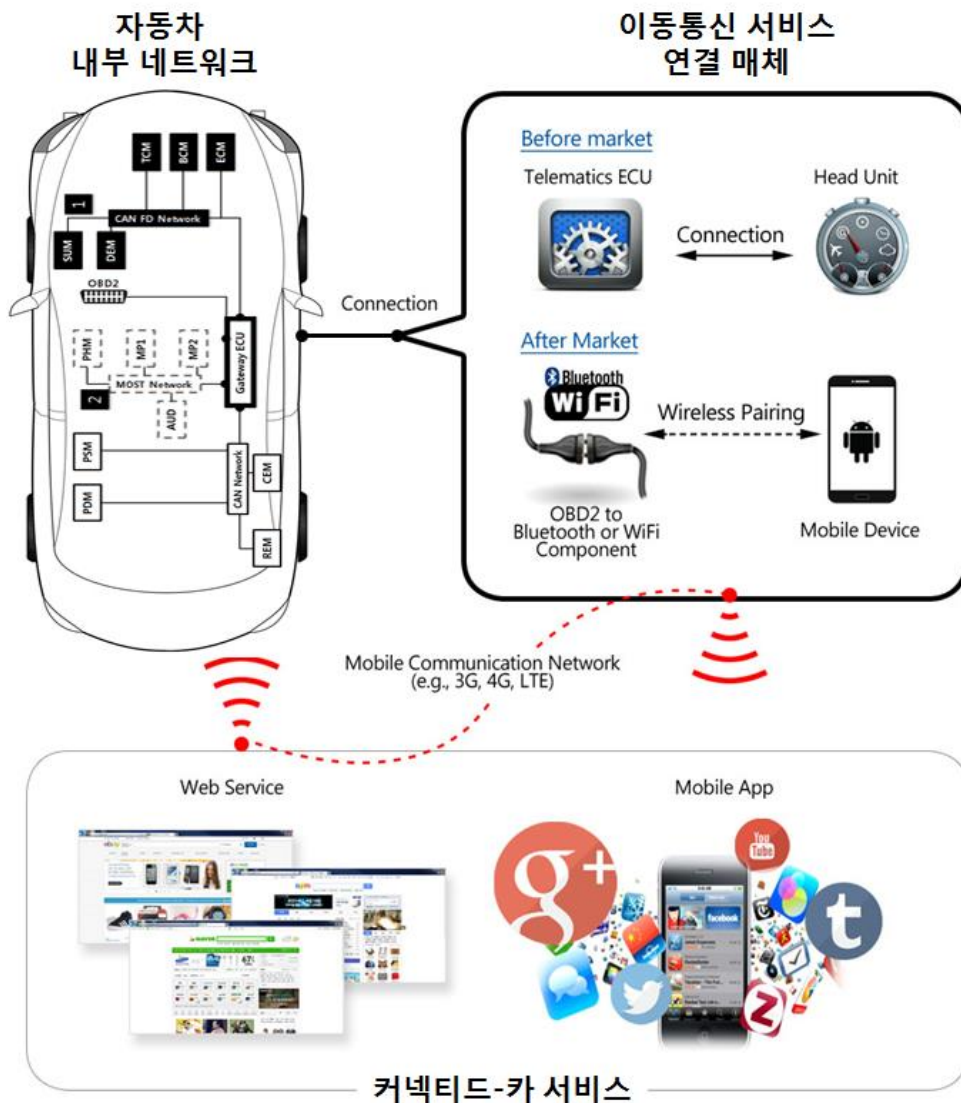


[ICT융합] 자동차-ICT 융합 및 보안 기술 동향

자동차와 정보통신기술의 융합

최신 자동차들은 운전자와 승객에게 안전하고 편안한 주행 환경을 제공하기 위해 다양한 정보통신기술(Information and Communications Technologies)들과 융합되고 있으며, 이러한 자동차-ICT 융합은 차세대 자동차 개발의 새로운 패러다임으로 자리잡았다. 효율적인 자동차-ICT 융합을 위해서 최신 자동차 제조에는 ECU(Electronic Control Unit)가 사용된다. ECU는 자동차의 주요 기능(예: 주행, 엔진, 안전, 조향 기능 등)을 컴퓨터로 제어하는 전자제어 장치로써, 자동차 산업에 도입된 후 지금까지 그 수요가 급격히 증가했다.



<그림 1> 자동차 내-외부 네트워크와 커넥티드 카 서비스 개념도

자동차에 탑재되는 ECU의 개수가 급증하면서 ECU들 사이의 효율적인 통신을 제공하기 위하여

CAN(Controller Area Network), CAN FD(CAN with Flexible Data Rate), LIN(Local Interconnect Network), MOST(Media Oriented System Transport), FlexRay등 다양한 통신기법들이 자동차 내부 네트워크에 적용되었다. 최근에는 이동통신 서비스와 자동차가 결합된 “커넥티드 카 서비스”가 상용화되면서 자동차 내부 네트워크와 외부 인터넷 망이 연결된 새로운 유형의 자동차 네트워크 환경이 형성되었다.

