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

Automotive IoT

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

OBD-II Dongle in Automotive IoT

Automotive IoT

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

On-Board Diagnostics (OBD)

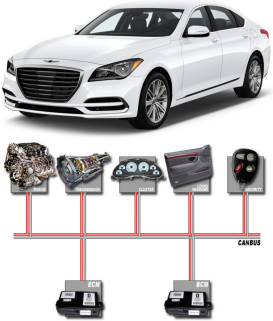
- A standard for vehicle diagnosis
- OBD-II is mandated in gasoline vehicles of US since 1996 [EW08]

OBD-II Dongle in Automotive IoT

OBD-II Dongle in Automotive IoT

CAN Bus Message →

← Vehicle Data



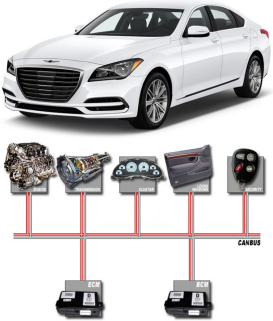
OBD-II Dongle in Automotive IoT

CAN Bus Message

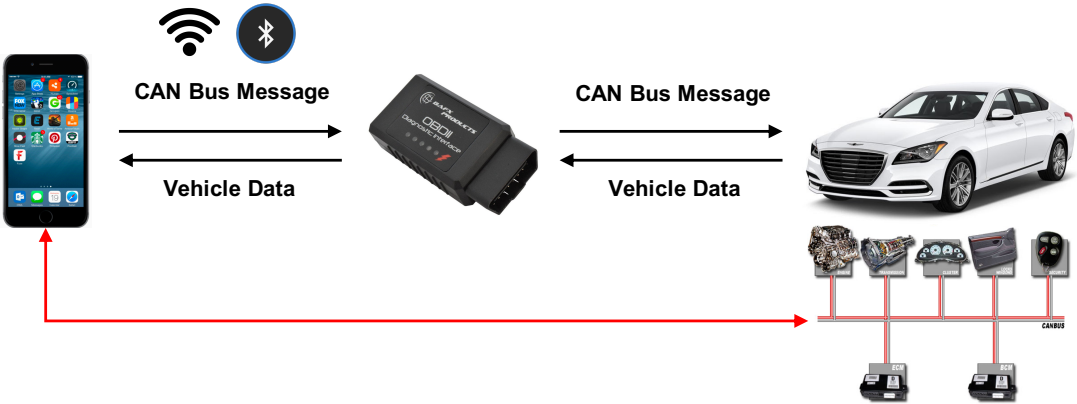
Vehicle Data

CAN Bus Message

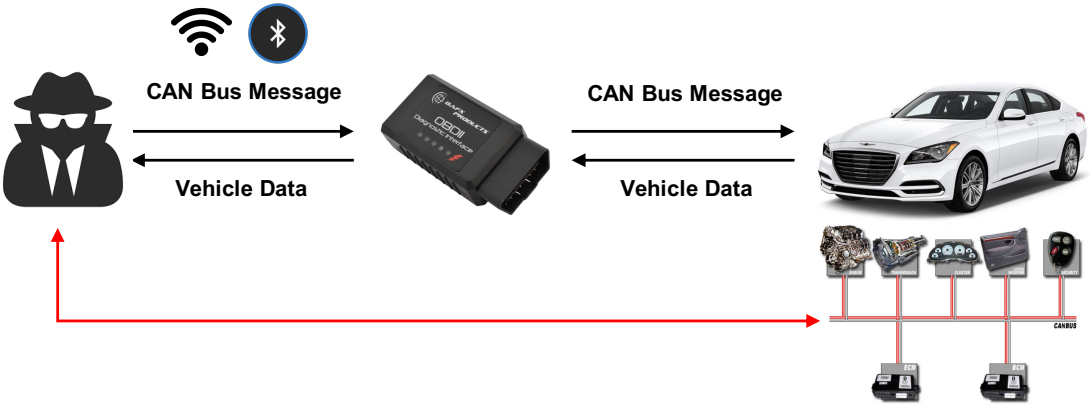
Vehicle Data



OBD-II Dongle in Automotive IoT



OBD-II Dongle in Automotive IoT



Wireless Attacks on an OBD-II Dongle

- Vulnerabilities in the authentication and message filtering process [Kov17]

A Remote Attack on the Bosch Drivelog Connector Dongle

Wireless Attacks on an OBD-II Dongle

- Vulnerabilities in the authentication and message filtering process [Kov17]
- They allow attackers to remotely stop the engine of a moving vehicle

A Remote Attack on the Bosch Drivelog Connector Dongle

Motivation

Driver

Motivation

Driver

Repair Technician

Motivation

Driver

Repair Technician

Auto Insurance Company

Motivation

Driver

Repair Technician

Auto Insurance Company

- Are they really secure against remote attacks?

