정 보 보 호 학 회 지
제 30 권 제6호, 2020. 12

국제 학술대회를 중심으로 자동차 보안 기술 동향

최 원 석*

요 약

운전자의 편의성 및 안전성 향상을 위하여, 과거 기계적으로 제어되던 차량의 많은 기능들이 최근에는 전자제어장치에 의하여 전자적으로 제어되고 있다. 고급 차량의 경우에는 약 100개의 전자제어장치가 탑재되어 있다고 알려져 있으며, 이러한 전자제어장치는 CAN 통신 프로토콜을 이용하여 자동차 내부에서 네트워크를 형성하여 센서 정보나 제어 요청 등이 송·수신된다. 하지만, 자동차의 많은 기능이 전자적으로 제어됨에 따라, 이를 타겟으로 하는 차량 사이버공격에 대한 위협도 함께 증가하고 있다. 실제로 2015년에 사전 조작 없는 차량을 대상으로 원격에서 제어하는 사이버공격이 시연되기도 하였다. 따라서, 유엔유럽경제위원회 (UNECE)에서는 자동차 사이버 보안 요구사항에 관한 내용을 법규로 지정하였고, 2022년 7월 유럽에서 생산되는 모든 차량에 자동차 사이버 보안을 위한 기술적 조치가 의무화되어야 한다. 이로 인해, 자동차 사이버보안은 산업계와 학계 모두 실제 차량에 적용 가능한 자동차 보안기술 개발에 집중하고 있다. 본 고에서는 국제 학술대회를 중심으로 차량에 대한 사이버보안 취약점 및 보안기술 연구 동향을 산업계와 학계를 구분지어 설명하도록 하겠다.

Ⅰ. 서 론

IEEE S&P 2010 학회에서 Koscher et al. 연구팀은 최초로 차량에 대한 사이버공격 가능성에 대하여 발표하였으며, C. Miller와 C. Valasek은 DEFCON 2013에서 Ford사의 Escape 차량과 Toyota사의 Prius 차량을 대상으로 차량 해킹을 시연하였다. 2010년 Koscher et al. 연구팀의 연구결과에서는 실험 차량의 종류나 제어 메시지에 대한 자세한 내용을 밝히지 않고 블라인드 처리한 것과 달리, 2013년 C. Miller와 C. Valasek은 차량 제어 메시지뿐만 아니라, 차량 해킹 방법론과 시행착오까지 상세히 밝히고 있는 것이 두 연구 사이의 큰 특징이다 [2]. 결과적으로, C. Millier와 C. Valasek의 연구결과를 통해 많은 사람들이 차량 해킹에 대한 원리를 이해할 수 있게 하였고, 자동차 보안에 대한 연구를 가속화하는 계기가 되었다. 게다가, C. Millier와 C. Valasek는 2015년도에 Black Hat US에서 모바일 네트워크를 경유하여 어떠한 사전 조작도 없는 차량의 내부 네트워크로 악성 패킷을 주입하는 것에 성공하여 원격으로 자동차 임의제어가 가능함을 보여주었다 [3].

자동차와 관련된 사이버 보안 강화 요구가 과거에는 잠재적 수요에 그쳤다면, 최근에는 현실적인 요구사항 및 의무사항으로 변화하고 있다. 특히, 유엔유럽경제위원회 (United Nations Economic Commission for Europe, UNECE)의 WP.29의 자동차 사이버 보안 요구사항에 따라 2022년 7월 유럽에서 생산되는 모든 차량에 자동차 사이버 보안을 위한 기술적 조치가 의무화되었다. 이처럼 자동차 사이버 보안 기술의 시급성으로 인해, 자동차 사이버보안 분야는 학계에서도 산업계와 마찬가지로 바로 차량에 적용이 가능한 현실적인 보안기술 연구에 집중하고 있다.

본 논문은 자동차 사이버 공격에 대한 기본원리를 이해하기 위한 배경지식을 설명하고, 자동차 보안관련 국제 학회를 중심으로 자동차 사이버 공격 동향 및 사이버 보안 기술 동향을 설명하도록 하겠다.

Ⅱ. 자동차 내부네트워크 배경지식

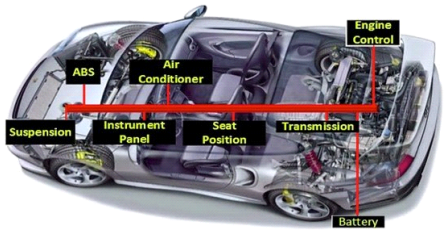
이번 장에서는 자동차 사이버보안 취약점 연구와 사이버보안 기술에 대한 이해를 돕기 위한 자동차 내부네트워크의 동작원리와 관련된 기본 배경지식에 대하여 설명하도록 하겠다.

