

Mobility Cybersecurity Overview

2025.08

자동차융합대학



GENERAL MOTORS
GM TECHNICAL CENTER KOREA



국민대학교
KOOKMIN UNIVERSITY

CONTENTS

01

자동차 사이버보안 개요

02

자동차 사이버공격 사례

03

자동차 사이버공격 대응기술

Prologue#1



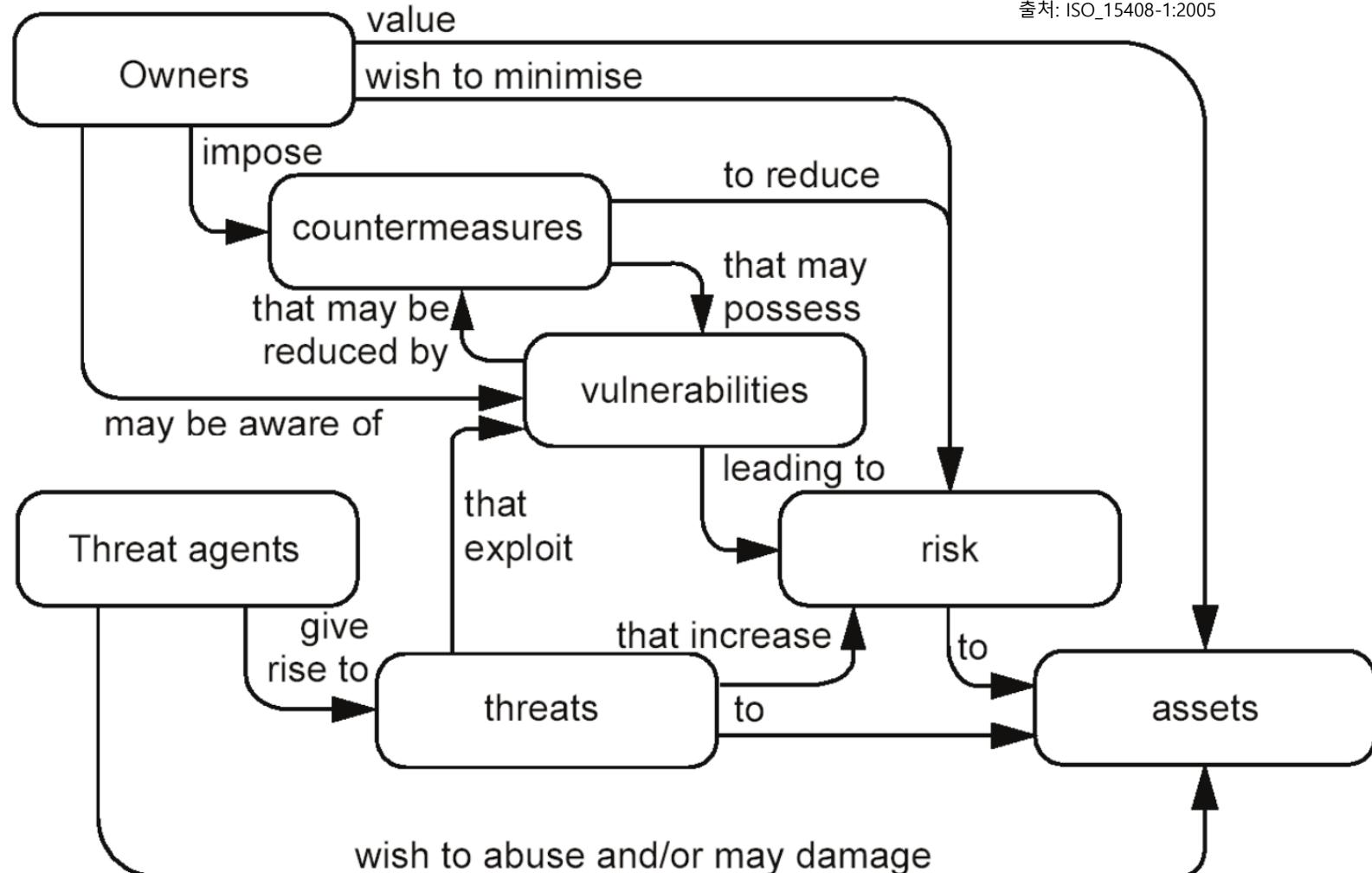
Prologue#2



01

자동차
사이버보안 개요

사이버보안 용어설명 – Security Concepts



[그림] Security Concepts and Relationships

이미지 출처: Adobe Stock

■ Spoofing

- 사전적인 의미로 '속이다' 라는 뜻이다. 즉, Spoofing 공격이란 속이는 것을 이용한 공격 기법들을 의미한다.
- ARP (Address Resolution Protocol, IP → MAC) Spoofing
 - 중간자 공격 (Man-In-the-Middle Attack)
- E-mail Spoofing
 - 보통 Spam Mail이라는 용어로 사용

■ Sniffing (Snooping)

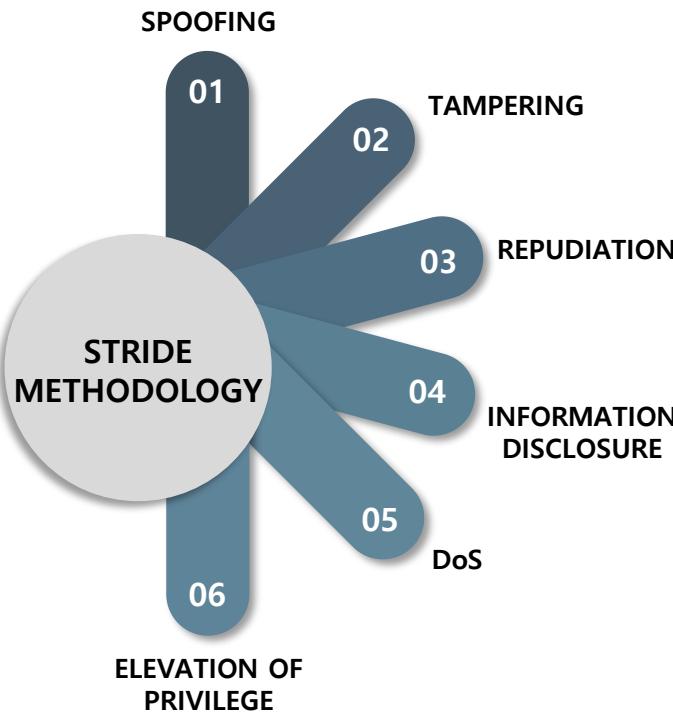
- 네트워크 상에서 자신이 아닌 다른 상대방들의 패킷 교환을 엿듣는 것
- Eavesdropping, Wiretapping, Hijacking 등과 유사한 의미로 사용
 - 단, hacking 목적이 다를 수 있음



이미지 출처: Adobe Stock

사이버보안 용어설명 – Security 주요 요소

	Threat	Security Attribute	Threat Definition
S	Spoofing identity	Authentication	Pretending to be something or someone other than yourself
T	Tampering with data	Integrity*	Modifying something on disk, network, memory, or elsewhere
R	Repudiation	Non-repudiation	Claiming that you didn't do something or were not responsible; can be honest or false
I	Information Disclosure	Credential*	Providing information to someone not authorized to access it
D	Denial of Service (DoS)	Availability*	Exhausting resources needed to provide service
E	Elevation of Privilege	Authorization	Allowing someone to do something they are not authorized to do



*Security 3대 요소

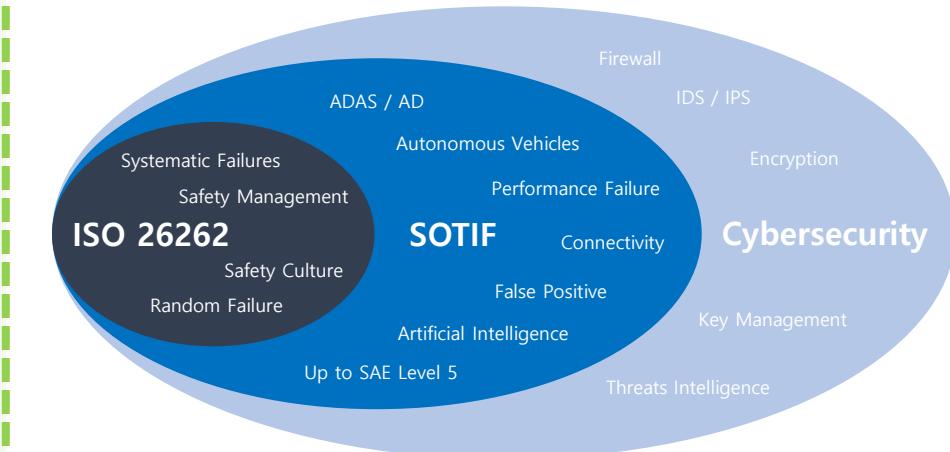
- 자동차는 IT 기술을 적극적으로 사용하여 운전의 편의성과 안전성을 높여 왔음. 예를 들어, 운전자 보조 기술, 인포테인먼트, 차량 간 통신(V2V), 차량-인프라 통신(V2I) 등의 기술이 대중화되면서 운전의 편리성은 증가하지만, 이에 따른 보안 위협 상승
- 자동차 사이버보안(Automotive Cybersecurity)은 자동차 내부 시스템과 통신 네트워크를 보호하여 자동차를 사이버 공격으로부터 안전하게 유지하는 기술
 - 즉, 최신 자동차에 사용되는 많은 전자 기술과 통신 기술을 보호하여 해킹, 바이러스, 악성 코드 등으로 인한 위협으로부터 차량을 보호하고 안전한 운행을 보장하는 기술
 - 자동차에 대한 사이버 공격은 운전자와 승객의 생명과 안전을 직접적으로 위협함. 그리고 이러한 공격은 자동차 내부의 기술적 결함이나, 인프라 시스템의 취약점 등을 통해 이루어질 수 있음



이미지 출처: Adobe Stock

자동차 사이버보안 개념 - Standard 관점

	ISO26262	ISO21448 (SOTIF)	ISO21434 (CSMS)
개요	<ul style="list-style-type: none"> - 기능 안전 (Functional Safety) - 차량에 탑재되는 E/E (Electric/Electronic) 시스템 결함 	<ul style="list-style-type: none"> - 의도된 기능으로부터의 안전 - E/E 시스템 결함이 없는 기능에서 발생할 수 있는 위험 	<ul style="list-style-type: none"> - 외부 위협으로부터의 안전 - 차량 생산 생명주기를 기준으로 사이버보안 분야에 대한 주요 접근 방법론 제시
내용	정의된 기능(요구사항)을 충실히 구현하였는지 여부를 검증	정의된 기능의 도치 않은 결함을 발생시킬 수 있는지 여부를 검증	의도성이 있는 외부 위협으로부터 안전한지 여부를 검증
중점	Safety (안전)		Security (보안)



[그림] ISO26262, SOTIF, Cybersecurity의 내용과 범위

CSMS*: Cyber Security Management System

■ UNECE WP.29에서 의무적으로 적용(22년 7월) 해야 하는 사이버 보안 규정 (UNR.155) 채택

- CSMS* 지원을 위해 차량 라이프 사이클 전반에 걸친 사이버 보안 활동 관리 필요 (TARA: Threat Analysis and Risk Assessment)

■ 시스템 오동작, Sensor Spoofing, 차량 해킹 등 차량 안전 및 보안 관련 위협 증가

- 커넥티드 카, 자율주행 차량 외 상당수의 자율주행체(UAV 등)가 유사한 문제점을 가짐



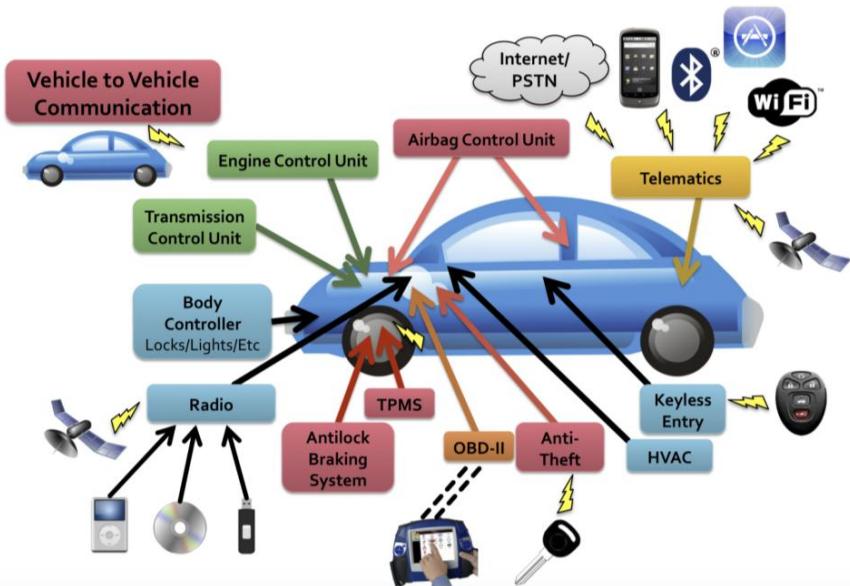
시스템 오동작으로 인한 사고사례
(Tesla Autopilot, Uber, Google Waymo)



드론을 이용한 테러 위협
(출처 : MBC News, TV조선)

■ 보안 결함으로 인한 차량 리콜 증가

- C사 (원격제어, 2015년/2016년)
- H사 (커넥티드서비스, 2017년 / 이모빌라이저, 2022년)
- T사 (원격제어, 2016년/2017년 / 후미등, 2022년/2023년)



[그림] 자동차 내부 네트워크에 접근 가능한 Attack Surface

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

■ C.A.S.E

- 미래자동차는 연결(Connectivity), 자율주행(Autonomous), 공유(Sharing), 전동화(Electrification)라는 4가지 키워드로 정리할 수 있다.



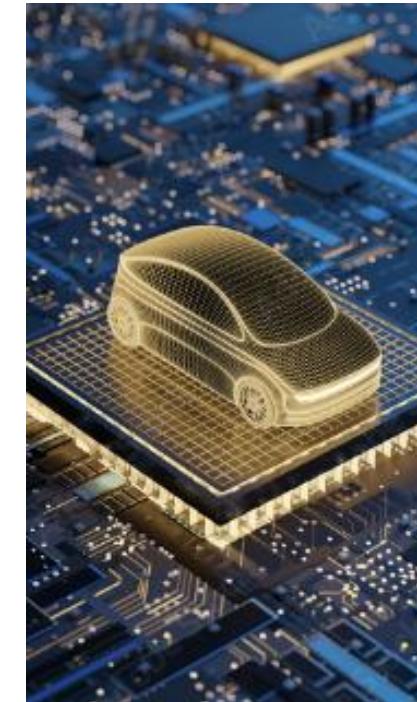
Connectivity



Autonomous



Sharing



Electrification

이미지 출처: Adobe Stock

■ C.A.S.E

- 미래자동차는 연결(Connectivity), 자율주행(Autonomous), 공유(Sharing), 전동화(Electrification)라는 4가지 키워드로 정리할 수 있다.



