Automated Cross-Platform Reverse Engineering of CAN Bus Commands From Mobile Apps

Haohuang Wen[1] , Qingchuan Zhao[1] , Qi Alfred Chen[2] , and Zhiqiang Lin[1]

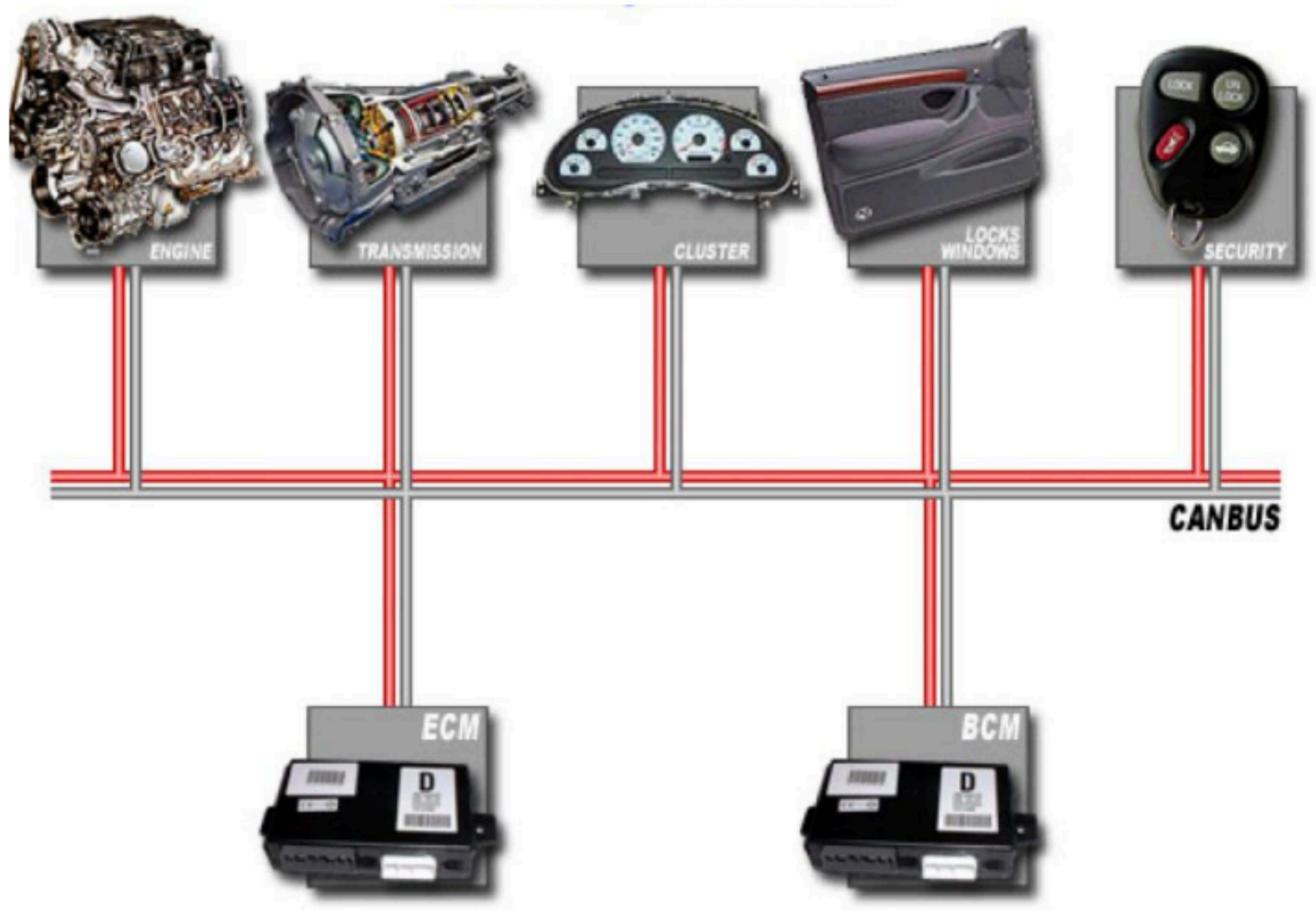
Ohio State University[1]
University of California, Irvine[2]

Presented by: Yuan Gao
10/18/2022

Acknowledgments: Some slide material derived from authors.

Introduction

In-vehicle Network and CAN Bus



Control Area Network (CAN) bus.

SOF	Identifier	RTR	IDE	DLC	Data Field								CRC	ACK	EOF
					Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7			

CAN bus command.

Applications of CAN Bus Commands

Driver Behavior Monitoring

An On Board Diagnostic (OBD-II) dongle, used by insurance company Progressive to monitor driver behavior

Vehicle Control

An In-Vehicle Infotainment (IVI) system.