본 연구는 2020년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2020R1C1C1007446)
* 한성대학교 IT융합공학부 (교수, wonsuk@hansung.ac.kr)

2.1. 전자제어장치 (ECU)

운전자와 탑승자의 편의성 (Convenience)와 안전성 (Safety)을 위하여, 과거에는 기계적으로 제어되던 다수의 차량 기능들이 전자적으로 제어되고 있다. 자동차의 전자적 제어를 위하여 전자제어장치 (Electronic Control Unit, ECU)라 불리는 여러 개의 임베디드 컴퓨터 (Embedded Computer)가 차량에 탑재되고 있다. 최초의 ECU는 Engine Control Unit으로 불렸으며 엔진을 전자적으로 제어하여 차량의 배출가스를 조절하기 위해 개발되었는데, 최근에는 엔진뿐만 아니라 많은 부분들이 ECU을 이용하여 전자적으로 제어하고 있다. 현재 판매되고 있는 고급차량의 경우 약 100개의 ECU들이 차량에 탑재되어 동작하는 것으로 알려져 있다. 이처럼 여러 개의 ECU들은 자신의 상태정보를 다른 ECU들과 공유하기 위해, CAN (Controller Area Network)이라 불리는 통신 프로토콜을 이용하여 네트워크를 구성하고 있다. [그림 1]는 각 기능을 담당하고 있는 ECU들이 CAN 프로토콜을 이용하여 네트워크를 구성하고 있는 개념을 보여주고 있다.

CAN 프로토콜은 1986년 Bosch 社에 의하여 개발되었다 [5]. CAN 프로토콜은 네트워크를 버스 (Bus Topology) 형태로 구성하여 필요한 케이블의 양을 최소화하여 차량의 전체 중량을 줄일 수 있는 장점을 갖고 있고, 통신 시 에러가 적은 높은 신뢰성 (Reliability)로 인하여 현재까지 모든 차량의 자동차 내부 네트워크를 위한 통신 프로토콜로 사용되고 있다.



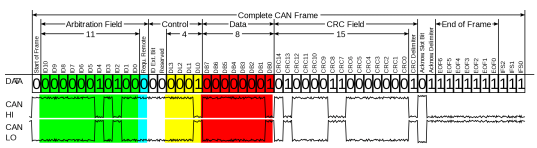
〔그림 1〕 자동차 내부 네트워크 개념도 〔4〕

2.2. CAN 프로토콜

CAN 프로토콜은 1986년 개발되었지만, 차량 내부 네트워크를 구성하기에 적합한 장점으로 인해 현재까지 널리 사용되고 있다. 하지만 개발당시에는 사이버보안 위협에 대한 개념조차 제대로 정립되지 않은 시기였기 때문에, 현재 CAN 프로토콜은 여러 사이버보안 위협에 그대로 노출된 채 자동차에 적용되고 있다. 최근 발표되고 있는 자동차 사이버보안 위협 대부분은 이러한 CAN 프로토콜의 보안 취약점을 이용하고 있다. 이번 절에서는 자동차 사이버보안 위협과 연관되어 있는 CAN 프로토콜의 동작 원리에 대하여 알아보도록 하겠다.

2.2.1. Bit Coding

CAN 프로토콜은 전기적 신호를 이용하여 0 또는 1 비트를 표현하기 위해, NRZ (Non-Return-to-Zero) 인코딩 방법을 사용한다. CAN 프로토콜은 CAN-H와 CAN-L라 불리는 2개의 선을 이용하여 통신을 수행하는데, 2개의 선의 전압차이 없는 경우에는 비트 1을 표현하고, 2개의 선의 약 2.5V 전압차가 있는 경우에는 비트 0을 표현한다. CAN 프로토콜에서는 비트 1을 Recessive 비트라 하며, 비트 0을 Dominant 비트라고도 한다. [그림 2]은 CAN 데이터 프레임에서 각 비트를 표현하기 위해서 CAN-H와 CAN-L 파일의 전압 변화를 보여주고 있다.



〔그림 2〕 CAN 데이터 프레임 및 비트 Signaling 〔12〕

2.2.2. 데이터 프레임

CAN 프로토콜은 4가지 CAN 프레임 i) Data Frame, ii) Remote Frame, iii) Error Frame, iv) Overload Frame을 정의하고 있다. 이중 Overload 프레임은 현재 사용되지 않고 있으며, ECU는 데이터 프레임을 사용하여 메시지를 전송하고 있다. [표 1]는 데이터 프레임에 정의되어 있는 필드와 그에 대한 설명을 보여주고 있다. 데이터 프레임에서 눈여겨 볼 필드로는 ID (Identifier), DLC, Data filed가 있다. ID 필드는 해당 데이터 프레임의 전송 우선순위를 의미하며, 하나의 ECU에게 고유하게 할당되기 때문에, 같은 ID를 갖는 메시지가 동시에 CAN Bus에 전송되는 일이 없으며,

