인프라로, 차량과 업데이트 서버 간의 통신을 중계하고 데이터를 안전하게 보관한다.

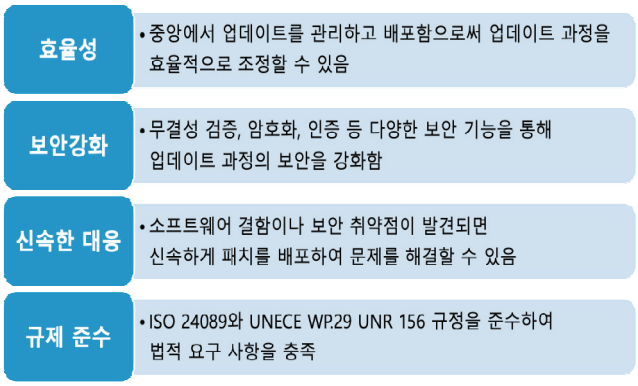
구체적으로 OTA 업데이트는 차량의 소프트웨어와 펌웨어를 무선으로 업데이트인 SOTA (Software Over-The-Air)와 FOTA (Firmware Over-The-Air)로 구성되어 있다. 먼저, FOTA 업데이트는 차량의 펌웨어를 무선으로 업데이트 하는 기술이다. 이는 ADAS(Advanced Driver Assitance Systems)와 같은 시스템에서 ECU (Electronic Control Units)를 원격으로 업데이트 하는데 사용된다. FOTA를 통해 버그를 수정하고, 시스템 기능을 향상시키며, 펌웨어 버전을 업그레이드 할 수 있다. 다음으로, SOTA 업데이트는 차량 소프트웨어를 무선으로 업데이트 하는 기술이다. 이는 소프트웨어 업데이트, 보안 패치, 새로운 기능 등에 차량에 무선으로 전송하고 설치할 수 있게 한다. 예를 들어, 스마트 홈의 스마트 난방 시스템이나 연겨로딘 차량의 네비게이션 맵 업데이트 등에 사용될 수 있다.

OTA 업데이트 과정으로 주요 단계는 1) 업로드, 2) 전송 그리고 3) 다운로드 및 설치로 구성되어 있다. 구체적으로, 새로운 업데이트 파일을 OTA 서버에 업로드한다. 이때, 서버는 업데이트 파일을 검증한 후 클라우드 서버로 전송하게 된다. 클라우드 서버는 검증된 업데이트 파일을 저장하고, 이를 차량에 전송할 준비를 한다. 클라우드는 여러 지역에 분산되어 있으므로 효율적으로 배포가 가능하다. 마지막으로 차량은 주기적으로 클라우드 서버에 접속하여 새로운 업데이트가 있는지 확인하고, 필요한 경우 업데이트 파일을 다운로드하여 설치한다. 이 과정에서 보안 인증과 데이터 무결성 검사가 이루어진다.

2.2 SUMS (Software Update Management System)

SUMS(Software Update Management System)는 차량 소프트웨어의 업데이트를 관리하고 조정하는 시스템이다. 이는 OTA 업데이트를 효과적으로 수행하고, 업데이트 과정의 보안과 무결성을 보장하는 데 중요한 역할을 한다. SUMS는 ISO 24089와 UNECE WP.29 UNR156 규정에 따라 설계되고 운영되며, 이를 통해 차량 소프트웨어 관리의 표준화와 보안성을 높인다. SUMS는 업데이트 패키지 관리, 업데이트 배포, 상태 모니터링, 무결성 검증, 로그 및 보고를 통해 차량 소프트웨어 업데이트를 관리한다.

SUMS는 ISO 24089와 UNECE WP.29 UNR156 규정을 준수하여 법적 요구 사항을 충족한다. UNECE WP.29 UNR156은 유럽 경제 위원회 세계 차량 규제 조정 포럼(UNECE WP.29)이 제정한 자동차 사이버 보안 관리 규정이다. 이 규정은 소프트웨어 업데이트 관리체계(SUMS)를 위한 법규 UNR156을 채택하였으며, 차량에 대한 소프트웨어 업데이트 관리에 대한 보안 요구사항을 준수하도록 한다. 이러한 법규 대응을 위한 표준인 ISO 24089는 차량 소프트웨어 업데이트 절차에 대한 지침을 제공하며, 업데이트의 무결성, 신뢰성, 인증 절차 등을 포함한다.



