자동차-ICT 기술 융합 및 보안 기술 동향

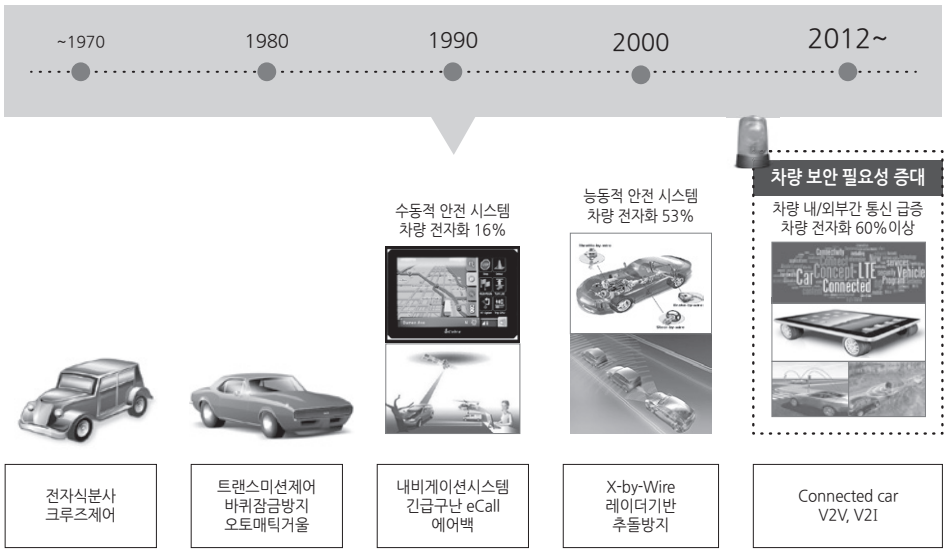
이동훈 고려대학교 정보보호대학원 교수

1. 머리말

IT 기술의 발전과 함께 자동차에도 다양한 IT 기술이 적용되고 있다. 전자식 연료분사장치가 등장하고, ABS(Anti-Lock Braking System), 자동차 자세 제어장치와 같은 전자식 제어장치가 등장하였다. 최신식의 자동차는 기계 장치뿐 아니라 100MB 이상의 바이너리 코드(Binary Code)와 함께 수많은 컴퓨터(ECU[1]:Electronic Control Unit)를 탑재하고 있다[1]. 이를 통해 자동차 조작의 대부분을 전자식으로 제어하고 에어백과 같은 안전장치, 오디오나 에어컨과 같은 편의장치 역시 전자식으로 제어하고 있다. 자동차의 제어가 전자식으로 전환됨에 따라 자동차 운전자의 편의성은 비약적으로 증대되었다. 하지만 과거 폐쇄망 성격을 갖던 자동차 내부 네트워크가 자동차 내부의 OBD-Ⅱ[2](On-Board Diagnostic) 단자를 통한 연결이나, 텔레매틱스 서비스의 발전에 따라 외부에 개방되었고, 이에 따라 악의적인 해커에 의한 외부 공격 위협성 역시 증가하게 되었다[2]. 자동차 내부에 탑재되는 ECU들은 CAN(Controller Area Network), LIN(Local Interconnect Network), FlexRay, MOST(Media Oriented Systems Transport) 등의 통신 기술을 이용하여 상호 간의 통신을 수행한다. CAN 프로토콜은 한 쌍의 꼬임선으로 구성되어 있는 물리적인 특성 때문에 외부 전자파나 노이즈에 강한 장점을

1) ECU(Electronic Control Unit)란 자동차 내부 장치들의 동작을 컴퓨터로 제어하는 전자제어 장치이다. 초기 개발 목적은 엔진의 핵심기능을 정밀하게 제어하여, 엔진의 효율이나, 연비의 향상을 위한 것이었다. 이후 자동차에 각종 편의장치, 안전장치 등을 탑재하기 위해 ECU의 활용 범위를 조향, 차체제어, 에어백 등 다양한 분야로 확대하였다.