〔표 1〕 CAN 메시지 데이터 프레임 포맷

필드	길이 (bits)	설명
Start-of-frame (SOF)	1	프레임이 제일 처음을 의미함
Identifier	11	메시지의 우선순위를 나타내면 하나의 ECU에 유일하게 할당되어 있음
Remote transmission request (RTR)	1	Remote Frame 여부를 나타내며, Data Frame의 경우 0임
Identifier extension bit (IDE)	1	확장 ID 사용 여부를 나타냄 (기본 값은 0임)
Reserved bit (r0)	1	예약 비트 (기본값은 0)
Data length code (DLC)	4	데이터 필드의 길이를 바이트로 나타냄
Data field	0-64	전송될 데이터 페이로드
CRC	15	Cyclic redundancy check
CRC delimiter	1	CRC이후 1비트를 나타냄 (기본값은 1)
ACK slot	1	메시지 전송 성공을 의미함
ACK delimiter	1	ACK 비트 이후에 1비트를 나타냄 (기본값은 1)
End-of-frame (EOF)	7	잘못된 계산식데이터 프레임의 마지막을 의미함

만약 그런 경우가 발생하면 에러로 간주하여 에러 핸들링 절차를 진행한다. 데이터 프레임의 데이터 필드는 0~8바이트로 가변 길이를 갖고 이를 DLC 필드에 표시한다. 데이터 필드에는 ECU가 실제로 자신의 상태정보나 차량의 제어를 요청하는 정보를 포함하고 있다.

Ⅲ. 자동차 사이버보안 취약점 연구 동향

자동차 사이버보안 취약점은 학계를 중심으로 연구되어 발표되고 있으며 산업계의 경우 자동차 제조회사에서 내부적인 연구 및 테스트를 진행하고 점검하는 것으로 알려져 있지만 외부로 공개는 하지 않는 것이 일반적이다. 이번 장에서는 국제 유명 학술대회를 중심으로 자동차 사이버보안 취약점 분석 내용에 대한 발표내용을 소개 하겠다. [표 2]는 국제학술대회를 중심으로 발표된 자동차 사이버보안 취약점 연구 목록을 보여주고 있다.

〔표 2〕 국제 학술대회에서 발표된 자동차 사이버보안 취약점 연구

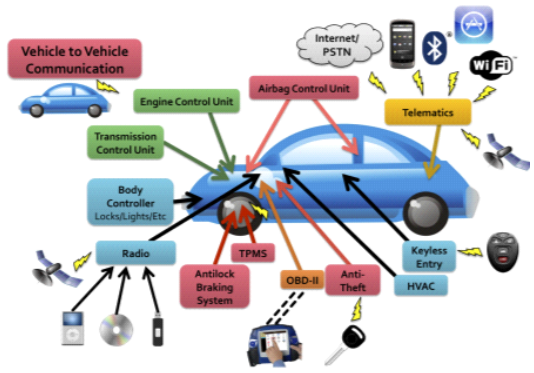
제목	발표 학술대회
Experimental security analysis of a modern automobile [1]	2010 IEEE Symposium on Security and Privacy
Comprehensive experimental analyses of automotive attack surfaces [13]	2011 USENIX Security Symposium
Adventures in automotive networks and control units	2013 DEF CON 21
Remote exploitation of an unaltered passenger vehicle	Black Hat USA 2015
Error handling of in-vehicle networks makes them vulnerable	2016 ACM Computer and Communications Security

3.1. Koscher et al. 의 연구[1]

2010년 IEEE S&P 학술대회에 미국의 워싱턴 대학의 Koscher et al. 연구팀은 세계 최초 자동차 사이버보안 위협에 대한 연구 결과를 발표하였다. 자동차 진단을 위한 OBD2 표준 인터페이스로 인해 자동차 내부 네트워크의 접근이 용이해 졌으며, 이를 통해 자동차 내부 네트워크의 CAN 통신 Trace를 분석할 수 있었다. 분석을 통해 차량을 제어할 수 있는 메시지들을 발견하여 이를 다시 자동차 내부 네트워크에 주입함으로써 자동차를 제어하는데 성공하였다. ECU가 본격적으로 차량에 탑재되기 시작한 초기인 점을 감안하면, Koscher et al.의 연구 결과는 매우 시기 적절하였고, 현재 자동차 사이버보안 기술 연구의 초석이 되었다고 말할 수 있다.

