Plug-N-Pwned: Comprehensive Vulnerability Analysis of OBD-II Dongles as A New Over-the-Air Attack Surface in Automotive IoT

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

[1]Ohio State University

[2]University of California, Irvine

USENIX Security 2020

OBD-II Dongle in Automotive IoT

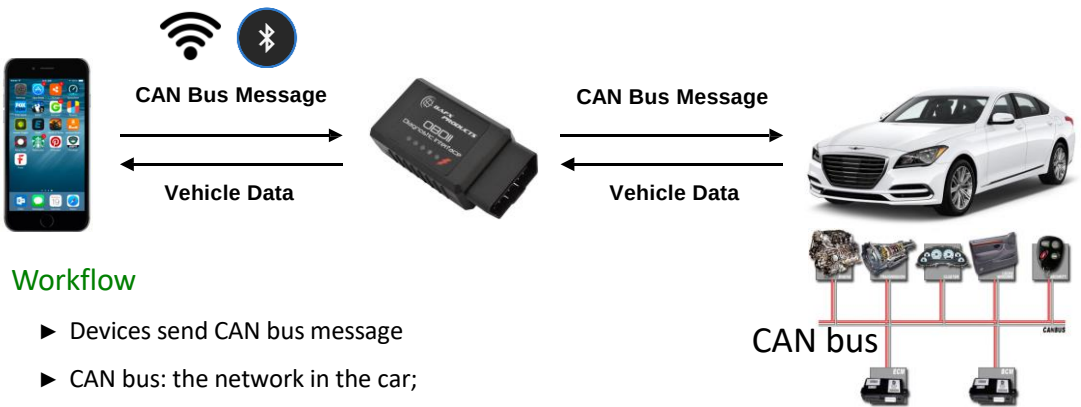
OBD-II Dongle

- On-Board Diagnostics (OBD) is a standard widely adopted for vehicle to report its internal working status.
- OBD-II dongles: run OBD protocol and convert commands into human-readable information
- They can be inserted into vehicles' OBD-II port
- A device can connect with these dongles and control vehicles

Automotive IoT

- Remote vehicle control
- Remote vehicle diagnosis
- Remote status monitoring

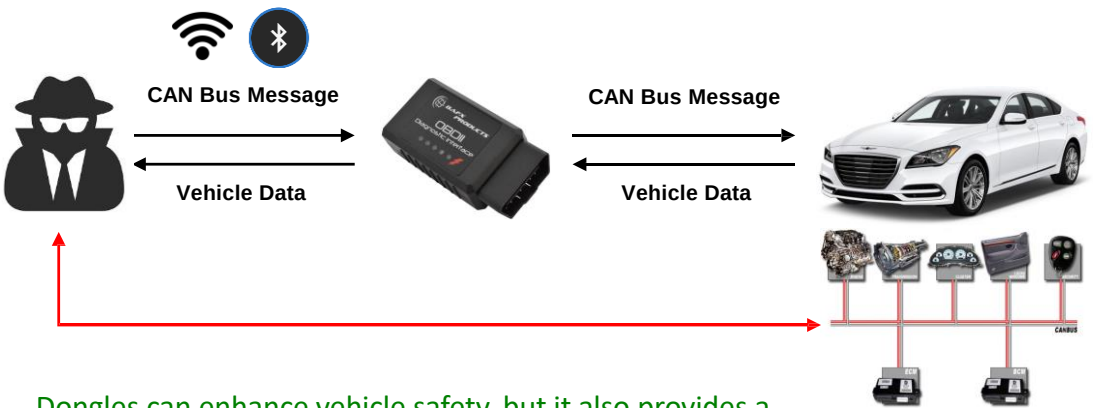
OBD-II Dongle in Automotive IoT



Workflow

- Devices send CAN bus message
- CAN bus: the network in the car;
- dongles forward it to the CAN bus;

