커넥티드 카 보안을 위한 침해 위협 분석 및 대응방안 연구

이영헌, 류정현, 김남용, 박종혁*
*서울과학기술대학교 컴퓨터공학과
e-mail : {movestos, jh.ryu, nykim, jhpark1}@seoultech.ac.kr

Research Trends and Considerations of Invasion Threat and Countermeasures for Connected Car Security

Young Hun Lee, Jung Hyun Ryu, Nam Yong Kim, Jong Hyuk Park*
Department of Computer Science and Engineering, Seoul National University of Science and Technology (SeoulTech), Seoul, 01811, REPUBLIC OF KOREA
e-mail : {movestos, jh.ryu, nykim, jhpark1}@seoultech.ac.kr

요 약

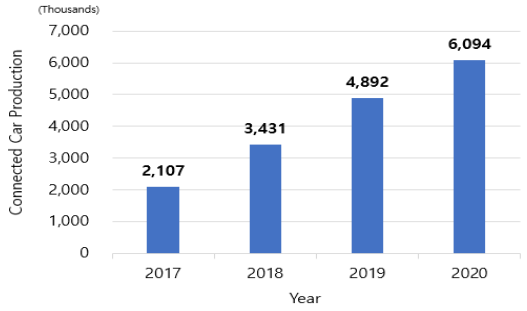
최근 4차 산업혁명은 기존에 한정적이던 사물들의 역할을 끝없이 확장시키는 특징을 가진다. 인터넷을 기반으로 인간, 사물, 환경 등 모든 것은 연결이 가능한 Internet of Things(IoT) 시대가 다가오고 있다. 사람과 사물, 사물과 사물 간의 정보를 상호 소통하여 안전기능과 사용자의 편의성을 향상시키고 있으며, ICT의 융복합의 발전에 따라 자동차도 기존과 다르게 IoT 환경에 포함된다. 커넥티드 카는 차량, 인프라, 모바일 디바이스, 주변 환경 간의 통신을 통해 실시간으로 다양한 정보를 자동차를 중심으로 수집할 수 있게 되었으며 이를 기반으로 커넥티드 카 산업이 발전하고 있다.

그러나 이러한 발전 과정 속에서 커넥티드 카의 보안성의 문제는 반드시 해결되어야 한다. 보안성이 확보되지 않는다면, 자동차에서 발생하는 운전자에 대한 악의적인 공격을 통해 일반적인 보안 침해사고 수준을 넘어 사고를 유발시킬 경우 인명과 재산상의 큰 피해를 발생시킬 수 있다. 본 논문에서는 커넥티드 카의 통신구조를 알아보고 취약점 분석과 이에 대한 대응 방안을 제안하여 안전한 커넥티드 카의 활용 방안을 연구한다.

1. 서론

최근 ICT(Information and Communication Technology) 발전에 따라 점차 지능화되고 있는 자동차의 기술은 여러 산업과 결합되어 확장되고 있으며, 자동차와 무선통신을 결합했던 과거 텔레틱스(Telematics)의 기술 개념에 최근 IoT, 5G 등 이동통신 기술 발전, 운전자의 편의성을 위한 인포테인먼트 서비스와 결합하여 대중화 되고 있다[1].

미국의 IT분야 리서치&어드바이스 전문 업체인 가트너는 2016년 9월 보고서를 통해 2020년에 이르면 내장형 모듈이나 휴대용 기기를 통해 네트워크 통신이 가능한 신규 자동차 생산량이 6천94만대로 증가할 것이라고 전망하였다[2].



(그림 1) 커넥티드 카 생산량 전망치

기존 자동차는 이동수단으로써의 기능만을 수행했다면, 최신 자동차의 경우 기계 장치 뿐 아니라 100MB 이상의 바이너리 코드(Binary Code)와 함께 수많은 컴퓨터(ECU : Electronic Control Unit)를 탑재하고 있다[3].