Applications of CAN Bus Commands

- recently on Autonomous Driving

TESLA

WAYMO

THE
AUTOWARE
FOUNDATION

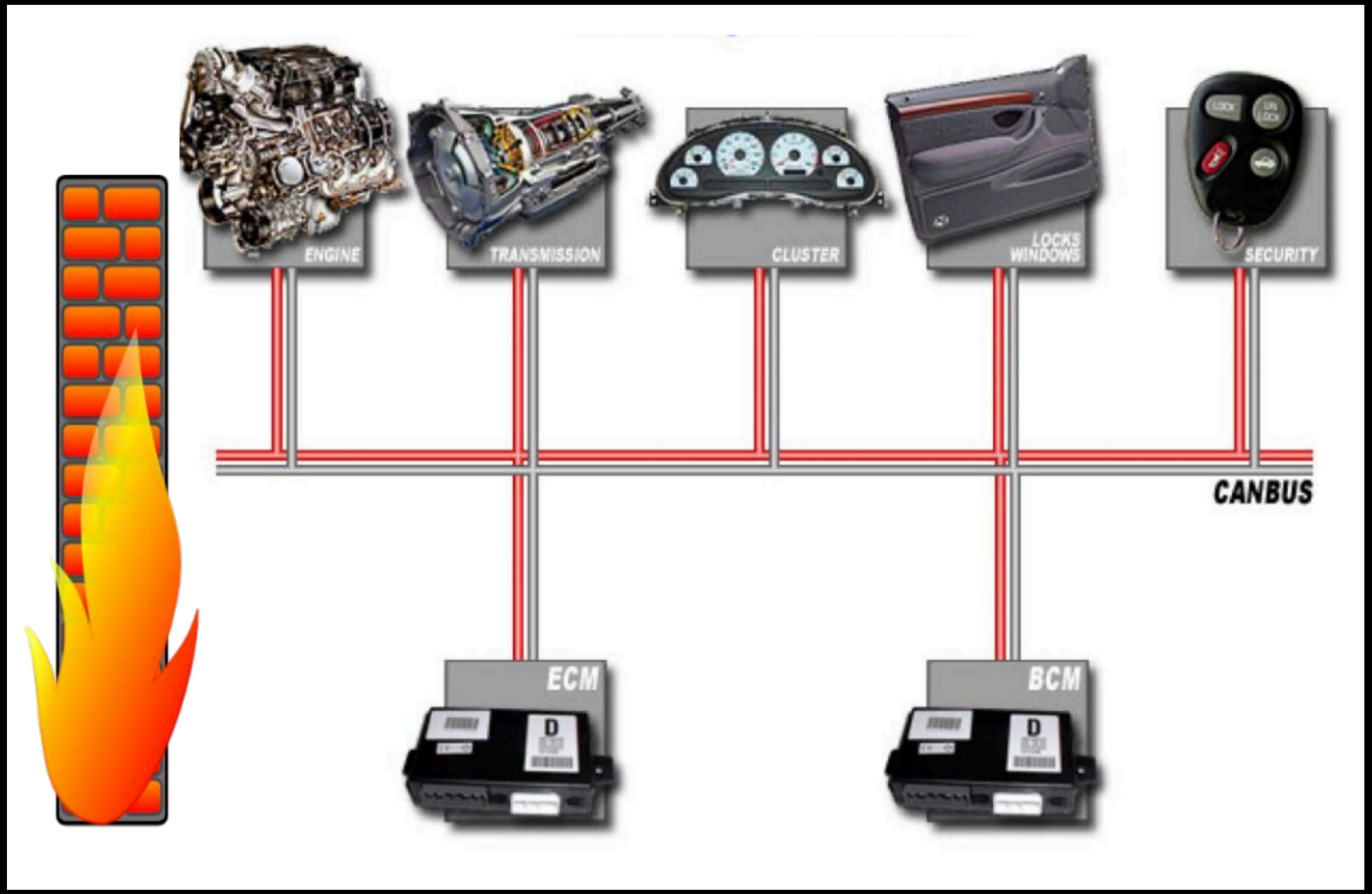
Applications of CAN Bus Commands

- Security

Vehicle Hacking

The Jeep Cherokee hacking

Vehicle Security Monitoring

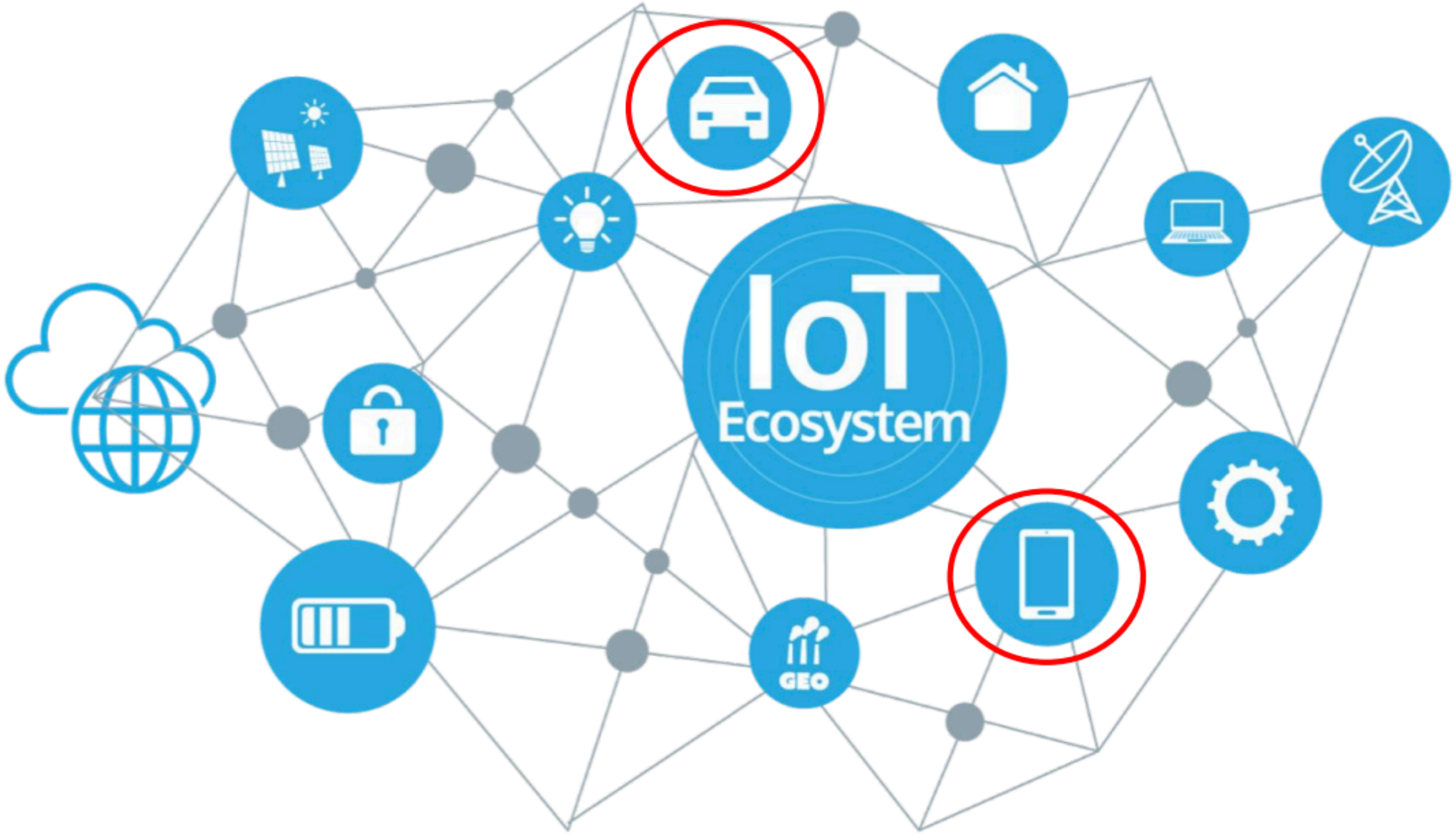


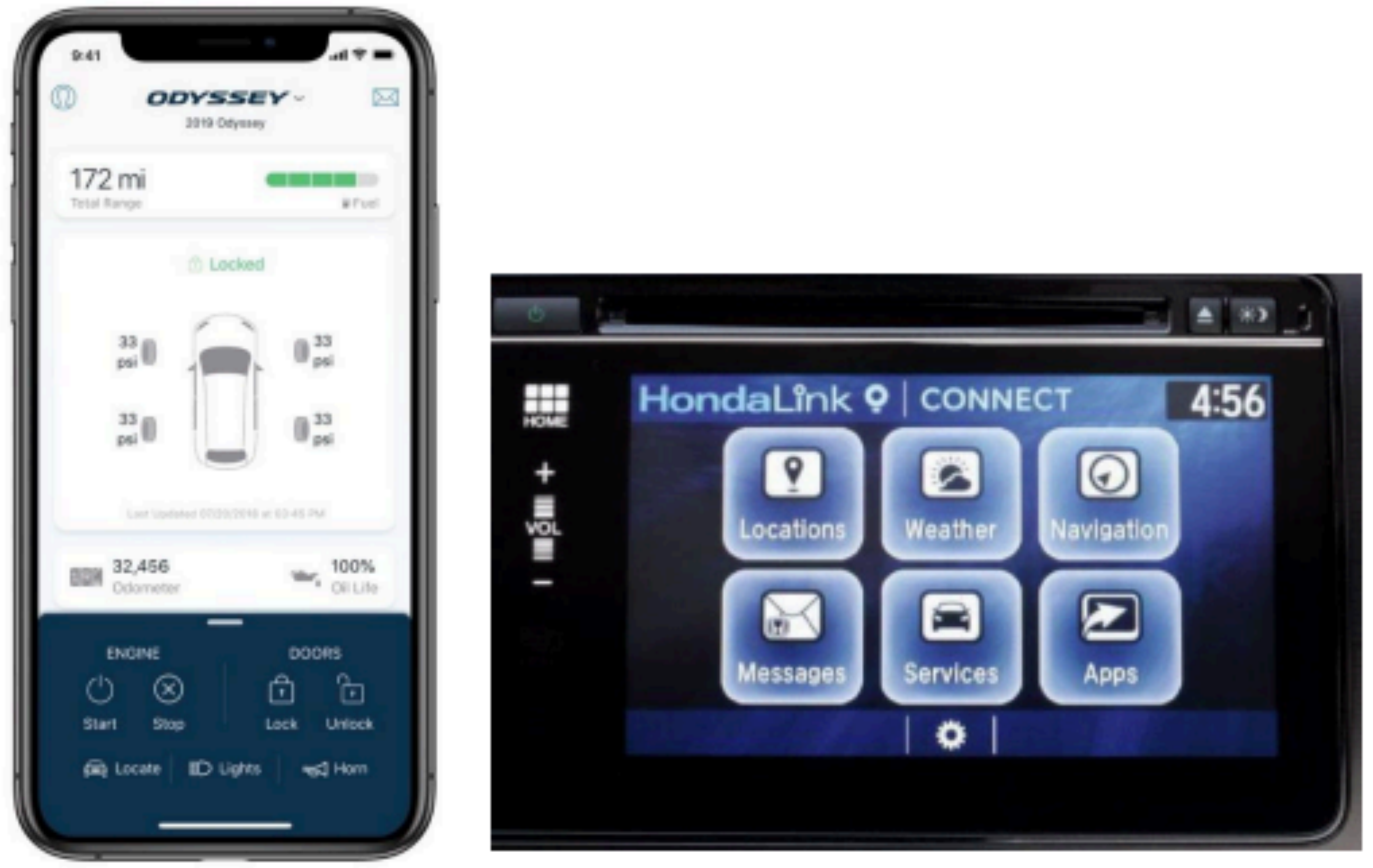
CAN Bus Firewall

Reverse Engineering of CAN Bus Commands

- **State-of-the-art**
  - Fuzzing with random CAN bus commands
  - Manually triggering physical actions and observing the CAN bus
- **Shortcoming**
  - **Limited scalability:** CAN bus commands are highly customized and diversified
  - **Excessive cost:** Significant manual effort and real automobiles are required