OBD-II Dongle in Automotive IoT



Dongles can enhance vehicle safety, but it also provides a new remote attack interface

Wireless Attacks on an OBD-II Dongle

- Vulnerabilities in the authentication and message filtering process (2017)
- They allow attackers to remotely stop the engine of a moving vehicle

A Remote Attack on the Bosch Drivelog Connector Dongle

Motivation

Driver

Repair Technician

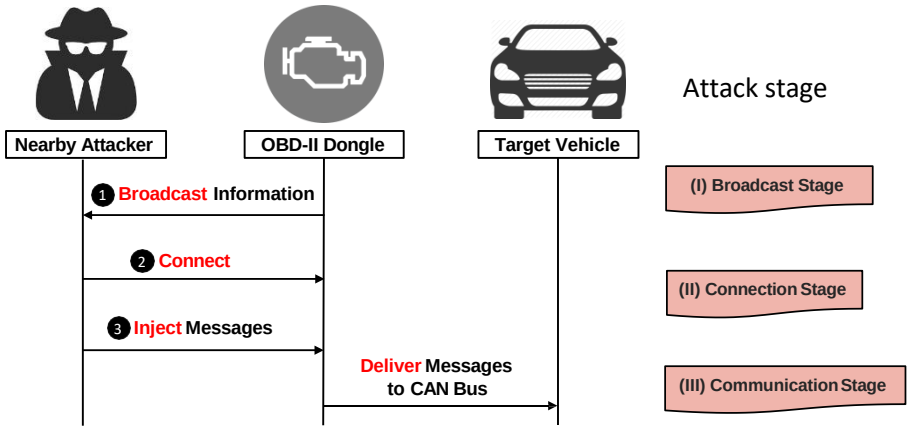
Auto Insurance Company

- Are dongles really secure against remote attacks?

Contributions

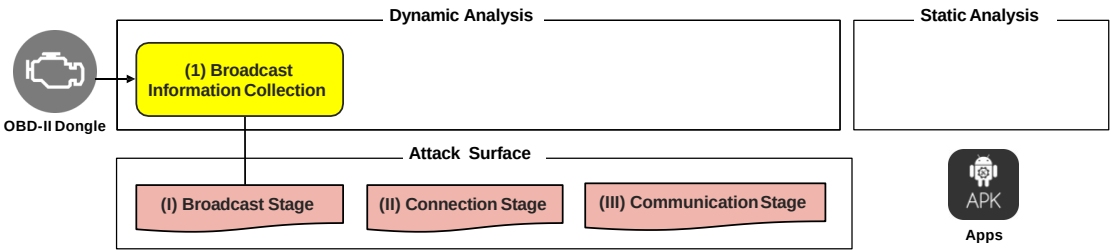
1. **Comprehensive vulnerability analysis**. They conducted the *first* vulnerability analysis on 77 wireless OBD-II dongles on Amazon US and implemented an automatic testing tool DongleScope.
2. **Vulnerability discovery and quantification**. They identified **5 types** of vulnerabilities across **3 attack stages**. They show that each of the dongles has at least two vulnerabilities.
3. **Attack case-study**. Then they constructed 4 classes of concrete attacks and **validated them on a testing vehicle**, which can lead to privacy leakage, property theft, and even safety threats.

Attack Model



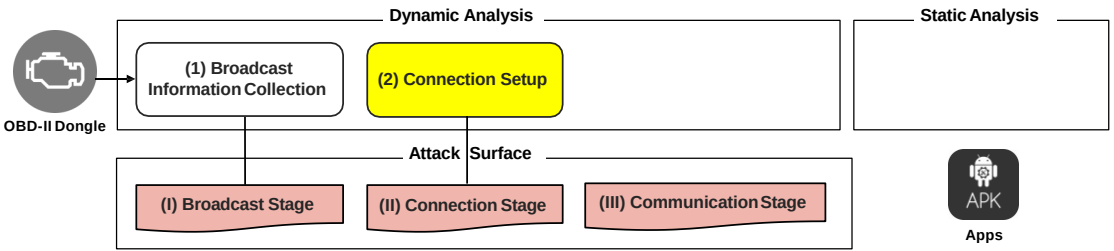
Goal: exploit the new vehicle attack surface exposed by wireless OBD-II dongles and thus achieves wireless attacks onto the CAN bus of a victim vehicle.