Our Contributions

1. **Comprehensive vulnerability analysis**. We conducted the *first* comprehensive vulnerability analysis on all 77 wireless OBD-II dongles on Amazon US in February 2019, and implemented an automatic testing tool DongleScope.

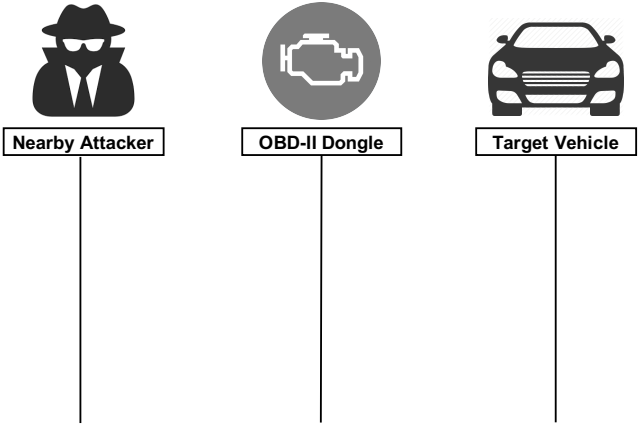
Our Contributions

1. **Comprehensive vulnerability analysis**. We conducted the *first* comprehensive vulnerability analysis on all 77 wireless OBD-II dongles on Amazon US in February 2019, and implemented an automatic testing tool DongleScope.
2. **Vulnerability discovery and quantification**. We identified 5 types of vulnerabilities across 3 attack stages, in which 4 are newly discovered. We show that each of the dongles has at least two vulnerabilities.

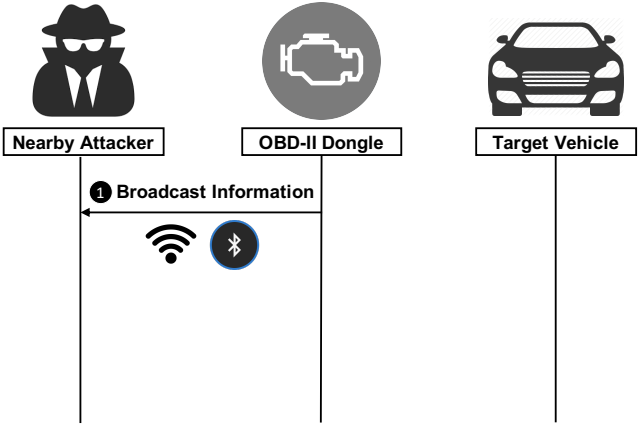
Our Contributions

1. **Comprehensive vulnerability analysis**. We conducted the *first* comprehensive vulnerability analysis on all 77 wireless OBD-II dongles on Amazon US in February 2019, and implemented an automatic testing tool DongleScope.
2. **Vulnerability discovery and quantification**. We identified 5 types of vulnerabilities across 3 attack stages, in which 4 are newly discovered. We show that each of the dongles has at least two vulnerabilities.
3. **Attack case-study**. We constructed 4 classes of concrete attacks and validated them on a testing automobile, which can lead to privacy leakage, property theft, and even safety threats.