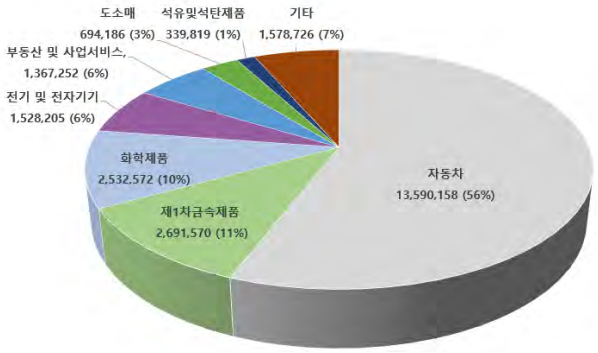
최신 자동차는 운전자가 주행 중 다양한 기능들 제공받을 수 있도록 100개 이상의 ECU를 장착하고 지속적으로 ECU의 수를 증가시키고 있으며 이를 외부 네트워크와 연결시켜 원거리에서도 조작할 수 있게 되었다. 하지만 이러한 외부 연결은 기존 ICT환경에서의 보안 취약점이 커넥티드 카에도 포함된다[4].

자동차 내부에 탑재되는 ECU들은 MOST(Media Oriented Systems Transport, LIN(Local Interconnect Network), FlexRay, CAN(Controller Area Network), 등의 통신기술을 활용하여 상호간 통신한다. 그 중 가장 많이 사용되는 CAN통신은 보안에 대한 설계를 하지 않고 통신이 이루어지고 있으며, 이에 따라 외부 네트워크로부터 연결될 경우 공격에 매우 취약하며 이를 이용한 공격 사례가 <표 1>과 같이 발생하고 있다.

<표 1> 커넥티드 카 보안위협 사례

연도	국가	내용
2012	영국	OBD2에 접속, 주차된 BMW 해킹 및 원격제어로 무단 탈취
2013	미국	포드,도요타 차량에 대해 CAN과 전장 ECU를 해킹한 코드 공개
2015	미국	JEEP 차량의 인포테인먼트 시스템 이용, 차량 권한 탈취 시연
2017	미국	이모빌라이저 시스템 악용, 100여대 차량 시동 및 경적 제어

커넥티드 카의 보안 취약점에서 안전하지 못하다면 서비스업 등 연관 산업도 함께 피해를 입을 수 있으며, 차량이 해킹되면 차량 도난이나 운전자 정보 유출 등 2차 피해 가능성이 있다. (그림2)에서 자동차 보안의 피해는 다른 산업군에 비해 매우 높은 수준이다[5]. 커넥티드 카 산업의 발전을 위해서는 보안 기술 개발 선행을 통해 소비자의 불안감을 최소화해야 한다. 이에 따라 본 논문에서는 커넥티드 카 관련 보안 위협과 이에 대한 보안 기술을 제시한다.