〈그림 3〉 SUMS의 장점

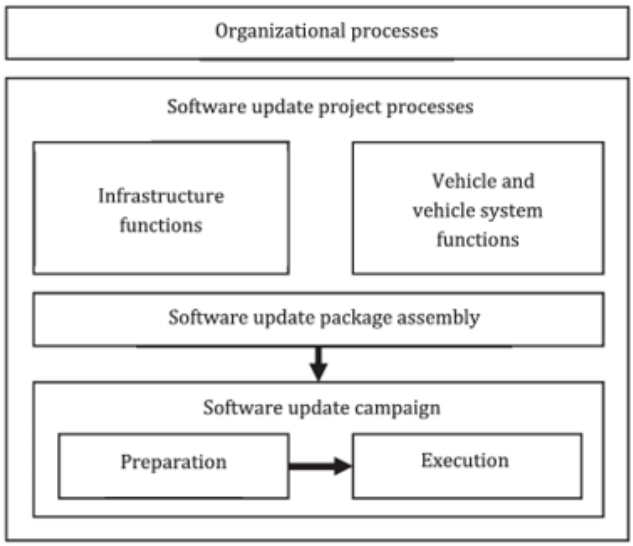
2.3 ISO 24089

OTA 업데이트를 통해 차량 소프트웨어를 원격으로 관리하고 업데이트 하는 기술이 보편화 되면서 이와 관련된 국제 표준의 필요성이 강조되고 있다. ISO 24089는 이러한 요구에 부응하여 차량 소프트웨어 업데이트의 보안 및 관리 표준을 제시하는 국제 표준이다. SIO 24089의 주요 내용으로는 소프트웨어 업데이트 관리, 보안 요구사항, 리스크 관리, 규제 준수가 있다. 소프트웨어 업데이트 관리는 소프트웨어 업데이트 프로세스의 계획, 개발, 배포, 설치 및 검

증을 포함하는 전반적인 관리 절차를 정의한다. 다시 말해, 업데이트 패키지의 생성과 무결성 검증, 배포 경로의 보안, 설치 후 검증 등의 구체적으로 절차를 규정한다. 보안 요구사항에서는 소프트웨어 업데이트 과정에서 발생할 수 있는 다양한 보안 위협을 방지하기 위한 보안 요구사항을 명시한다. 데이터 암호화, 인증, 접근 제어, 무결성 검증 등의 기술적 요구사항을 포함하여 업데이트 신뢰성을 보장한다. 리스크 관리의 경우 소프트웨어 업데이트 과정에서 발생할 수 있는 리스크를 식별하고 평가하며 이를 관리하기 위한 절차를 제시한다. 마지막으로 각국의 법적 규제와 산업 표준에 부합하는 업데이트 절차를 보장한다.

ISO 24089는 다양한 자동차 제조사와 소프트웨어 공급업체에서 채택되고 있다. Tesla는 OTA 업데이트를 통해 자사 차량의 소프트웨어를 지속적으로 개선하기 위해 표준을 준수하여 보안 강화와 신뢰성 확보를 달성하고 있다. 예를 들어, 업데이트 패키지의 무결성을 검증하고 배포 경로의 보안을 강화하는 등의 절차를 도입하고 있다. Toyota는 글로벌 시장에서 다양한 법적 규제를 준수하기 위해 ISO 24089를 채택하였다. 구체적으로, 소프트웨어 업데이트의 계획, 개발, 배포, 설치 및 검증 절차를 체계적으로 관리하며, 리스크 분석을 통해 잠재적인 위협을 사전에 파악한다. BMW는 자율 주행 기능을 포함한 첨단 차량 소프트웨어를 지속적으로 업데이트 한다. 데이터 암호화와 인증 절차를 강화하여 소프트웨어 업데이트 과정에서 발생할 수 있는 보안 위협을 효과적으로 차단하고 있다.

이처럼 ISO 24089는 차량 소프트웨어 업데이트의 보안과 신뢰성을 보장하기 위한 필수적인 규제 표준으로 Tesla, Toyota, BMW와 같은 선도 기업들은 ISO 24089를 채택하여, 안전하고 신뢰할 수 있는 소프트웨어 업데이트를 제공한다.