2) OBD-Ⅱ: OBD-Ⅱ 포트는 OBD는 ON-board Diagnosis의 약자로 자동차에 내장된 컴퓨터(ON-board Computer)로 자동차의 배출가스 제어부품이나 시스템을 감시, 고장이 진단되면 운전자에게 알려 자동차 점검을 받게 하는 시스템. 1996년 이후 미국 전역과 캐나다까지 OBD-Ⅱ가 설치된 자동차만 판매 가능하며 유럽, 일본, 한국으로 확대되었다.



※ 출처: Embedded Systems in Automotive Industry-BMW

[그림 1] 자동차-ICT 융합 발전 동향

가지고 있다[3]. CAN 프로토콜은 엔진이나, 브레이크와 같은 자동차의 구동에 관련한 제어와 오디오, 내비게이션과 같은 멀티미디어 기기의 제어에 핵심적인 역할을 한다. CAN 프로토콜은 국제표준화기구(ISO)와 미국의 자동차 엔지니어협회(SAE)에 의해 국제표준화가 되어 있지만, 현재 CAN 프로토콜에는 어떠한 보안 메커니즘도 적용되어 있지 않다[3].

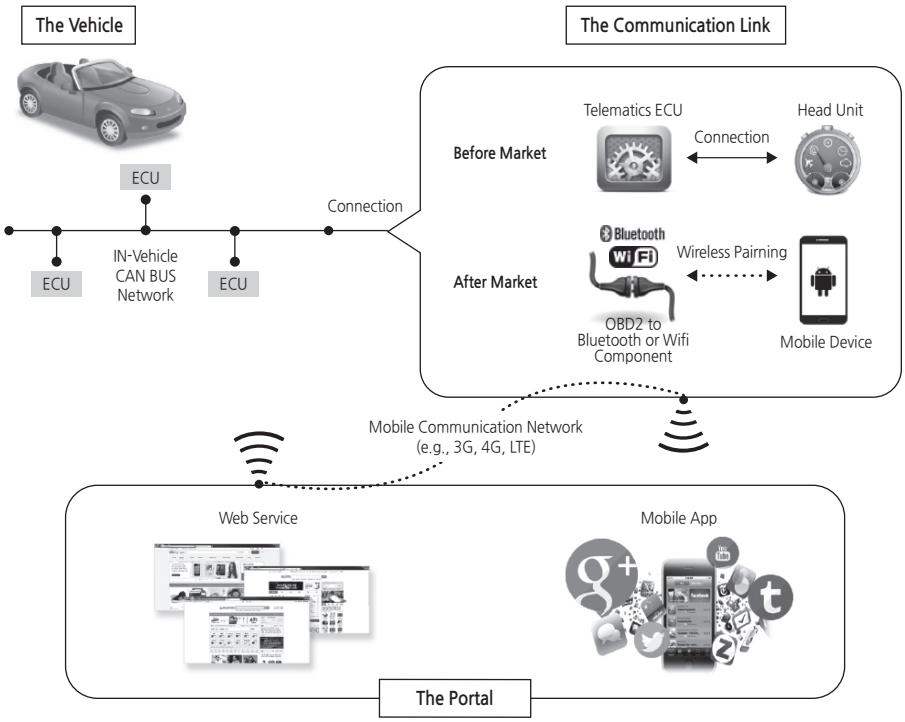
최근 연구에서는 CAN의 취약점 및 자동차 텔레매틱스 취약점을 이용한 공격 모델을 제시하고 있다. 더불어 취약점을 보완할 수 있는 방법 역시 연구가 진행되고 있으나 근본적인 보완책은 아직 미비한 상태이다[1][2][4][5].

2. 자동차-ICT(Information-Communication-Technology) 융합 동향

최근 자동차에는 자율주행 시스템, 능동형 안전 시스템과 같은 첨단 자동차 환경을 구축하고 배기가스 배출을 최소화하기 위해 다양한 ICT 기술들이 탑재되고 있다. 또한, 자동차와 이동통신기술이 융합된 커넥티드 카 산업이 새로운 블루오션으로 주목받고 있고, 휴대용 전자기기(예: 스마트폰, 태블릿 PC, MP3 플레이어)와 자동차를 연결한 각종 인포테인먼트(infotainment) 서비스들도 빠르게 성장하고 있다. [그림 1]은 자동차-ICT 융합의 발전 동향을 보여주고 있다.