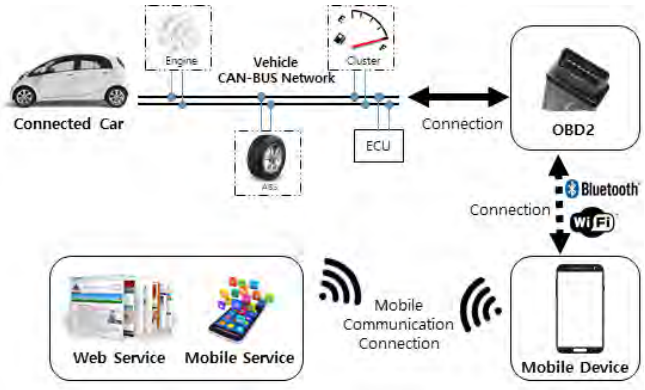
(그림 2) 자동차 보안 피해 총액

2. 커넥티드 카의 개념 및 네트워크 구성요소

● 커넥티드 카

커넥티드 카에 대한 정의는 정확하게 정의되지 않았으며, 자동차의 내부 또는 외부 망과의 연결 등 자동차에 네트워크 접속 기능을 추가하여 자동차 내부에서 다양한 정보서비스 및 엔터테이먼트 서비스를 지원하는 것으로 정의할 수 있다[6]. 커넥티드 카는 자동차에 통신기능이 장착되어 차량 연결성(Connectivity)을 강조하고 자동차에 IoT의 개념을 도입하였다. 현재는 차량, 인프라, 스마트 디바이스 간 실시간 정보교류를 통해 운전자에게 안전하고 편안한 운전 경험을 제공하고 있다[7][8].

현재 커넥티드 카의 구성은 (그림 3)과 같이 제어 및 모니터링 서비스가 자동차 내에 탑재되고, 미디어 컨텐츠 스트리밍 및 다양한 애플리케이션 서비스 등은 모바일 디바이스와 연결해 이용하는 형태가 주를 이루고 있으나, 궁극적으로는 모든 연결성, 플랫폼 및 솔루션이 자동차 내에 탑재되어 자동차 자체가 하나의 '커넥티드 디바이스(Connected Device)'가 되는 형태로 진화하고 있다[9].

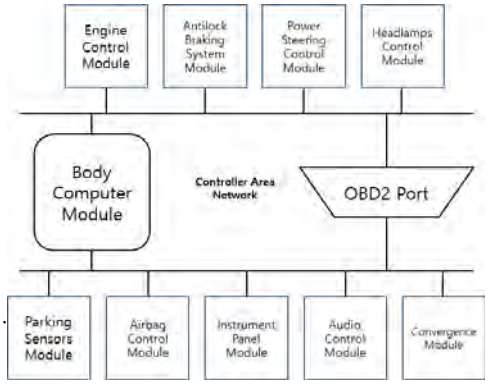


(그림 3) 커넥티드 카 구성[10]

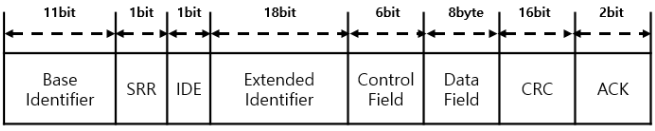
● CAN

CAN(Control Area Network)은 자동차 내 ECU들이 서로 통신하기 위해 설계된 표준 통신 규격이다. 1983년 독일의 자동차 부품 업체 보쉬가 처음 개발했고, 1986년 공식 출시됐다[11]. 생산용 자동차에 처음 적용된 것은 1989년으로 1993년 자동차 분야 품질관리표준을 제정하는 ISO에서 CAN을 국제표준규격(ISO 11898)으로 채택했다. 이후 CAN은 차량용 네트워크의 표준으로 자리 잡았다. (그림 4)는 CAN이 자동차에 장착된 여러 장치와 시스템이 상호 연결되는 방법을 명시하고 있다[12].

(그림 5)에서 CAN의 통신 메시지는 식별자 ID의 길이에 따라 11비트 식별자 ID(Base Identifier)를 가지는 표준 프레임 포맷(CAN 2.0A)와 29비트 ID를 가지는 확장형 포맷(CAN 2.0B)로 구분된다[13].



(그림 4) 일반적인 CAN 다이어그램



(그림 5) CAN 2.0 B 패킷 프레임 포맷

3. 커넥티드 카 관련 보안 위협

커넥티드 카는 공격자가 다양한 보안 취약점 경로를 통하여 자동차를 조작하거나 운전자에게 영향을 줄 수 있다. Wi-Fi, 블루투스, DSRC, OBD 시스템, USB, 자동차 어플리케이션 등 자동차에 연결된 많은 부분들이 공격의 가능성을 보여주고 있다. 특히, CAN은 인증 및 엑세스 제어 메커니즘이 존재하지 않는다[14]. CAN 버스에 연결된 모든 장치에 대한 통신 데이터들은 모두 신뢰되어 조작된 오류 메시지에 대해 진짜 오류메시지와 공격자가 의도적으로 생성한 가짜 메시지를 구별할 수 없게 된다. 이러한 CAN 설계 취약점을 악용하여 특정 장치를 통신을 어렵게 만들 수 있게 되었으며, 커넥티드 카 환경에서 보안 위협 가능성이 높아지게 되었다.