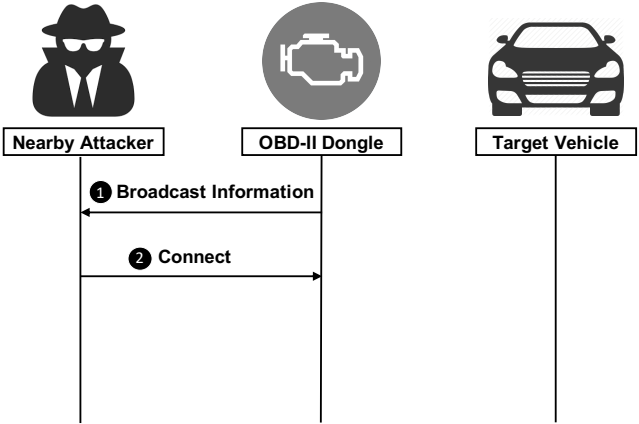
Attack Model



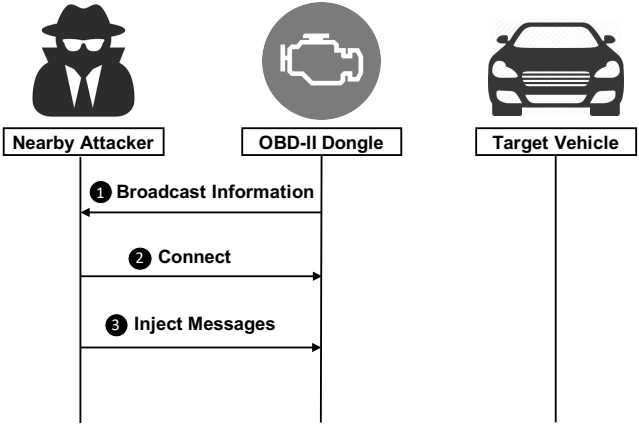
Attack Model



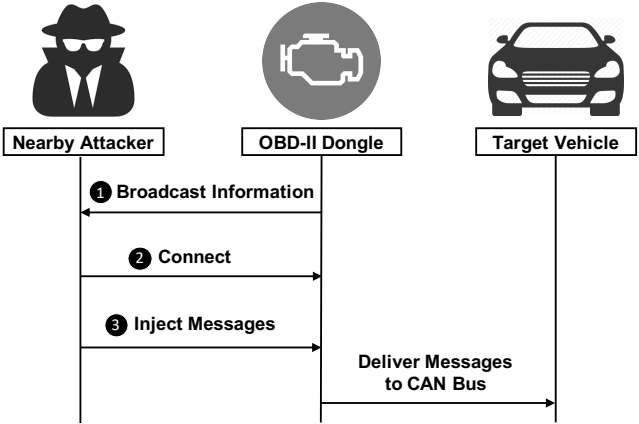
Attack Model



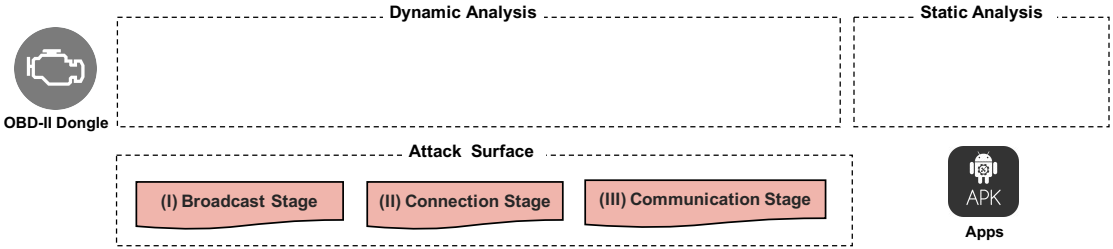
Attack Model



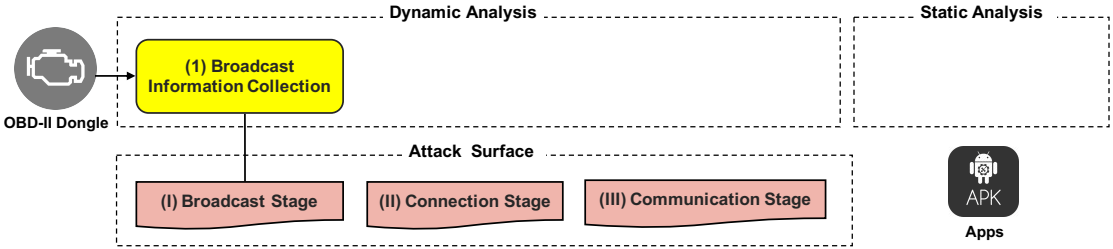
Attack Model



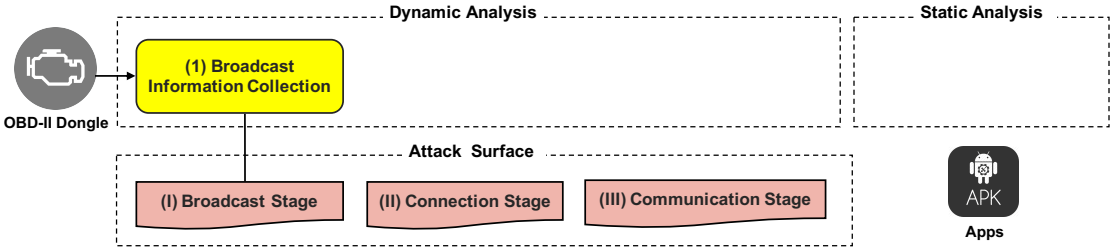
Broadcast Information Collection



Broadcast Information Collection