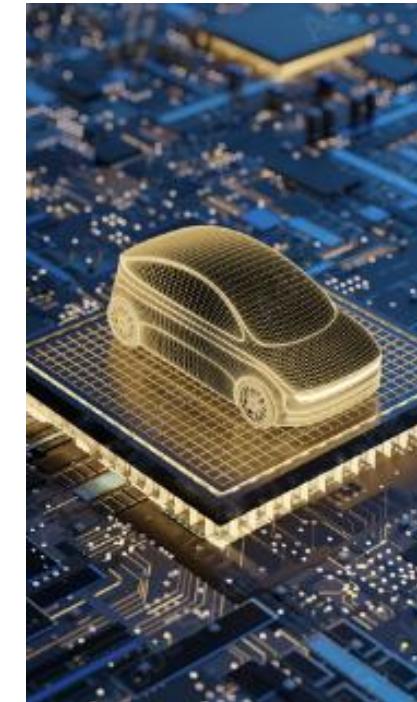
Connectivity



Autonomous



Security

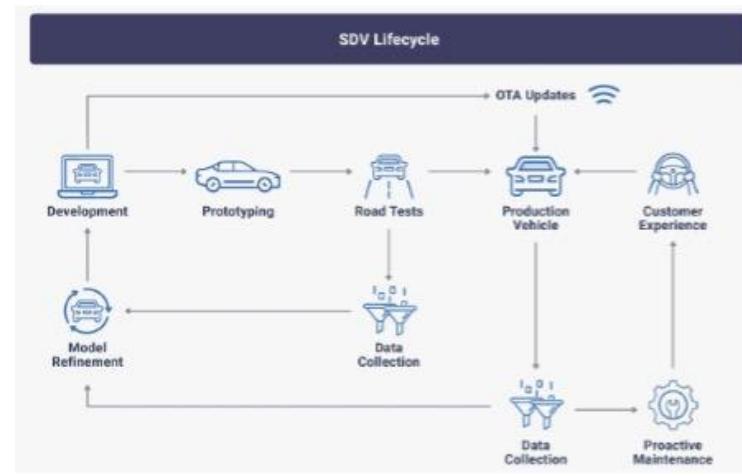


Electrification

이미지 출처: Adobe Stock

SDV 기술의 정의 및 의미

- ❖ SDV란 제품 수명주기 동안 OTA를 통해 성능/기능을 개선 및 추가, 다양한 서비스와 컨텐츠를 제공하여,
 - “고객”에게 지속적으로 **새로운 경험의 가치**를 줄 수 있는 차량,
 - “OEM”에게 개발 자원 절약 및 데이터 활용으로 제품 수명주기동안 **지속적인 수익을 창출** 하는 차량
 - “부품사”에게 HW규모의 경제와 **SW의 부가가치를 창출**하는 차량,
 - “IT/SP*”에게 APP 또는 플랫폼 **생태계를 확장할** 수 있는 차량
- ❖ 자동차의 수명 주기가 연장되고 SOP** 이후에도 성능 향상 가능



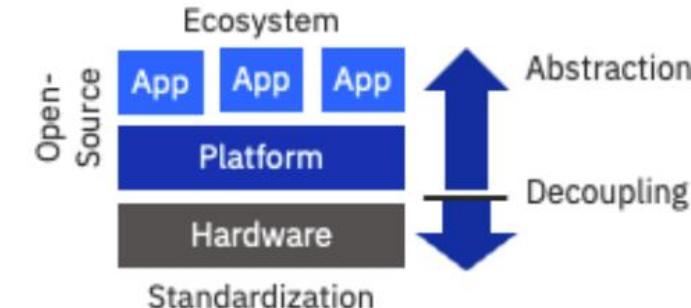
SDV Lifecycle (출처: BlackBerry QNX)

SDV 기술의 BASE

- ❖ SDV 기술의 기본(Base) 정의: 구성 요소
 - ECU 통합화 및 중앙화 E/E Architecture 기반으로 차량 복잡도와 비용 감소
 - 하드웨어 – 소프트웨어 디커플링을 통한 새로운 서비스/기능 제공
 - 소프트웨어 플랫폼 / 클라우드 서비스로 차량 기능 확장, 다양화
 - 차량 소프트웨어 OTA 업데이트로 차량 수명 주기와 성능 증대



- ❖ 디커플링, 추상화, 표준화 및 오픈소스를 통해 앱생태계 생성



02

자동차
사이버공격 사례

자동차 사이버공격 - 연구 동향

University of Washington
연구팀에서 실제 차량을
대상으로 해킹을 수행
(Security & Privacy 2010)



Tencent의 Keen Security
Lab의 연구팀은 테슬라
차량을 원격으로 제어함
(Black Hat USA, 2017)



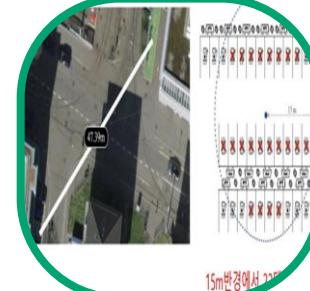
S. Kohler 등은 신호 주입
공격을 통해 전기자동차의
충전을 중단시키는 DoS
공격을 공개함
(NDSS 2023)



C. Miller and C. Valasek은
다양한 차량의 Remote
Attack Surface 공개하고,
JEEP 차량에 대해 무선
해킹 수행
(Black Hat 2013 - 2015)



B. Nassi 등은 AI 시스템을
속일 수 있는 Phantom
Attack을 공개함
(ACM CCS 2020)



자율주행 자동차
센서 공격에 대한
연구 증가

- Too Good to Be Safe: Tricking Lane Detection in Autonomous Driving with Crafted Perturbations, USENIX Security 2021
- Dirty Road Can Attack: Security of Deep Learning based Automated Lane Centering under Physical-World Attack, USENIX Security 2021
- Brokenwire: Wireless disruption of CCS electric vehicle charging, NDSS 2023

■ Experimental Security Analysis of a Modern Automobile (by University of Washington)

- 세계 최초의 자동차 사이버보안 위협에 대한 연구
 - ECU가 본격적으로 차량에 탑재하기 시작한 초기인 점을 감안하면 연구 결과가 매우 시기 적절하였음
 - 현재 자동차 사이버보안 기술 연구의 초석으로 평가받음
- 자동차 진단을 위한 OBD*II 표준 인터페이스를 통해 CAN** 통신 Trace 분석 후 제어 메시지 주입

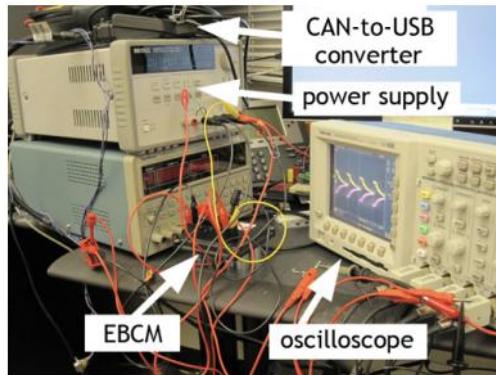


Figure 1. Example bench setup within our lab. The Electronic Brake Control Module (ECBM) is hooked up to a power supply, a CAN-to-USB converter, and an oscilloscope.

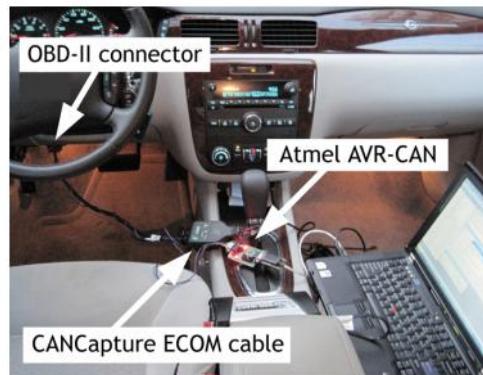


Figure 2. Example experimental setup. The laptop is running our custom CARSHARK CAN network analyzer and attack tool. The laptop is connected to the car's OBD-II port.



Figure 3. To test ECU behavior in a controlled environment, we immobilized the car on jack stands while mounting attacks.

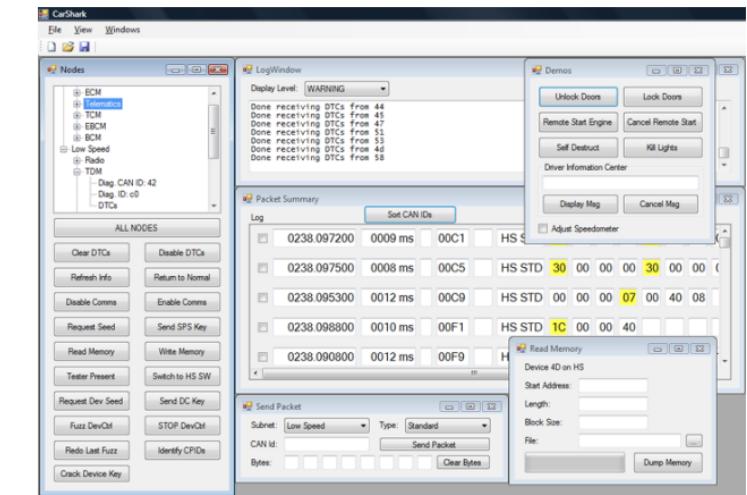
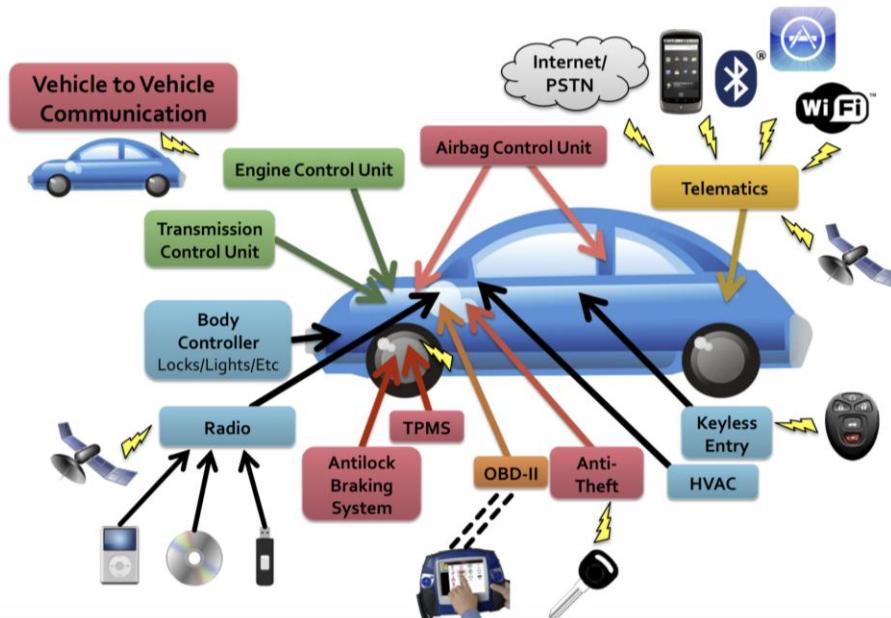


Figure 4. Screenshot of the CARSHARK interface. CARSHARK is being used to sniff the CAN bus. Values that have been recently updated are in yellow. The left panel lists all recognized nodes on high and low speed subnets of the CAN bus and has some action buttons. The demo panel on the right provides some proof-of-concept demos.

■ Comprehensive experimental analysis of automotive attack surfaces (by University of California)

- 이전 연구의 후속 연구로 외부에서 자동차 내부 네트워크에 접근 가능한 Attack Surface에 대한 연구 진행
- 각 Attack Surface에 대한 공격 시나리오 생성
 - Aqlink 프로토콜에서 허용되는 패킷의 최대 크기가 1024 bytes, 그러나 텔레매틱스 장비에서 해당 패킷을 처리하는 버퍼는 100 byte임 → buffer overflow 버그로 연결됨
 - 인증과정에서 사용되는 random number generator의 seed가 장비 off 과정에서 초기화 되는 flaw 발견



Vulnerability Class	Channel	Implemented Capability	Visible to User	Scale	Full Control	Cost
Direct physical	OBD-II port	Plug attack hardware directly into car OBD-II port	Yes	Small	Yes	Low
Indirect physical	CD	CD-based firmware update	Yes	Small	Yes	Medium
	CD	Special song (WMA)	Yes*	Medium	Yes	Medium-High
	PassThru	WiFi or wired control connection to advertised PassThru devices	No	Small	Yes	Low
	PassThru	WiFi or wired shell injection	No	Viral	Yes	Low
Short-range wireless	Bluetooth	Buffer overflow with paired Android phone and Trojan app	No	Large	Yes	Low-Medium
	Bluetooth	Sniff MAC address, brute force PIN, buffer overflow	No	Small	Yes	Low-Medium
Long-range wireless	Cellular	Call car, authentication exploit, buffer overflow (using laptop)	No	Large	Yes	Medium-High
	Cellular	Call car, authentication exploit, buffer overflow (using iPod with exploit audio file, earphones, and a telephone)	No	Large	Yes	Medium-High

[Ref] Checkoway, Stephen, et al. "Comprehensive experimental analyses of automotive attack surfaces." 20th USENIX security symposium (USENIX Security 11). 2011.

[Ref] Miller, Charlie, and Chris Valasek. "Adventures in automotive networks and control units." Def Con 21.260-264 (2013): 15-31.

■ Adventures in automotive networks and control units ('13)

- Miller and Valasek은 앞선 Koscher et al.의 연구('10)를 재연하여 2013년 Def Con21에 발표
 - 이전 연구의 경우 실험한 차량의 정보나 주입한 CAN 메시지에 대하여 모두 블라인드 처리한 반면, 본 연구 결과는 실험한 차량의 정보와 주입한 CAN 메시지 모두 공개
 - 특히, 본 연구는 Unified Diagnostic Services 진단 표준 프로토콜을 활용하여, 표준이 적용된 모든 차량에 적용할 수 있음

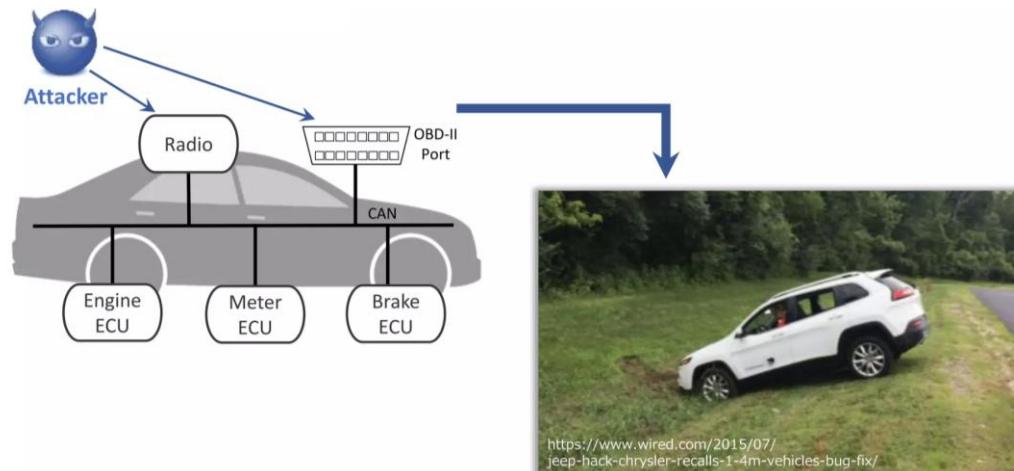
■ Remote exploitation of an unaltered passenger vehicle ('15)

- 기존 연구는 자동차 내부 네트워크에 접근을 한 상태에서 CAN 메시지를 주입함으로써 차량을 제어
- 본 연구는 사전 조작이 되지 않은 차량을 대상으로 원격에서 자동차 내부 네트워크에 접근하여 차량을 제어할 수 있음을 최초로 보임

Remote Exploitation of an Unaltered Passenger Vehicle
Dr. Charlie Miller (cmliller@openrc.org)
Chris Valasek (cvalasek@gmail.com)
August 10, 2015



<< 2015 White Paper >>



[Ref] Miller, Charlie, and Chris Valasek. "Remote exploitation of an unaltered passenger vehicle." Black Hat USA 2015. S 91 (2015): 1-91.

[Ref] 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.

■ Error handling of in-vehicle networks makes them vulnerable (by University of Michigan)

- 기존 연구와는 달리 CAN 프로토콜의 error handling 방법을 악용하여 ECU를 CAN 통신에서 bus-off 되도록 하는 공격 방법을 최초로 사용
 - CAN 프로토콜을 이용하는 ECU들은 서로 같은 아이디를 공유하여 메시지를 보내지 않는다는 가정 하에 서로 통신
 - 즉, 하나의 아이디는 오직 하나의 ECU에만 할당되어 사용된다. 따라서, 같은 아이디를 사용하는 메시지가 CAN Bus에서 동시에 발견되면 이는 error로 간주함
 - 이러한 현상이 일정 횟수 (ID당 256회) 이상 발생하게 되면 해당 ECU는 일정시간 통신에서 제외함

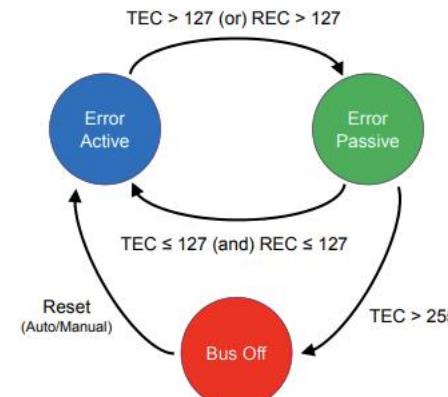
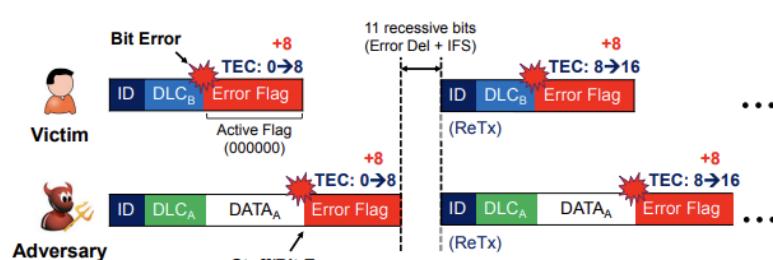
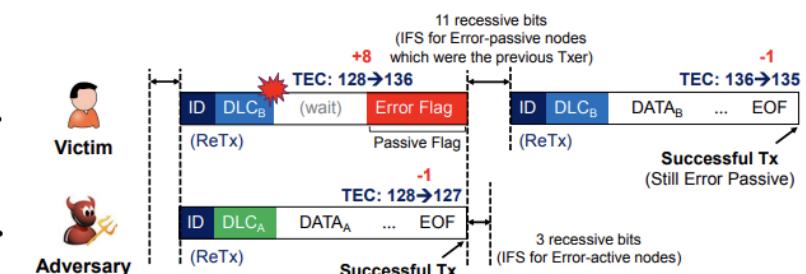


Figure 3: State diagram of fault confinement in CAN.