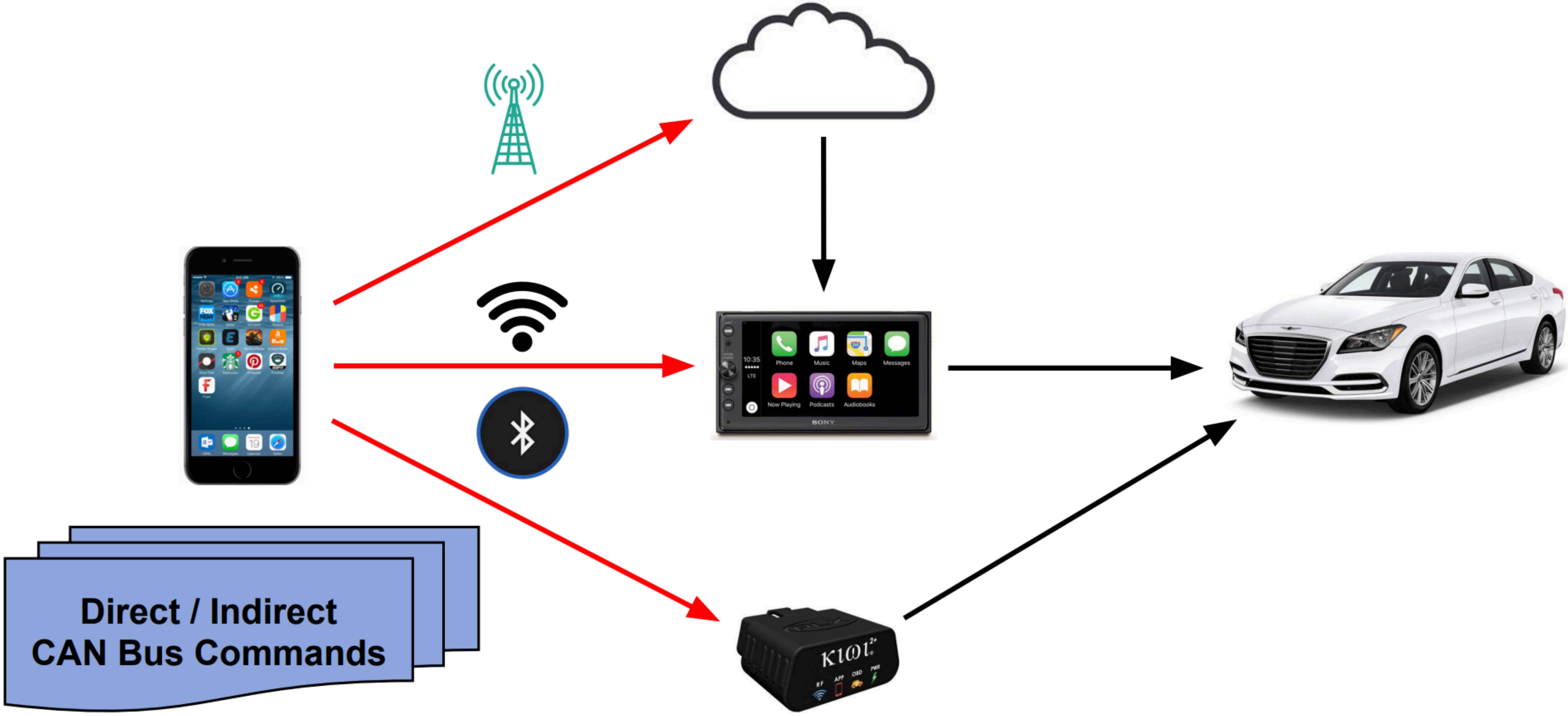
Observation





IVI App

OBD-II Dongle App



Direct / Indirect
CAN Bus Commands

Contributions

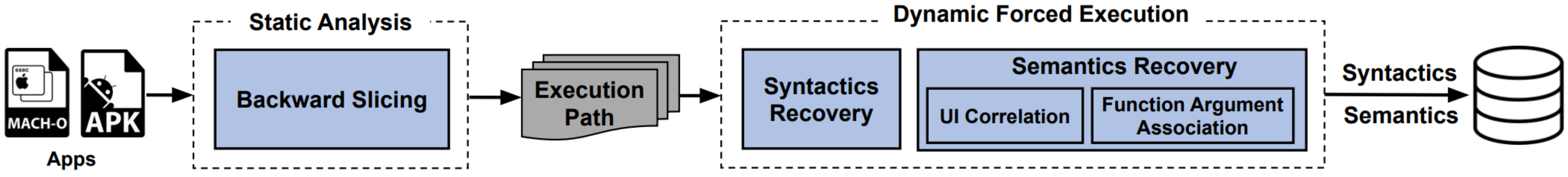
- **Novel Approach:** Authors propose a cost-effective and automatic approach for reverse engineering CAN bus commands through analyzing mobile apps.
- **Effective Techniques:** Authors design a suite of effective techniques to uncover CAN bus command syntactics (structure and format) and semantics (meaning and functionality).
- **Implementation and Evaluation:** Authors implemented CANHunter on both Android and iOS platforms, and evaluated it with 236 car mobile apps. It discovered 182619 unique CAN bus commands in which 86.1% of them are recovered with semantics.

CANHunter

Challenges and Insights

- **Challenges**
  - Precisely identify CAN bus command execution path
  - Command syntactics recovery
  - Command semantics recovery
- **Solutions**
  - Identify execution path with **backward program slicing**
  - Syntactics recovery with **dynamic forced execution**
  - Semantics recovery with **UI correlation** and **function argument association**

Overview of CANHunter



exec

MACH-O

APK

Apps

Static Analysis

Backward Slicing

Execution Path

Dynamic Forced Execution

Syntactics Recovery

Semantics Recovery

UI Correlation

Function Argument Association

Syntactics

Semantics

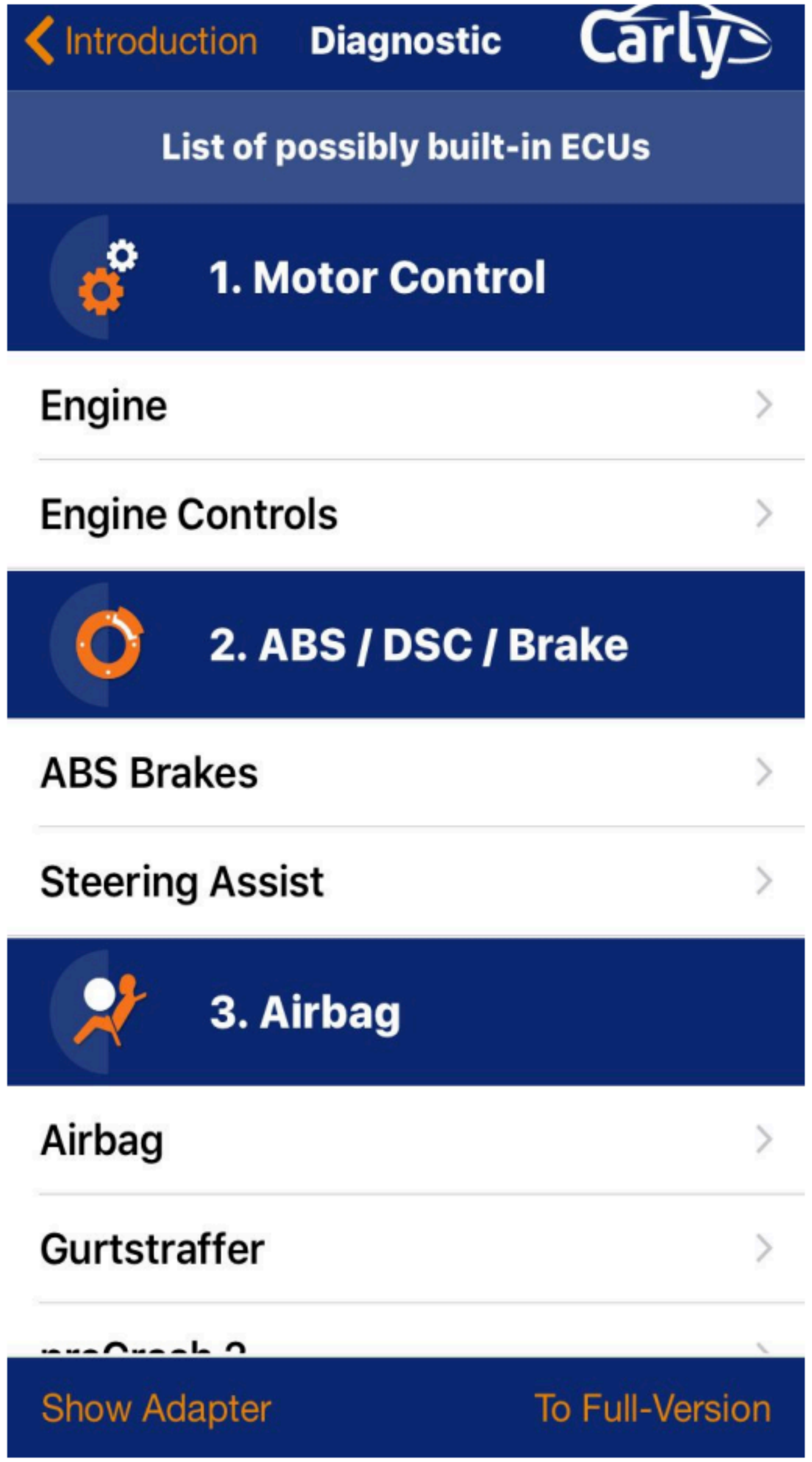
Backward Slicing

```
Screen_Info_Diag.viewDidLoad()
v4 = UIButton()
v4.setText(“Engine Controls”)
...
v4.addTarget(v4,”initECUs”)
// register button trigger function
```

```
MD_AllECUsToyota.initECUs()
v12.initWithRequestId(“0x7E0”,”Engine Controls”)
v12.frageID = ”0x7E0”
...
v22 = BaseFahrzeug.initWithName(“Corolla VIII”)
v22.ECU = v12
...
v25 = v24.createWorkableECUKategorie(v22)
```

```
WorkableModell.createWorkableECUKategorie(a3)
...
v6 = a3
v7 = v6.ECU.frageID
...
v8 = v7.substring(2,5)
v9 = NSString.stringWithForamt(“%@ 30 00 02”,v8)

...
v5.writeValue(v9,v14,1) // Target API
```