DONGLESCOPE: Broadcast Information Collection



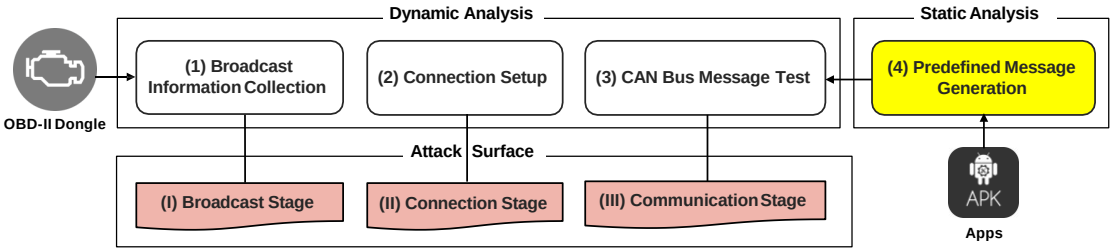
Stage	Measurement Objective(s)
(I)	Broadcast information: including network type, SSID, Unique ID;

Connection Setup



Stage	Measurement Objective(s)
(II)	② If connection can be established. ③ If multiple access allowed: establish connections with multiple mobile devices

Predefined Message Generation



Stage	Measurement Objective(s)
(III)	④ If predefined message can be injected: legal messages defined by developer ⑤ If other message can be injected: vehicle control and other safety related functions

Experiment Setup

Dynamic Analysis

- 77 wireless OBD-II dongles on US Amazon in February 2019.
  - 44 Wi-Fi dongles
  - 3 Bluetooth classic dongles
  - 30 Bluetooth Low Energy (BLE) dongles

Experiment Setup

Dynamic Analysis

- 77 wireless OBD-II dongles on US Amazon in February 2019.
  - 44 Wi-Fi dongles
  - 3 Bluetooth classic dongles
  - 30 Bluetooth Low Energy (BLE) dongles
- Testing vehicle: 2015 Honda Civic

Experiment Setup

App Name	Category	# Download	Dongle-specific?
Torque Lite	Communication	5,000,000	
DashCommand	Communication	1,000,000	
EOBD Facile	Auto & Vehicles	1,000,000	
ScanMaster	Communication	1,000,000	
Car Scanner	Auto & Vehicles	1,000,000	
OBDLink	Communication	1,000,000	C
BlueDriver	Auto & Vehicles	500,000	C
OBD Auto Doctor	Auto & Vehicles	500,000	
Carly for Toyota	Auto & Vehicles	100,000	C
FIXD	Auto & Vehicles	100,000	C
Carista	Auto & Vehicles	100,000	C
ZUS	Liftstyle	100,000	C
Automatic	Liftstyle	50,000	C
RepairSolutions	Auto & Vehicles	10,000	C
OBD Fusion	Communication	10,000	
Kiwi OBD	Tools	5,000	C
Automate	Tools	1,000	C
HaulGauge	Auto & Vehicles	500	C
ArtiBox	Tools	500	C
JDiag FasLink M2	Auto & Vehicles	100	C
DODYMPS	Tools	100	C

They also collected 21 mobile apps, which can be mapped to all 77 OBD-II dongles;

Vulnerability in Connection Stage

(I) Broadcast Stage | (II) Connection Stage | (III) Communication Stage

V1.1 Nearly all dongles have no connection-layer authentication

- 71 (92.21%) dongles can be arbitrarily connected by nearby devices
- With this vulnerability, an attacker can perform Dos attack by keeping connected with the target dongle