〈그림 4〉 ISO 24089 개요

3. 차량 사이버보안 위협 및 위험도 분석

완성차 및 전장부품사는 지속적으로 소프트웨어와 펌웨어 업데이트를 통해 최신 기능과 보안 패치를 제공한다. 이러한 업데이트는 차량의 성능과 안전성을 유지하는 데 필수적이지만, 클라우드를 통해 전달되는 과정에서 다양한 보안 위협에 노출될 수 있다. 악성 소프트웨어 및 펌웨어는 공격자가 클라우드 시스템의 취약점을 이용하여 차량 시스템에 침투하는 주요 수단 중 하나이다. 본 장에서는 악성 소프트웨어 및 펌웨어가 클라우드 보안 위협가 어떻게 연결되는지 주요 사례를 통해 구체적으로 알아볼 것이다.

3.1 클라우드 서버 침해

공격자는 클라우드 서버 자체를 해킹하여 소프트웨어 및 펌웨어 업데이트 파일에 접근하여 파일을 직접 수정하여 악성 코드를 삽입하거나 기존 기능을 변조할 수 있다. 공격자는 취약점을 이용하여 악성 코드를 업데이트 패키지에 삽입하여 데이터를 탈취하거나, 추가적인 명령을 실행할 수 있다. 이러한 변조는 클라우드 서버와 차량 간의 통신 과정에서 발생할 수 있으며, 차량의 성능, 안전성, 그리고 개인 정보 보호에 심각한 위협을 초래할 수 있다.

3.2 악성 업데이트 패키지 배포

클라우드 서버가 침해된 후, 공격자는 변조된 업데이트 패키지를 차량에 배포할 수 있다. 차량 시스템은 변조된 패키지를 정상적인 업데이트로 인식하고 설치하며, 결과적으로 악성 소프트웨어가 차량에 설치된다. 설치가 완료되면, 악성 코드는 차량의 제어 시스템에 영향을 미치거나 추가 명령을 받아 악의적인 활동을 수행한다. 예를 들어, 브레이크 시스템을 비활성화하거나 엔진 제어를 조작할 수 있다.

3.3 중간자 공격 (Man-in-the-Middle)

클라우드 서버와 차량 간의 통신이 암호화되지 않았거나 인증 절차가 취약한 경우, 공격자는 통신을 가로채서 악성 업데이트 파일을 주입할 수 있다. 이러한 공격은 업데이트 파일을 전송하는 중간 경로에서 발생한다.

이처럼 클라우드 기반 악성 소프트웨어 및 펌웨어는 공격자가 클라우드 시스템의 취약점을 이용하거나, 변조된 악성 패키지를 서버에 업로드하여 차량에 침투한다. 다음으로는 사이버보안 위협 실제 사례를 살펴볼 것이다.

3.4 Tesla OTA 업데이트 취약점(2020년)

이 취약점은 Tesla 차량의 소프트웨어 업데이트 과정에서 발생한 보안 문제로 공격자는 취약점을 악용하여 업데이트 파일을 변조하거나 악성 코드를 삽입할 수 있다[6].

공격 목표	위험도	설명
원격 제어 획득	높음	공격자가 브레이크, 가속기, 조향 등의 차량 시스템을 원격으로 제어하는 것을 목표로 한다. 이러한 공격은 차량과 탑승자의 안전을 심각하게 위협할 수 있으며, 공격자는 이를 통해 차량을 멈추거나 다른 방향으로 조향하는 등 다양한 악의적인 행동을 할 수 있다.
민감한 데이터 추출	높음	공격자는 GPS 위치, 운전자 데이터, 차량 원격 측정 데이터 등의 민감한 정보를 추출하려고 시도한다. 운전자의 이동 경로와 패턴을 파악할 경우, 심각한 보안 및 프라이버시 문제가 발생할 수 있다.
차량 기능 방해	중간	공격자가 차량의 정상적인 기능을 방해하여 오작동하거나 작동 불능 상태가 되게 한다. 사용자의 불편을 초래할 수 있으며, 특히 중요한 상황에서 차량이 제대로 작동하지 않게 되어 안전에 영향을 미칠 수 있다.
악성 코드 삽입	높음	공격자가 차량의 펌웨어에 악성 코드를 삽입하여 비인가된 명령을 실행하거나 사용자 활동을 감시한다. 이러한 악성 코드는 차량 시스템에 심각한 손상을 입히거나, 사용자 데이터를 탈취하는 데 사용될 수 있다.
업데이트 메커니즘 악용	높음	공격자가 OTA 업데이트 메커니즘의 취약점을 이용해 악성 펌웨어나 소프트웨어를 설치한다. 이를 통해 차량의 전체 소프트웨어 환경을 장악하고, 클라우드 기반 업데이트 시스템의 신뢰성을 크게 훼손할 수 있다.