Introduction Diagnostic Carly

List of possibly built-in ECUs

1. Motor Control

Engine

Engine Controls

2. ABS / DSC / Brake

ABS Brakes

Steering Assist

3. Airbag

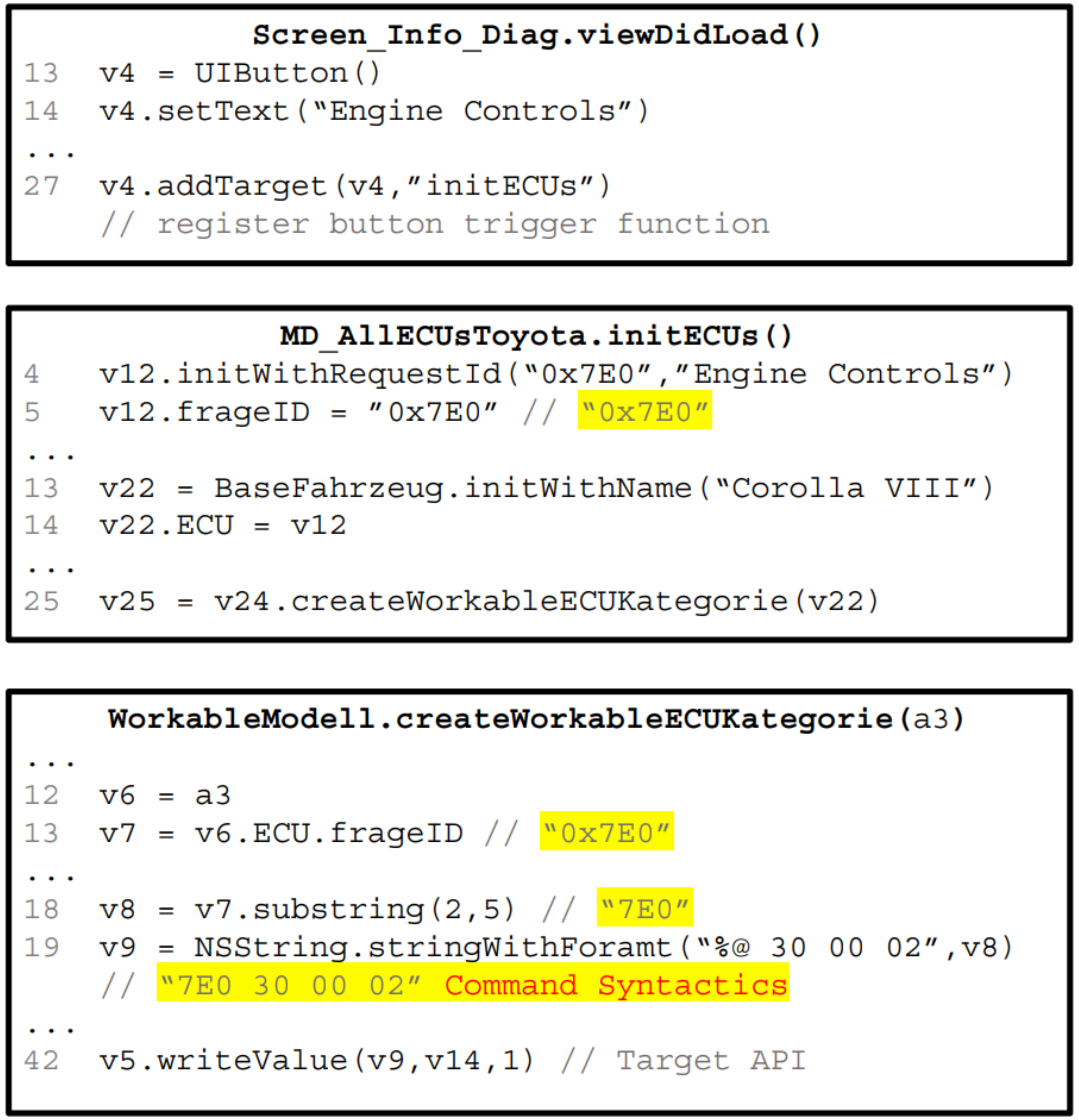
Airbag

Gurtstraffer

preCrash 2

Show Adapter To Full-Version

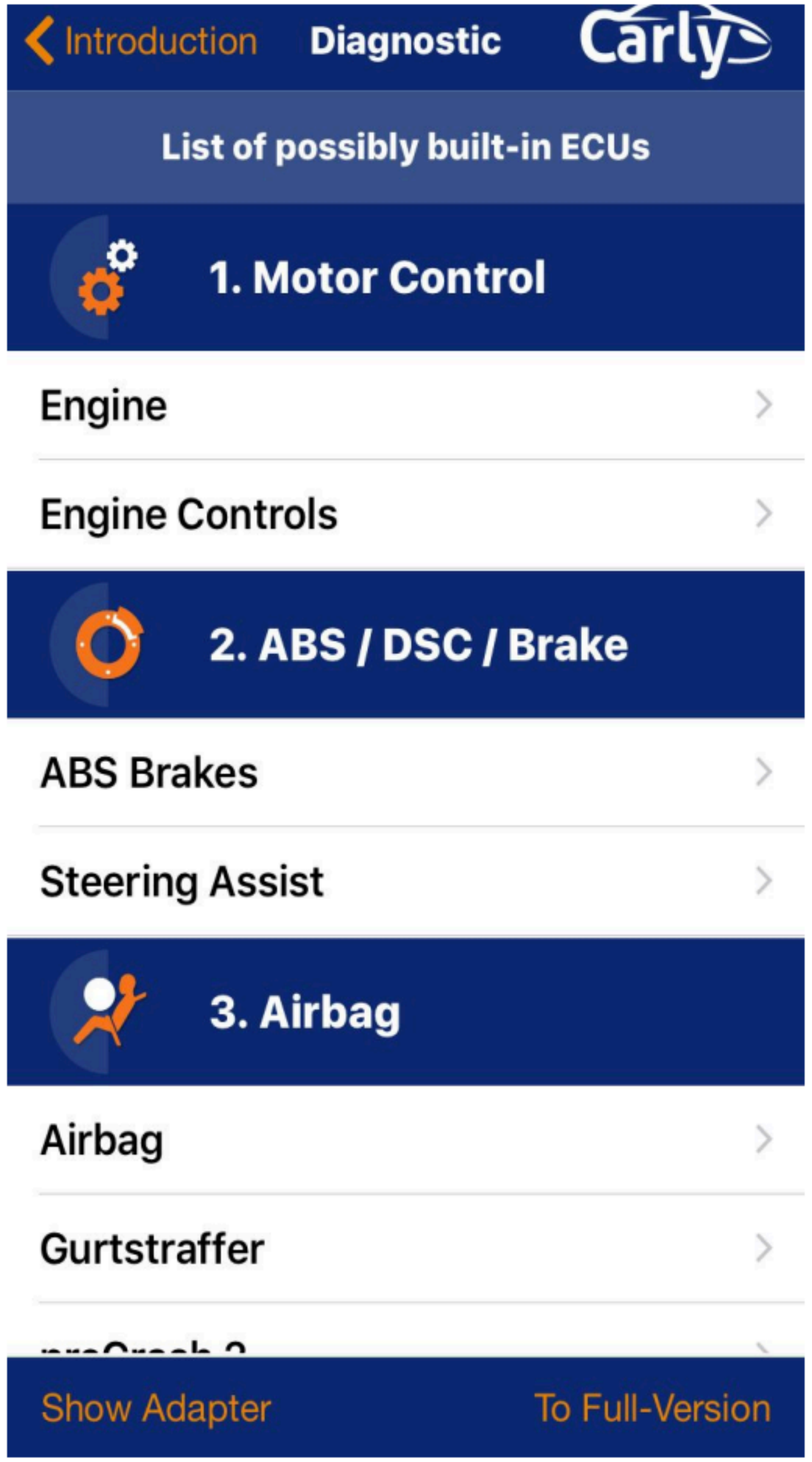
Syntactics Recovery



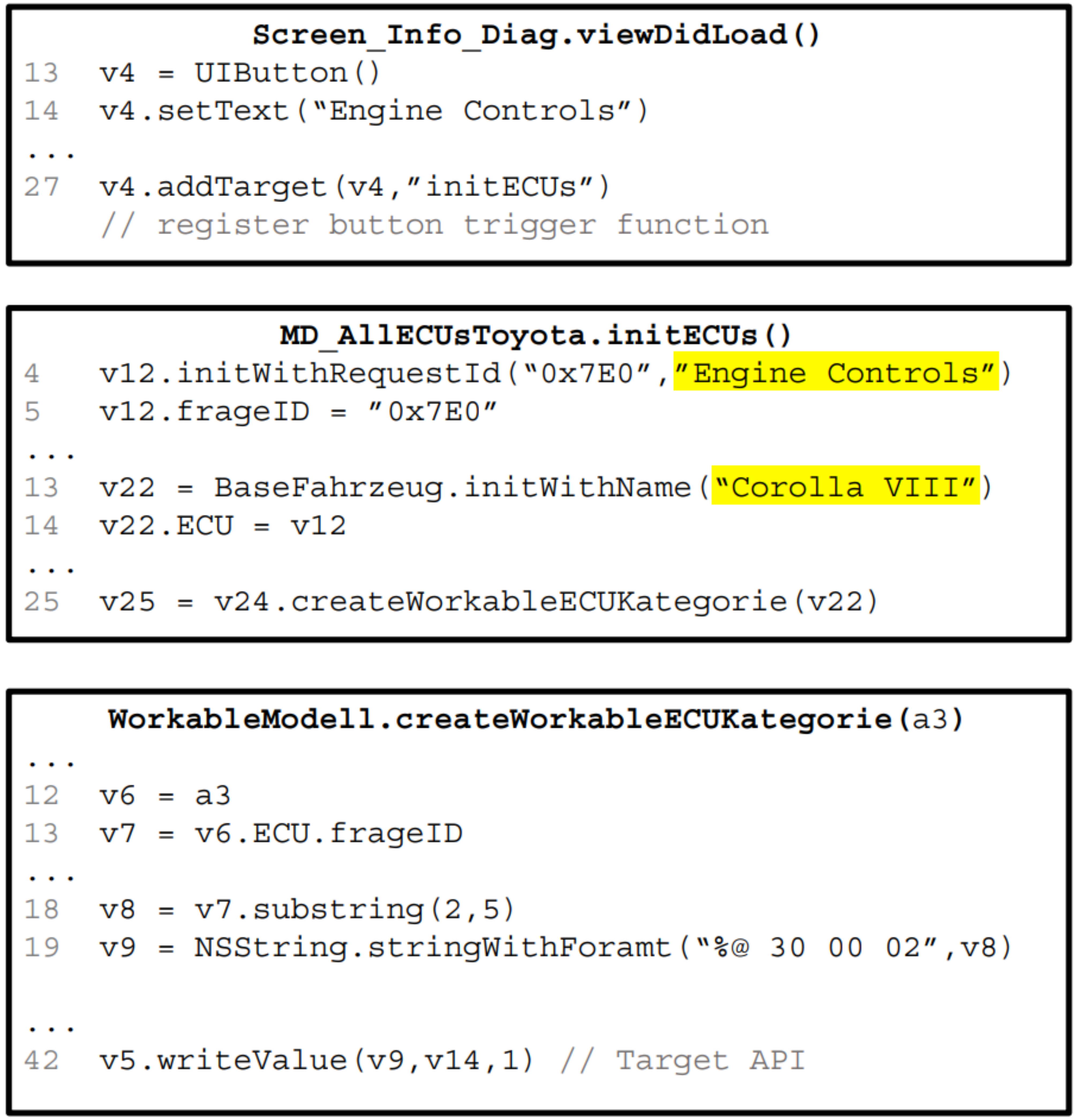
```
Screen_Info_Diag.viewDidLoad()
v4 = UIButton()
v4.setText("Engine Controls")
...
v4.addTarget(v4,"initECUs")
// register button trigger function
```

```
MD_AllECUsToyota.initECUs()
v12.initWithRequestId("0x7E0","Engine Controls")
v12.frageID = "0x7E0" // "0x7E0"
...
v22 = BaseFahrzeug.initWithName("Corolla VIII")
v22.ECU = v12
...
v25 = v24.createWorkableECUKategorie(v22)
```

```
WorkableModell.createWorkableECUKategorie(a3)
...
v6 = a3
