자동차 해킹 방어는 방대한 사업입니다!

자율성과 전기화가 증가하면서 더 많은 사이버 보안 조치가 요구되고 있습니다. 이 소프트웨어 공급 부문에서 창출되는 매출은 10 억 달러에 이릅니다.

커넥티드 카 및 자율주행 차량이 "화이트 햇" 해커와 악의적인 의도를 가진 침입자들의 사이버 공격에 취약하다는 건 반복적으로 입증된 사실입니다. 그렇기 때문에 차량 시스템에는 더욱 강력하고 효과적인 사이버 보안 솔루션이 반드시 장착되어야 합니다. OEM 업체, 공급업체 및 소프트웨어 회사들은 사물 인터넷(IoT)이 더욱 접목된 차량의 보안 과제들을 해결하기 위해 발빠르게 움직이고 있습니다. 그 결과, 자동차 사이버 보안 시장이 호황을 맞았습니다.

재미를 위해서든 혹은 스토킹, 개인정보 수집 또는 차량 탈취와 같은 악의적인 의도를 가지고서든, 해커는 차량 진단, ADAS 시스템, V2V 연결, 무선(OTA) 소프트웨어 업데이트, 와이파이, 셀룰러, 텔레매틱스 및 인포테인먼트 시스템 등 수많은 경로로 허가 받지 않은 액세스 권한을 탈취할 수 있습니다.

특히 전기차가 많아지면서 EV 충전소와의 연결성, 파워 그리드 진입 등과 관련된 새로운 취약점들이 나타났습니다. 이를 보면 차량을 위한 대책뿐만 아니라 인프라와 시스템을 위한 해킹 대책도 마련되어야 한다는 것은 명확합니다.

S&P Global Mobility 의 최근 사이버 보안 설문조사에 따르면, 자동차 공급업체들은 OTA 소프트웨어 업데이트 시스템에 관해 제정되는 규정을 준수하는 것과 더불어 차량과 고객 보호를 위한 보안 통신 및 업데이트를 준비하는 것을 우선 순위로 지정했습니다.

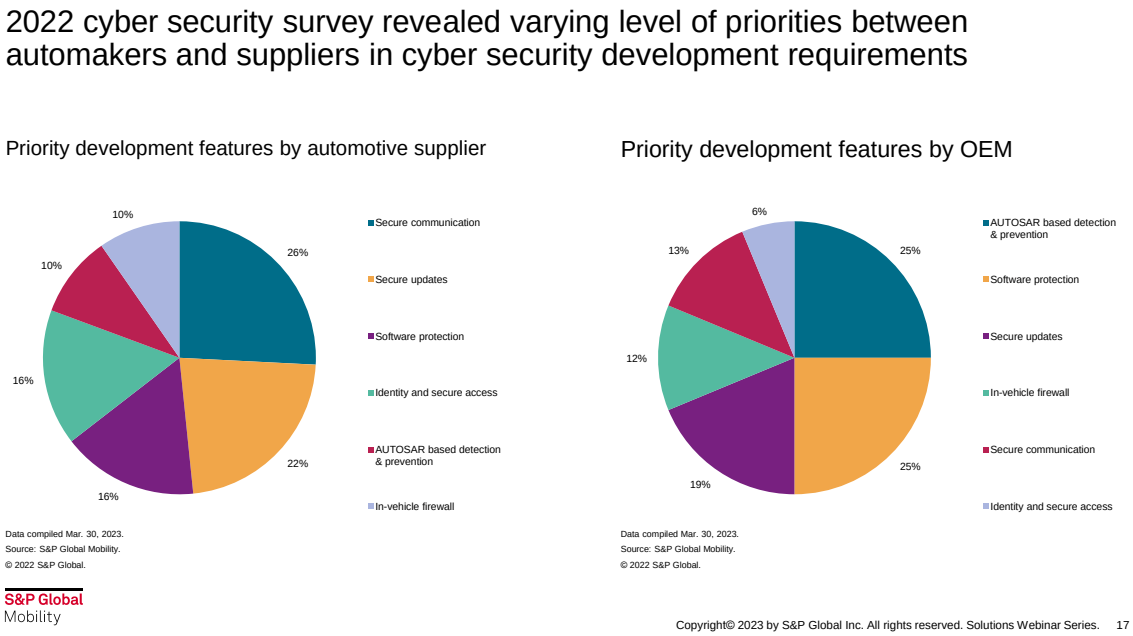
반면, OEM 업체들은 새로운 보안 요건을 충족하기 위해 보다 효율적이면서 경제적인 방식으로 사이버 보안 기술을 개발 및 배포할 수 있는 소프트웨어 보호·오픈 아키텍처에 집중했습니다.

S&P Global Mobility 의 수석 연구 분석가인 Manuel Tagliavini 는 "개별 차량도, 플릿 차량들도 개인이나 조직으로부터 사이버 공격을 당할 수 있다는 위협은 현실적"이라며, "악의적인 의도를 품은 외부인이 차량에 접근할 기회가 많아진 오늘 날에 소프트웨어 기업들은 자동차를 보호하기 위해 부단히 노력해야 할 것”이라고 전했습니다.