(a) Phase 1 – Victim in error-active mode.



(b) Transition from Phase 1 to 2.



(a) Communication with ECUs in a 2013 Honda Accord.



(b) Communication with ECUs in a 2016 Hyundai Sonata.

■ Free-Fall: Hacking Tesla from wireless to CAN bus

- 중국의 Tencent의 Keen 보안 연구팀이 Tesla를 대상으로 원격 공격 성공
 - 무선(Wi-Fi/Cellular)을 통해 침입하여 IC(Infotainment Cluster), CID(Center Information Display), GW(Gateway)와 같은 차량 내 여러 시스템을 손상
 - 악성 CAN 메시지를 CAN Bus에 주입하여 공격
- Tesla에 연구 결과를 제출한 지 열흘만에 Tesla는 OTA 메커니즘을 사용한 업데이트를 통해 대응
 - 코드 서명 보호 기능을 Tesla에 도입함

```

./control.py
control ./control.py

[REDACTED] KEEN [REDACTED]

A Simple Tesla Remote Control Panel.

Tesla> ?

Documented commands (type help <topic>):
=====
D mode braking    help    screen    sunroof    water    wiper
N mode exit      mirror_off    seat    trunk    window_off
P mode headlamp   mirror_on    steeringlamp    unlock

Undocumented commands:
=====
eth_20100

Tesla> braking

```

Documented commands:

```

FLASH:00046F30 93 81 00 14    stw    r31, 0x200+saved_too(r1)
FLASH:00046F31 93 81 00 18    stw    r31, 0x200+var_1B8(r1)
FLASH:00046F32 98 A1 00 CD    stb    r28, 0x200+compiler_reserved1(r1)
FLASH:00046F33 98 A1 00 C0    addi   r28, 0x200+var_1B8(r1)
FLASH:00046F34 3D 20 00 04    lis    r9, REBOOTsha
FLASH:00046F35 3D 20 00 04    addi   r9, r9, REBOOT$1
FLASH:00046F36 3D 20 00 0C    ldi    r29, 0x200+var_1B8(r1)
FLASH:00046F37 3D 20 00 04    lis    r9, AFP_VERSIONH
FLASH:00046F38 3D 20 00 04    stw    r9, 0x200+var_1A4(r1)
FLASH:00046F39 3D 20 00 0C    addi   r9, 0x200+var_1A4(r1)
FLASH:00046F3A 3D 20 00 04    lis    r9, MONITOR_CARBIN
FLASH:00046F3B 3D 20 00 04    stw    r9, 0x200+var_1A0(r1)
FLASH:00046F3C 3D 20 00 04    addi   r9, r9, MONITOR_CARBIN
FLASH:00046F3D 3D 20 00 04    lis    r9, 0x200+var_198(r1)
FLASH:00046F3E 3D 20 00 04    addi   r9, r9, 0x200+var_198(r1)
FLASH:00046F3F 3D 20 00 04    lis    r9, BL_VERSIONH
FLASH:00046F40 3D 20 00 04    stw    r9, 0x200+var_194(r1)
FLASH:00046F41 3D 20 00 04    addi   r9, r9, BL_VERSION$1
FLASH:00046F42 3D 20 00 04    lis    r9, REBOOT_for_UPDATEsha
FLASH:00046F43 3D 20 00 04    stw    r9, 0x200+var_190(r1)
FLASH:00046F44 3D 20 00 04    addi   r9, r9, REBOOT_for_UPDATE$1

```



[Ref] Nie, Sen, Ling Liu, and Yuefeng Du. "Free-fall: Hacking tesla from wireless to can bus." Briefing, Black Hat USA 25.1 (2017): 16.

■ (Passive attack) 충전 케이블에서 발생하는 EM(Electromagnetic) leakage를 악용한 도청 공격

- SDR(Software defined Radio)를 이용한 도청장치 구현
- 다양한 충전소 환경에서 도청 공격을 수행하여 통신 패킷 복원
- 차량의 식별자 정보(MAC)가 평문으로 전송되고 있음을 분석함

Site	Antenna	Peak SNR (dB)	BW (MHz)	Total PPDUs	Data PPDUs	Bi-direc.?	Start?	RX% Mean	CRC32% Mean	CRC32% Max	
A	In car	15	6	526	272	✓		99.3	1.1	1.8	3.3
B	In car	18	12	1063	567	✓		29.8	0.5	3.3	5.3
C	In car	25	14	2976	1819	✓		99.9	46.6	48.1	50.3
D	In car	10	12	556	293	✓		88.2	1.4	2.3	3.0
E	In car	9	4.5	569	306			100	11.0	11.1	11.2
F	In car	21	12	3660	2009	✓	✓	99.3	27.8	36.8	45.8
	Bay behind	15	8	1434	1430	✓		99.3	43.5	43.5	43.5
	Outside car	10	10	12987	8255	✓		76.2	34.9	46.6	89.5
	Two cars	14	11	2449	2274			99.1	24.3	47.5	70.8
G	In car	19	12	5837	3670	✓	✓	99.0	51.1	60.3	71.4
	Next bay	15	13	4157	2749	✓		99.7	91.8	91.8	91.8
	By cable	29	23	23984	17246	✓	✓	80.2	52.9	74.0	99.8
H	In car	16	12.5	15052	9362	✓		99.2	69.9	71.0	72.8
	Outside car	20	11	16243	10407	✓		99.5	27.7	61.6	80.6
	By cable	35	25	19535	14717	✓	✓	92.1	34.2	70.0	92.8
	Two cars	15	12	24121	21006			99.6	42.2	71.9	94.8
I	In car	20	12	1501	1193	✓	✓	98.0	94.8	97.4	100.0
J	In car	20	7	14231	10291	✓	✓	81.0	1.0	33.6	67.9
	Outside car	23	7	1084	935	✓	✓	96.0	49.2	49.2	49.2
K	In car	8	5	1971	1278	✓		92.5	0.0	22.0	38.3
L	Outside car	8	7	3004	1849	✓		25.8	0.0	0.0	0.0
M	In car	20	12	13631	9743	✓	✓	98.8	42.4	64.9	82.5
N	In car	24	14	4317	3364	✓	✓	68.3	0.0	44.5	72.6

<다양한 장소에서의 공격 성능 평가>



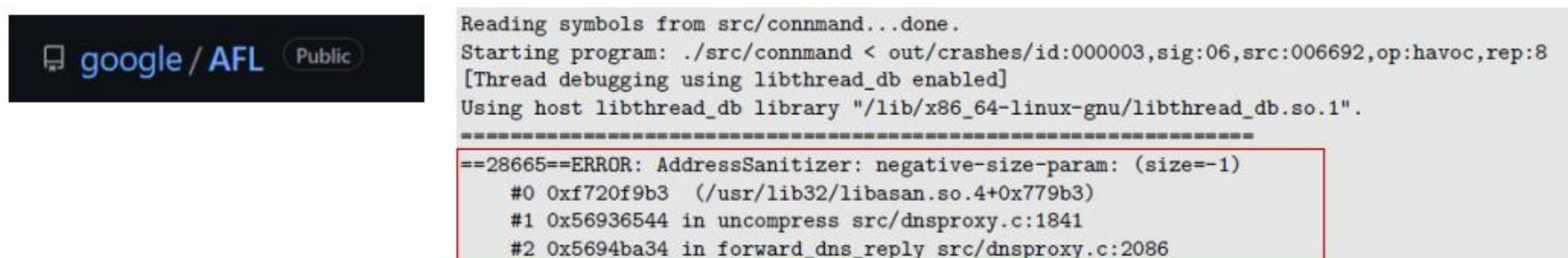
<실험 환경 구성>

Vehicle	MAC
BMW i3	f0:7f:0c:02::**::**
VW e-Golf	00:7d:fa:01::**::**
Jaguar I-PACE	00:1a:37:70::**::**

<복원된 차량 고유 식별자 정보>

■ TBONE – A zero-click exploit for Tesla MCUs

- Tesla 모델이 사용하고 있는 WiFi 관련 오픈소스에 취약점이 존재함을 발견함
 - Tesla 모델은 WiFi 관련 오픈소스인 ConnMan (무선망 연결관리)를 사용하고 있는 것으로 파악됨
 - 해당 오픈소스의 one-day 취약점을 이용하여 차량의 문 열기, 좌석 위치 변경 등을 수행할 수 있음을 보임
 - Initial entry over WiFi
 - ✓ Tesla's SSID
 - Tesla의 Autoshop 서비스 센터는 "Service WiFi"라는 AP 서비스를 제공함
 - 해당 무선 채널은 WPA2-PSK 보안 설정이 되어 있음
 - 하지만 해당 무선 채널 보안에 사용되는 password는 SNS 등에서 쉽게 찾을 수 있음
 - ✓ ConnMan
 - ConnMan은 효율적인 무선망 관리를 지원함
 - Fuzzing with AFL fuzzer (forward_dns_reply() function in src/dnsproxy.c) → uncompress() function (메모리 버그 발견)

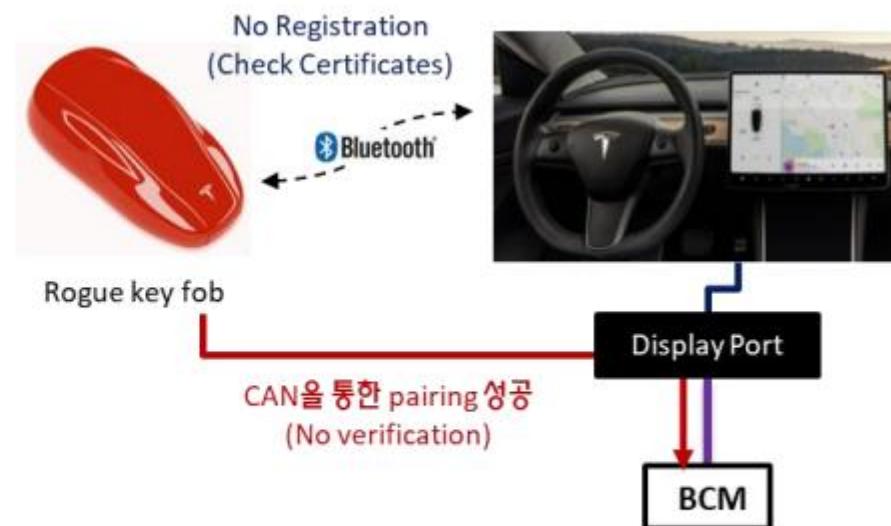
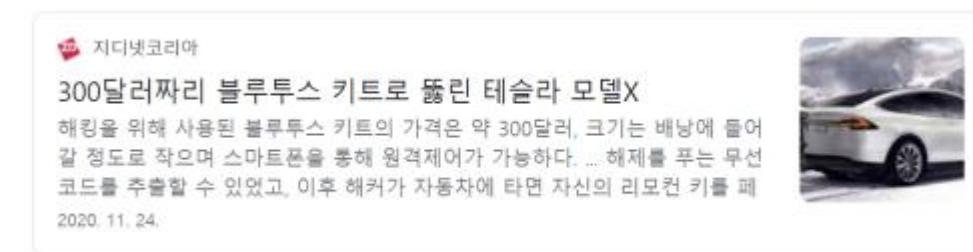
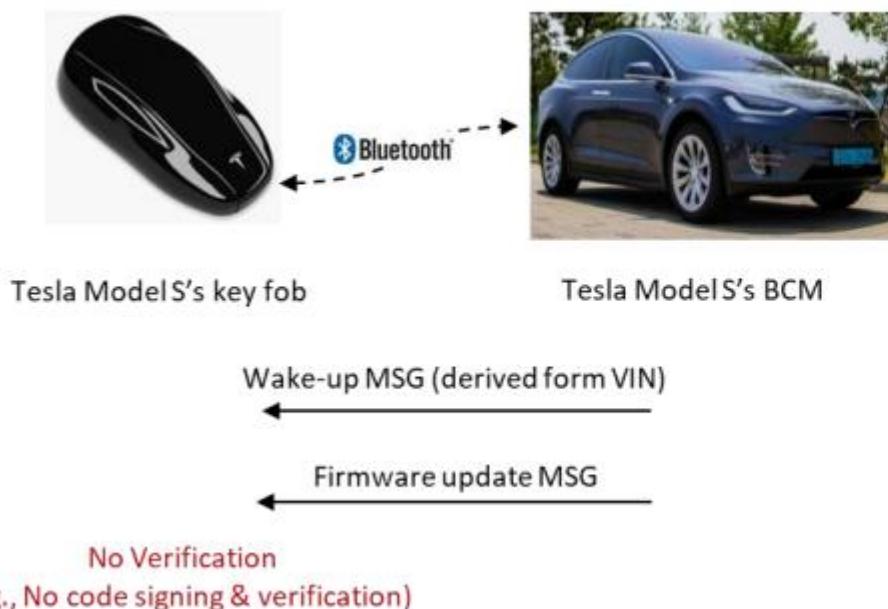


```
Reading symbols from src/connman...done.
Starting program: ./src/connman < out/crashes/id:000003,sig:06,src:006692,op:havoc,rep:8
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
=====
==28665==ERROR: AddressSanitizer: negative-size-param: (size=-1)
#0 0xf720f9b3  (/usr/lib32/libasan.so.4+0x779b3)
#1 0x56936544 in uncompress src/dnsproxy.c:1841
#2 0x5694ba34 in forward_dns_reply src/dnsproxy.c:2086
```

[Ref] Weinmann, Ralf-Philipp, and Benedikt Schmotzle. "Tbone—a zero-click exploit for Tesla MCUs." White Paper, ComSecuris (2020).