3.2. Checkoway et al. 의 연구[13]

Koscher et al. 연구팀과 같은 연구팀인 Checkoway et al. 연구팀은 이전 연구결과를 통해 자동차 내부 네트워크에 CAN 메시지를 주입함으로써 차량의 기능을 원격에서 제어할 수 있음을 밝혔다. 따라서, 후속 연구로



〔그림 3〕 자동차 내부 네트워크에 접근 가능한 Attack Surface〔13〕

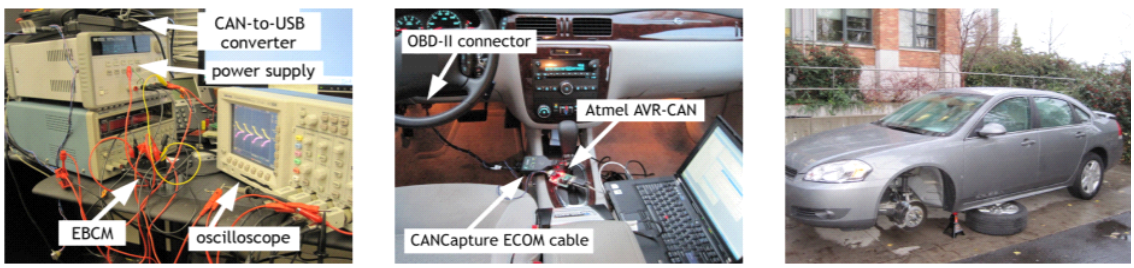
써 외부에서 공격자가 자동차 내부 네트워크에 접근 가능한 Attack Surface에 대한 연구를 진행하였다. 예를 들어, 정비소에서 사용하는 차량용 정비기기가 자동차 해킹에 사용되어 ECU를 감염시켜, 정비 이후에 해당 ECU를 공격자가 원격에서 완전히 장악할 수 있는 공격 시나리오를 제시하였다. [그림 3]는 Checkoway et al. 연구팀에서 제시한 자동차 내부 네트워크에 접근 가능한 Attack Surface를 보여주고 있다.

3.3. Miller and Valasek의 연구[2]

Miller and Valasek은 앞서 설명한 Koscher et al. 의 연구를 재연하여 2013년 Def Con21에 발표하였다. 이전 연구의 경우 실험한 차량의 정보나 주입한 CAN 메시지에 대하여 모두 블라인드 처리하여 연구결과를 발표한 것과 비교하여 Miller and Valasek의 연구결과 같은 경우에는 실험한 차량의 정보와 주입한 CAN 메시지를 모두 공개하였다. 심지어, 연구과정에 있어 경험한 시행착오 까지 모두 상세히 기술하였다. 이를 통해, 많은 사람들이 자동차 사이버보안 취약점 연구 수행 방법에 대하여 이해할 수 있게 되어 관련된 활발한 연구가 진행될 수 있는 촉진제 역할을 하였다. 특히, Miller and Valasek의 연구는 UDS (Unified Diagnostic Services) 진단 표준 프로토콜을 활용하여, 표준이 적용된 모든 차량에 적용할 수 있는 취약점 분석 연구결과를 발표하였다.

3.4. Miller and Valasek의 연구[3]

Miller and Valasek의 2013년 연구결과는 자동차 내부 네트워크에 접근을 한 상태에서 CAN 메시지를 주입함으로써 차량을 제어할 수 있음을 의미하였다. 따라서, 도로위의 차량이 해당 연구결과에 적용된다고 보기에는 어려움이 있었다. 그러나 2015년 Millier and Valasek은 Black Hat USA 학술대회에서 사전 조작이 되지 않은 차량을 대상으로 원격에서 자동차 내부 네트워크에 접근하여 차량을 제어할 수 있음을 발표하였다. 이는 차량에 탑재되어 있는 텔레매틱스 디바이스의 취약점을 이용한 연구결과이다. 해당 차량의 텔레매틱스 디바이스의 IP 주소를 이용하여 포트 스캐닝을 수행하였고 취약점이 존재하는 프로세스에 접속하였다. 텔레매틱스 디바이스는 일반적으로 자동차 내부 네트워크에 연결되어 있기 때문에, 해당 텔레매틱스 디바이스를 완전히 장악한 이후에는 2013년도 연구결과와 유사하게 차량을 제어할 수 있는 CAN 메시지를 주입하여 차량 제어에 성공하였다. 사전 조작되지 않은 차량을 원격에서 임의의 제어할 수 있다는 점에서 기존 자동차 사이버보안 취약점 연구결과와 달리 해당 연구결과가 발표된 이후에 많은 차량 제조회사에 해당 문제를 적극적으로 해결하기 위해 대응하였다.