〈그림 5〉 사이버보안 공격 위험도 분석

Tesla Modes S와 Model X 차량은 업데이트 패키지에 대한 보안성 검증이 부재되어 있었고, 업데이트 패키지의 무결성을 확인하는 과정에서 인증 및 암호화가 충분하지 않았다. 이로 인해 공격자는 중간자 통해 업데이트 패키지를 가로채고 공격(Man-in-the-Middle)을 변조할 수 있었다. Tesla는 이러한 취약점을 극복하기 위해 보안 패치를 통해 OTA 시스템의 취약점을 패치하였다. 또한, OTA 업데이트 프로세스를 강화하여 변조된 업데이트가 차량에 전달되지 않도록 추가적인 보안 조치를 도입하여 OTA 업데이트의 무결성과 보안성을 높였다.

3.5 Nissan Leaf 앱 취약점 (2016년)

이 취약점은 앱과 클라우드 서버 간의 통신이 충분히 암호화되지 않아 발생한 문제로 공격자는 이러한 통신을 가로채서 차량의 기능을 제어할 수 있다[7]. 먼저, 앱과 클라우드 서버 간의 취약한 통신을 통해 차량의 에어컨 시스템을 원격으로 조작 가능하다. 뿐만 아니라 통신 암호화의 부재로 인해 공격자는 차량 소유자의 개인 정보에도 접근이 가능하다. Nissan은 이를 보완하기 위해 앱과 서버 간의 통신을 강화하는 보안 업데이트를 실시하였다. 이 업데이트를 통해 통신 암호화를 강화하고, 클라우드 서버와의 인증 절차를 개선하여 유사 공격을 방지하였다. 또한, 차량 소유자들에게 최신 보안 패치를 적용하도록 권장하였다.

3.6 Volkswagen 및 Audi 클라우드 서버 침해 (2019년)

Volkswagen과 Audi의 클라우드 서버가 해킹되어 약 330만 대의 차량 데이터가 노출된 사례로, 클라우드 서버의 보안 설정 미비와 취약한 데이터베이스 관리로 인해 발생하였다[8]. 공격자는 클라우드 서버의 취약점을 이용하여 차량과 관련된 다양한 데이터를 탈취했고, 클라우드 서버를 통해 소프트웨어 업데이트 파일을 변조하여 대규모 차량 네트워크에 심각한 보안 위협을 야기하였다. Volkswagen과 Audi는 침해 사건을 인식한 즉시 클라우드 서버와의 통신 암호화를 통해 클라우드 서버의 보안 설정을 강화하고, 데이터베이스 관리 절차를 개선하였다. 또한, 침입 탐지 시스템(IDS)을 도입하여 비정상적인 활동을 실시간으로 모니터링하고 대응할 수 있도록 하였다.