2.1 ECU와 자동차 내부 네트워크

자동차에 정보통신기술을 효율적으로 융합시키기 위해서는 ECU 사용이 필수적으로 요구된다. 자동차 내부에 탑재되는 ECU는 도입 초기부터 지금까지 그 수요가 꾸준히 증가하여 최근에 개발되는 고급 자동차의 경우 약 70여 개 이상의 ECU들이 자동차 내부에 탑재되고 있다[6]. 자동차에 탑재되는 ECU의 개수가 급증하면서 ECU들 사이의 효율적인 통신을 위하여 CAN(Controller Area Network),



[그림 2] 자동차 내부 네트워크 및 커넥티트 카 환경

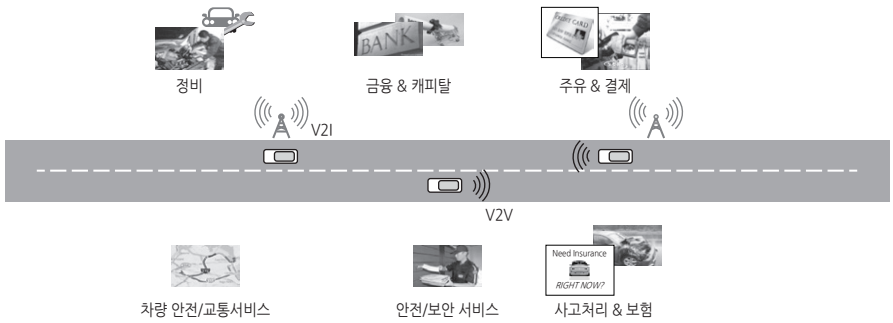
LIN(Local Interconnect Network), MOST(Media Oriented System Transport), FlexRay 등 다양한 통신기법들이 자동차 내부 네트워크에 적용되었다. 그중 CAN은 가장 대표적인 자동차 내부 네트워크 기술로써 효율적인 자동차 내부 네트워크 환경 구축을 목표로 1980년대 초반 BOSCH사에 의해 개발되었다. CAN은 버스 네트워크 토플로지를 지원하는 송신자 ID 기반의 브로드캐스트 통신기법으로 자동차 내부에 설치된 통신 회선의 복잡성을 획기적으로 감소시켰다. CAN은 ISO 11898표준으로 제정되었다[7].

2.2 커넥티트 카(Connected Car)

최근 들어 자동차에 외부 인터넷망과 통신이 가능한 모듈이 직접 설치되거나 자동차 내부 OBD-Ⅱ 단자에 무선통신모듈을 설치하고 스마트폰과 연결하여 외부 인터넷망 연결이 가능한 커넥티드 카가 등장하였다[그림 2]. 자동차 운전자는 외부 인터넷망 통신을 통해 서비스 공급자들로부터 교통정보 및 다양한 멀티미디어 서비스를 지원받을 수 있다. 현재 현대자동차의 블루링크, 기아자동차의 UVO, GM의 OnStar, BMW의 Connected Drive 그리고 쉐보레의 마이링크 서비스 등 메이저 자동차 제조사들은 독자적인 커넥티트 카 환경을 구성하고 있다.

2.3 지능형 자동차 네트워크(VANET, Vehicular Ad Hoc Network)

지능형 자동차 네트워크는 MANET(Mobile Ad Hoc Network)의 한 종류로 도로 상의 자동차들의 안전한 운행 및 운행 효율성 제고 등을 위해 연구



[그림 3] 지능형 자동차 네트워크 환경

되고 있다. 급변하는 운행 정보 제공을 위해 지능형 자동차 네트워크는 자동차와 자동차간의 통신(V2V, Vehicle to Vehicle), 자동차와 인프라스트럭처 간의 통신(V2I, Vehicle to Infrastructure)으로 구성된다. 도로 상의 각각의 자동차들은 자신의 자동차와 관련된 정보들인 속도, 위치, 가속정보 등을 주변 자동차 및 인프라스트럭처에 전송하여 다른 운전자들로 하여금 사고나 기타 긴급 상황에 대비할 수 있도록 하며, 교통정체 등의 주변 상황 정보를 공유하여 도로 위에서의 주행 효율성을 높일 수 있도록 한다. 이 밖에도 지능형 자동차 네트워크를 통해 콘텐츠의 자유로운 공유 등의 다양한 기능도 제공할 수 있다.