● OBD취약점

OBD(On Board Diagnostics)시스템은 1996년, 미국에서 의무적으로 장착 되도록 시행되었으며, EU에서도 2001년부터 의무 장착이 시행되었다. 자동차에 부착된 OBD단자는 자동차의 문제점에 대하여 보고할 수 있도록 하였고 장착된 여러 센서들의 수집, 진단 데이터 값들을 외부로 보고할 수 있게 하였다. OBD단자는 CAN 버스에 물리적으로 접근할 수 있어 서비스 제공자가 보고된 문제를 수정할 수 있게 하지만, 공격자가 악의적인 코드를 주입 할 수 있다. 이러한 OBD동글들은 다양한 구매처에서 구매할 수 있으며 가격이 많이 비싸지 않아 악용될 우려가 있다.

한 연구에서 OBD단자를 활용하여 차량의 바이러스가 ECU들에게 침투되면 특정한 조건이 성립하였을 때 차문 잠김과 같은 기능을 실행 할 수 있게 하였다. 최근 연구결과에 따르면 50%이상의 OBD동글들이 노출된 키값, 통신 도청 등의 취약점 등을 가지고 있다[15].

과거 OBD단자를 통한 이러한 공격들은 자동차에 물리적으로 접근해야 가능하였지만 현재는 3G/4G, 블루투스, Wi-Fi 등 무선으로 연결되어 원격 공격의 가능성이 높아지고 있다.

● DSRC 취약점

DSRC(Dedicated Short-Range Communication)은 ITS(Intelligent Transport Systems) 서비스를 제공하기 위해 도로변에 설치된 노면설비인 RES(Road Side Equipment)와 자동차가 고속으로 주행하며 단말기를 통해 10~100m 이내, 일 대 다수 통신기능, 양방향 통신하는 시스템을 말한다[16]. DSRC가 장착된 자동차들은 다른 DSRC가 장착된 자동차나 도로주변부 장치들과 정보교류를 하게 되며 운전자에게 도로의 교통상황을 전달한다.

하지만 (그림 6)처럼 외부 노드가 해킹되어 DSRC가 장착된 자동차에 공격자가 임의로 조작한 정보를 전송하여 사고를 유발시킬 수 있다. IEEE 1609.2에서 DSRC는 인가되고 암호화된 상태로 메시지가 전달되어야한다고 정의하고 있지만, DoS(Denial of Service), 위치추적, 허위정보 전송 등의 공격의 가능성이 여전히 존재한다.

(그림 6) ITS환경에서 DSRC를 통한 공격

● 자동차 관리 어플리케이션 취약점

최근 많은 운전자들은 모바일 디바이스를 통해 자동차로부터 다양한 편의를 제공 받는다. 또한 여러 자동차 제조업체에서 제공해주는 자동차 관리 어플리케이션을 이용하여 자동차를 진단하거나 광범위한 정보를 수집하여 활용한다.

하지만 이러한 모바일디바이스, 어플리케이션에 대하여 공격자가 고의적으로 변조하거나 악성코드를 설치할 경우, 커넥트 카에 대한 제어권이 탈취당할 수 있다. 최근 진행된 연구에 따르면, 자동차 정비기기를 통해 ECU를 임의 조작할 수 있는 CAN 데이터 프레임을 획득 및 변조 과정을 거친 뒤, 배포된 자동차 진단용 어플리케이션을 분석하고 리패키징을 통해 구글 플레이에 재배포를 하여 임의로 자동차를 제어할 수 있었다[17].