〔그림 4〕 Checkoway et al. 연구팀의 자동차 사이버보안 위협 연구 환경〔1〕

3.5. Cho and Shin의 연구 [14]

앞서 설명한 자동차 사이버보안 취약점 연구와 달리, Cho and Shin은 CAN 프로토콜의 에러 핸들링 방법을 악용하여 ECU를 CAN 통신에서 bus-off 되도록 하는 공격 방법을 2016년 ACM CCS 학술대회에 발표하였다. CAN 프로토콜을 이용하는 ECU들은 서로 같은 아이디를 공유하여 메시지를 보내지 않는 다는 가정 하에 서로 통신한다. 하나의 아이디는 오직 하나의 ECU에만 할당되어 사용된다. 따라서, 같은 아이디를 사용하는 메시지가 CAN Bus에서 동시에 발견되면 이는 에러상황을 간주하게 되고, 이러한 현상이 일정 횟수 이상 발생하게 되면 해당 ECU는 일정시간 통신에서 제외되도록 CAN 프로토콜이 디자인 되어 있다. ECU들은 Error Counter를 관리하여 자신이 전송 시 에러가 발생하면 Error Counter를 증가하고 해당 Error Counter가 256이 넘어가게 되면 일정 시간동안 통신을 중단한다. Cho and Shin의 연구결과는 의도적으로 타겟 ECU에 할당된 아이디와 같은 아이디오 메시지를 전송하여 타겟 ECU의 메시지 전송을 의도적으로 멈추게 만드는 공격 방법이다.

Ⅳ. 자동차 사이버보안 기술 연구 동향

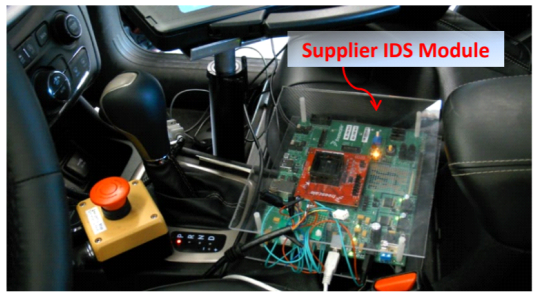
자동차 사이버보안 취약점과 그로 인한 위협에 대응하기 위하여, 산업계와 학계 모두 자동차 사이버보안 기술에 대한 연구에 집중하고 있다. 특히, UNECE의 자동차 사이버보안 요구사항으로 인해 자동차 사이버보안 기술 개발과 탑재는 매우 중요하고 시급한 일이 되었다. 따라서, 자동차 사이버보안기술 분야의 한 가지 특징으로 산업계와 학계 모두 현재 자동차에 바로 적용하기 위한 연구 내용과 목표를 설정하고 있다. 이번 장에서는 산업계와 학계를 구분지어 자동차 사이버보안 기술에 대하여 발표되고 있는 내용을 설명하겠다.

4.1. 산업계 중심의 연구 동향

4.1.1. University of Michigan Transportation Research Institute (UMTRI)

Michigan 대학의 산하 기관인 UMTRI는 교통 안전 (Trasporation Safety)과 관련된 다양한 분야에 있어서 연구 (Research), 개발 (Development), 교육 (Education)을 진행하고 있다. UMTRI는 미국의 자동차 제조 연합의 지원을 받아 운영되고 있으며 미국의 SAE (Society of Automotive Engineers)로부터 교통안전 프로젝트를 수행하고 있다. 특히, 2019년 Michigan 공대가 해당 기관에 합류하여, 차량용 IT 기술까지 연구 분야를 넓혀가고 있다.

2019년도에는 NHTSA (The National Highway Traffic Safety Administration)의 요청을 받아, 상용 차량용 침입탐지 시스템 (Automotive Intrusion Detection System) 3종에 대하여, 평가를 진행하였다 [6]. UNECE의 자동차 사이버보안 요구사항에 맞추어 자동차 제조회사들은 자신들의 차량에 Automotive Intrusion Detection System (Automotive IDS)를 탑재할 예정이기 때문에, IDS 기술을 평가하기 위한 방법론이 필요하였고, UMTRI에서 최초로 공식적인 방법론을 제시하였다. 해당 보고서의 내용을 살펴보면, Automotive IDS 평가를 위한 정성적 평가지표와 정량적 평가지표를 확인할 수 있다. 또한, [그림 5]과 같이 실제 차량에서 Automotive IDS를 평가하기 위한 기본 환경을 확인할 수 있다.



〔그림 5〕 UMTRI의 Automotive IDS 평가환경 〔6〕

4.1.2. ESCAR 학술대회

자동차 사이버보안만을 주제로 하는 국제 학술대회로 ESCAR (Embedded Security in Cars)가 있다. 자동차 사이버보안이 본격적으로 관심을 받기 시작한 것이 10년이 채 되지 않은 것과 비교하여, ESCAR 학술대회는 18년이라는 상대적으로 긴 역사를 갖고 있다. ESCAR는 매년 미국, 유럽, 아시아 지역에 각각 개최되

며, 이 중 ESCAR Europe이 가장 큰 규모를 갖고 있다. 일반적으로 ESCAR Europe은 독일 그리고 ESCAR ASIA는 일본에서 개최되고 있다.