v7 = v6.ECU.frageID // "0x7E0"
...
v8 = v7.substring(2,5) // "7E0"
v9 = NSString.stringWithForamt("%@ 30 00 02",v8)
// "7E0 30 00 02" Command Syntactics
...
v5.writeValue(v9,v14,1) // Target API
```



Semantics Recovery

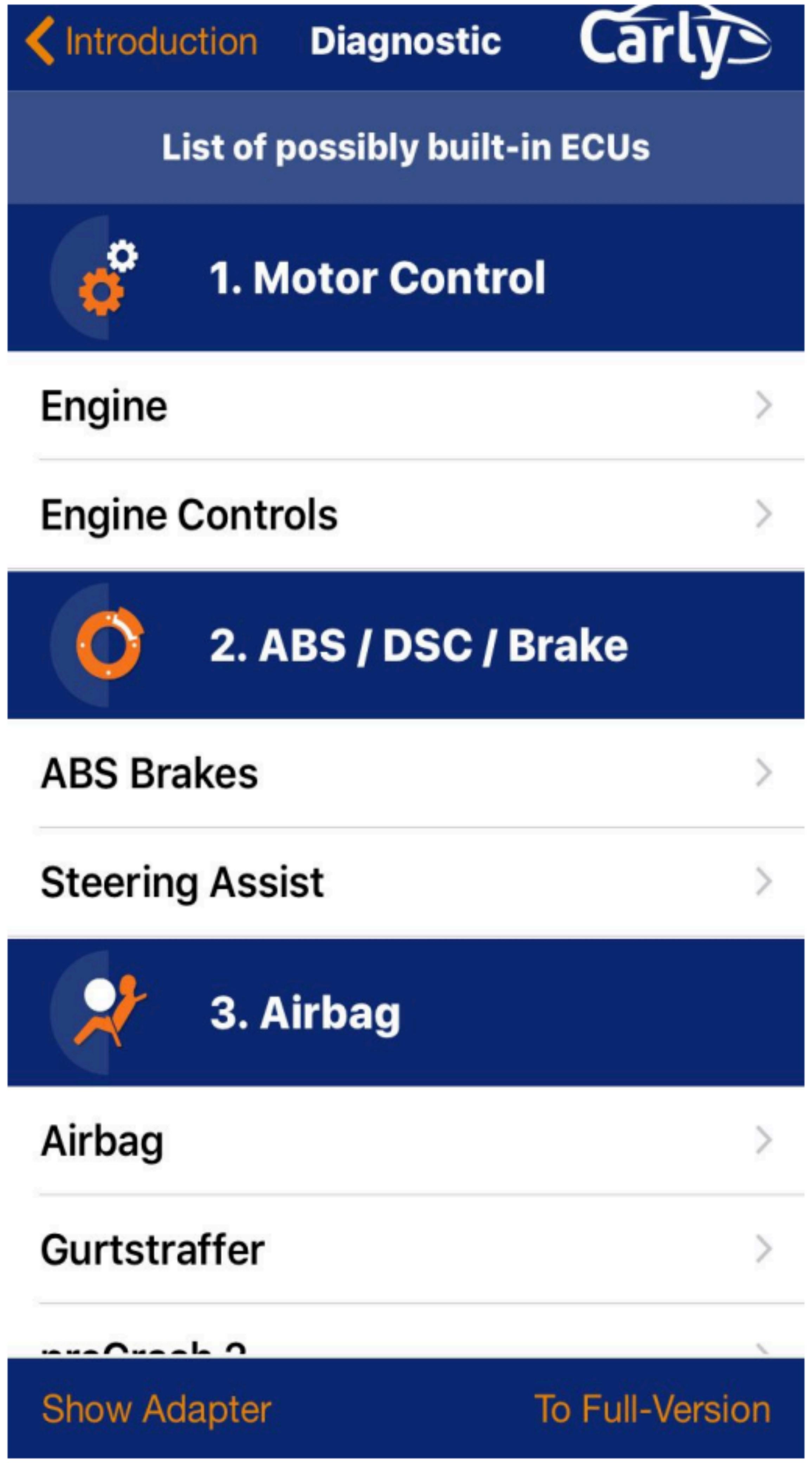


```
Screen_Info_Diag.viewDidLoad()
v4 = UIButton()
v4.setText(“Engine Controls”)
...
v4.addTarget(v4,”initECUs”)
// register button trigger function
```

```
MD_AllECUsToyota.initECUs()
v12.initWithRequestId(“0x7E0”,”Engine Controls”)
v12.frageID = ”0x7E0”
...
v22 = BaseFahrzeug.initWithName(“Corolla VIII”)
v22.ECU = v12
...
v25 = v24.createWorkableECUKategorie(v22)
```

```
WorkableModell.createWorkableECUKategorie(a3)
...
v6 = a3
v7 = v6.ECU.frageID
...
v8 = v7.substring(2,5)
v9 = NSString.stringWithForamt(“%@ 30 00 02”,v8)

...
v5.writeValue(v9,v14,1) // Target API
```