현재 운전자는 커넥티드 카의 편의성을 지속적으로 높이기 위해서 자동차 제조사가 제공하는 파일을 다운로드받아 차량 USB를 통해 업데이트 할 수 있다. 그러나 해당 업데이트 파일은 인증이나 암호화 되지 않은 상태로 제공되어 공격자가 자동차 내부 시스템에 임의로 접근할 수 있는 많은 정보를 포함할 수 있으며, 업데이트 파일 내부에 악성코드를 삽입하는 공격이 이뤄질 수 있다[18].

4. 커넥티드 카 취약점에 따른 대응 방안

● OBD에 대한 대응

외부로부터 직접적으로 노출되어 있는 OBD단자는 물리적인 보안 장치를 설치하여 CAN 유입을 방지할 수 있다. 무선으로 연결되는 경우, 내부 네트워크의 KMS(Key Management System)를 통하여 암호화와 ECU 인증을 도입하여 대응하도록 한다. 또한, CAN의 평소 통신 흐름과 다른 이상 흐름이 감지될 경우 침입 탐지/방지 시스템(IDS/IPS)를 도입하여 사전 차단할 수 있도록 하고, 접근제어와 무결성을 보장받을 수 있도록 ECU 자가 검증과 정상 소프트웨어만의 동작을 위해 시큐어 부트, 시큐어 플래싱을 구성하여 취약점에 대응할 수 있다.

● DSRC에 대한 대응

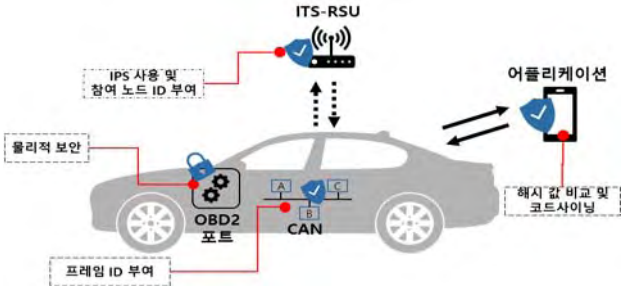
외부 인프라 간 통신 보안을 위해 ITS의 V2V, V2I를 구성하는 통신인 DSRC 서비스 과정에 메시지 인증, 암호화

과정을 도입하고, 노드에 IPS(Intrusion Prevention Systems)을 사용하여 DoS 공격을 사전 방지하여 대응한다. 또한 국제 표준기술(IEEE 1609.2, CAMP VSC3)로 인증된 보안규격을 통해 통신을 할 수 있도록 하고, 통신에 참가하는 노드들에 ID를 개별 부여하여 인증과 접근제어 과정을 통해 외부 네트워크인 DSRC의 취약점에 대응한다.

● 자동차 관리 어플리케션에 대한 대응

자동차 관리를 위한 어플리케이션 및 업데이트 파일에 대한 변조에 대응하기 위해서 MD5를 활용한 해시(Hash) 값 비교를 통해 검사한다. 또한 코드사이닝(CodeSigning)을 통해 관리 어플리케이션의 정확한 출처와 변조 여부를 검증하여 무결성을 유지하며 코드 난독화를 통해 변조의 가능성에 대응이 가능하다.

따라서 커넥티드 카에 대한 보안은 (그림 7)과 같이 자동차 내부와 외부의 방법이 함께 고려되어야 하며 효율적이고 표준 기반의 보안 솔루션이 요구된다.



(그림 7) 커넥티드 카 보안 취약점 대응 방안

5. 결론

본 논문에서는 커넥티드 카 네트워크 구성을 파악하고 이에 따른 보안 위협과 대응기술에 대해 서술하였다.

ICT 기술의 발전과 통신의 기술의 발전으로 커넥티드 카는 운전자의 편의성과 안정성을 증가시키고 있다. 하지만 이로 인해 자동차와 외부로 연결되어 있는 통신을 통해 지능적이고 복합적인 공격의 가능성이 발생하였다.