S&P Global
Mobility

클라이언트 소프트웨어 시장은 2021 년부터 2028 년까지 CAGR 36%을 달성할 것으로 예상됩니다. 도로 위를 주행중인 전기차가 늘어나면서, 동 기간 ECU 사이버 보안 클라이언트 솔루션의 매출은 무려 CAGR 72.9%에 이를 것으로 전망됩니다. 결과적으로, 사이버 보안 소프트웨어 부문의 전체 수익은 연말까지 10 억 달러를 초과할 가능성이 높습니다.

컴플라이언스도 이러한 성장을 앞당겼습니다. WP29 및 중국의 개인정보보호법과 같은 세계적인 규정들이 사이버 보안을 신차 플랫폼의 필수 요건으로 규정했습니다. 이에 따라 자동차 제조업체와 공급업체 양측에서 사이버 보안 관련 지출이 급등했습니다.

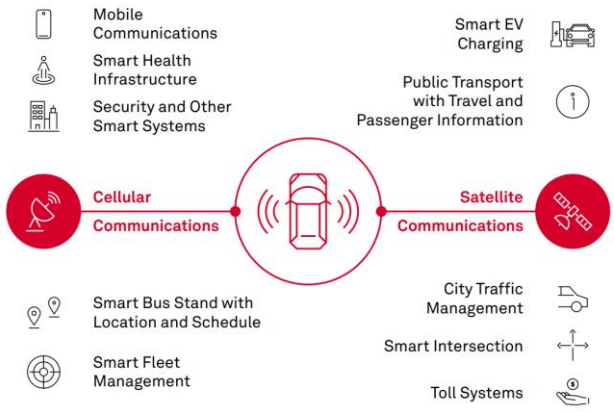


분산형에서 중앙집중식 전원 아키텍처로 들어서면서 신차 개발 주기가 단축되었고, 유지보수 기간에 관한 규제에 따라 차량을 지속적으로 보호할 필요성이 대두되었습니다. 이에 따라 자동차 제조업체와 공급업체가 자동차 수명 전반을 아우르는 구독형 사이버 보안 솔루션을 선보일 기회가 열렸습니다. 사이버 보안 업데이트는 초기에는 자동차 내부 부품 위주로 진행되고, 2030 년부터는 클라우드와의 고급 연결도 포함하여 진행될 예정입니다.

자동차 OEM 업체들은 인하우스 소프트웨어 설계 및 개발 프로세스와 전체 공급망에 있어, 자동차 사이버 보안에 포괄적인 접근방식을 채택하는 것이 중요하다는 것을 인지하기 시작했습니다. 회사들은 기존의 침입 감지 및 방지 시스템(IDPS)에 의존하는 것이 아닌, 차량 내부와 클라우드에서 데이터를 분석하고 처리하는 기능을 포함하여 사이버 위협에 실시간으로 대응할 수 있는 침입 탐지 및 대응 시스템(IDRS)을 필히 개발해야 합니다.

Cybersecurity is extending from the vehicle to the whole infrastructure

The approach is expected to be applied from the vehicle to the complete Automotive value chain



S&P Global Mobility

현재로선 이러한 온보드 기능을 수행하는 데 한계가 있습니다. 대부분의 ECU 는 프로세싱 기능이 제한적이기 때문에, 수집된 데이터 중 일부만이 차량 내부에서 분석된 후 클라우드로 전송되어 추가적으로 처리됩니다. 이 때 보안 운영 센터와 AI 기계학습의 도움으로 사이버 보안 위협의 지표가 되는 비정상적인 활동을 탐지할 수 있습니다. 향후 AI 기반 센서 융합 솔루션이 개발되고 차량 및 클라우드 기기 간의 데이터 융합이 이루어진다면, 여러 대의 차량으로부터 데이터를 집계하여 잠재적인 위협에 대한 빅데이터를 분석하는 것도 가능해질 수 있습니다.

소프트웨어와 해킹 기술은 급변하는 데 비해 자동차 제품의 주기는 느리게 진행됩니다. 혁신을 촉진하고 효과적인 사이버 보안 솔루션을 개발하기 위해서는 자동차 제조업체, 기술 제공업체 및 보안 전문가 간의 협력이 반드시 필요합니다.

- *모빌리티 뉴스 및 자산 커뮤니티에서 웨비나, 팟캐스트, 사고 리더십에 관한 기사와 백서를 포함하여 최신 뉴스와 연구 자료들을 받아보세요.*

- *S&P Global Mobility 행사 프로그램 일정에서 사고 리더(thought leader), 전문가 및 파트너들과 만나고, 소통하고 협업할 수 있는 기회를 놓치지 마세요.*

- *자동차 사이버보안에 관한 on-demand 웨비나 보러가기*