■ Tesla Model X의 Bluetooth 기반 스마트키 공격

- Tesla Model X의 스마트키 취약점이 보고됨
 - Bluetooth 기반 key fob 업데이트 취약점
 - CAN network 기반 key fob pairing 프로토콜 취약점



자동차 사이버공격 사례 - TCES ('21)

1) 공격틀 제작 (< \$300)



공격틀은 Rogue BCM과 Rogue key fob의 두 가지 역할을 수행함

2) VIN 확인 및 입력



Tesla Model 의 차대번호 (VIN) 확인 후 공격틀에 입력

3) 차주의 key fob과 공격틀의 pairing



VIN번호를 이용하여 Fake Wake-up신호를 보낸 후, Pairing 진행

4) 차주의 key fob에 악성 펌웨어 업데이트



악성 펌웨어는 Tesla Model X의 door open 명령을 악성틀에게 전송함

5) 악성틀을 이용한 문 열기



악성틀을 이용하여 Tesla Model X의 문을 개방함

6) Rogue key fob 등록

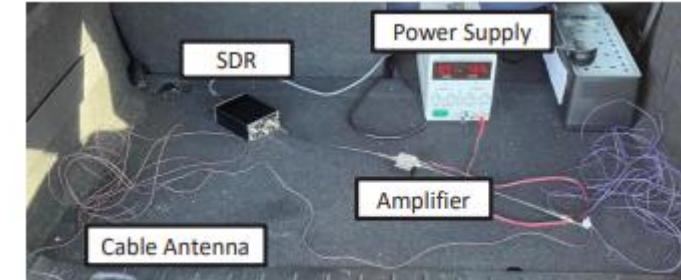


Display의 개방된 포트를 이용하여 Rogue key fob을 차량에 등록함

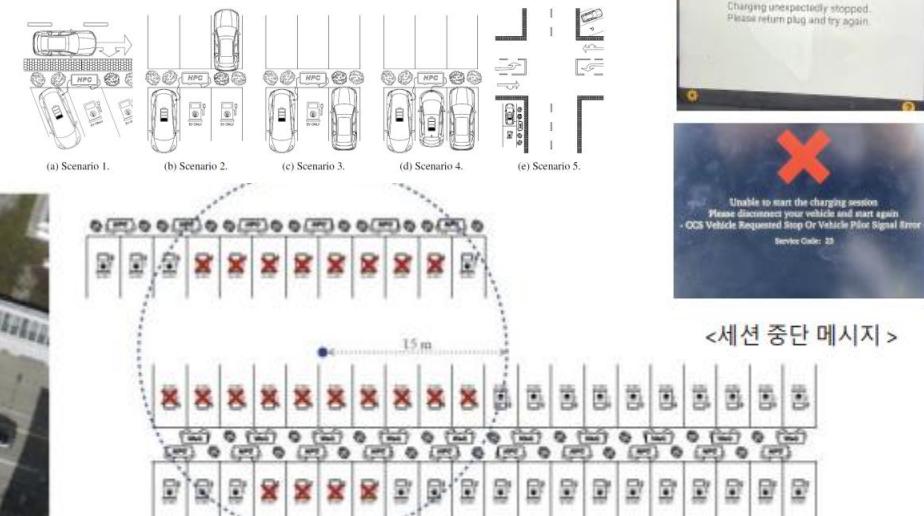
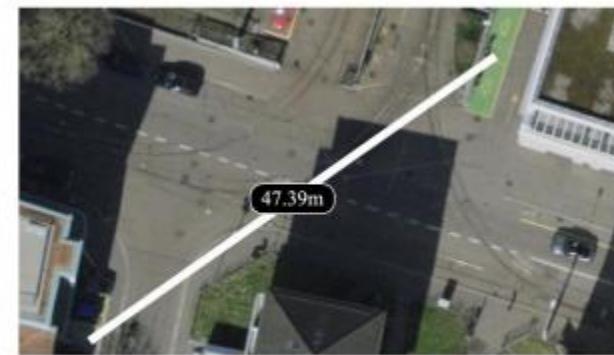
[COSIC researchers hack Tesla Model X key fob - YouTube](#)

■ Brokenwire: Wireless Disruption of CCS Electric Vehicle Charging

- (Active Attack) 신호 주입 공격을 통해 세션을 중단시키는 DoS 공격
 - PLC 통신 보드 구현을 통한 프로토타입 검증 수행
 - SDR을 이용하여 low-cost 신호 주입 공격 장치를 구현함
 - 야외에서 최대 47m 거리에서 충전 세션을 중단시킬 수 있음을 확인함
 - 실내의 경우 다른 층(floor)에 위치한 공격자에 의해서도 공격이 가능함을 확인
 - 현재 Responsible Disclosure로 인해 세부 공격은 확인하기 어려움



<신호 주입 공격 모듈 구성>



15m반경에서 22대의 차량을 동시에 공격 가능함

[Ref] Köhler, Sebastian, et al. "Brokenwire: Wireless disruption of ccs electric vehicle charging." arXiv preprint arXiv:2202.02104 (2022).

■ Tesla 자동차 대상 물체 인식 알고리즘 공격

- Adversarial Example을 통해 물체 인식에 사용되는 딥러닝 알고리즘을 공격하는 기존의 연구를 Tesla 차량에 적용
- 테슬라 차량에 탑재된 카메라로부터 수집된 데이터를 처리하는 딥러닝 알고리즘을 분석하여 의도적으로 오동작을 유발하는 연구를 수행 (Adversarial Example 생성)
 - Model 유추: 딥러닝 모델에 query를 날린 후 결과를 확인하면서 모델 유추
 - Loss function 조작: 다른 class로 분류되도록 하되 loss가 가장 작도록 loss function을 구성
- 공격 시나리오
 - 비가 오지 않는 상황에서 와이퍼가 동작하도록 유발
 - 도로위에 작은 마킹을 통해 Autopilot 기능의 오동작 유발



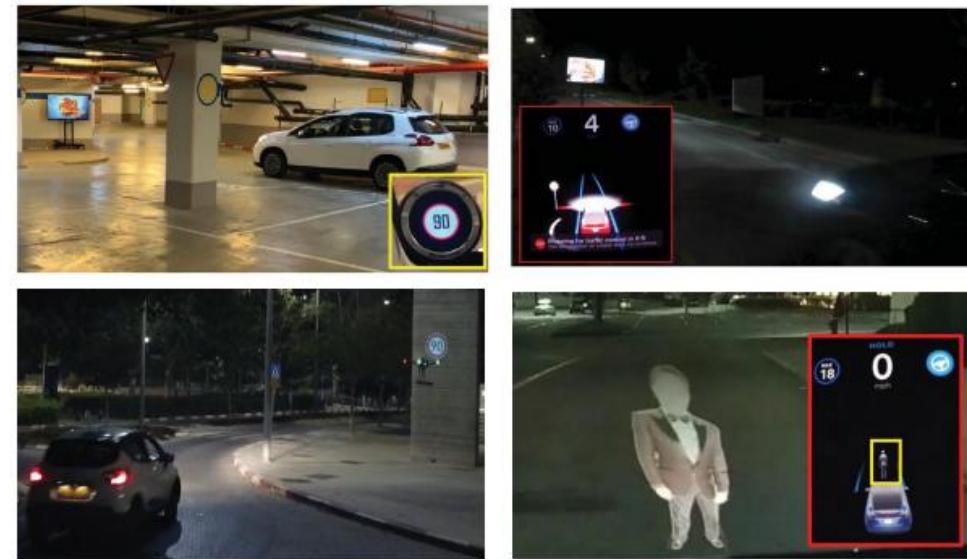
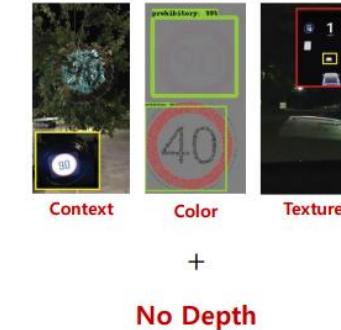
Adversarial example을 통한 와이퍼의 오동작 유발



Autopilot 오동작 유발을 위한 도로위의 마킹

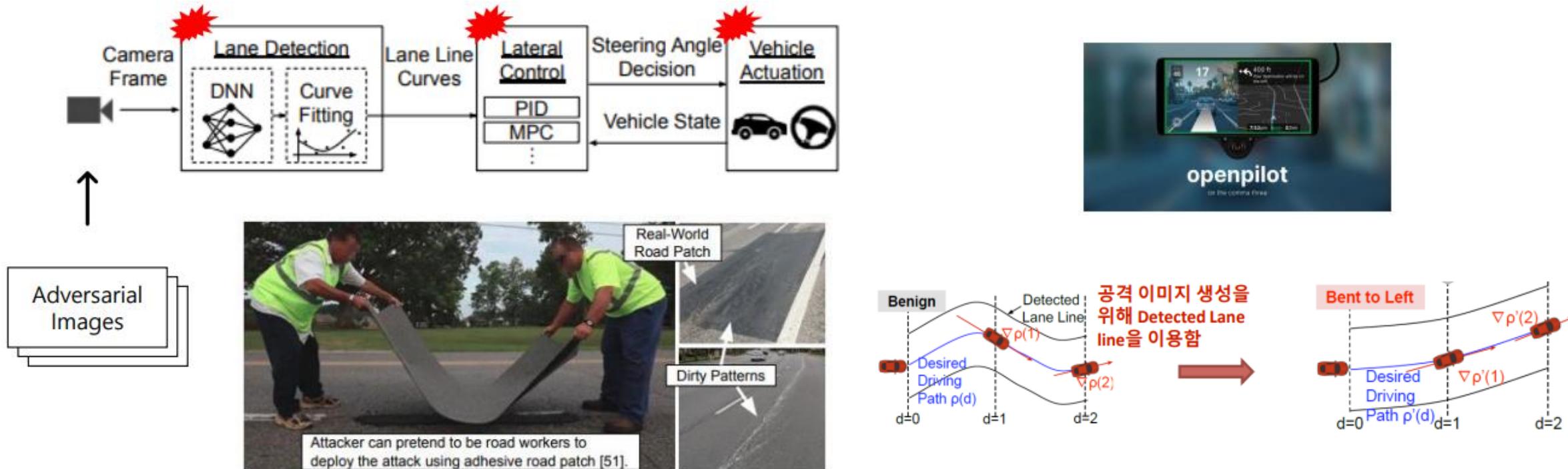
■ Phantom of the ADAS: Securing Advanced Driver-Assistance Systems from Split-Second Phantom Attacks

- Phantom 공격
 - Projector (with drone)를 통한 영상 송출
 - Digital screen을 통한 영상 송출
- Split-second Phantom 공격
 - ADAS 시스템에 인식될 수 있는 짧은 시간동안 이미지를 송출함
 - ADAS Camera에서 인식될 수 있는 최소의 시간동안 fake 이미지 생성함
 - ✓ 따라서, 인간의 눈으로는 이상현상을 감지하기 어려움
- Tesla ADAS 취약점
 - Color, Context, 그리고 Texture를 고려하지 않음
 - Tesla의 ADAS는 감지된 object의 depth를 확인하지 않음
 - ✓ Sensor Fusion: Radar 정보보다 Camera 이미지에 기반한 판단



■ Dirty Road Patch (DRP) Attack

- Openpilot의 LKAS (Lane Keeping Assist System) 시스템이 오작동하도록 adversarial example을 생성하는 공격 방 법론을 제안
- 여러 환경요인으로 인해 더러워진 도로의 패턴 (e.g., 흙, 얼룩 등)과 유사한 이미지를 생성하도록 최적화 문제를 정 의하고, 실제 도로에 배치함으로써 공격 수행



[Ref] Sato, Takami, et al. "Dirty road can attack: Security of deep learning based automated lane centering under {Physical-World} attack." 30th USENIX Security Symposium (USENIX Security 21). 2021.

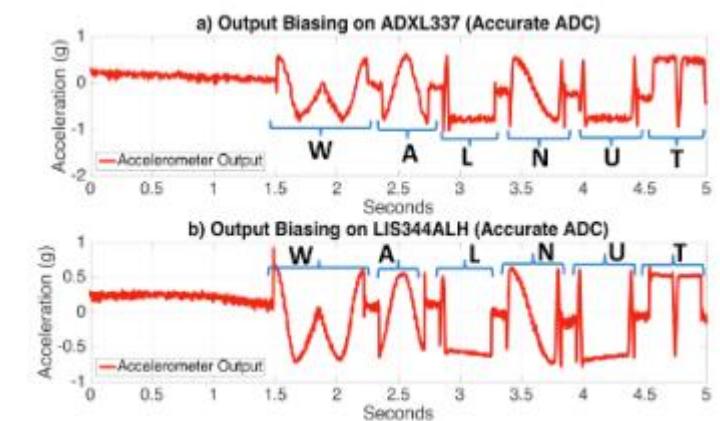
■ Rocking Drones ('15)

- 드론에 탑재된 MEMS(MicroElectroMechanical System) 자이로스코프 대상으로 음향 신호 주입 공격 수행
 - 음향 신호 주입 공격으로 인해 자이로스코프 출력 오류 생성 → 드론 추락



■ WALNUT ('17)

- MEMS 가속도 센서 대상 음향 신호 주입 공격
- 센서 Spoofing 공격 기법 제시
 - Signal Aliasing 유도하여 DC 성분의 출력 생성
 - Amplitude & Phase Modulation
 - ✓ 음향 신호 주파수를 변조하여 원하는 출력 생성
 - 최종적으로 MEMS 가속도 센서 Spoofing → WALNUT 철자 출력



■ Injected and Delivered ('18)

- IMU (가속도 센서 및 자이로스코프)에 대한 음향 신호 주입 공격 및 취약점 분석
 - 공격 음향 신호의 진폭과 위상을 변조 → 누적 방향 각도 조작

03

자동차
사이버공격
대응기술

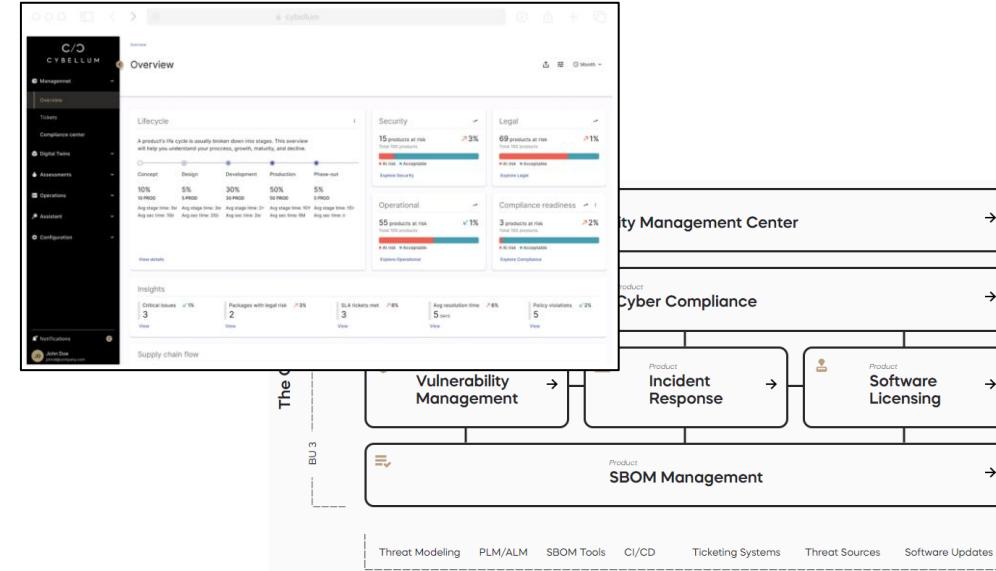
■ Analytics

- Automotive Vulnerability Analysis System (VAS)

- 해킹 방지를 위해 자동차 Firmware or Software에 대한 취약점 분석 기술

- CAN Bus Reversing

- CAN Data 기반으로 CAN ID 식별 등의 DBC 파일 정보 Reversing



출처: <https://cybellum.com/>

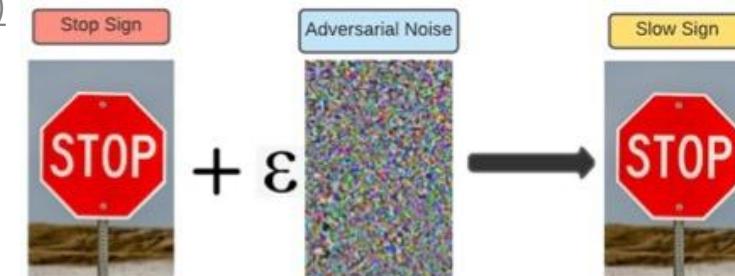
■ Detections

- Automotive Intrusion Detection System (IDS)

- In-vehicle or Vehicle to Back-end Infra에 대한 공격 침입 탐지 시스템
- 통신 Protocol에 의존적으로 연구되고 있으며, 최근에는 Automotive Ethernet 위주로 연구 진행

- Automotive AI Security (driver Identification, mitigation of AI adversarial attack)

- Driving Data를 기반으로 운전자 식별 관련 연구
- Poisoning attack 등 Automotive AI 모델의 Adversarial Attack에 대한 대응 기술 연구



출처: <https://insights2techinfo.com/self-driving-automobiles-and-adversarial-attacks/>

■ Cybellum

- 이스라엘의 자동차 사이버보안 전문 기업으로 LG전자가 미래성장동력으로 키우는 전장사업의 포트폴리오를 고도화하고 글로벌 경쟁력을 한층 더 강화하기 위해 2021년에 인수합병
- 자동차 내부 취약점 분석
 - 사이버보안의 디지털 트윈(Digital Twin)
 - ✓ 소스코드 없이 바이너리 파일 내에서 자동차 소프트웨어의 모든 특성을 추출하여 SBOM*, 라이선스, 하드웨어 아키텍처, 운영 체제, 소프트웨어의 구성, 제어 흐름, API 호출 등을 포함한 각 차량의 구성요소를 분석
 - 인텔리전스(Intelligence) 기반 방어
 - ✓ 다양한 위협 인텔리전스 데이터베이스를 기반으로 새로운 취약점, 기존 위협에 대한 변경 사항 및 새로운 공격 방법을 추적
 - 위험기반 우선순위 지정
 - ✓ 차량의 각 구성 요소가 작동하는 취약점 간의 연관관계를 바탕으로 차량과 관련 없는 취약점을 걸러내고 취약점에 대한 우선 순위를 지정하여 개선 사항을 제공
- 국제 표준 준수 검증
 - ISO/SAE 21434 준수 여부 검증 및 CERT C, MISRA C등 표준 준수 여부 검증