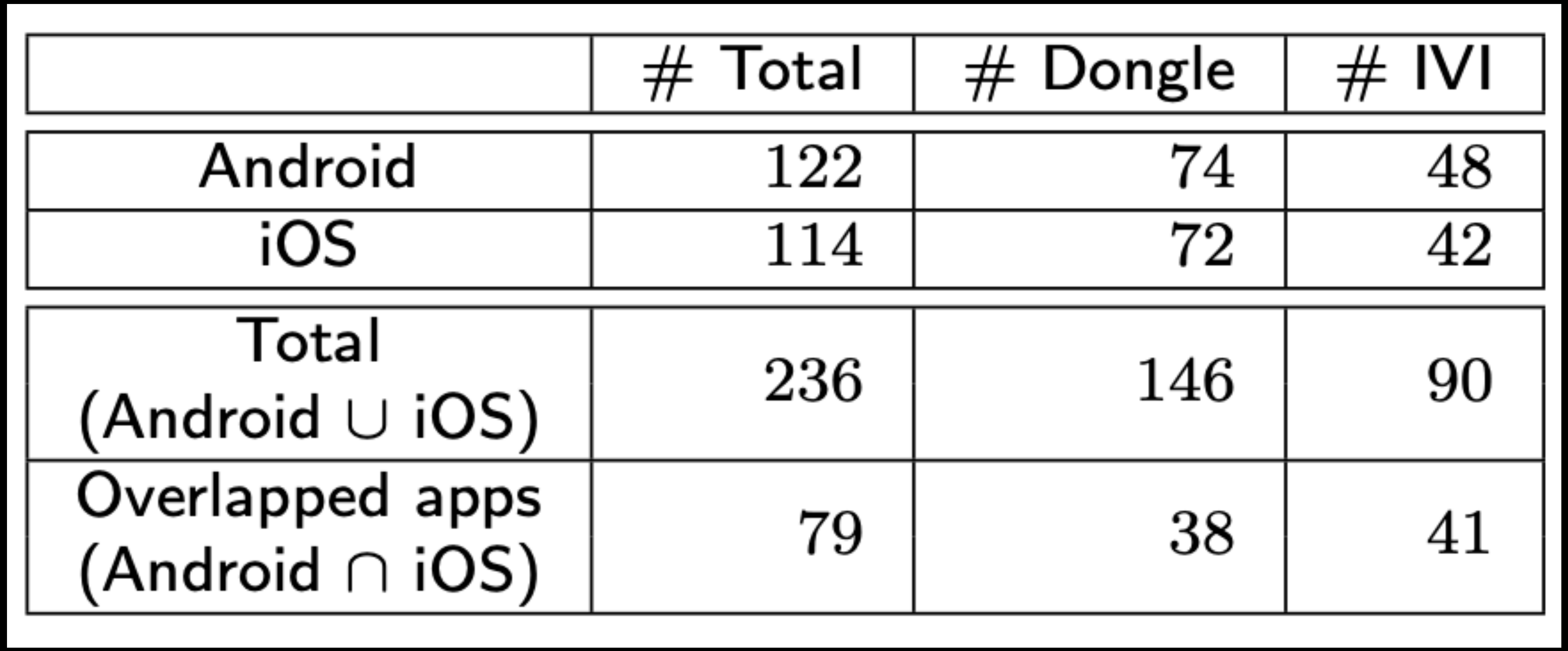


Evaluation

Result Characteristics

- App Categories

- Crawled 236 vehicle apps in April 2019
- 182619 CAN bus commands are discovered
- 107 apps expose direct CAN bus commands
- 109 apps expose indirect commands
- 20 apps are obfuscated



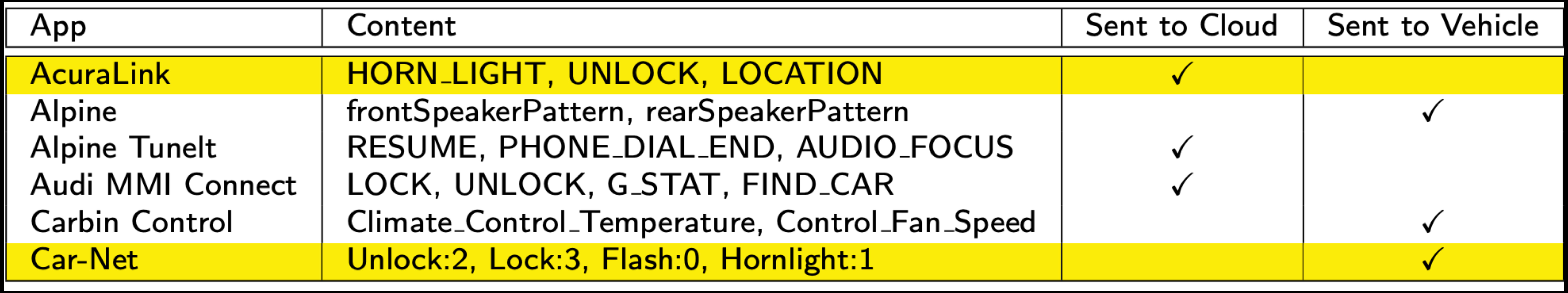
	# Total	# Dongle	# IVI
Android	122	74	48
iOS	114	72	42
Total (Android ∪ iOS)	236	146	90
Overlapped apps (Android ∩ iOS)	79	38	41

Table: Distribution of collected apps

Result Characteristics

- App Categories

- Indirect (i.e., Interpreted) CAN Commands
  - IVI apps usually use interpreted commands for vehicle control
  - Interpreted commands are usually strings or numbers



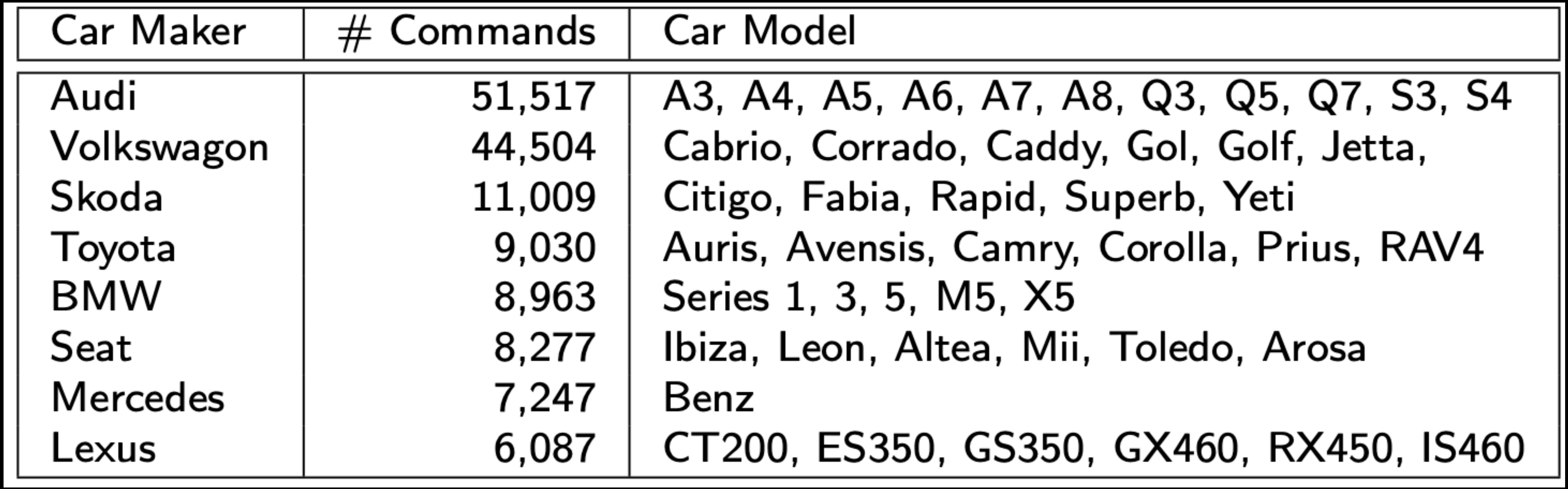
App	Content	Sent to Cloud	Sent to Vehicle
AcuraLink	HORN_LIGHT, UNLOCK, LOCATION	✓	
Alpine	frontSpeakerPattern, rearSpeakerPattern		✓
Alpine TuneIt	RESUME, PHONE_DIAL_END, AUDIO_FOCUS	✓	
Audi MMI Connect	LOCK, UNLOCK, G_STAT, FIND_CAR	✓	
Carbin Control	Climate_Control_Temperature, Control_Fan_Speed		✓
Car-Net	Unlock:2, Lock:3, Flash:0, Hornlight:1		✓

Table: Interpreted commands from IVI apps.