그림 5는 악성 소프트웨어 및 펌웨어 공격을 통한 공격자의 목표와 그 위험도를 보여주고 있다. 먼저, 원격 제어 공격은 가장 심각한 위협 중 하나로, 공격자는 차량의 중요한 제어 시스템(예: 브레이크, 가속기, 조향 장치 등)을 원격으로 제어할 수 있다. 이는 운전자 및 탑승자의 안전을 직접적으로 위협하며 심각한 사고를 유발할 수 있다. 민감한 데이터 추출 역시 위험도가 높은데, 공격자는 차량에서 수집되는 다양한 민감한 데이터를 탈취할 수 있다. 이러한 데이터에는 GPS 위치 정보, 운전 습관, 차량 상태 데이터 등이 포함될 수 있다. 이러한 데이터 유출은 프라이버시를 침해할 뿐 아니라 범죄 행위에 악용될 수 있다. 차량 기능 방해의 경우 공격자는 차량의 특정 기능을 방해하거나 중단시킬 수 있다. 예를 들어 차량의 엔진을 비활성화할 수 있고 이러한 공격은 차량의 일상적인 사용을 방해하여 사용자의 불편을 초래할 수 있으므로 위험도는 중간에 해당한다. 악성 코드 삽입의 경우 위험도가 높은데 그 이유는 공격자는 펌웨어 내 악성 코드를 삽입하여 비인가된 명령을 실행하거나 사용자 활동을 감시할 수 있기 때문이다. 이러한 악성 코드는 차량 시스템을 손상시키고 데이터를 탈취하며 전체 시스템의 신뢰성을 저하시킬 수 있다. 마지막으로 업데이트 메커니즘 악용도 위험도가 높은 편인데 그 이유는 공격자는 OTA 업데이트의 메커니즘 취약점을 악용하여 악성 소프트웨어나 펌웨어를 설치할 수 있기 때문이다. 이를 통해 차량의 소프트웨어 환경을 장악하고 지속적으로 악의적인 활동을 수행하고 결론적으로 클라우드 기반 업데이트 시스템의 신뢰성을 훼손할 수 있다.

4. 최신 차량 보안 기술 동향 및 산업 적용

최근 차량은 첨단 기술 및 연결성을 통해 운전자에게 편리함과 안전성을 제공하고 있다. 이러한 차량의 디지털화는 클라우드 기술과 밀접하게 연관되어 있으며, 클라우드 기반의 보안 솔루션이 차량 보안의 핵심 요소로 자리 잡고 있다. 본 장에서는 최신 차량 보안 기술 동향과 클라우드 기술을 살펴볼 것이다.

4.1 OTA(Over-the-Air) 업데이트

OTA 업데이트는 차량 소프트웨어와 펌웨어를 원격으로 업데이트 할 수 있는 기술로 이를 통해 제조사는 신속하게 보안 패치를 적용하며 새로운 기능을 제공할 수 있다. 앞서 설명한 것처럼 이러한 OTA 업데이트는 클라우드 서버를 통해 제공되며, 클라우드 인프라는 대규모 업데이트 배포와 보안 관리에 필수적이다. 대표적으로 Tesla는 OTA 업데이트를 통해 차량의 소프트웨어를 지속적으로 개선하고 보안 패치를 제공한다. 2020년, OTA 업데이트를 통해 자사 차량의 취약점을 수정하고, 새로운 자율 주행 기능을 추가하였고 이를 통해 차량 소유주는 서비스 센터를 방문하지 않고도 최신 기능을 이용할 수 있게 한다. BMW 역시 ConnectedDrive 시스템을 통해 OTA 업데이트를 제공하여 차량의 인포테인먼트 시스템, 네비게이션, 엔진 제어 소프트웨어 등을 업데이트 한다. 2018년에는 OTA 업데이트로 차량의 원격 잠금 해제 기능을 개선하였다.

4.2 클라우드 기반 침입 탐지 시스템 (IDS)

IDS는 차량 네트워크에서 발생하는 비정상적인 활동을 실시간으로 감지하고 대응하는 시스템으로, 클라우드 기반으로 운영되면 대량의 데이터를 분석하여 위협을 탐지할 수 있다. 산업 적용 사례로 General Motors (GM)은 자사의 OnStar 시스템을 통해 클라우드 기반 IDS를 운영하고 있다. 이 시스템은 차량에서 발생하는 데이터를 클라우드로 전송하여 분석하고, 실시간으로 위협을 감지하여 대응한다. 또한, Ford도 차량의 네트워크 트래픽을 모니터링하고 비정상적인 활동을 감지하기 위해 클라우드 기반 IDS를 도입하였다. 이를 통해 실시간으로 보안 위협을 파악하고 필요한 경우 원격으로 차량을 안전 모드로 전환할 수 있다.

4.3 블록체인 기술

블록체인은 데이터의 무결성과 신뢰성을 보장하는 기술로, 소프트웨어 업데이트, 부품 추적, 데이터 공유 등의 영역에서 보안을 강화한다. Renault는 차량 유지보수 기록을 블록체인에 저장하여 투명성을 확보하고, 기록의 변조를 방지한다. 이를 통해 차량 소유자는 유지보수 이력을 신뢰할 수 있게 된다. BMW는 블록체인을 활용하여 부품 공급망을 추적한다. 이를 통해 부품의 출처와 이력을 투명하게 관리하여 위조 부품의 사용을 방지하고 있다.