가장 최근에 Vitual로 개최된 ESCAR 2020 Europe [7]에서 다루어진 주제를 살펴보면, Secure ECUs, Attacks and Response, Cryptography, Privacy, Secure communication, Secure Processes가 있다. ESCAR 학술대회 같은 경우에는 산업계에서 주도하는 학술대회로써 과거에는 자동차 도메인에 국한된 내용만을 다루었지만, 최근에는 많은 소프트웨어 기술이 차량에 적용됨에 따라, 사이버보안 일반적인 내용까지 학술대회 주제로 다루고 있는 것을 확인할 수 있다.

4.2. 학계 중심의 연구 동향

자동차 사이버보안을 주제로 학계에서 주도하는 국제 학술대회는 존재하지 않지만, 보안 분야 저명 학술대회에서 자동차 사이버보안을 주제로 하는 연구결과가 계속해서 발표되고 있다. 특히, 보안 분야에서 이야기하는 4대 국제 학술대회인 IEEE S&P, ACM CCS, Usenix Security, NDSS에서 자동차 보안에 대한 연구결과는 매년 발표되고 있다. 학계에서 다루어지는 자동차 보안에 대한 연구결과는 크게 Automotive IDS와 CAN Bus Reversing으로 구분될 수 있고, 이에 대하여 아래와 같이 설명하겠다.

4.2.1. Automotive IDS

UNECE의 자동차 사이버보안 요구사항을 만족하기 위하여, 가장 활발히 연구되고 있는 내용은 자동차 내부 네트워크 침입을 탐지하는 Automotive IDS에 관한 연구이다. 보안 취약점이 존재하는 CAN 프로토콜을 자동차 내부 네트워크 통신 프로토콜로 계속해서 유지할 수 있는 Automotive IDS 기술이 주목 받고 있다. Automotive IDS는 학술대회 뿐만 아니라 여러 유명 학회에서 연구결과가 발표되고 있다. 여기서는 유명 학술대회인 Usenix Security와 ACM CCS에서 발표된 2개의 연구결과에 대하여 설명하도록 하겠다.

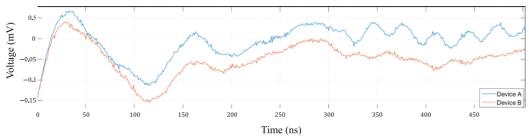
4.2.1.1. Cho and Shin의 연구[8]

2016년 Usenix Security 학술대회에서 Cho and Shin은 Automotive IDS 기술을 제안 발표 하였다. 공격자들도 쉽게 모방할 수 있는 특징을 이용하여 자동차 내부 네트워크의 침입을 탐지하는 기존 연구 결과와 달리는 Cho and Shin이 제안한 Automotive IDS 기술은 ECU의 하드웨어적 특징을 이용한다. 프로세서는 주기적으로 발생하는 Clock에 맞춰 동작하기 때문에 Clock Generator에 의하여 시간 측정을 할 때 미세한 차이가 존재한다. 디바이스 마다 존재하는 Clock Offset은 ECU가 자동차 내부 네트워크에서 주기적으로 메시지를 보낼 때에도 존재한다. Cho and Shin은 이러한 사실을 이용하여 CIDS라 불리는 Automotive IDS를 발표하였다. 자동차 내부 네트워크에서 전송되는 대부분의 메시지들은 ECU들이 주기적으로 전송하며, 이를 위해 일정 시간을 카운트 할 때 미세한 차이가 발생한다. 만약, 공격자가 자동차 내부 네트워크에 침입하여 악의적인 메시지를 주기적으로 전송하면, 이러한 미세한 차이를 흉내 낼 수 없기 때문에, CIDS는 침입을 탐지할 수 있게 된다.

하지만, 자동차 내부 네트워크에서 ECU는 메시지를 주기적으로 전송하는 것만 아니라, 특정 이벤트가 발생할 때 전송하는 On-event 방식으로 메시지를 전송한다. CIDS는 주기적으로 전송되는 메시지를 대상으로 침입하는 공격은 탐지할 수 있지만, On-event 방식으로 전송되는 메시지를 이용하는 공격은 탐지할 수 없다는 단점을 갖고 있다.