취약점을 이용한 커넥티드 카에 대한 공격의 피해는 기존의 IoT 사물과 다르게 개인정보 탈취와 금전적인 손해뿐만 아니라 더 나아가 운전자의 안전과 생명을 위협한다.

본 연구를 통해 커넥티드 카에 발생할 수 있는 물리적 접근, 외부 네트워크, 자동차 관리시스템의 취약점에 대하여 하드웨어적 보안 장치 및 암호화, 인증, 접근제어, 해시 값을 통한 무결성, 코드 난독화를 통해 여러 보안 대응 방안을 도출 하였다. 따라서, 논의한 커넥티드 카의 보안 취약점과 대응방안을 통해 커넥티드 카의 보안 및 발전에 기여하여 향후 다양한 환경에서 적용되길 기대한다.

Acknowledgement

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No 2016R1A2B4011069).

참고문헌

[1] 김상국, “커넥티드 카(Connected Car)-IoT/M2M 기술 환경 하에서 커넥티드 카 급격한 시장 기대”, KISTI MARKET REPORT, 2014.

[2] Gartner, "Gartner Says Connected Car Production to Grow Rapidly Over Next Five Years", September 2016

[3] K. Koscher 외 10명, “Experimental Security Analysis of a Modern Automobile", IEEE Symposium on Security and Privacy, pp.447-462, 2010.

[4] P. Kleberger 외 2명, "Security aspects of the in-vehicle network in the connected car," 2011 IEEE Intelligent Vehicles Symposium (IV), pp.528-533, 2011.

[5] 황원식 외 1명, “사물인터넷 시대 안전망, 융합보안산업”, 산업연구원(KEIT), vol.586, 2014.

[6] 박석지, "커넥티드 카 서비스 동향. 전자파기술“, vol.26, no6, pp.24-30, 2015.

[7] 전해영. "사물인터넷 (IoT) 관련 유망산업 동향 및 시사점.", 현대경제연구원 VIP Report, pp.1-16, 2016.

[8] 심현보, "커넥티드 카의 기술", 한국정보통신학회논문지, vol.20, no.3, pp.590-598, 2016.

[9] 강서진, "커넥티드 카(Connected Car) 개발 동향과 미래 변화", KB금융지주 경영연구소, vol.15, 2016.

[10] 이동훈, “자동차-ICT 융합 및 보안 기술 동향”, TTA 저널, vol.153, pp.29-34, 2014.

[11] Johansson K.H 외 2명, “Vehicle Applications of Controller Area Network”, Handbook of networked and embedded control systems, pp.741-765, 2005.

[12] PALANCA, Andrea 외 3명, “A stealth, selective, link-layer denial-of-service attack against automotive networks”, International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. Springer, pp.185-206, 2017.

[13] Robert Bosch GmbH, "CAN Specification Version 2.0", 1991.

[14] 조아람 외 4명, “CAN 버스 공격에 안전한 메시지 인증 및 키 분배 메커니즘", 정보보호학회논문지, vol.22, no.5, pp.1057-1068, 2012.

[15] W. Yan, "A two-year survey on security challenges in automotive threat landscape," 2015 International Conference on Connected Vehicles and Expo (ICCVE), Shenzhen, pp. 185-189, 2015.

[16] 문영준, “단거리무선전용통신(Dedicated Short Range Communication)의 용어개념”, 교통기술과정책, vol.3, pp. 242-244, 2006.

[17] 이정호 외 3명, “커넥티드 카 환경에서 안드로이드 앱 리패키징을 이용한 자동차 강제 제어 공격”, 정보보호학회논문지, vol.26, no.3, pp.679-691, 2016.

[18] kaspersky & IBA, "Case study: Kaspersky Lab's analysis of the BMW ConnectedDrive system", 2014.