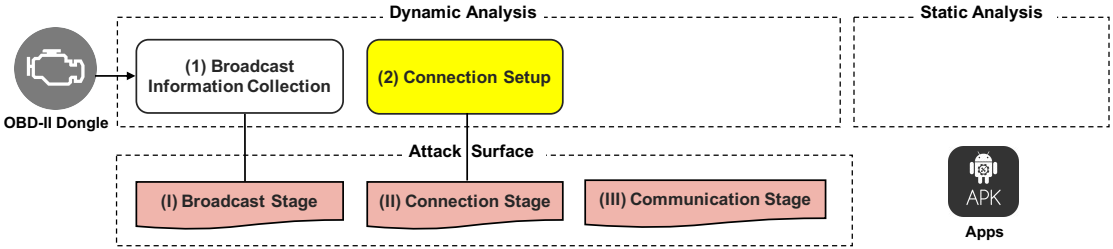


Broadcast Information Collection

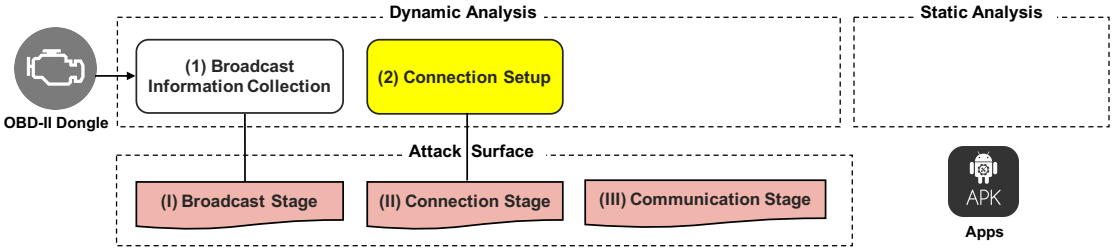


Stage	Measurement Objective(s)
(I)	Broadcast information

Connection Setup

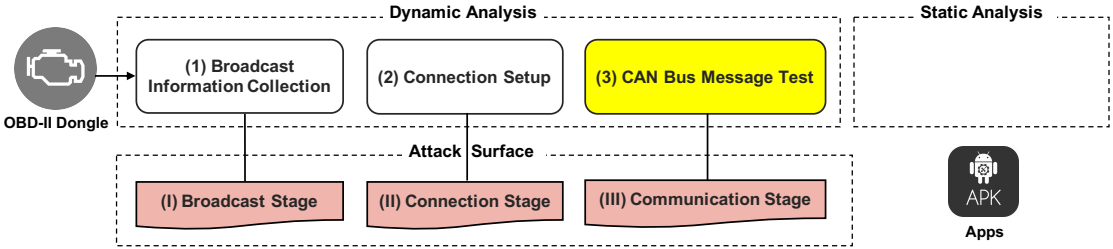


Connection Setup

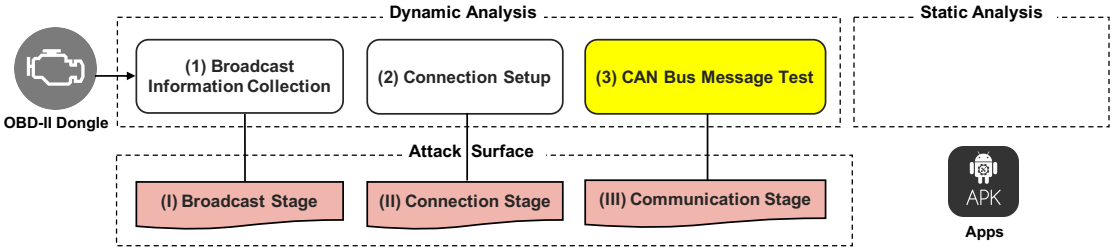


Stage	Measurement Objective(s)
(II)	② If connection can be established. ③ If multiple access allowed.