3. 자동차-ICT 융합 기술 보안 위협

최근에 보안에 대한 적절한 고려 없이 다양한 ICT 기술이 자동차에 적용되면서 자동차 또한 사이버 공격의 대상이 되고 있다. 2010년부터는 실제 자동차를 이용하여 사이버 공격을 수행하는 연구결과들이 발표되고 있다.

3.1 내부 네트워크 보안 위협

CAN은 다양한 기종의 자동차에 내부 네트워크로 구축되어 있다. 그러나 CAN은 브로드캐스트 통신 프로토콜임에도 불구하고 데이터 암호화나 인증기능을 전혀 제공하지 않는다. 따라서 공격자는 CAN 통신 내용을 도청할 수 있고 통신구간 메시지를 위-변조할 수 있다[8]. 2010년 K. Koscher 등의 연구팀에서 발표한 자동차 해킹 연구는 자동차 업계와 학계에 엄청난 반향을 일으켰다[1]. 이들은 실제 양산 자동차를 이용한 해킹 실험을 수행하여 자동차 내부 네트워크의 문제점을 지적하고 메시지 재전송 공격을 통해 자동차를 제어할 수 있음을 보였다. 이후 각종 보안컨퍼런스에서는 해당 연구팀의 자동차 해킹결과에 기반을 둔 현실적인 자동차 해킹 결과들이 발표되고 있다

3.2 커넥티드 카 서비스 보안 위협

2011년 Stephen Checkoway 등의 연구팀에서 발표한 커넥티드 카 취약점 분석 연구에서는 Aqlink 프로토콜의 취약점을 분석하고 원격으로 자동차를 제어하는 공격을 수행하였다[9]. Aqlink 프로토콜은 미국에서 텔레매틱스 단말에 사용되는 통신 프로토콜로 2002년부터 Ford의 Sync 서비스와 GM의 OnStar 서비스에서 사용되고 있다. 해당 연구팀에서는 Aqlink 프로토콜의 구현상에서 발생한 세 가지 취약점(Buffer OverFlow 취약점, 난수가 초기화되는 취약점, 인증 취약점)을 이용하여 자동차를 원격으로 제어하는 데 성공하였다.

3.3 지능형 자동차 네트워크 보안 위협

지능형 자동차 네트워크가 자동차에 적용될 경우, 각 자동차는 주기적으로 주변 자동차에게 안전 메시지를 보낸다. 안전메시지에는 주변의 상황, 자동차 속도, 자동차 위치 등이 포함된다. 따라서 지능형 자동차 네트워크기술이 현실화될 경우, 운전자의 위치정보를 보호하기 위한 익명성 보장 기술들이 제공되지 않는다면 주기적으로 발생하는 안전메시지를 이용하여 자동차의 이동 경로를 추적할 수 있다.

4. 자동차 보안 프로젝트 및 표준

4.1 자동차 보안 프로젝트

4.1.1 국내 자동차 보안 프로젝트

자동차 내부 네트워크 보안을 위해 국내에서는 각종 국책 연구 과제들을 진행하고 있다. 2014년 2월 종료된 '카-헬스케어 보안기술 개발' 연구과제에서는 실제 자동차를 이용한 해킹 실험을 통해 CAN 통신의 취약점을 증명하고 이러한 위협으로부터 CAN 통신을 보호할 수 있는 암호화 및 인증 기법을 설계했다. 현재 미래창조과학부에서는 실제 자동차 산업에 적용할 수 있는 보안기술을 개발하기 위해 융합보안 분야의 신규 국책 연구 과제를(자동차 전장 ECU 간 보안전송기술 개발) 진행하고 있다.

4.1.2 해외 자동차 보안 프로젝트

해외에서는 자동차-ICT 융합 기술 보안에 대한 다양한 프로젝트가 진행되고 있다. 특히 유럽에서 자동차 보안 프로젝트들이 활발히 진행되었으며, 대표적인 프로젝트로는 SEVECOM(SEcure VEhicle COMmunication), EVITA(E-safety Vehicle Intrusion Protected Applications), PRESERVE (Preparing Secure V2X Communication Systems) 등이 존재한다. SEVECOM 프로젝트는 지능형 자동차 네트워크에 대한 보안 위협을 정의하고 이를 위한 암호 프리미티브를 정의하고 있다[10]. EVITA 프로젝트에서는 자동차 내부네트워크 보호를 위한 HSM(Hardware Security Module)를 개발하였다[11]. PRESERVE 프로젝트는 유럽에서 진행되었던 다양한 자동차 보안 프로젝트들을 통합하고 있다[12].