4.4 제로 트러스트 아키텍처 (Zero Trust Architecture)

제로 트러스트 아키텍처는 모든 접근을 신뢰하지 않고 지속적으로 검증하는 보안 모델로, 네트워크 경계를 넘어서 모든 통신과 데이터에 대한 엄격한 인증과 권한 부여를 요구한다. Toyota는 제로 트러스트 아키텍처를 적용하여 내부 네트워크와 차량 간의 통신을 보호한다. 이를 통해 외부와의 모든 통신을 철저히 검증하고, 내부 시스템에 대한 비인가된 접근을 차단한다. Honda는 클라우드 서비스와의 통신에서 제로 트러스트 모델을 적용하여, 각 통신의 무결성과 신뢰성을 보장하는데 이는 특히 자율 주행 차량의 데이터 통신 보안에 중요하다.

4.5 AI 기반 보안

차량 네트워크에서 발생하는 다양한 데이터를 분석하여 이상 징후를 감지하고, 잠재적인 위협을 예측한다. Audi는 AI 기반 보안 시스템을 도입하여 차량 내의 모든 센서 데이터를 분석하고, 실시간으로 이상 징후를 감지한다. 이를 통해 비정상적인 패턴을 신속하게 식별하고 잠재적인 위협에 대응한다. Mercedes-Benz는 머신러닝을 활용하여 차량의 네트워크를 분석하고 사이버 공격의 징후를 조기에 탐지한다.

이처럼 자동차 산업에서는 다양한 최신 보안 기술이 적용되고 있다. OTA 업데이트, 클라우드 기반 IDS, 블록체인, 제로 트러스트 아키텍처, AI 기반 보안 등은 차량의 안전성과 신뢰성을 높이는 데 중요한 역할을 한다. 이를 통해 자동차 제조사들은 사이버 보안 위협에 효과적으로 대응하고, 운전자에게 보다 안전한 운전 경험을 제공할 수 있다.

5. 차량 OTA 업데이트와 클라우드 보안의 통합 관리

클라우드 기반 OTA(Over-the-Air) 업데이트는 차량의 소프트웨어와 펌웨어를 원격으로 업데이트 할 수 있는 효율적인 방법이다. 그러나, 3장에서 본 사례에서처럼 클라우드 기반 OTA 업데이트는 다양한 보안 위협에 노출될 수 있어, 이를 효과적으로 관리하고 보호하는 것이 중요하다. 본 장에서는 클라우드 기반 OTA 업데이트의 보안 중요성과 해결 방안에 대해 논의할 예정이다.

먼저, 클라우드 기반 OTA 업데이트의 보안 중요성을 위해 먼저 데이터 기밀성 및 무결성 보호가 필요하다. 차량과 클라우드 서버 간에 전송되는 데이터는 전송 중 변조되거나 탈취될 경우 차량의 소프트웨어가 손상될 수 있기 때문이다. 이를 해결하기 위해서는 차량과 클라우드 서버 간의 모든 통신을 종단 간 암호화하여 기밀성 및 무결성을 보호해야 한다. 최근에는 AES-256과 같은 강력한 암호화 알고리즘을 사용하여 데이터의 기밀성을 유지한다. 두 번째로, 인

증 및 접근 제어를 해야 한다. 즉, OTA 업데이트는 신뢰할 수 있는 소스에서만 배포되어야 하고 이를 위해 클라우드 서버와 차량 간의 상호 인증이 필수적이며 비인가된 접근을 차단해야 한다. 인증 및 접근 제어가 미비할 경우 공격자는 악성 소프트웨어를 차량에 설치할 수 있다. 클라우드 서버와 차량 간의 상호 인증을 위해 디지털 인증서를 사용하고 있고, 클라우드 서버에 접근하는 모든 계정에 대해 다중 요소 인증(MFA)을 적용하여 비인가된 접근을 차단한다. 마지막으로는 각국 정부와 규제 기관들은 차량 사이버보안에 대한 엄격한 규제를 시행하고 있다. 클라우드 기반 OTA 시스템은 이러한 규제를 준수해야 하며 규제 준수를 통해 차량 보안의 신뢰성을 확보해야 한다. 즉, 유럽연합의 UNECE WP.29 규정과 같이 각국의 차량 제조사는 ISO/SAE 21434[5] 혹은 ISO 24089와 같은 보안 표준을 준수하여 시스템의 신뢰성 확보를 해야 한다.

