기술사업화 이슈&마켓

Tech-Biz Issue and Market

디지털뉴딜

출처: Frost & Sullivan Blog (ww2.frost.com) 제 197 호 | 2021.07.14

새로운 기회와 자동차 아키텍처; 사이버보안 규정은 커넥티드 자동차 생태계를 어떻게 바꿔놓을 것인가?

"커넥티드 차량 생태계와 자동차 OEM에 핵심적인 역할을 차지하게 될 사이버보안 규제"

- **연결성(connectivity)**이 확대되는 자동차 산업 전반에 걸쳐 대대적인 변화가 일어나면서 2025년까지 **커넥티드 자동차가 전 세계 자동차 시장의 약 86%를 차지할 것으로 전망**
  - 따라서 해커에게 취약한 위협 지점이 많이 발생할 것임
    - **사이버 공격과 데이터 유출 사고는 운전자 안전, 데이터 프라이버시, 서비스 연속성에 직접적인 타격을 주기 때문에 자동차 산업에 심각한 위험을 초래함**
    - 그러므로 단기적, 장기적으로 자동차 고객의 안전과 보안을 보장하려면 **적절한 지침과 규제 의무**가 반드시 필요하지만, 최근까지 커넥티드 자동차 생태계에 대한 명확하고 시행 가능한 표준이 없었음
  - 하지만 이제는 유엔 유럽경제위원회(UECE)의 **WP.29와 ISO/SAE 21434 표준**이라는 **자동차 사이버보안 이니셔티브가 제시**됨
    - 이렇게 꼭 필요했던 자동차 보안 지침이 마련되었으므로 상황이 달라질 것으로 예상됨

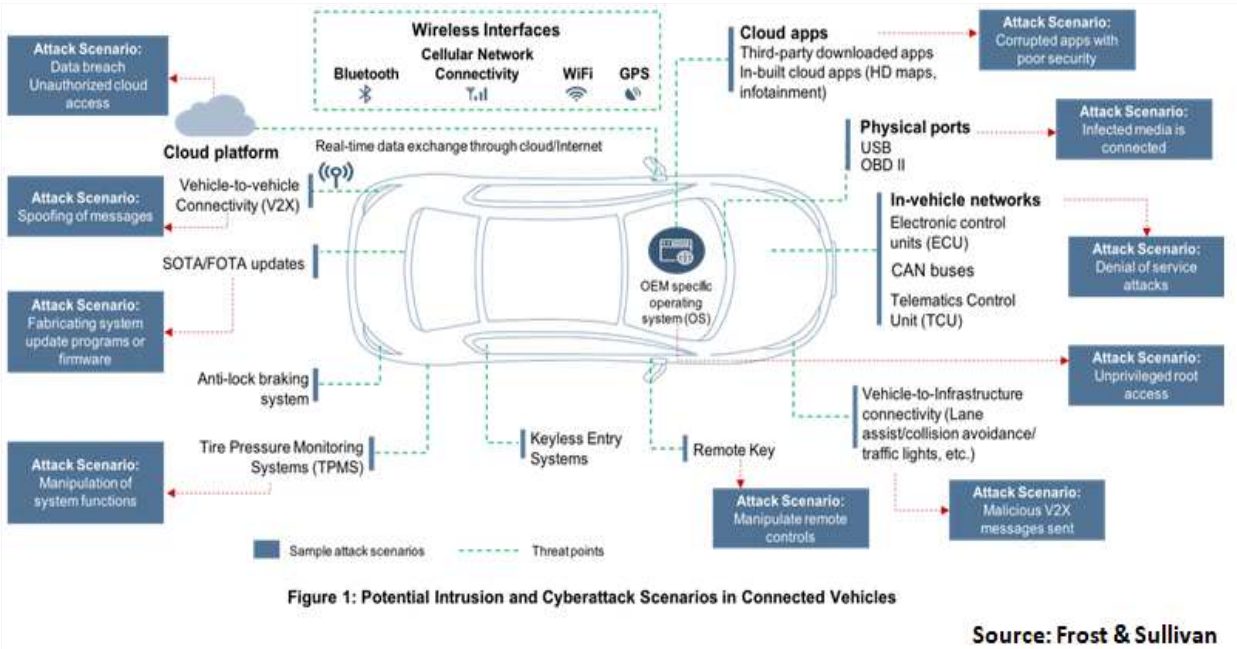

Figure 1: Potential Intrusion and Cyberattack Scenarios in Connected Vehicles

Source: Frost & Sullivan

〈그림 1〉 커넥티드 자동차의 잠재적 침입/사이버 공격 시나리오
출처 : New Opportunities and Vehicle Architectures … Car Ecosystem, Sep 7, 2020