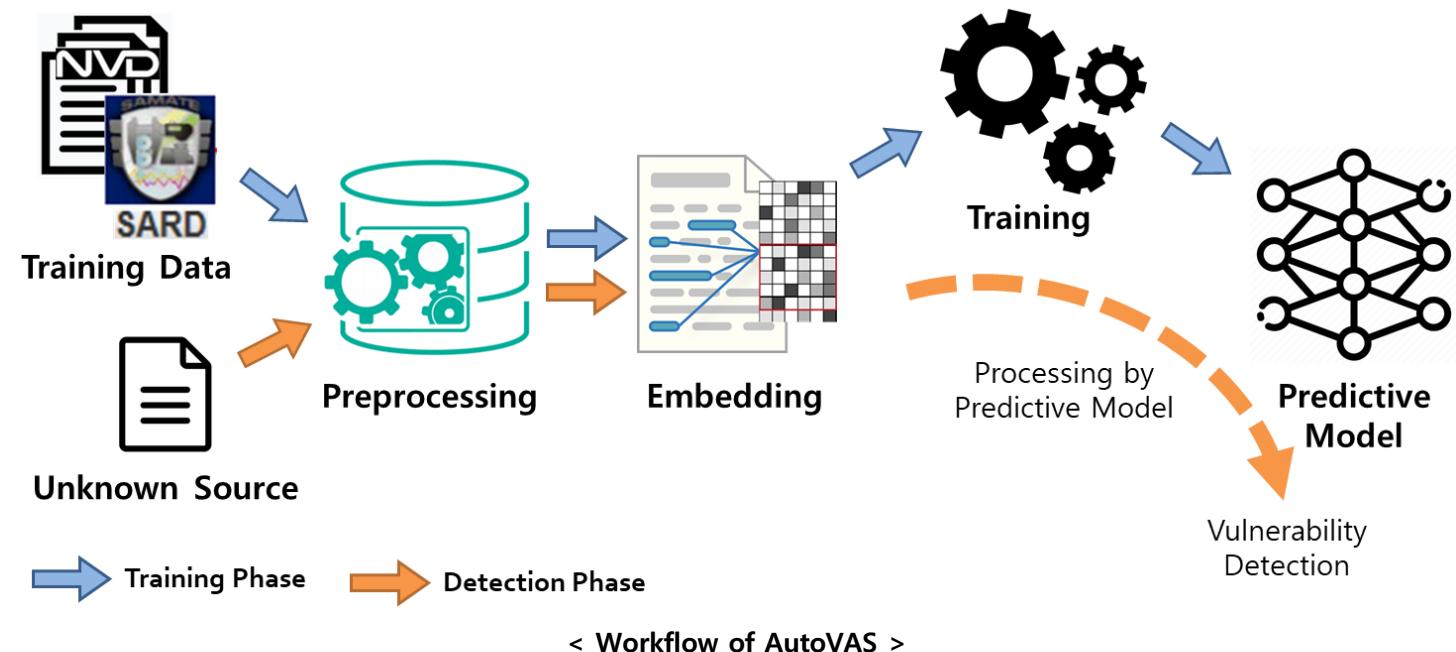
- SBOM(Software Bill Of Material)*: 최종 배포/활용되는 소프트웨어를 구성하는 모든 컴포넌트 명세서

■ Automated Vulnerability Analysis System (AutoVAS)

- Dataset
 - NVD based on CVE**
 - SARD based on CWE***

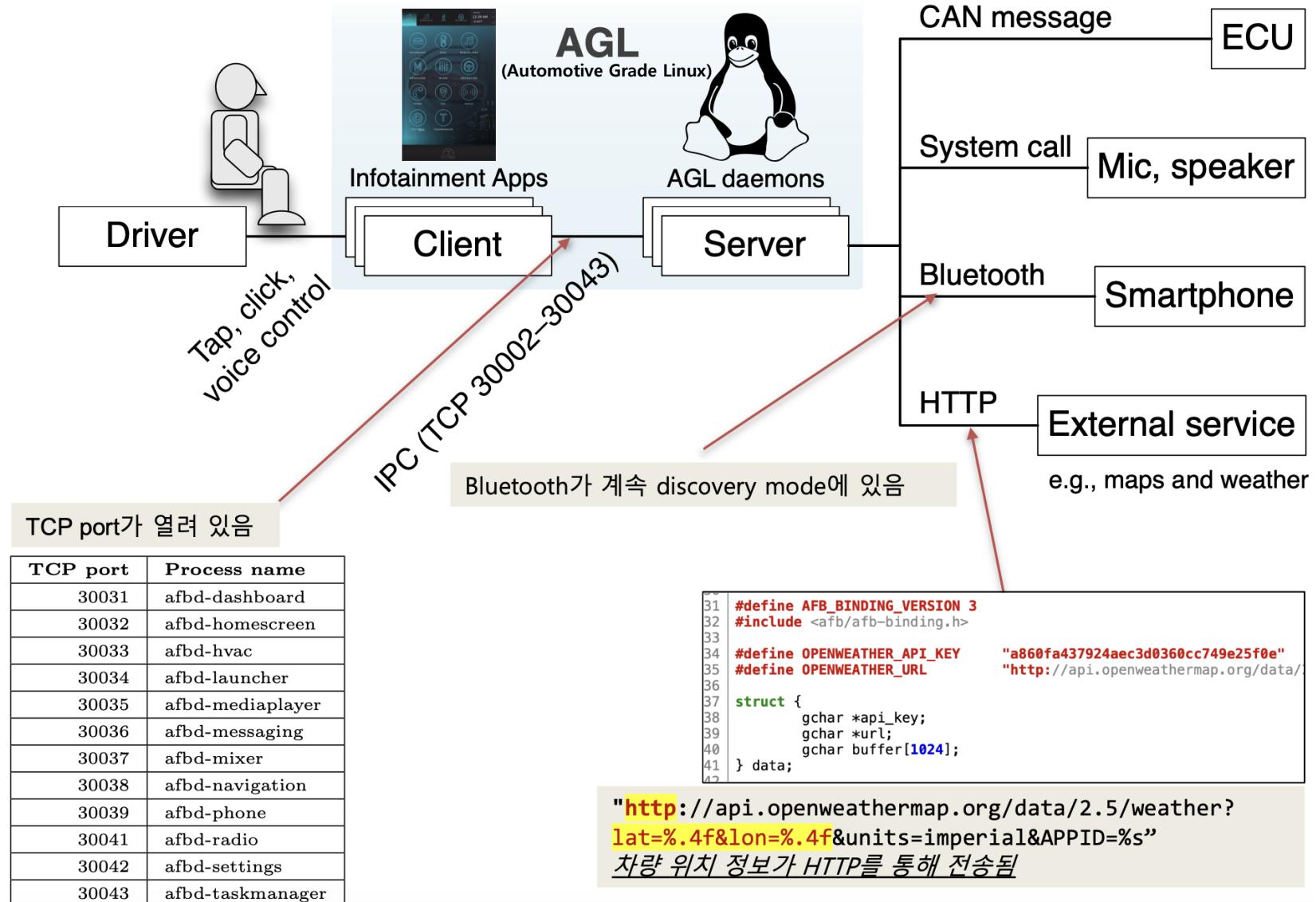
- Source code Representation:
 - Program slicing
 - Symbolization & Tokenization
 - Source Code Embedding

- Neural Network
 - RNN model
 - ✓ LSTM, GRU
 - NLP model
 - ✓ BERT, GPT



- CVE**: Common Vulnerabilities and Exposures
- CWE***: Common Weakness Enumeration

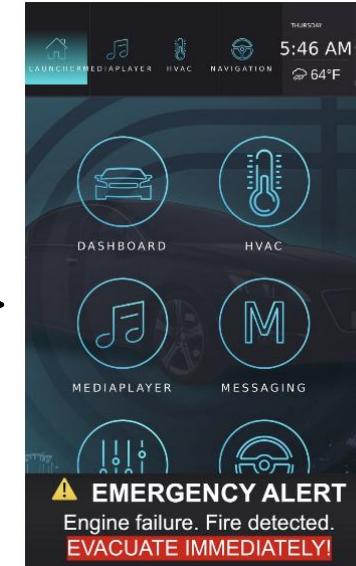
■ Findings



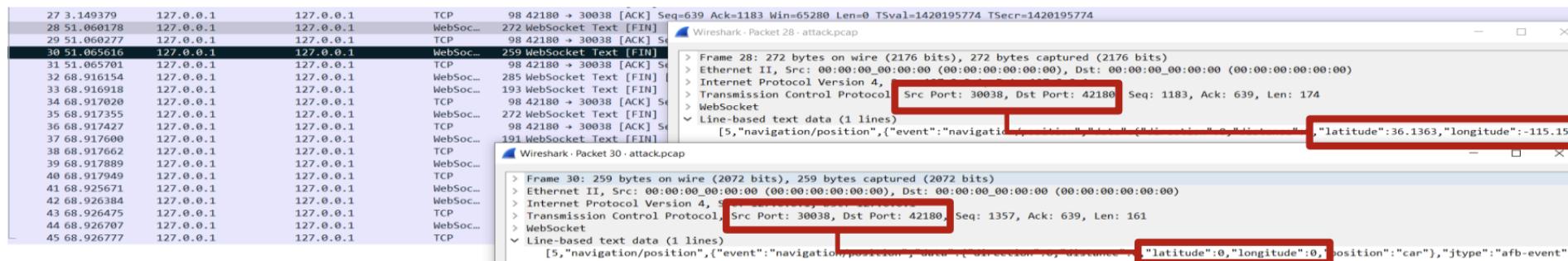
■ Attack#1. Command Injection Attack (CVE-2022-24595)

- Change temperature in HVAC service to trigger CAN messages

```
vcan0 7DF [8] 02 01 0C 00 00 00 00 00
vcan0 7DF [8] 02 01 0D 00 00 00 00 00
vcan0 7DF [8] 02 01 0C 00 00 00 00 00
vcan0 030 [8] 64 10 10 F0 0A 01 00 00 'd....'
vcan0 7DF [8] 02 01 0D 00 00 00 00 00
vcan0 7DF [8] 02 01 0C 00 00 00 00 00
vcan0 7DF [8] 02 01 0D 00 00 00 00 00
```

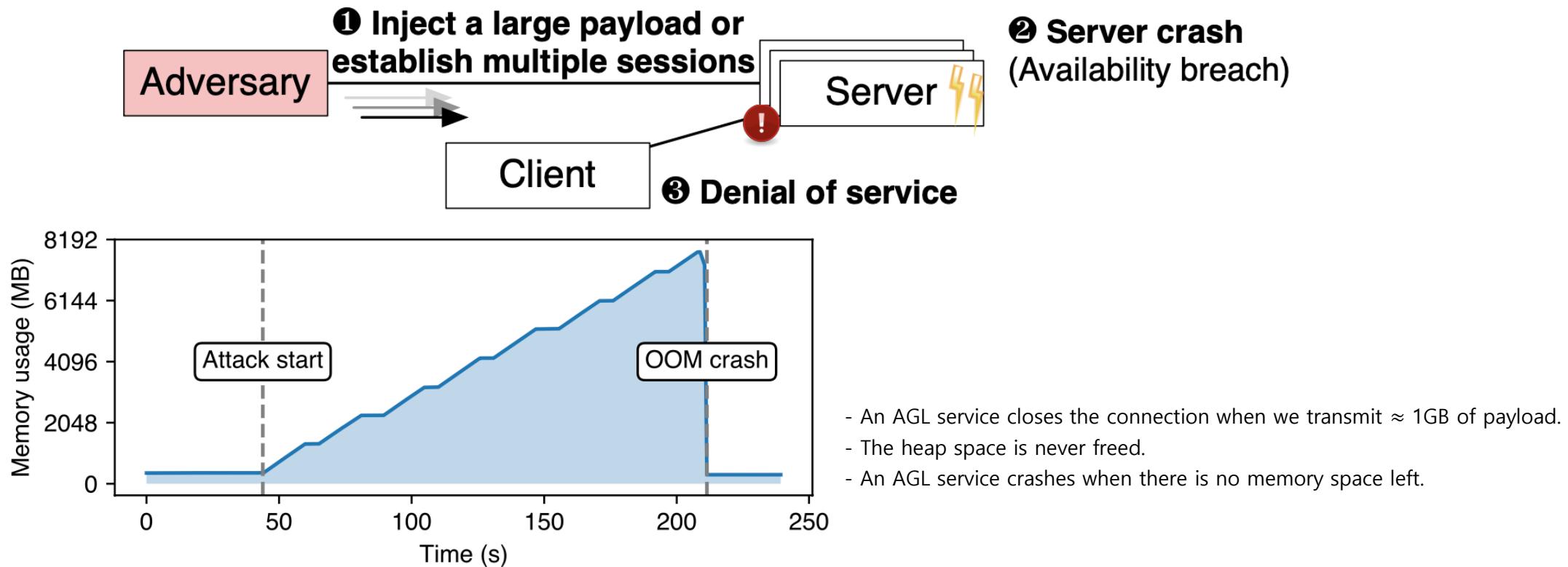


- Change the current location to (0, 0) and send the location message manipulated by an external attacker



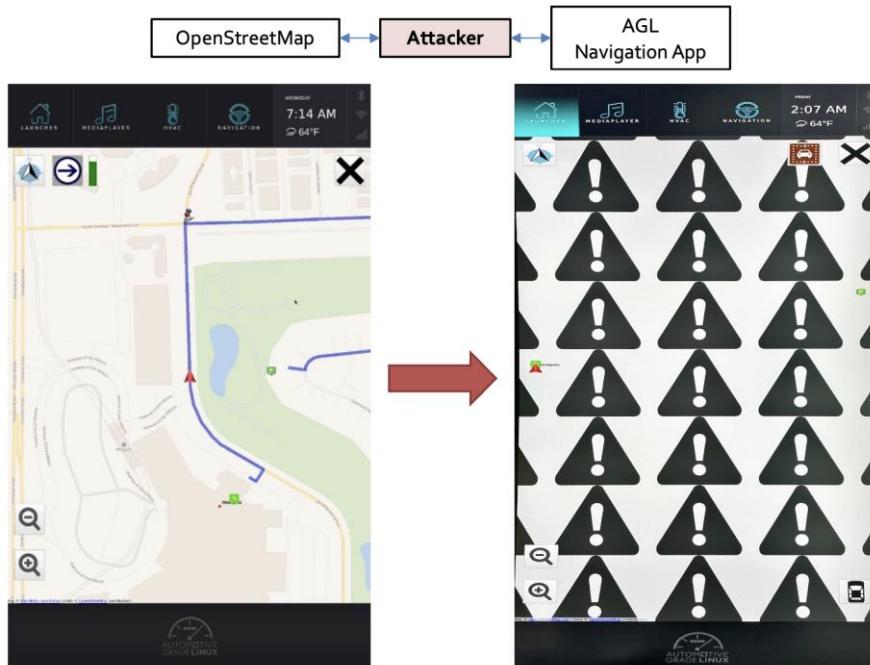
■ Attack#2. DoS Attack (CVE-2022-24596)

- CVE-2022-24596 due to Improper Input Validation & Resource Management
 - AGL services could be crashed with an out-of-memory (OOM) crash.
 - ✓ After the OOM crash, a driver cannot utilize infotainment services until reboot.