6. 결 론

현대 자동차 산업은 디지털화와 연결성의 발전에 힘입어 차량의 소프트웨어와 펌웨어를 원격으로 관리하는 클라우드 기반 OTA(Over-the-Air) 업데이트를 광범위하게 채택하고 있다. OTA 업데이트는 차량 성능 개선, 새로운 기능 도입, 보안 패치 배포 등의 중요한 역할을 하며, 이를 통해 자동차 제조사들은 신속하고 효율적으로 차량을 유지보수할 수 있다. 또한 차량 사이버보안 시장은 차량의 연결성 증가로 빠르게 성장하고 있고 이에 따라 보안 솔루션에 대한 수요를 촉진하고 있다.

그러나 이러한 시스템은 다양한 사이버 보안 위협에 노출될 수 있으며, 이에 대한 철저한 보안 대책이 필수적이다. 악성 소프트웨어 및 펌웨어 공격은 차량 사이버 보안에서 가장 심각한 위협 중 하나로, 공격자는 원격 제어 획득, 민감한 데이터 추출, 차량 기능 방해, 악성 코드 삽입, 업데이트 메커니즘 악용 등의 목표를 가지고 있으며, 각각의 목표는 차량과 탑승자의 안전에 심각한 영향을 미칠 수 있다. 따라서 효과적으로 방지하기 위해서는 강력한 보안 메커니즘과 업데이트가 필수적이다.

이처럼 클라우드 기반 OTA 업데이트와 보안의 통합 관리는 현대 차량의 디지털화와 연결성 증가에 따른 필수요소다. 따라서, 자동차 제조사들은 더욱 안전하고 신뢰할 수 있는 차량 환경을 구축하고 사이버 위협에 효과적으로 대응해야 한다. OTA 업데이트와 클라우드 보안을 통합 관리함으로써 일관된 보안 정책 적용, 종단 간 데이터 보호, 효율적인 위협 대응을 통해 자동차 제조사들은 신뢰할 수 있는 차량 환경을 구축할 수 있다. 앞으로도 차량 사이버보안 시장은 지속적으로 성장할 것이며, 이는 자동차 산업의 안전한 디지털 전환을 지원하는 중요한 요소로 작용할 것이다.

참고문헌

[1] Halder, Subir, Amrita Ghosal, and Mauro Conti. “Secure over-the-air software updates in connected vehicles: A survey.” Computer Networks 178 (2020): 107343.

[2] Mahmood, Shahid, Hoang Nga Nguyen, and Siraj Ahmed Shaikh. “Systematic threat assessment and security testing of automotive over-the-air (OTA) updates.” Vehicular Communications 35 (2022): 100468.

[3] JRathore, Rajkumar Singh, et al. “In-vehicle communication cyber security: challenges and solutions.” Sensors 22.17 (2022): 6679.

[4] ISO: ISO 24089 Road vehicles - Software update engineering (2023)

[5] ISO/SAE: ISO/SAE 21434: Strassenfahrzeuge, Cybersecurity Engineering (2021)

[6] Nie, Sen, Ling Liu, and Yuefeng Du. “Free-fall: Hacking tesla from wireless to can bus.” Briefing, Black Hat USA 25.1 (2017): 16.

[7] Kaltakis, Mr Konstantinos, Emmanouil Kafetzakis, and Ioannis Giannoulakis. “AUTOMOTIVE AND 5G NETWORK THREATS.”

[8] Volkswagen and Audi Cars Remotely Exploitable for Eavesdropping and Tracking, 2018, [Online Access], https://www.bitdefender.com/blog/hotforsecurity/volkswagen-audi-cars-remotely-exploitable-eavesdropping-tracking/

저자약력

서 지 원

jwseo@dankook.ac.kr

2016년 서울여자대학교 정보보호학과 (학사)
2023년 서울대학교 전기정보공학 (Ph.D., 석박사통합)
2023년~2024년 한국자동차연구원 융합보안연구실 선임연구원
2024년~현 재 단국대학교 사이버보안학과 조교수
관심분야 : System Security, Automotive Security