V1.2 Only 1 dongle has application-layer authentication

- Implying that 76 dongles can be directly compromised once the connection is established

Dongle Name	Type	Authentication
OBDLink MX	Wi-Fi	Password
Ourmit OBD2 Scanner	Wi-Fi	Button
OBDLink MX+	Bluetooth	Button
TOPDON Auto Mate	BLE	Button
OBDII Scanner TOPDON	BLE	Button
TOPDON AutoMate Code Reader	BLE	Button

Table 5: Connection Layer Authentication on Dongles.

Vulnerability in Connection Stage

(I) Broadcast Stage | (II) Connection Stage | (III) Communication Stage

V2. 29 dongles allow unauthorized access even when another device is connected

- This vulnerability increases the flexibility for attacks
- Only Wi-Fi dongles have such vulnerability

attackers can attack these dongles even when the vehicle owner's device is connected

Vulnerability in Communication Stage

(I) Broadcast Stage

(II) Connection Stage

(III) Communication Stage

V3. 67% of the dongles fail to filter out undefined CAN bus messages

- First uncovered in the Bosch dongle [Kov17] but never quantified before
- Dangerous CAN bus messages (e.g., vehicle control related ones) can be injected

they send an undefined CAN bus message which should not be accepted by the dongle and delivered to the CAN bus.

Vulnerability in Communication Stage

(I) Broadcast Stage

(II) Connection Stage

(III) Communication Stage

V4. 3 dongles are vulnerable to over-the-air firmware subverting or extraction

- Three dongle firmware images can be extracted from their mobile apps
- Two dongles are vulnerable to firmware subverting

Dongle Name	Vulnerable?	Firmware Available?
Automatic Pro		
Carly WiFi GEN2	C	C
BlueDriver Pro OBDII		C
Innova 3211a Drive	C	C

Vulnerability in Broadcast Stage

(I) Broadcast Stage

(II) Connection Stage

(III) Communication Stage

V5. Vulnerability status of half of the dongles can be fingerprinted with broadcast information

- Broadcast information includes: Wi-Fi SSID, UUID, Device name,etc.
- Increase success rate of attacks

Connection Name	Type	# Dongle	Vulnerability				
			V1.1	V1.2	V2	V3	V4
V-Link	Wi-Fi	4	C	C	C	C	
FastLink M2	BLE	4	C	C		C	
OBDBLE	BLE	3	C	C		C	
V-checker	BLE	2	C	C		C	
OBDII SCANNER	Wi-Fi	1	C	C	C	C	
OBDLink MX	Wi-Fi	1		C		C	

Attack Overview

Attack Case		Precondition						# Vulnerable Dongle (%)		
		V1.1	V1.2	V2	V3	V4	V5	w/o V2,V5	w/ V2	w/ V5
A1.1	Location Leakage	✓	✓	◯			◯	65 (84.42%)	27 (35.06%)	26 (33.77%)
A1.2	Diagnostic Data Leakage	✓	✓	◯			◯	65 (84.42%)	27 (35.06%)	26 (33.77%)
A1.3	CAN Bus Traffic Leakage	✓	✓	◯			◯	65 (84.42%)	27 (35.06%)	26 (33.77%)
A2	Property Theft	✓	✓	◯	✓		◯	46 (59.74%)	20 (25.97%)	24 (31.17%)
A3	Vehicle Control Interference	✓	✓	◯	✓		◯	46 (59.74%)	20 (25.97%)	24 (31.17%)
A4	In-vehicle Network Infiltration	✓	✓	◯		✓	◯	2 (2.60%)	0	2 (2.60%)

Table 9: Proposed Attack Cases and Vulnerable Dongle Statistics. ✓indicates mandatory precondition, ◯ indicates optional precondition that are not necessary but can increase the attack flexibility (e.g., with V2) or attack success rate (e.g., with V5).

they construct 4 classes of concrete attacks and validated them on the testing vehicle.