Result Characteristics

- Car Models

- identify CAN bus commands from over 360 car models across 21 car makers



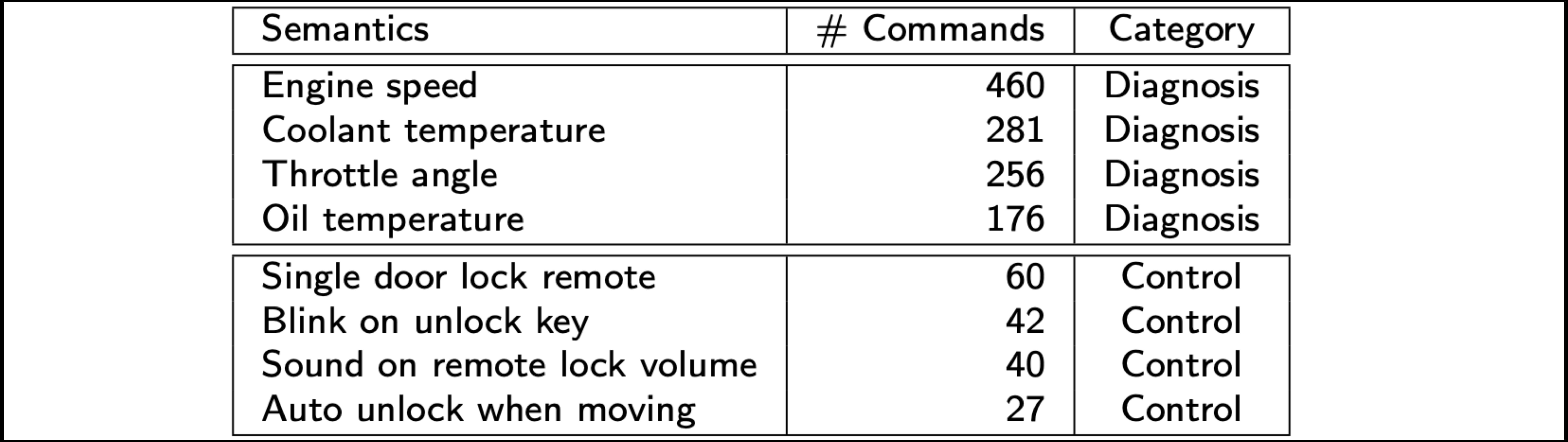
Car Maker	# Commands	Car Model
Audi	51,517	A3, A4, A5, A6, A7, A8, Q3, Q5, Q7, S3, S4
Volkswagon	44,504	Cabrio, Corrado, Caddy, Gol, Golf, Jetta,
Skoda	11,009	Citigo, Fabia, Rapid, Superb, Yeti
Toyota	9,030	Auris, Avensis, Camry, Corolla, Prius, RAV4
BMW	8,963	Series 1, 3, 5, M5, X5
Seat	8,277	Ibiza, Leon, Altea, Mii, Toledo, Arosa
Mercedes	7,247	Benz
Lexus	6,087	CT200, ES350, GS350, GX460, RX450, IS460

Table: Distribution of CAN Bus commands over part of car makers

Result Characteristics

- Semantics

- 157296 (86.1%) CAN bus commands are recovered with semantics
- The semantics can be categorized into diagnosis and vehicle control



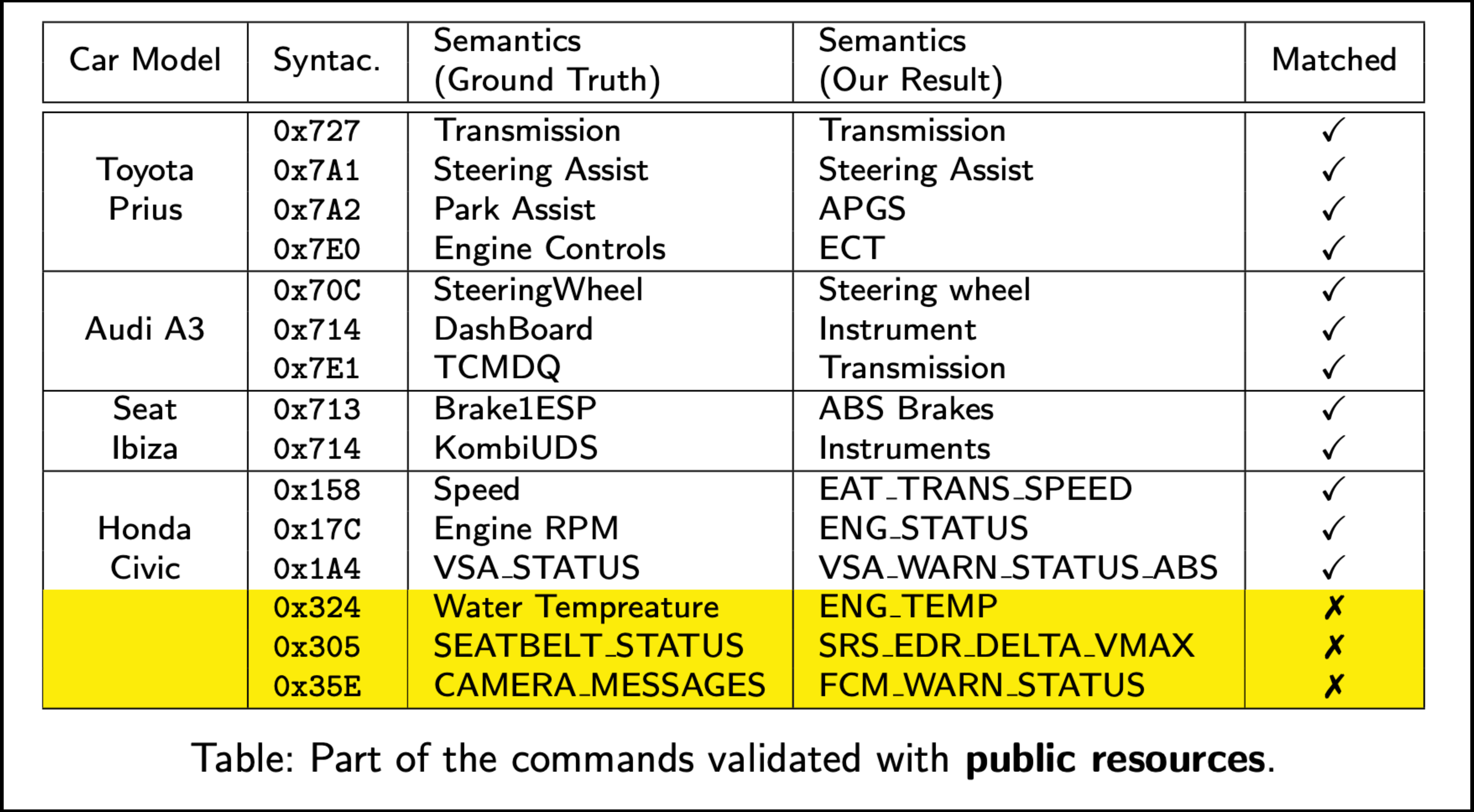
Semantics	# Commands	Category
Engine speed	460	Diagnosis
Coolant temperature	281	Diagnosis
Throttle angle	256	Diagnosis
Oil temperature	176	Diagnosis
Single door lock remote	60	Control
Blink on unlock key	42	Control
Sound on remote lock volume	40	Control
Auto unlock when moving	27	Control

Table: Distribution of CAN bus commands over part of semantics

Correctness Evaluation

- Over 70% of the command syntactics and semantics are validated
- They tried the following three sources for validation:
  - Public resource
  - Cross validation
  - Real car testing