- 미국 도로교통안전국, 유럽연합 네트워크 및 정보보안 에이전시, 유럽 자동차제조업체 협회, 자동차 엔지니어협회, Auto-ISAC과 같은 기관들이 사이버 보안 표준을 발표
  - 관련 이해와 인식을 확산하고자 노력하면서 안전한 자동차 및 차량 부품을 생산하도록 지원함
  - 커넥티드 자동차 생태계에 대한 표준화된 보안 프레임워크가 없으므로 커넥티드 차량 생태계는 사이버 공격에 매우 취약한 상태지만 2021년부터는 달라질 것으로 예상됨

- UNECE의 WP.29와 ISO/SAE 21434라는 두 가지 이니셔티브/표준
  - ISO/SAE 표준은 아직 초안 단계에 있으나 WP.29는 2020년 6월 유엔 유럽경제위원회 자동차 국제기준조화회의(UNECE)에서 채택되었으며 2021년 1월에 시행됨
  - 차세대 커넥티드 차량의 안전을 염두로 자동차업계를 준비시키는 역할을 하며, 상호 보완 효과도 기대 가능

- ISO/SAE 21434: 설계에 의한 보안을 강조함
  - ISO/SAE 표준에서는 자동차 OEM과 공급 업체 간 보안을 위해 공통 기반을 구축하도록 제안하고 있음
  - 설계, 개발, 생산, 폐기까지 자동차 라이프사이클의 모든 단계에서 효과적인 사이버 보안 프레임워크를 도입
  - 이 표준을 준수하여 모든 차량, 하드웨어/소프트웨어 구성요소, 네트워크, 통신 채널, 연결 플랫폼의 보안을 확보
  - 사이버 보안을 커넥티드 자동차 생태계 전반에서 필수 요소로 보고, 공급망의 취약 부분들에 제한을 가함

- WP.29: 종단 간(end-to-end) 차량 수명주기에 대한 보안
  - ISO/SAE와 달리, WP.29는 OEM의 전반적인 공급망에 사이버 위험을 관리할 책임이 있다고 간주함
  - OEM이 4가지 원칙에 초점을 맞춘 전체적인 보안 접근 방식을 채택해야 한다고 강조
    - **차량 개발 중 설계 단계에서 보안을 고려함**
    - **모든 차량에 침입 감지 및 이에 대한 보호 기능을 탑재함**
    - **차량 주기 내내 자동차 사이버 위험을 관리함**
    - **무선 업데이트를 통해 보안 통신 채널을 구축함**

- 상기 원칙을 준수하려면 규정된 두 가지 핵심 요건인 **사이버보안 관리 시스템(CSMS) 승인**과 **자동차 유형(Vehicle Type) 승인**을 얻어야 함
  - **CSMS 승인**: OEM이 사내에 위협 평가 및 완화 프레임워크인 CSMS를 마련할 것을 요구함

- OEM은 자사의 CSMS가 차량 개발 단계를 포함하여 오너십사이클 전체에 걸쳐 위협 식별, 분류, 복원을 적절히 처리한다는 것을 증명해야 함

※ 오너십사이클(ownership cycle): 고객이 자동차를 구매한 시점부터 그다음 자동차로 교체할 때까지의 주기

- 본 규정에는 메시지 스푸핑, 데이터 유출, 차량 코드/데이터의 무단 조작, 서비스 거부 공격, 권한 없는 사용자 액세스, 악성 콘텐츠 전송 등 30종이 넘는 위협이 열거되어 있음
- 인증서를 발급받으려면, OEM은 자사의 CSMS가 위협 목록의 내용 전체를 식별하고 언급된 각각의 위협에 대해 필요한 완화(mitigation)를 제공함을 증명해야 함

- **자동차 유형 승인**: OEM이 새로운 차량 유형을 승인받기 위해 준수해야 하는 여러 단계
  - 규제 당국은 차량 아키텍처와 위험 평가 절차가 규정에서 명시된 대로 구현되고 실행되는지 테스트함
  - OEM은 외부 공급업체 부품을 차량에 사용한 경우, 부품의 보안을 확인해야 함
  - 자동차 제조업체는 차량 개발 단계에서의 사이버 보안 절차 구축 ISO/SAE 21434 가이드라인을 참조 가능
- ISO/SAE 표준과 WP.29는 사이버 보안 관리의 효율적인 절차를 알려주지만, 의도적으로 기술 수준의 세부사항은 언급하지 않음
  - 따라서 OEM은 요구사항을 충족하는 사이버 보안 기술 KPI에 대해 자유롭게 결정할 수 있음
  - 기술적 요건이 너무 엄격하면 역동적으로 변화하는 사이버 보안 세계에서 역효과를 낳을 수 있기 때문

자동차 제조업체는 이러한 변화에 대처할 준비가 되어 있는가?