CAN Bus Message Test

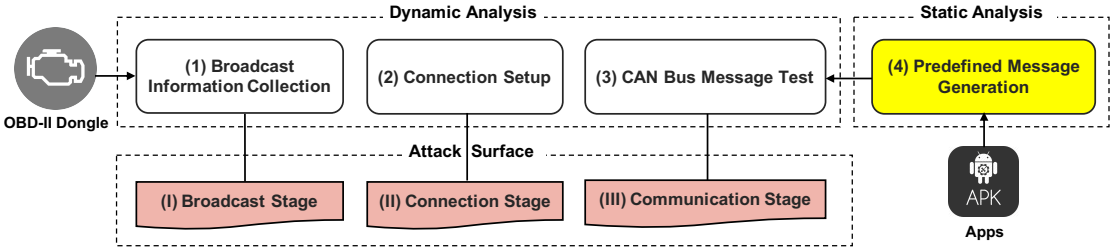


CAN Bus Message Test



Stage	Measurement Objective(s)
(III)	④ If predefined message can be injected. ⑤ If other message can be injected.

Predefined Message Generation



Stage	Measurement Objective(s)
(III)	④ If predefined message can be injected. ⑤ If other message can be injected.

Experiment Setup

Dynamic Analysis

- 77 wireless OBD-II dongles on US Amazon in February 2019.

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	✓
BlueDriver	Auto & Vehicles	500,000	✓
OBD Auto Doctor	Auto & Vehicles	500,000	
Carly for Toyota	Auto & Vehicles	100,000	✓
FIXD	Auto & Vehicles	100,000	✓
Carista	Auto & Vehicles	100,000	✓
ZUS	Liftstyle	100,000	✓
Automatic	Liftstyle	50,000	✓
RepairSolutions	Auto & Vehicles	10,000	✓
OBD Fusion	Communication	10,000	
Kiwi OBD	Tools	5,000	✓
Automate	Tools	1,000	✓
HaulGauge	Auto & Vehicles	500	✓
ArtiBox	Tools	500	✓
JDiag FasLink M2	Auto & Vehicles	100	✓
DODYMPS	Tools	100	✓

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.

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

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	✓	✓	✓	✓	
FastLink M2	BLE	4	✓	✓		✓	
OBDBLE	BLE	3	✓	✓		✓	
V-checker	BLE	2	✓	✓		✓	
OBDII SCANNER	Wi-Fi	1	✓	✓	✓	✓	
OBDLink MX	Wi-Fi	1		✓		✓	

Vulnerability in Connection Stage

(I) Broadcast Stage

(II) Connection Stage

(III) Communication Stage

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

- 71 (92.21%) dongles can be arbitrarily connected by nearby devices

Vulnerability in Connection Stage

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

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

- 71 (92.21%) dongles can be arbitrarily connected by nearby devices

V1.2 Only 1 dongle has application-layer authentication by default

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

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

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

Vulnerability in Communication Stage

(I) Broadcast Stage

(II) Connection Stage

(III) Communication Stage

V3. 67% of the dongles fail to provide a CAN bus messages filtering capability

- First uncovered in the Bosch dongle [Kov17] but never quantified before

Vulnerability in Communication Stage

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

V3. 67% of the dongles fail to provide a CAN bus messages filtering capability

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

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 companion mobile apps

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

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 companion mobile apps
- Two dongles are vulnerable to firmware subverting

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

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%)

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%)

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%)

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%)