4.2 자동차 보안 표준

4.2.1 WAVE(IEEE 1609)

IEEE 1609에서는 지능형 자동차 네트워크를 위한 WAVE(Wireless Access in Vehicular Environments) 표준화를 진행하고 있다. IEEE 1609는 1609.1부터 1609.4까지 네 가지의 파트로 나누어져서 표준화가 진행되고 있다. 특히, IEEE 1609.2에서는 지능형 자동차 네트워크에서 쓰이는 보안 메시지 규격과 보안 통신을 위한 처리 절차를 기술하고 있다. 하지만 프라이버시 보호를 위한 익명 인증 메커니즘에 관해서는 여전히 표준화가 진행중이다[13].

4.2.2 AUTOSAR와 ISO 26262

자동차용 전자제어장치의 기능안전성과 상호호환성을 높이기 위해 AUTOSAR(AUTomotive Open System Architecture)와 ISO 26262 표준이 제정되었다. AUTOSAR는 개방형 자동차 표준 소프트웨어 구조로서, 주요 자동차 제조사와 자동차 전장부품 개발사들에 의해 개발되었다. 2009년부터 자동차용 암호 서비스에 대한 스펙을 추가하여 2014년 현재 자동차 암호 서비스에 대한 2.2.0버전이 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.

5. 맺음말

본 고에서는 자동차-ICT 융합기술 동향에 대해 살펴보고 이에 대한 보안 위협과 함께 자동차 보안 프로젝트 및 표준에 대해 소개하였다. 향후, 운전자의 편의 및 자동차 사고를 예방하기 위해 더욱더 다양한 ICT 기술들이 자동차에 적용될 것이다. 하지만 보안에 대한 적절한 고려없이 ICT 기술들이 적용될 경우, 자동차에 대한 사이버 공격을 통해 운전자의 생명이 위협받을 수 있다. 따라서 안전한 자동차-ICT 융합 환경 구축을 위해서는 자동차에 대한 보안 기술 연구가 선행되어야 할 것이다.

[참고 문헌]

[1] K. Koscher, A. Czeskis, F. Roesner, S. Patel, and T. Kohno, 'Experimental security analysis of a modern automobile', IEEE Symposium on Security and Privacy, 2010.

[2] M. Wolf, A. Weimerskirch, and T. Wollinger, 'State of the art: embedding security in vehicles', EURASIP Journal on Embedded Systems, 2007.

[3] Sato Michicho, 자동차 네트워크 시스템, 성인당, 2010.

[4] T. Hoppe, S. Kiltz, and J. Dittmann. 'Security threats to automotive CAN networks – practical examples and selected short-term countermeasures', SAFECOM '08, 2008.

[5] D. K. Nilsson and U. E. Larson, 'A Defense-in-Depth Approach to Securing the Wireless Vehicle Infrastructure', Journal of Networks, 2009.

[6] R. Charette, 'This car runs on code', www.spectrum.ieee.org/feb09/7649, 2009.

[7] K.H. Johansson, M. Torngren, and L. Nielsen, 'Vehicle applications of controller area network', Springer. Handbook of Networked and Embedded Control Systems., 2005.

[8] T. Hoppe and Jana Dittman, 'Sniffing/Replay Attacks on CAN Buses: A simulated attack on the electric window lift classified using an adapted CERT taxonomy', in Proc. Workshop on Embedded Systems Security, 2007.

[9] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, 'Comprehensive experimental analyses of automotive attack surfaces', Proc. 20th USENIX Conf. on Security, 2011.

[10] http://www.sevecom.org/

[11] http://www.evita-project.org/index.html

[12] http://www.preserve-project.eu/

[13] 한국방송통신전파진흥원, 지능형 교통시스템의 차량 통신 보안 기술 동향과 전망, 방송통신 기술 이슈&전망, 2014.