■ Attack#3. MITM* attack (CVE-2022-24597)

- CVE-2022-24597 due to Insecure communication over HTTP
- AGL tries to connect OpenStreetMap.org via HTTP communicatinos

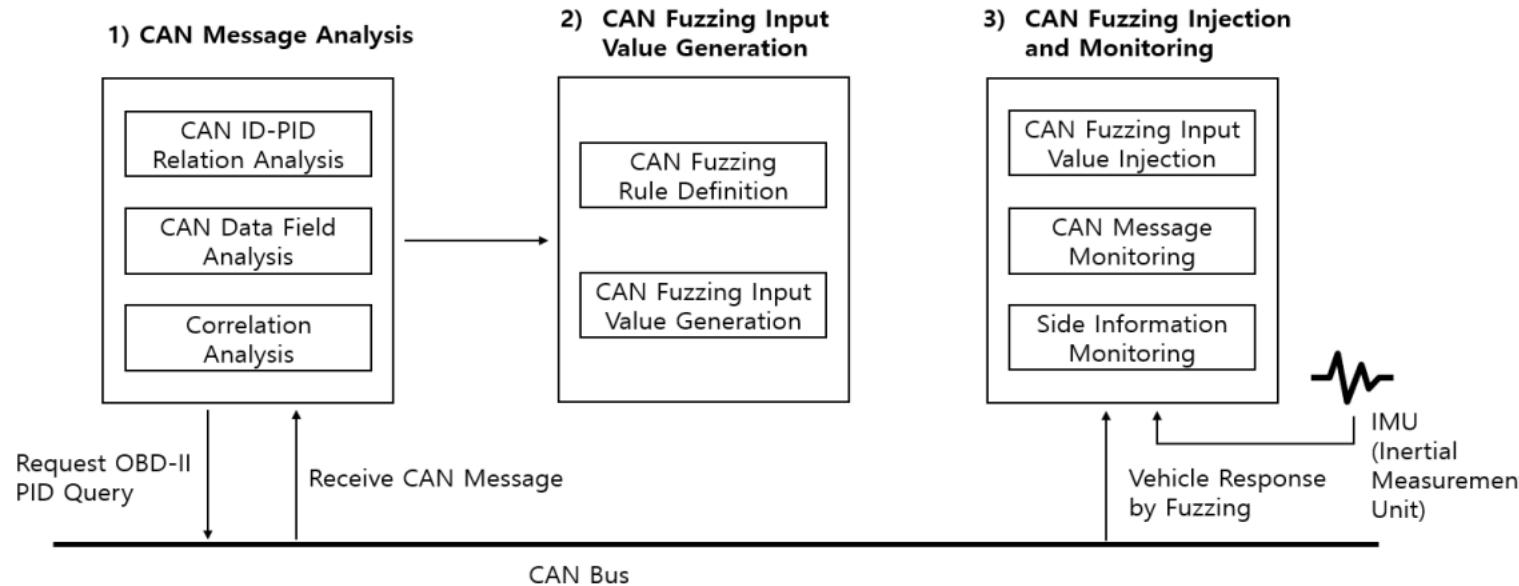


- Since there is no client authentication, an unauthorized client can hijack various vehicle information.

- MITM*: Man In The Middle

■ Efficient ECU Analysis Technology Through Structure-Aware CAN Fuzzing

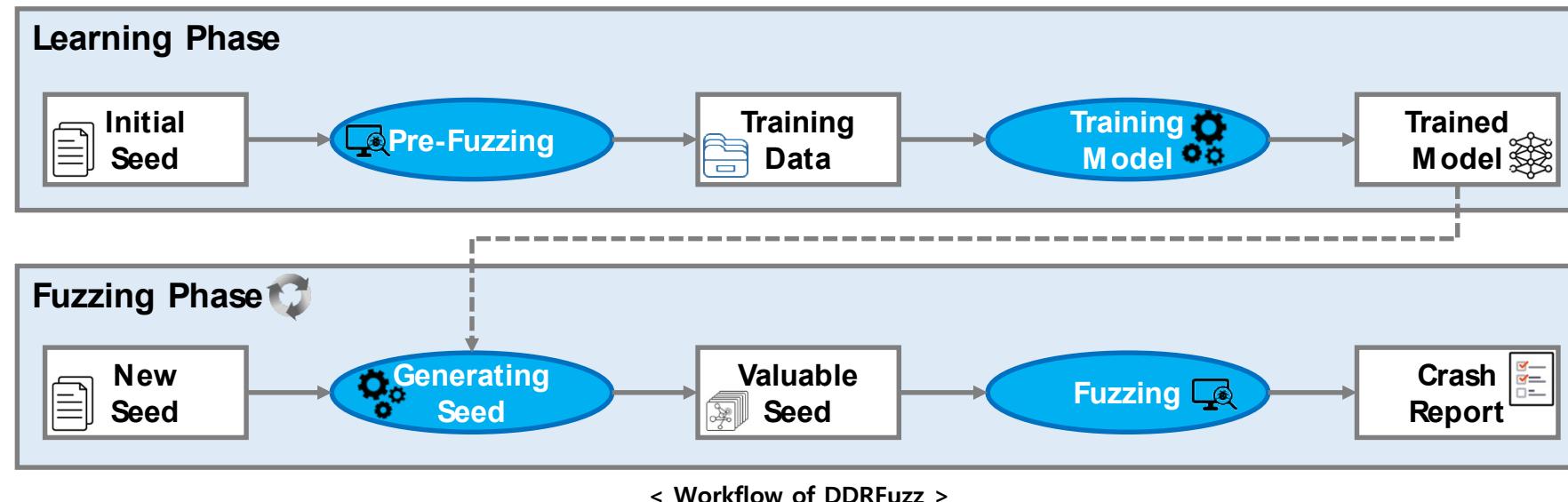
- CAN 메시지 특성이 반영된 Rule 기반으로 CAN Fuzzing 입력 값을 생성하고, Fuzzing 결과를 모니터링할 수 있는 방법론을 최초로 제시
 - CAN 메시지의 특성이 반영된 Non-Random CAN Fuzzing 기술을 제안함으로써, 기존 Random CAN Fuzzing 기술들에 비해 CAN Fuzzing에 소요되는 시간을 절약할 수 있음



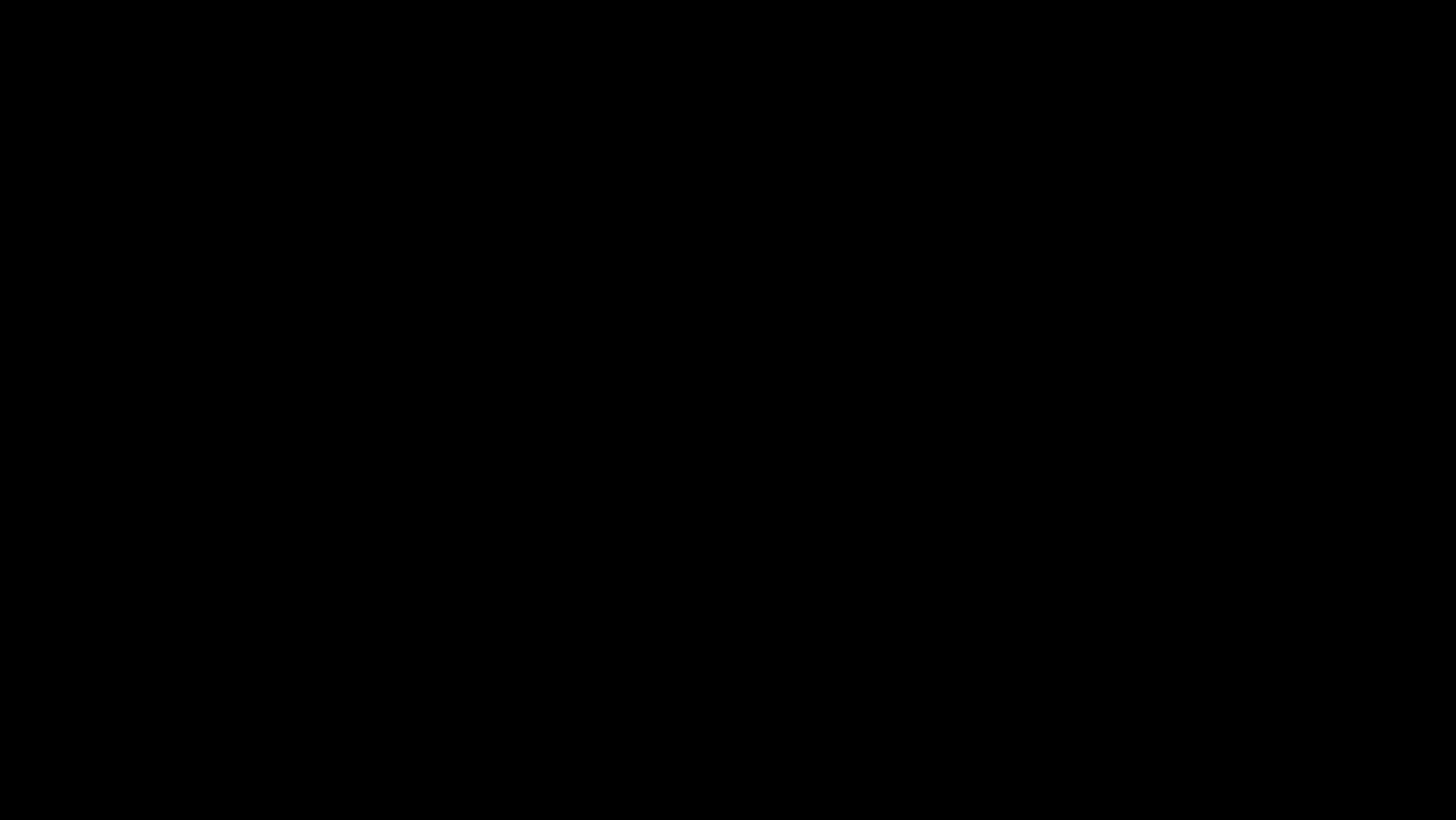
[Ref] 김동영, 전상훈, 류민수 and 김휘강. (2022). 자연어 처리 모델을 활용한 퍼징 시드 생성 기법. 정보보호학회논문지, 32(2), 417-437.

■ Data-DRiven Fuzzing (DDRFuzz)

- Learning Phase
 - To *gather training data using pre-fuzzing* (triggering crash and new coverage)
 - A seed generative model based on a sequence-to-sequence (seq2seq) model
- Fuzzing Phase
 - To *obtain valuable seeds* through trained seq2seq model
 - Easy to *integrate with several base fuzzers* since separation between learning and fuzzing phase.

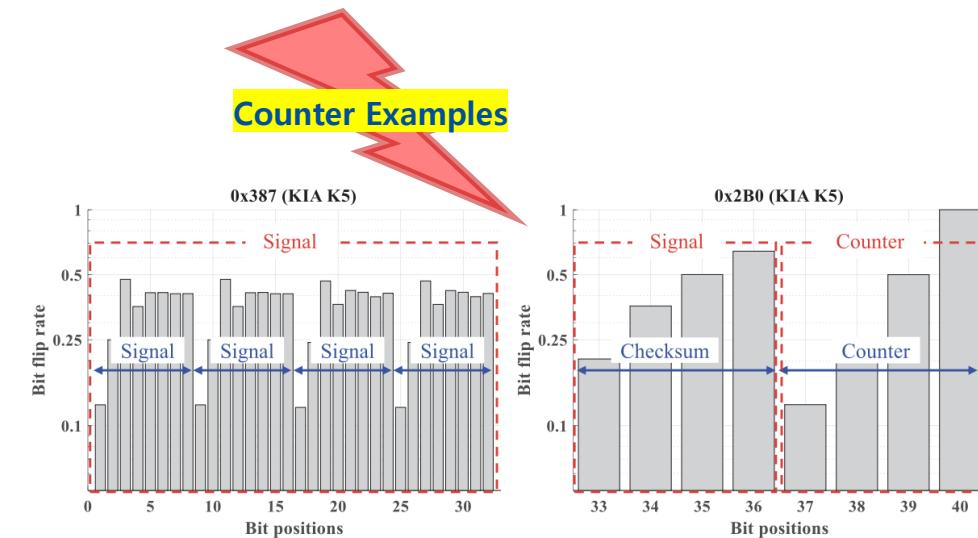
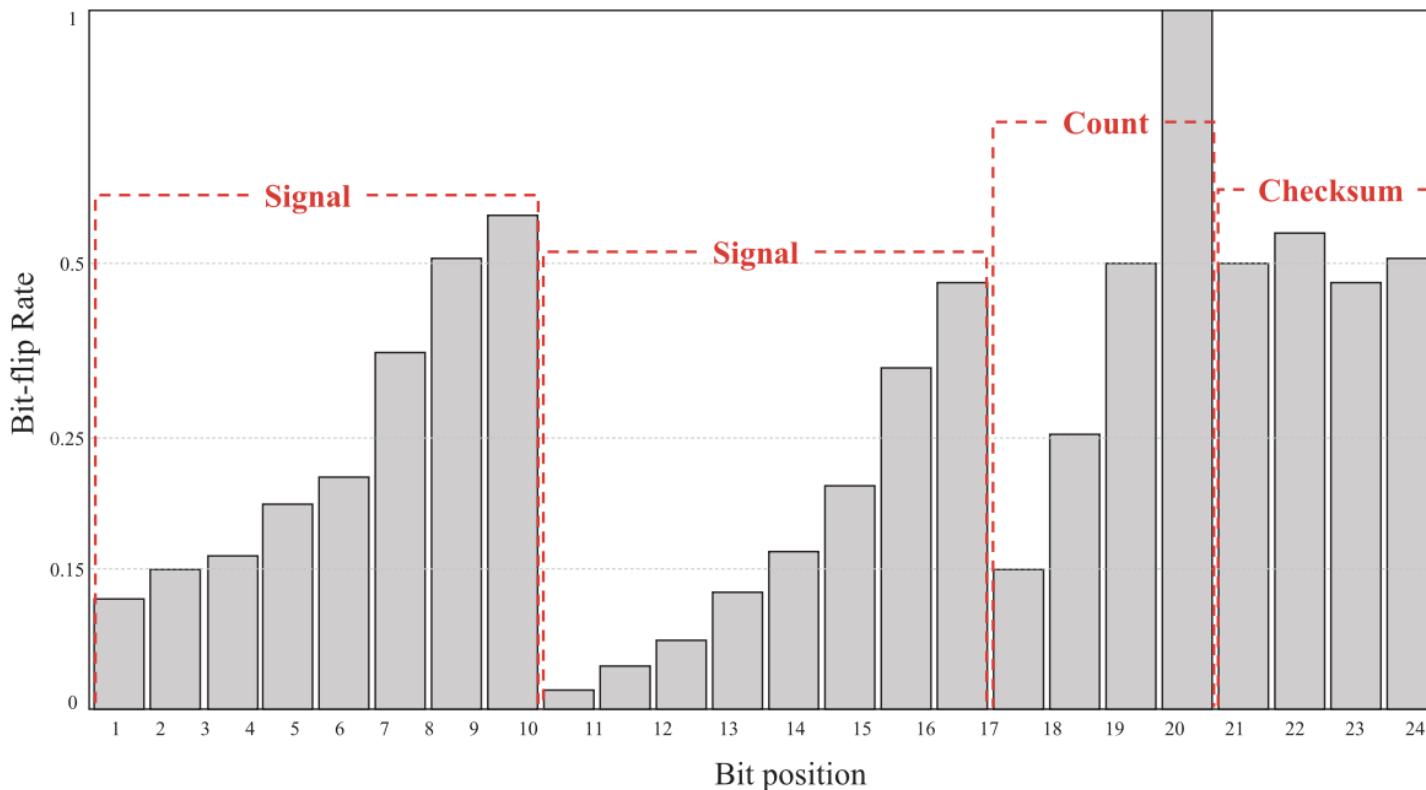


■ Fuzzing Demo



■ CAN Data 식별#01

- CAN Data의 Bit Flip Rate를 기준으로 경계 값을 식별
 - Bit Flip Rate가 순차적으로 증가하다가 경계 값을 지나면 감소하는 pattern을 기준으로 CAN Data를 식별하는 방법