4.2.1.2. Kneib et al. 의 연구 [9]

2018년 ACM CCS 학술대회에서 Kneib et al. 연구팀은 ECU가 CAN 통신 프로토콜을 이용하여 메시지를 전송할 때, PHY 레벨에서 전기적 신호를 Signaling 할 때 고유한 특징을 분석하는 Scission라 불리는 Automotive IDS를 발표하였다. 앞서 설명한 Cho and Shin이 발표한 CIDS 기술과 유사하게, 공격자가 쉽게 모방할 수 없는 PHY 레벨에서 특징을 분석하였다. 화자인식 분야에서 서로 다른 사람이 동일한 문장을 이야기 한다고 하더라도, 각 사람의 고유한 음색을 분석하여 사람을 식별하는 것과 마찬가지로, Scission는 ECU가



〔그림 6〕 동일한 메시지에 대하여, 두 ECU의 전기 신호 차이 〔10〕

메시지를 전송하기 위하여 PHY레벨에서 전기적 신호를 이용하여 Signaling 하는 미세한 차이를 분석하였다. 이러한 개념은 2017년 Choi et al. 연구팀에 의하여 최초로 제안되었으며, [그림 6]는 Choi et al.의 연구에서 확인할 수 있는 내용으로써, 서로 다른 두 개의 ECU가 동일한 메시지를 보낼 때 PHY 레벨에서의 전기적 신호는 미세한 차이를 보이고 있다.

공격자가 자동차 내부 네트워크에 침입하여 악의적인 메시지를 주입할 때에는 다른 ECU를 이용하게 될 것이고, 공격자가 이용하는 ECU의 PHY레벨에서 전기적 신호는 원래 ECU와 다른 특징을 보일 것이다. 그렇기 때문에, Scission는 자동차 내부 네트워크의 침입을 탐지할 수 있다. 하지만, PHY레벨에서의 전기적 신호를 측정하기 위해서는 별도의 장치가 필요하게 된다. Automotive IDS는 일반적으로 자동차 내부의 Gateway ECU에 SW 형태로 구현되기 때문에, 전기적 신호를 측정하는 것은 불가능 하다.

4.2.2. CAN Bus Reversing

산업계에서 수행되는 자동차 사이버보안 연구와 다르게, 학계에서는 CAN Bus를 적절하게 Reversing하는 연구가 진행되고 있다. 일반적으로 CAN DBC format 파일이라 불리는 정보는 자동차 내부 네트워크에서 CAN 통신 프로토콜을 이용하여 ECU가 송수신하는 메시지에 대하여 명세하고 있다. DBC 파일을 통해 자동차를 강제로 제어할 수 있는 메시지 구조를 쉽게 파악할 수 있기 때문에, 자동차 제조회사에서는 이러한 정보를 철저하게 비밀로 관리하고 있다. 하지만 Automotive IDS와 같이 자동차 사이버보안 연구를 위해서는 DBC 파일의 일부 정보가 요구되는 경우가 있다. 자동차 제조회사와 같은 산업계에서는 이러한 정보를 이미 보유하고 있겠지만, 학계에서는 그렇지 않기 때문에 CAN Bus Reversing과 관련된 연구를 진행하고 있다. 여기서는 CAN Bus Reversing 연구들 중에서 2019년 ACM CCS 학술대회에 발표된 Pese et al.의 연구팀의 연구결과를 설명하겠다.

LibreCAN이라 불리는 Pese et al. 연구팀의 연구결과는 DBC 파일이 주어지지 않은 상태에서 DBC 파일의 일부 정보를 CAN 통신 Trace 파일만을 분석하여 유추할 수 있음을 발표하였다 [11].

[그림 7]와 같이 자동차 내부 네트워크에서 ECU가 주기적으로 전송하는 메시지를 수집하여 이를 분석하면, 해당 ECU가 어떤 기능을 담당하는지 확인할 수 있다. Pese et al. 연구팀의 핵심 아이디어는 OBD2-PID 표준을 함께 결합하여 Trace파일을 분석하는 것이다. OBD2-PID는 국제 표준으로써 엔진과 같이 차량의 기능을 진단하기 위한 프로토콜이다. 이를 이용하여 차량 상태에 대한 요청과 응답을 주기적으로 수행하여 시계열 데이터를 확보한다. 이후, CAN Trace파일에서 상관관계가 높은 Payload와 그에 맞는 ID 값을 찾으면 해당 ID가 특정 기능을 담당하는 ECU라 할 수 있다. 하지만, LibreCAN은 DBC 파일이 주어지지 않은 상태에서 제한적으로 수행할 수 있는 접근 방법으로써, 실제 상용 Automotive IDS 에 탑재될 때 사용될 수 있기에는 부정확한 측면이 존재한다.