자동차-ICT 융합과 보안 위협

이처럼 자동차-ICT 융합이 가속화되면서 기존 ICT 환경에서 존재했던 보안 위협들이 자동차 환경으로 전이되고 있다. 이러한 위협들은 운전자의 프라이버시 침해 또는 금융손실을 발생시키고 더 나아가 인명사고로까지 이어질 수 있다. 실제로 2010년 K. Koscher 등의 연구팀은 “Experimental Security Analysis of a Modern Automobile”라는 논문을 통해 자동차 해킹의 심각성을 발표했다. 이들은 실제 판매되고 있는 자동차를 대상으로 해킹 실험을 수행했고, 자동차 내부 네트워크에 심각한 보안 취약점이 있음을 증명했다. 그 후 “Comprehensive Experimental Analyses of Automotive Attack Surfaces”라는 논문을 통해 커넥티드 카 서비스의 취약점을 이용하면, 원격으로 자동차를 제어할 수 있음도 발표했다. 이외에도 2011년 이후 각종 해킹 컨퍼런스나 국-내외 자동차 보안 관련 프로젝트들은 차량용 ECU와 내-외부 네트워크의 취약점 분석에 대한 연구 결과를 꾸준히 발표하고 있다. 이러한 연구 결과들을 통해 기존 ICT 환경에서 존재했던 보안 위협들이 실제 자동차 환경에 전이되고 있음을 확인할 수 있다.

자동차 보안 프로젝트 및 표준화 동향

자동차 환경에서 정보보호기술의 중요성이 커지면서 국-내외 연구 단체 및 표준화 단체에서는 자동차 보안과 관련된 각종 프로젝트와 표준화를 진행하고 있다. 대표적인 자동차 보안 프로젝트와 표준화 동향은 다음과 같다.

• 자동차 보안관련 프로젝트

자동차 보안관련 프로젝트들은 유럽의 자동차 OEM과 연구기관이 가장 활발한 연구활동을 수행하고 있다. 대표적인 프로젝트로는 SEVECOM(SEcure VEhicle COMmunication), EVITA(E-safety Vehicle Intrusion Protected Applications), PRESERVE(Preparing Secure V2X Communication Systems) 등이 있다. SEVECOM 프로젝트는 지능형 자동차 네트워크에 대한 보안 위협과 이를 해결하기 위한 암호 프리미티브를 정의하고 있다. EVITA 프로젝트에서는 자동차 내-외부네트워크 보호를 위한 HSM(Hardware Security Module)을 개발했다. PRESERVE 프로젝트는 유럽에서 진행되었던 다양한 자동차 보안 프로젝트들을 통합하는 연구를 수행했다(2014년 종료). 국내에서는 자동차 내부 네트워크 보안 아키텍처를 설계하고 이를 실제 자동차 환경에 적용하기 위해 융합보안 분야의 신규 국책 연구 과제를(자동차 전장 ECU 간

보안전송기술 개발, 2014년 4월 시작) 진행하고 있다.

- **자동차 보안관련 표준화**

자동차 환경에서 정보보호와 관련된 표준화가 진행된 것은 그리 오래되지 않았다. 자동차 관련 표준들 중 정보보호와 가장 밀접한 관련이 있는 대표적인 표준은 AUTOSAR(AUTomotive Open System Architecture)와 ISO 26262 표준이다. AUTOSAR는 개방형 자동차 표준 소프트웨어 구조로서, 주요 자동차 제조사와 자동차 전장부품 개발사들에 의해 개발되었다. 2009년부터 자동차용 암호 서비스에 대한 스펙을 추가하여 2015년 현재 자동차 암호 서비스에 대한 2.2.0 버전이 발표되었다. ISO 26262 표준은 기능안전 국제표준(IEC 61508)을 자동차 전기/전자 시스템에 적응시킨 국제 표준으로 자동차에 탑재되는 소프트웨어의 오류로 인한 사고를 방지하기 위해 제정되었다. 약 10개국 27개 자동차 제조사 및 부품 공급업체가 참여하여 자동차 안전 관련 요구사항을 지정하고 자동차용 전자제어장치의 기능안전을 정의하고 있다. 또한, 정보통신 응용서비스 보안 표준을 개발하고 있는 ITU-T SG17 국제표준화 기구에서도 2013년도부터 ITS 보안 표준화를 논의하였으며, 현재 차량 내부에 소프트웨어(OS, 보안모듈 등)를 안전하게 자동으로 업데이트 하는 표준(X.itssec-1), 차량 통신 시스템을 위한 보안 지침(X.itssec-2) 표준을 개발하고 있다.

자동차-ICT 융합의 핵심 정보보호

운전자의 편의와 자동차 사고를 예방하기 위해 자동차-ICT 융합은 지금보다 더 가속화 될 것이다. 하지만 보안에 대한 완벽한 고려 없이 자동차-ICT 융합만 서둘러 진행 할 경우, 자동차에 대한 사이버 공격 또한 가속화 될 것으로 전망된다. 안전한 자동차-ICT 융합 환경을 조성하기 위해 자동차의 특성을 고려한 체계적인 보안 기술 연구 및 표준화가 필수적으로 준비 되어야 할 것이다.

이동훈(고려대학교 정보보호대학원 교수, donghlee@korea.ac.kr)

우사무엘(고려대학교 정보보호대학원 연구원, samuelwoo@korea.ac.kr)