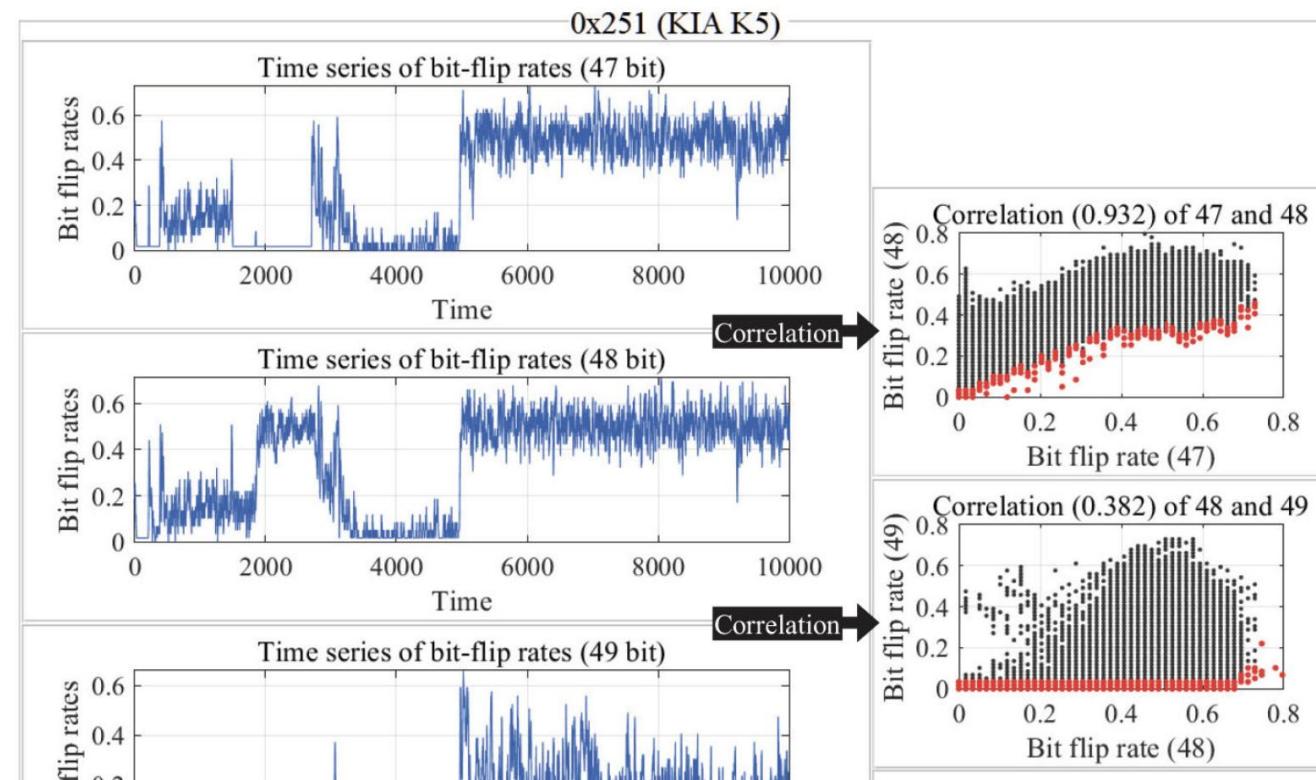


[Ref] M. Marchetti and D. Stabili, "READ: Reverse Engineering of Automotive Data Frames," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 4, pp. 1083-1097, April 2019, doi: 10.1109/TIFS.2018.2870826.

[Ref] Choi, Wonsuk, et al. "An enhanced method for reverse engineering CAN data payload." IEEE Transactions on Vehicular Technology 70.4 (2021): 3371-3381.

■ CAN Data 식별#02

- CAN Data의 Bit flip rate 대신 time series의 pattern을 이용해서 경계 값 식별
 - Bit position 대신 time을 기준으로 x축을 구성 후에 time-series의 pattern을 기준으로 CAN Data를 식별하는 방법
 - Bit flip의 counter example의 경우에도 time series로 변환 후 경계값 식별됨을 확인



■ LibreCAN

- 앞선 CAN Data 경계 값 식별 방식을 기반으로 DBC2-PID 표준을 결합하여 CAN Message 구조 유추

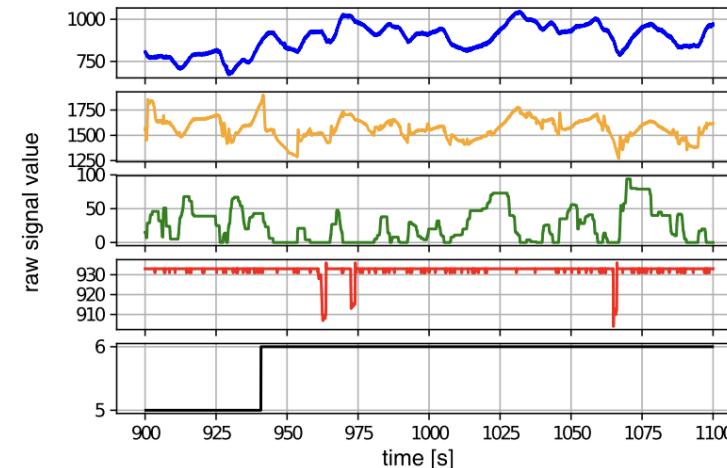
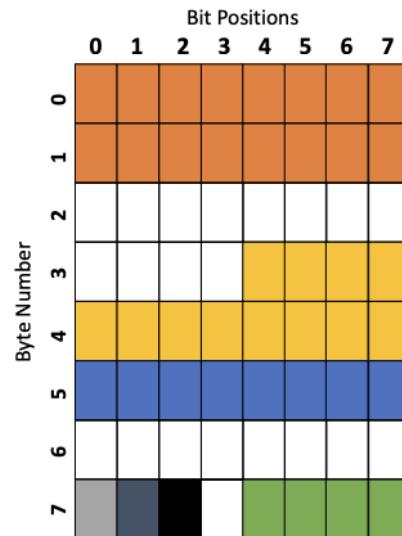


Figure 2: Example of CAN signals

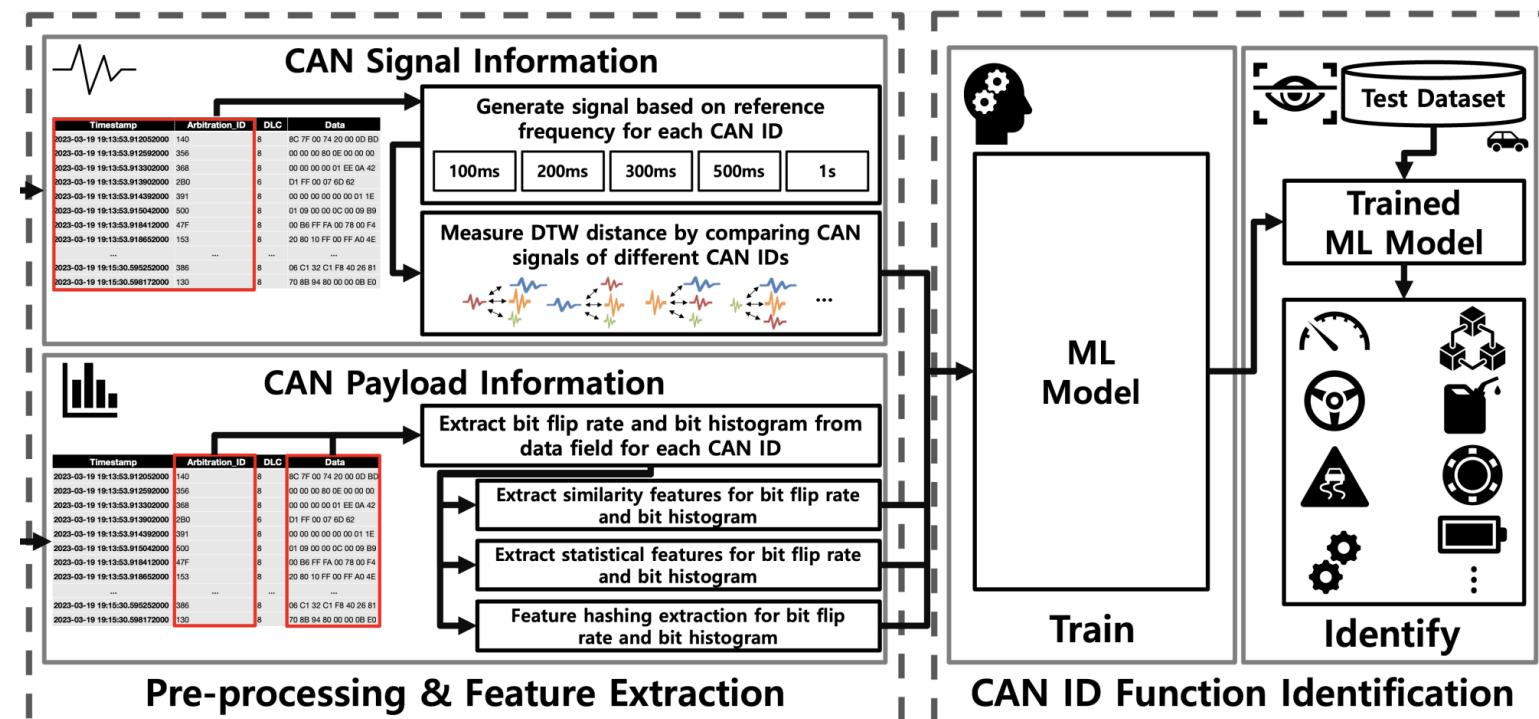
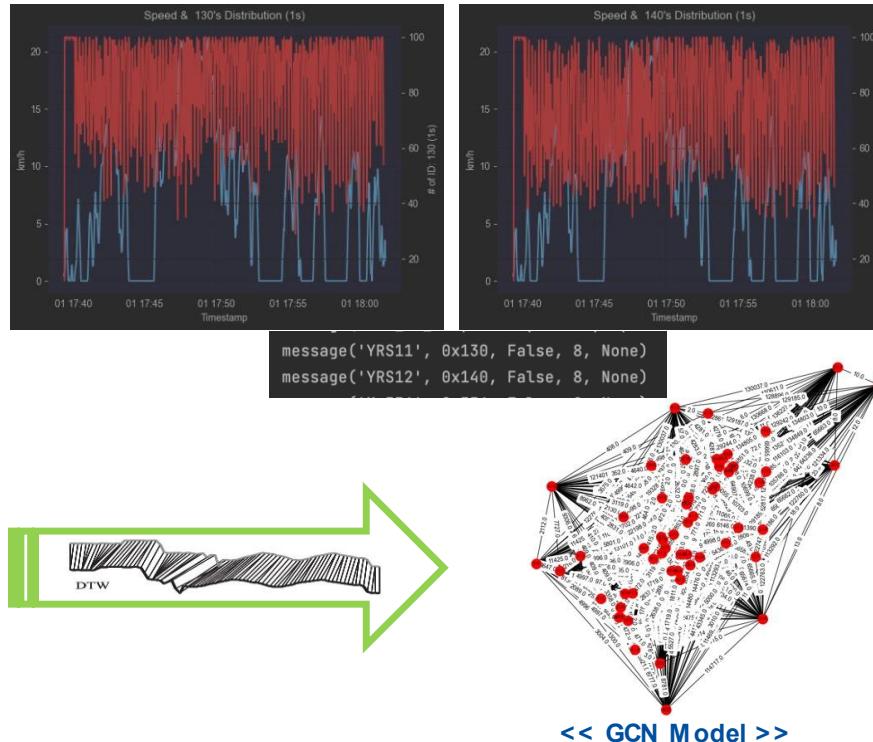
TRACE			
TIME	ID	PAYLOAD	FILTERED IN
00.000	700	1111111100000000	STAGE 3
00.001	100	0000000000000000	CANDIDATE
00.002	300	000002000E20BE20	STAGE 1
00.004	900	FFFFFFFFFFFFFF	CANDIDATE
00.008	300	000002000E20BE20	STAGE 1
00.009	300	000002000E20BE20	STAGE 1
00.011	600	000000024CB016EA	STAGE 2
00.015	800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

REFERENCE		POWERTRAIN	
ID	PAYLOAD	ID	CORRELATION SCORE
100	0000A00A000BC300	100	0.7433
200	0070070070070070	200	0.5192
300	00000000075BCD15	300	0.7990
400	056089000A00A000	400	0.6648
500	0012300AE0030000	500	0.9882
600	000000024CB016EA	600	0.7102
700	1000000001100001	700	0.8361
800	0000000000000FF	800	0.1034
900	0F00B9900A0A0F0E	900	0.2023

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

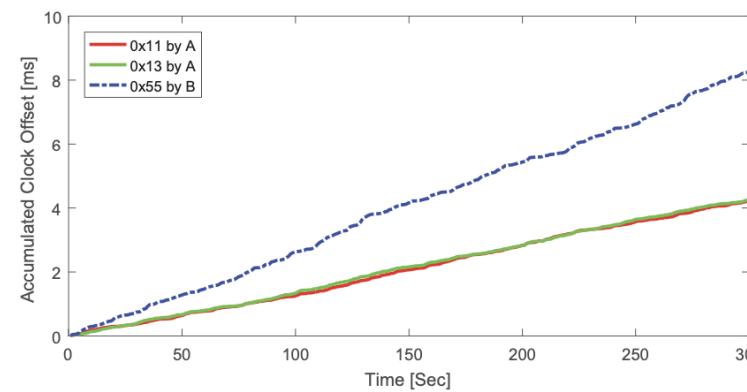
■ DTW(Dynamic Time Wrapping)와 GCN(Graphic Convolution Network)을 이용하여 CAN ID 식별

- 기존 방법은 시계열 데이터의 align이 맞지 않는 경우 적용하기 어렵다는 단점을 보완하기 위해 연구
- DTW를 사용해서 여러 시계열 데이터의 유사도를 동적으로 분석

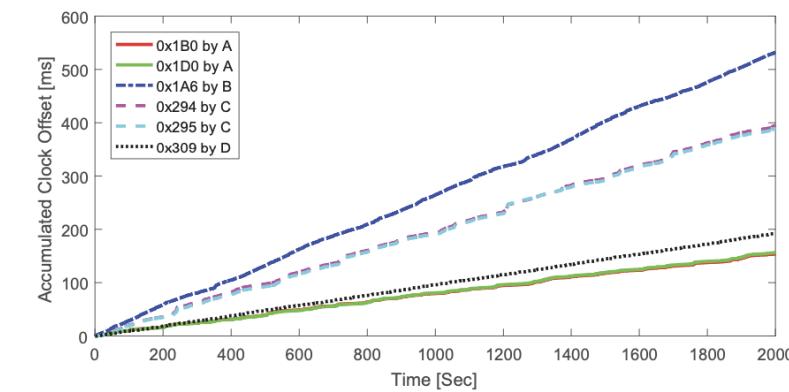


■ Clock-based IDS (Intrusion Detection System)

- 자동차 내부 네트워크에서 ECU가 CAN 통신 프로토콜을 이용하여 주기적으로 메시지를 전송할 때, ECU의 Clock 생성기의 하드웨어 특성이 미세하게 다르다는 점을 이용
 - 자동차 내부 네트워크의 여러 ECU들은 항상 자신들의 Unique한 clock으로 time을 counting하기 때문에, clock offset을 계속 누적하여 선형 그래프로 표현되고, 각 ECU의 선형 그래프는 고유의 기울기를 갖음
 - 이러한 선형 그래프의 기울기를 Clock Skew라고 하고, Clock Skew를 계산함으로서 ECU Fingerprinting이 가능해짐
- 즉, Clock Skew 기반의 ECU Fingerprinting 기술을 이용하여 CAN Traffic의 이상 유무를 판단



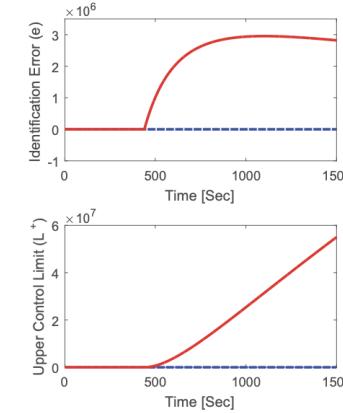
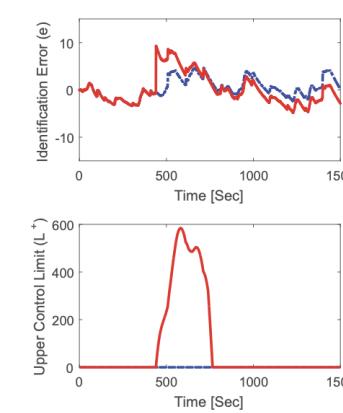
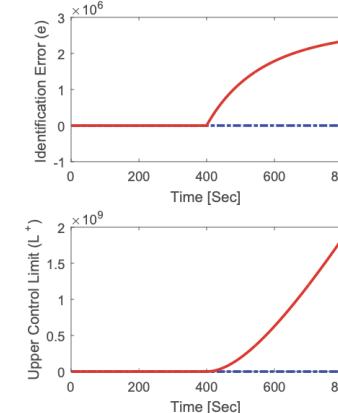
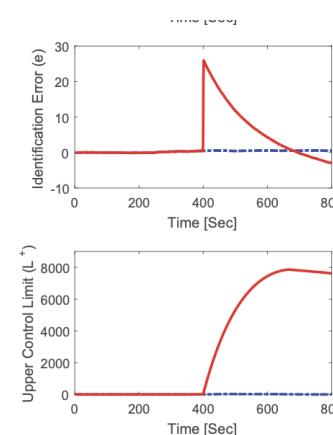
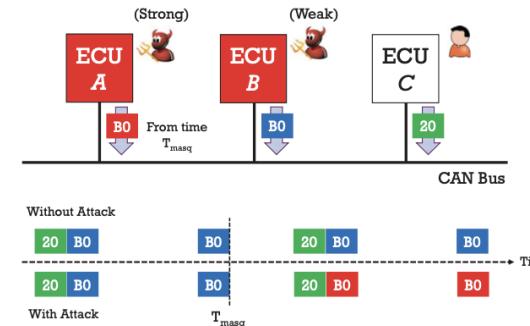
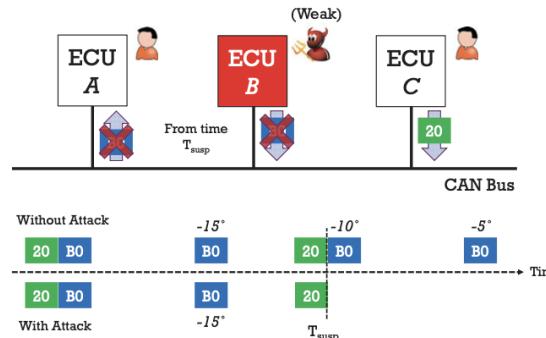
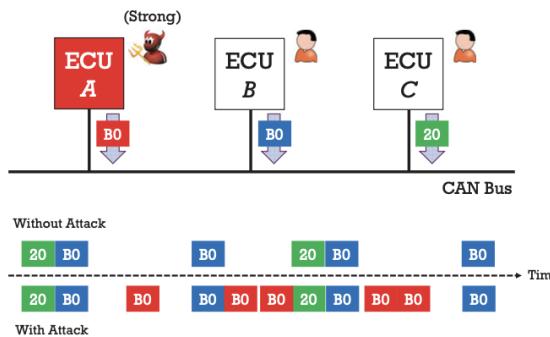
(a) CAN bus prototype.