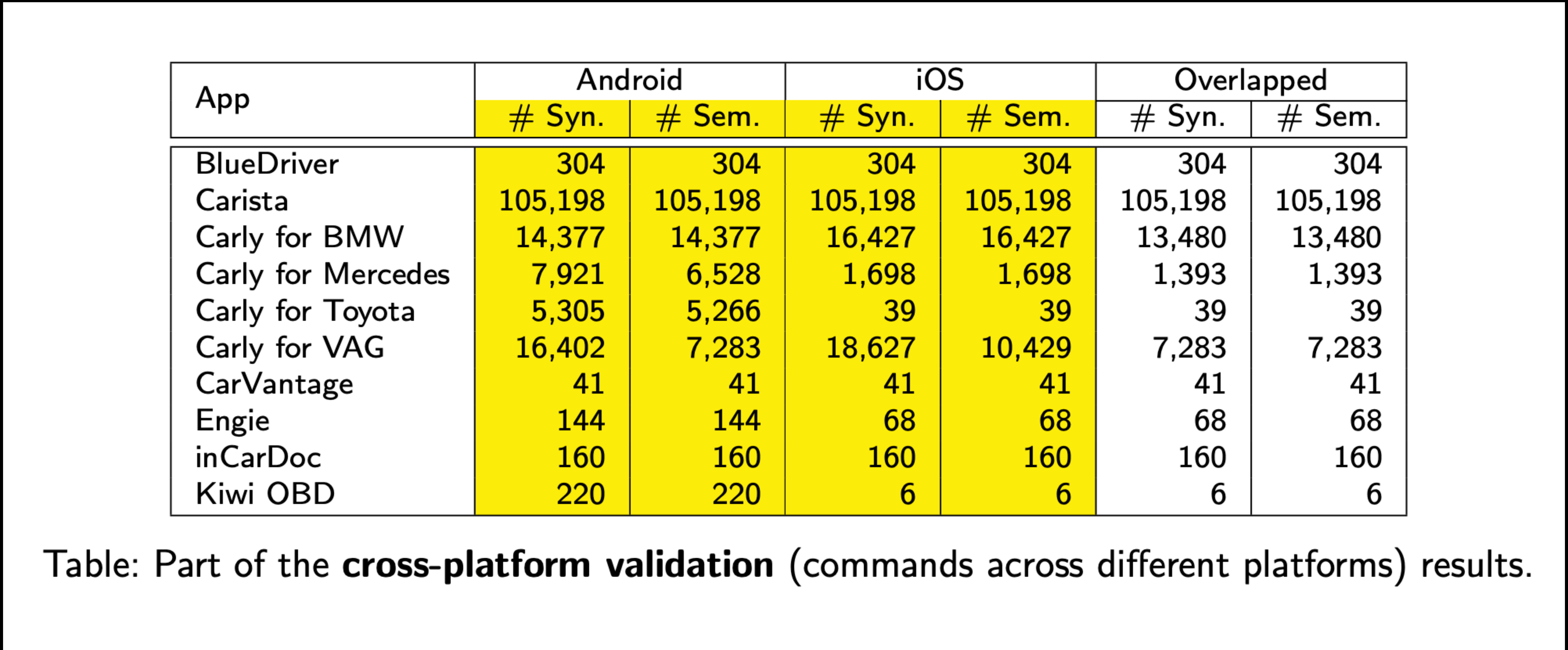
Correctness Evaluation



Car Model	Syntac.	Semantics (Ground Truth)	Semantics (Our Result)	Matched
Toyota Prius	0x727	Transmission	Transmission	✓
	0x7A1	Steering Assist	Steering Assist	✓
	0x7A2	Park Assist	APGS	✓
	0x7E0	Engine Controls	ECT	✓
Audi A3	0x70C	SteeringWheel	Steering wheel	✓
	0x714	DashBoard	Instrument	✓
	0x7E1	TCMDQ	Transmission	✓
Seat Ibiza	0x713	Brake1ESP	ABS Brakes	✓
	0x714	KombiUDS	Instruments	✓
Honda Civic	0x158	Speed	EAT_TRANS_SPEED	✓
	0x17C	Engine RPM	ENG_STATUS	✓
	0x1A4	VSA_STATUS	VSA_WARN_STATUS_ABS	✓
	0x324	Water Tempreature	ENG_TEMP	✗
	0x305	SEATBELT_STATUS	SRS_EDR_DELTA_VMAX	✗
	0x35E	CAMERA_MESSAGES	FCM_WARN_STATUS	✗

Table: Part of the commands validated with **public resources**.

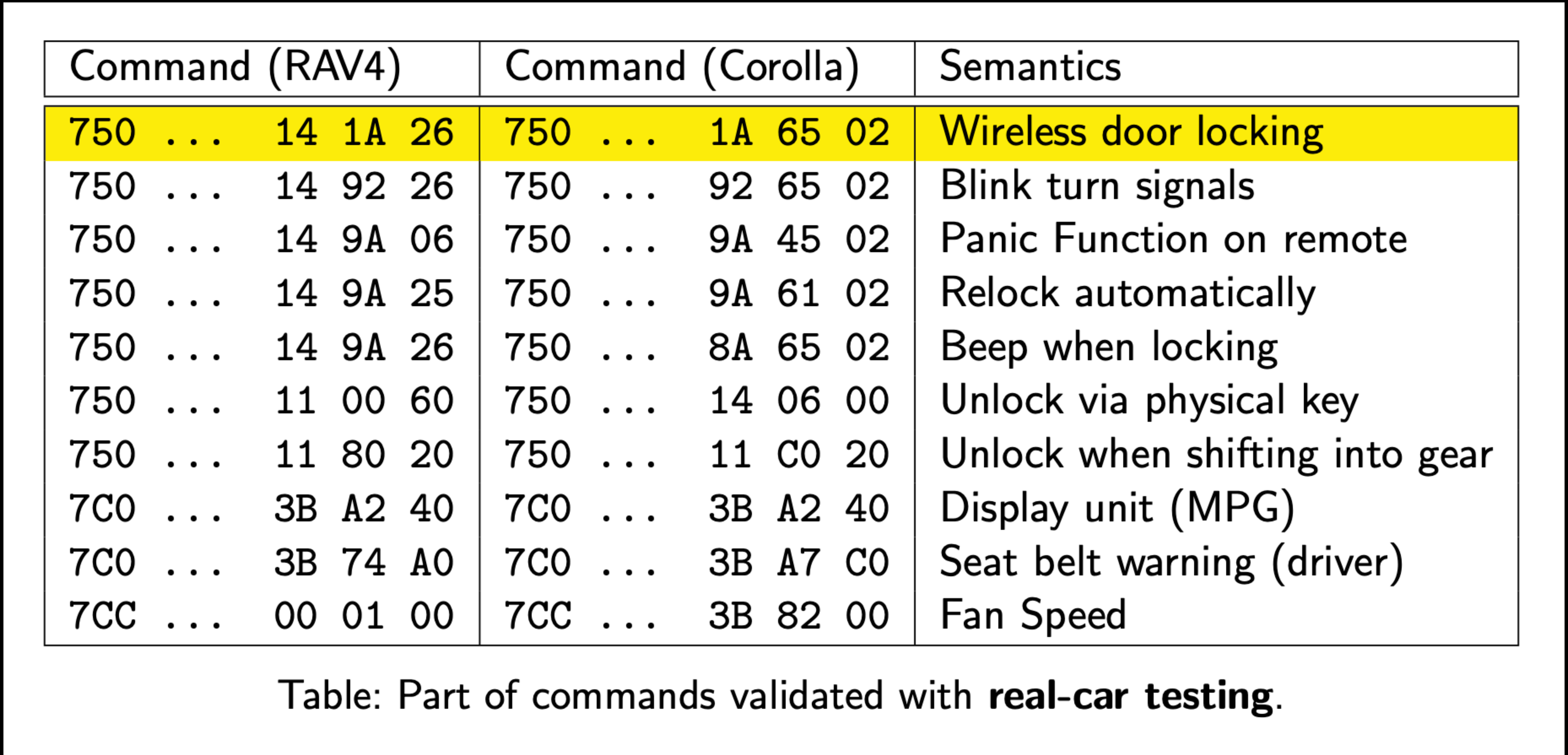
Correctness Evaluation



App	Android		iOS		Overlapped	
	# Syn.	# Sem.	# Syn.	# Sem.	# Syn.	# Sem.
BlueDriver	304	304	304	304	304	304
Carista	105,198	105,198	105,198	105,198	105,198	105,198
Carly for BMW	14,377	14,377	16,427	16,427	13,480	13,480
Carly for Mercedes	7,921	6,528	1,698	1,698	1,393	1,393
Carly for Toyota	5,305	5,266	39	39	39	39
Carly for VAG	16,402	7,283	18,627	10,429	7,283	7,283
CarVantage	41	41	41	41	41	41
Engie	144	144	68	68	68	68
inCarDoc	160	160	160	160	160	160
Kiwi OBD	220	220	6	6	6	6

Table: Part of the **cross-platform validation** (commands across different platforms) results.

Correctness Evaluation



Command (RAV4)	Command (Corolla)	Semantics
750 ... 14 1A 26	750 ... 1A 65 02	Wireless door locking
750 ... 14 92 26	750 ... 92 65 02	Blink turn signals
750 ... 14 9A 06	750 ... 9A 45 02	Panic Function on remote
750 ... 14 9A 25	750 ... 9A 61 02	Relock automatically
750 ... 14 9A 26	750 ... 8A 65 02	Beep when locking
750 ... 11 00 60	750 ... 14 06 00	Unlock via physical key
750 ... 11 80 20	750 ... 11 C0 20	Unlock when shifting into gear
7C0 ... 3B A2 40	7C0 ... 3B A2 40	Display unit (MPG)
7C0 ... 3B 74 A0	7C0 ... 3B A7 C0	Seat belt warning (driver)
7CC ... 00 01 00	7CC ... 3B 82 00	Fan Speed

Table: Part of commands validated with **real-car testing**.

References

- Paper
- GitHub repo
- Presentation

Q&A

Discussions

- Any idea on how we can prevent reverse engineering?
  - From app
  - From CAN bus
- Should we ask companies to standardize the CAN bus commands?