- WP.29가 시행되면 60개 이상의 국가에서 신규 차량 유형 승인에 영향을 미칠 것으로 예상함
  - 이 규정은 UNECE의 1958년 협정 당사국(유럽, 아프리카, 아시아태평양 지역 몇몇 국가)에 적용되므로 협정 당사국이 아닌 미국과 캐나다는 이 규정이 면제됨
  - 이 규정이 적용되는 국가 목록에 미국과 캐나다를 포함할 가능성에 대해 조만간 결정이 내려질 것임
- WP.29의 요구 사항을 준수해야만 목록에 포함된 국가에서 차량을 판매할 수 있음
  - WP.29를 적용하기 위해 OEM은 향후 개선이 필요한 부분을 파악하고 새로운 프로세스 로드맵을 만들어야 함

최근, OEM이 설계/개발 단계부터 차량 보안을 시행하도록 지원하는 사이버 보안 전문업체가 많음

- 하지만 강력한 CSMS를 구축하고 자동차의 전체 수명주기에 걸쳐서 보안 위험을 모니터링해야 함
- OEM은 기술적인 전문성이 부족하며 초기 비용이 매우 크기 때문에 자체적으로 시행하는 것은 매우 어려움
  - WP.29를 적용에 대해 처리 기간이 엄격하게 정해져 있는데, 대부분의 경우에 새로 승인을 받으려면 2022년 중반까지 처리해야 하므로 일정으로 인해 OEM의 어려움이 더욱 가중됨
  - 가치 사슬 전반에 보안 관련 요구 사항을 충족하는 것은 매우 복잡하고, 공급업체와 지속적인 협업이 필요

- OEM은 사이버보안 컨설팅 서비스를 위해 기술 공급업체, 보안 협력업체, 컨설팅 회사, 다양한 업계 전문가 등과 파트너십 체결/CSMS를 설정/공급망에 관련 위험 관리/감사 및 인증 확인을 시행하는 등, WP.29 규정을 준수하기 위해 노력할 것으로 예상
  - 처리기한이 엄격하게 정해져 있으며 광범위한 점검을 해야 할 차량의 숫자가 많다는 점, 감사에 드는 예산은 제한되어 있다는 점을 고려할 때, OEM은 외부 솔루션에 의존할 수밖에 없음
  - 일부 OEM은 사내에 IT 및 보안 전문부서를 만들거나 CDO/CIO를 고용해서 보안 아키텍처 문제를 직접 관리하는 쪽을 선호할 것임
  - 그러나 이러한 표준이 충분히 확립될 때까지는 감사 서비스로 외부 컨설팅 회사에 의존해야 함

향후 전망; 관련 규정이 마련됨에 따라 이 부문에 다음과 같은 새로운 기회가 열릴 것으로 예상

- 신규 스타트업은 고급 침입 탐지 기술 및 사이버 보안 관리 서비스를 갖춘 상태로 시장에 진입하면서, 기존의 경쟁 구도에 도전장을 내밀고 있음
- 온보드(on-board) 보안 보호를 전문으로 하는 기존 자동차보안업체는 시장에서 계속 살아남기 위해 자사 솔루션을 업그레이드하여 자동차 CSMS를 솔루션에 포함해야 함
- IT 서비스업체는 OEM이 구축한 CSMS를 관리할 수 있는 백엔드 사이버 보안 서비스와 IT 기술을 제공하기 위해 자동차 사이버 보안 시장을 겨냥하여 포트폴리오를 확장할 것임
- 자동차 공급 업체는 OEM의 규정 준수를 도와주기 위해, 설계별 보안 차량용 부품, CSMS, 전문 컨설팅 서비스를 제공하기 시작할 것임

(결론) 보안은 커넥티드 차량 생태계와 자동차 OEM들에게 더 핵심적인 역할을 차지하는 개념이 될 것이며, OEM은 새로운 규정을 준수하는 절차를 마련하는 과정에 착수할 것임

- 유엔 유럽경제위원회(UECE)의 WP.29와 ISO/SAE 21434 표준 **자동차 사이버보안 이니셔티브가 제시**됨
  - 두 가지 핵심 요건인 사이버보안 관리 시스템(CSMS) 승인과 자동차 유형(Vehicle Type) 승인
  - WP.29가 시행되면 60개 이상의 국가에서 신규 차량 유형 승인에 영향을 미칠 것으로 예상