STAGE 1: Constant Messages
STAGE 2: Reference Messages
STAGE 3: Powertrain Messages

TRACE

TIME	ID	PAYLOAD	FILTERED IN
00.000	700	1111111100000000	STAGE 3
00.001	100	0000000000000000	CANDIDATE
00.002	300	000002000E20BE20	STAGE 1
00.004	900	FFFFFFFFFFFFFFFF	CANDIDATE
00.008	300	000002000E20BE20	STAGE 1
00.009	300	000002000E20BE20	STAGE 1
00.011	600	000000024CB016EA	STAGE 2
00.015	800	00000000075BCD15	CANDIDATE
00.016	500	0000000000000000	STAGE 3
00.018	400	056089000A00A000	STAGE 2
00.020	200	0000000000000000	CANDIDATE

REFERENCE

ID	PAYLOAD
100	0000A00A000BC300
200	0070070070070070
300	00000000075BCD15
400	056089000A00A000
500	0012300AE0030000
600	000000024CB016EA
700	1000000001100001
800	00000000000000FF
900	0F00B9900A0A0F0E

POWERTRAIN

ID	CORRELATION SCORE
100	0.7433
200	0.5192
300	0.7990
400	0.6648
500	0.9882
600	0.7102
700	0.8361
800	0.1034
900	0.2023

〔그림 7〕 CAN Trace 파일 분석을 통한 CAN 메시지 구조 유추 〔11〕

V. 결 론

본 고에서는 국제 학술대회를 중심으로 자동차 보안 연구 동향에 대하여 알아보았다. 특히, 자동차 사이버보안 취약점 연구와 사이버보안 기술을 분류하여 설명을 하였고, 사이버보안 취약점 연구 같은 경우에는 학계의 연구 결과만을 다루었다. 산업계에서는 내부적으로 취약점 연구를 수행하기는 하지만, 해당 내용을 외부에 공개하지 않는 것이 일반적이기 때문에 국제 학술대회에서는 학계의 연구 결과만을 확인할 수 있었다. 자동차 사이버보안 기술의 경우에는 취약점 연구와 달리 산업계와 학계 모두 활발한 연구를 진행하고 있었다. 게다가, 다른 보안 분야에서 볼 수 있는 산업계와 학계의 연구 차별성과 달리, 자동차 사이버보안 분야에서는 보안 기술 개발의 시급성으로 인하여 산업계와 학계의 연구 목표가 매우 유사하고 학계에서도 바로 차량에 탑재 가능한 기술 연구를 수행하고 있다는 사실을 알 수 있었다.

참 고 문 헌

[1] Koscher, Karl, et al. "Experimental security analysis of a modern automobile." 2010 IEEE Symposium on Security and Privacy. IEEE, 2010.

[2] Miller, Charlie, and Chris Valasek. "Adventures in automotive networks and control units." Def Con 21 (2013): 260-264.

[3] Miller, Charlie, and Chris Valasek. "Remote exploitation of an unaltered passenger vehicle." Black Hat USA 2015 (2015): 91.

[4] Introduction to CAN (Controller Area Network), https://www.allaboutcircuits.com/technical-articles/introduction-to-can-controller-area-network/, accessed: 2020-11-29

[5] Specification, C. A. N. "Bosch." Robert Bosch GmbH, Postfach 50 (1991).

[6] Stachowski, Stephen, Ron Gaynier, and David J. LeBlanc. An assessment method for automotive intrusion detection system performance. University of Michigan, Ann Arbor, Transportation Research Institute, 2019.

[7] escar 2020 Europe, https://www.escar.info/escar-europe/program.html, accessed: 2020-11-29

[8] Cho, Kyong-Tak, and Kang G. Shin. "Fingerprinting electronic control units for vehicle intrusion detection." 25th {USENIX} Security Symposium ({USENIX} Security 16). 2016.

[9] Kneib, Marcel, and Christopher Huth. "Scission: Signal characteristic-based sender identification and intrusion detection in automotive networks." Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. 2018.

[10] Choi, Wonsuk, et al. "Identifying ecus using inimitable characteristics of signals in controller area networks." IEEE Transactions on Vehicular Technology 67.6 (2018): 4757-4770.

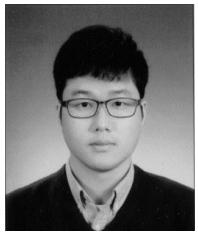
[11] Pesé, Mert D., et al. "LibreCAN: Automated CAN Message Translator." Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. 2019.

[12] CAN BUS, https://en.wikipedia.org/wiki/CAN_bus, Accessed: 2020-11-29

[13] Checkoway, Stephen, et al. "Comprehensive experimental analyses of automotive attack surfaces." USENIX Security Symposium. Vol. 4. 2011.

[14] Cho, Kyong-Tak, and Kang G. Shin. "Error handling of in-vehicle networks makes them vulnerable." Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. 2016.

〈저 자 소 개〉



최 원 석 (Wonsuk Choi)

정회원

2008년 2월 : 서울시립대학교 수학과 졸업

2013년 2월 : 고려대학교 정보보호대학원 정보보호학과 석사

2018년 8월 : 고려대학교 정보보호대학원 정보보호학과 박사

2018년 9월~2020년 2월 : 고려대학교 정보보호연구원 연구교수

2020년 3월~현재 : 한성대학교 IT융합공학부 조교수

<관심분야> 자동차 보안, IoT 보안, 암호학