A1. Vehicle-related Data Leakage

Location Leakage (V1.1, V1.2)

- PID 09 02 can be used to query the vehicle VIN
- Precisely locate the victim vehicle

Diagnostic Data Leakage (V1.1, V1.2)

- Read vehicle diagnostic data (e.g., odometer, fuel rate, engine RPM)
- Driver behaviour fingerprinting [CPL15,ETKK16]

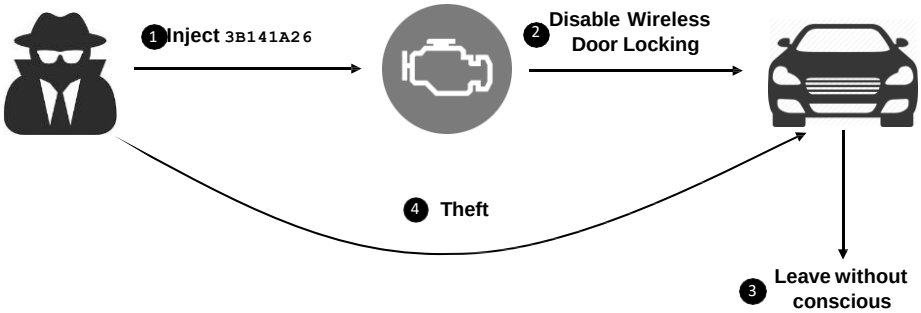
CAN Bus Traffic Leakage (V1.1, V1.2, V3)

- Dump the CAN bus traffic with ATMA command
- CAN bus protocol reverse engineering

A2. Property Theft (V1 and V3)

The attacker can inject one CAN bus message to disable the wireless door locking.

A2. Property Theft



When the driver leaves the vehicle and locks the vehicle remotely with his key as usual, he may not know the locking is unsuccessful. Afterwards, the attacker can sneak into the vehicle.

A3/ A4

Vehicle Control Interference (V1.1, V1.2, V3)

- With the same vulnerabilities, the attacker can also send other messages to cause vehicle control interference;

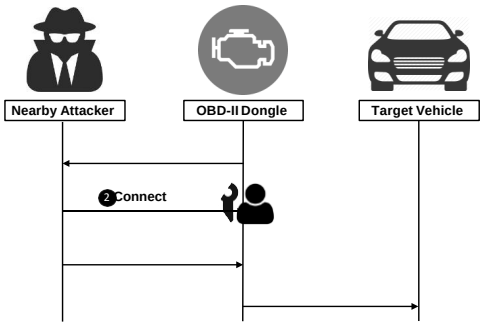
In-vehicle Network Infiltration (V1.1, V1.2, V4)

- allow an unauthorized attacker to send a malicious firmware packet

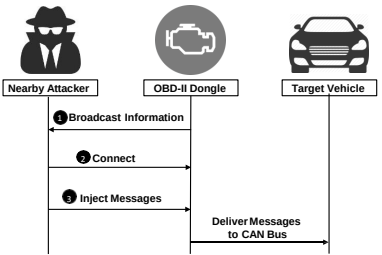
  to subvert the dongle's firmware

Countermeasures

1. **Authentication on CAN bus**. A fundamental solution [VHSV11,NLJ08, GMVHV12,KMT+14,RG16].
2. **Firewall on the OBD-II port**. Physical gateway module for Chrysler [gat].
3. **Authentication on OBD-II dongles**. Secure dongle firmware (e.g., OpenXC [ope19]).



Conclusion



DongleScope

- Comprehensive security analysis
- Automatic testing tool DongleScope

Vulnerability Analysis

- Uncovered and quantified 5 vulnerabilities
- Constructed 4 concrete attacks

The source code is available at https://github.com/OSUSecLab/DongleScope.