(b) Honda Accord 2013.

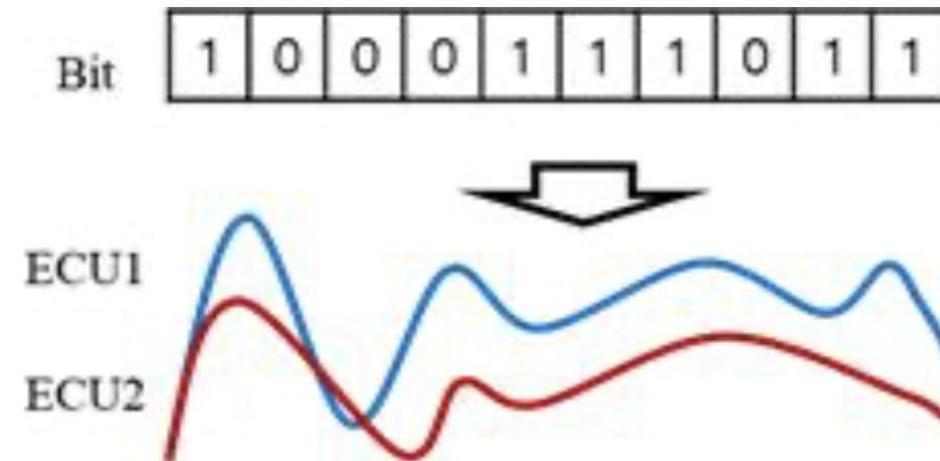
■ Clock-based IDS (cont'd)

- Representative Attack for in-vehicle



■ Voltage-based IDS

- ECU의 전력신호를 분석하여 Fingerprinting하는 기술을 Automotive IDS에 적용
 - CAN 통신 프로토콜은 CAN-H와 CAN-L라고 불리는 전기선에 전압차를 줌으로써 비트를 표현
 - 2가닥 전기선에 약 2.5v 전압차가 있다면 비트 0을 표현하고, 전압차가 없는 idle 상태라면 비트 1을 표현
 - 이처럼 비트 시퀀스를 아날로그 신호로 인코딩하는 signaling 과정에서 각 ECU의 하드웨어 특성으로 인해 아날로그 신호가 미세하게 차이 발생하며, 이러한 특징을 이용해 ECU Fingerprinting에 활용



[Ref] Choi, Wonsuk, et al. "VoltageIDS: Low-level communication characteristics for automotive intrusion detection system." IEEE Transactions on Information Forensics and Security 13.8 (2018): 2114-2129.

■ DATA 필드를 포함한 이상여부 탐지

- 대상 차량에 대해 보다 정확한 탐지 정확도
- 공격 탐지 결과에 대한 자세한 정보를 얻을 수 있음
 - 어떤 공격이 발생했는지? (DoS, Fuzzy, ...)
 - 무엇을 위한 공격인지? (차량 문 잠금,...)

■ DATA 필드를 제외한 이상여부 탐지

- 보다 빠른 탐지 속도
- 여러 차량에 대해 적용 가능한 범용적 방법론
- 종류
 - Time interval-based IDS
 - Entropy-based IDS

■ Time-interval based IDS

- 메시지 발생 주기를 이용해 공격 탐지
 - 차량 시스템에서 발생하는 Arbitration ID별 평균 메시지 발생 횟수 측정
 - 각 ID별 정상 수신 interval을 정의
 - 실제 메시지를 수신하면서, 임계 값 초과 시마다 Score 조정
 - Score가 과도하게 높아지면 주입 공격에 대한 경고를 알림

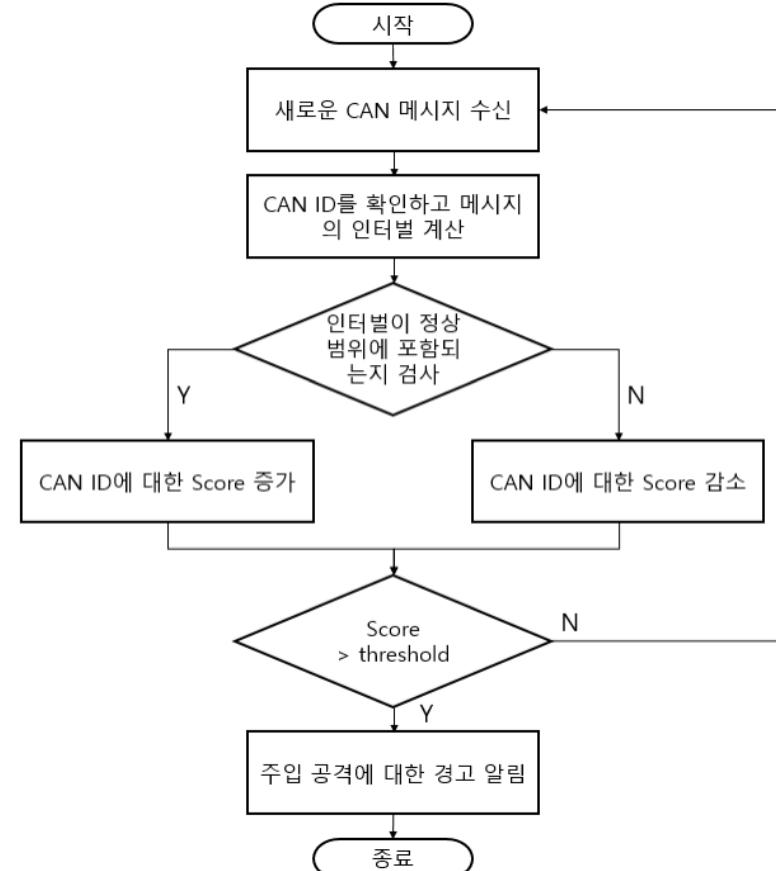
Normal Status: Immediate response (within reasonable time)

```
Timestamp: 0.651241 ID: 0153 100 | DLC: 0
Timestamp: 0.651485 ID: 0153 000 | DLC: 8 00 80 10 ff 00 ff 40 ce
```

Under Attack Status: Remote Frame 01F1 is requested but get no response (within reasonable time)

```
Timestamp: 0.254877 ID: 01f1 100 | DLC: 0
Timestamp: 0.255148 ID: 0080 000 | DLC: 8 00 17 c8 09 19 11 19 8d
Timestamp: 0.255230 ID: 0000 000 | DLC: 0
Timestamp: 0.255479 ID: 0081 000 | DLC: 8 7f 84 8e 00 00 00 00 bd
Timestamp: 0.255576 ID: 0000 000 | DLC: 0
Timestamp: 0.255824 ID: 018f 000 | DLC: 8 00 36 19 00 00 3f 00 00
Timestamp: 0.255922 ID: 0000 000 | DLC: 0
```

(In general, offset is within 5, Time Interval is 0.001196 by car vendor's default setting.)



■ Entropy-based IDS

- 대상 차량 내 모든 메시지 ID에 대한 엔트로피(H')를 계산
- DoS 공격 시 내부 네트워크의 엔트로피가 감소함에 따라 공격을 탐지
- DoS 공격 시 특정 ID에 대한 점유율이 올라가기 때문에 불확실성이 낮아짐을 확인
- 특정 ID와 CAN Bus에서 사용되지 않은 ID들을 이용하여 임의의 메시지들을 삽입할 경우 불확실성은 증가하여 엔트로피 값은 높아지는 것을 확인
- 따라서 엔트로피 값의 정상 범위를 의미하는 상한선과 하한선을 지정하고 시간 단위 별 엔트로피 값을 모니터링하는 이상 탐지 시스템을 설계

$$H' = - \sum_{i=1}^n p_i \log p_i$$

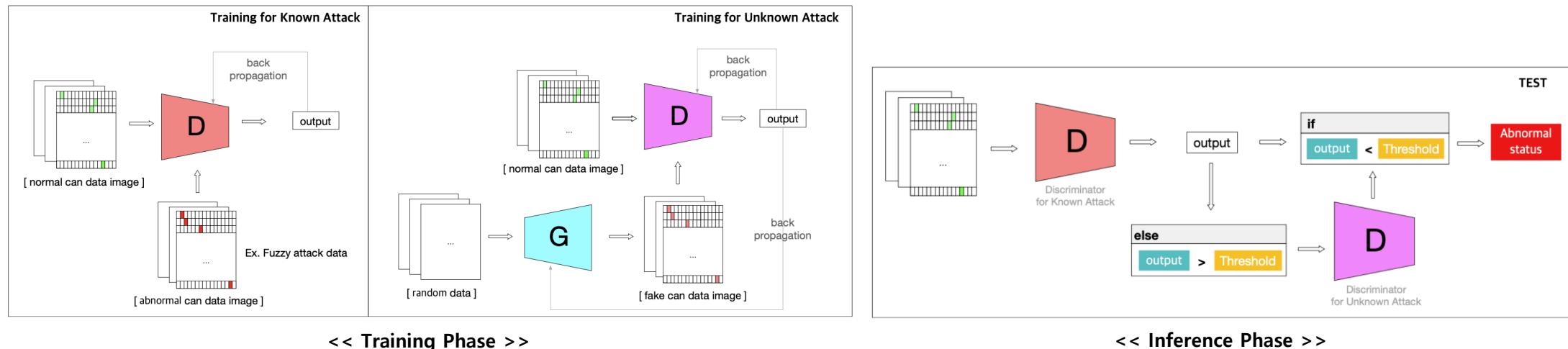
n : 차량 내부 네트워크에서 사용되는 CAN ID 수
 p_i : 전체 메시지 중 특정 CAN ID의 비율 ($0 \leq p_i \leq 1$)

CAN ID	사용 횟수	p_i	$\log p_i$	H^i
0x153	2	0.003 ↓	-5.81 ↑	
0x164	8	0.012 ↓	-4.42 ↑	
0x2c0	6	0.009 ↓	-4.71 ↑	
	...			
0x000	284	0.850 ↑	-0.160 ↓	

점차 낮아짐

■ AI based IDS

- GAN based IDS
 - To respond unknown attacks, GAN can be one of the best solution to detect undiscovered/unknown attacks
 - Known attack detection
 - ✓ Training the 1st discriminator using known attack and normal data
 - Unknown attack detection
 - ✓ Training the 2nd discriminator using only normal data without attack data
 - ✓ The 2nd discriminator is trained to distinguish between real data and fake data



[Ref] Seo, Eunbi, Hyun Min Song, and Huy Kang Kim. "GIDS: GAN based intrusion detection system for in-vehicle network." 2018 16th Annual Conference on Privacy, Security and Trust (PST). IEEE, 2018.

■ AI based IDS

- **Automotive Ethernet에 대한 요구사항**
 - **잡음:** 통신 회선에서 잡음을 적게 방출시켜야 하며, 외부로부터의 잡음에 robust 해야함
 - **우선 순위:** 전달되는 payload의 우선순위를 매길 수 있어야 하며, 해당 payload는 반드시 정해진 시간 내에 처리되어야 함
 - ✓ Powertrain 계열의 데이터는 다른 데이터보다 우선 처리하여 반드시 예상되는 지연시간 내에 도착해야 함
 - ✓ Powertrain 관련 데이터를 기존처럼 Best-effort로 처리하면, 자동차의 특성상 사고 발생 가능성 존재
 - **대역폭 예약:** 특정 서비스를 위해 사용 가능한 대역폭의 일부를 항상 사용 가능하도록 유지해야 함
 - ✓ ADAS와 연동된 카메라는 항상 일정한 스트림을 유지하여 처리 장치에 영상 정보를 전달해야 함
 - ✓ 오디오 데이터는 항상 일정한 대역폭을 사용해 스피커에 데이터를 전달해야 함
 - **동기화:** 동일 네트워크로 연결된 장치들은 매우 적은 오차로 시간을 맞출 수 있어야 함
 - ✓ ADAS와 연동된 여러 센서들의 데이터는 정확한 시간으로 동기화 되어야 올바른 처리가 가능함
 - ✓ 차량에 탑재된 10개 이상의 스피커는 동시에 같은 소리를 재생할 수 있어야 함

No	분류	공격유형	설명
1	Availability	DoS attack	<ul style="list-style-type: none"> PHY, DLL상의 collision을 발생시켜 통신을 자연시킬 수 있음 동일한 회선으로 연결된 모든 노트가 통신을 멈추게 됨 가용성을 저하시키거나 통신을 무력화 시킬 수 있음
2	Integrity	Replay attack	<ul style="list-style-type: none"> 회선에서 발생된 패킷을 저장해 두었다가 이후 재 발송 재송신된 데이터가 UDP 세그먼트인 경우 상위 계층에 그대로 영향을 미침 재송신된 데이터가 TCP 세그먼트인 경우 통신 단절을 유도할 수 있음
3		Fuzzing attack	<ul style="list-style-type: none"> 공격자는 차량에서 사용되는 MACAddr, IPAddr을 임의로 설정하여 프레임/패킷 발송 차량에서 사용되는 임의의 주소 정보에 세그먼트만 임의로 설정하여 전송
4		Impersonation attack	<ul style="list-style-type: none"> ARP Spoofing 등의 공격을 통해 데이터가 원래 전달되어야 할 곳으로 향하지 않도록 함 이후 공격 노드가 두 노드 사이의 중간자로 활동하고 정상 노드로 위장할 수 있음
5	Confidentiality	Packet snipping	<ul style="list-style-type: none"> 물리적 접근이 가능한 노드는 데이터를 자유롭게 읽을 수 있음 상위 계층에서 SSL/TLS가 적용된 Payload를 제외하고 모두 평문이 노출됨

- I. SDV 개념의 확산으로 인해 E/E Architecture가 점차 중앙 집중형으로 변화됨에 따라 보안 위협은 더욱 커질 것
- II. 자동차를 대상으로 하는 공격은 주로 네트워크와 센서를 이용하는 공격이 많음. 최근에는 자율주행 자동차의 센서 공격에 대한 연구가 많아지고 있음.
- III. 대응 방안에 대한 연구는 크게 두 가지로 구분되어 진행됨
 - ✓ 자동차 취약점 분석 및 위협 시나리오 개발 (Automotive VAS and Exploit Scenarios)
 - ✓ 위협 탐지 시스템 (Intrusion Detection System)

Thank You



- Lab: <https://mose.kookmin.ac.kr>
- Email: sh.jeon@kookmin.ac.kr