A1. Vehicle-related Data Leakage

Location Leakage

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

A1. Vehicle-related Data Leakage

Location Leakage

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

Diagnostic Data Leakage

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

A1. Vehicle-related Data Leakage

Location Leakage

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

Diagnostic Data Leakage

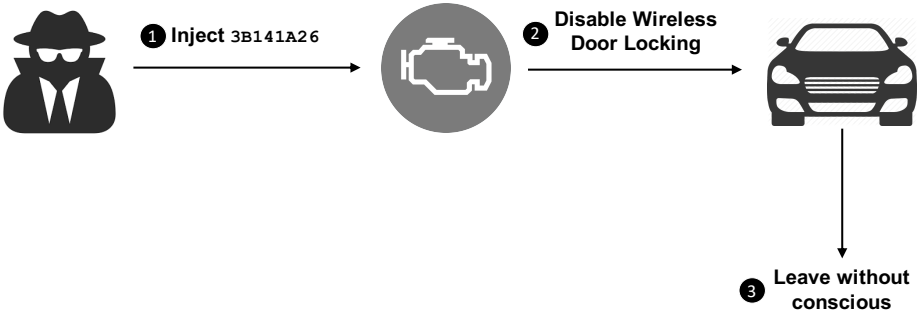
- Read vehicle diagnostic data (e.g., odometer, fuel rate, engine RPM)
- Driver behaviour fingerprinting [CPL15, ETKK16]

CAN Bus Traffic Leakage

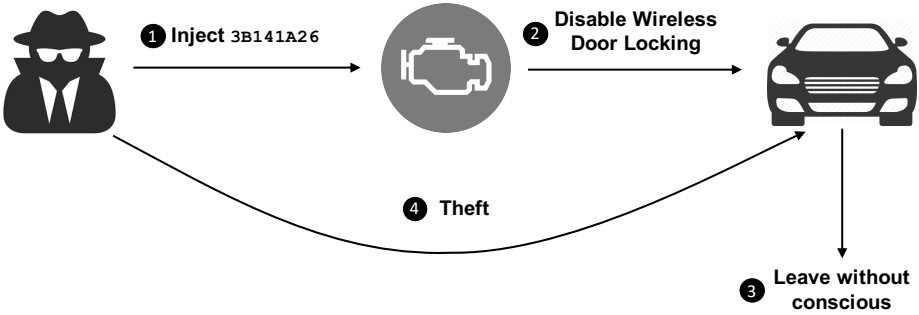
- Dump the CAN bus traffic with `ATMA` command
- CAN bus protocol reverse engineering

A2. Property Theft

A2. Property Theft

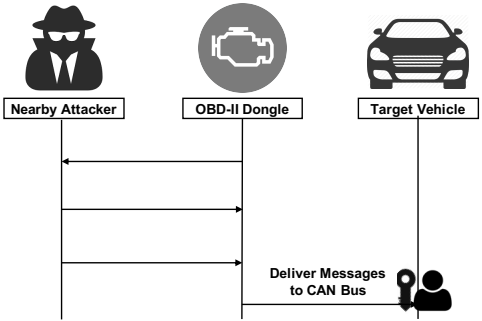


A2. Property Theft



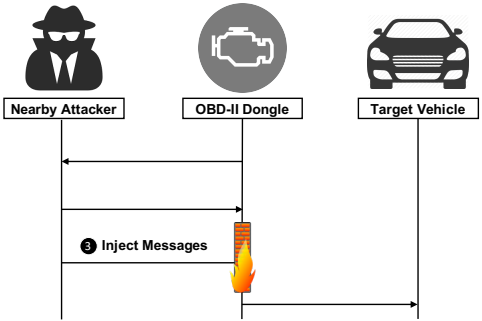
Countermeasures

1. **Authentication on CAN bus**. A fundamental solution [VHSV11, NLJ08, GMVHV12, KMT+14, RG16].



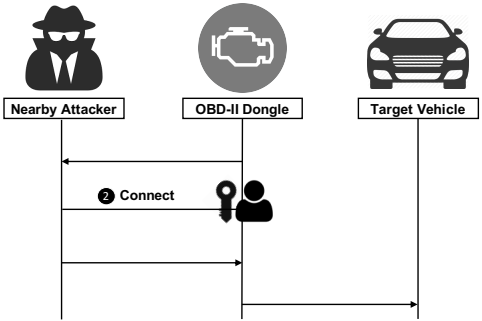
Countermeasures

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].

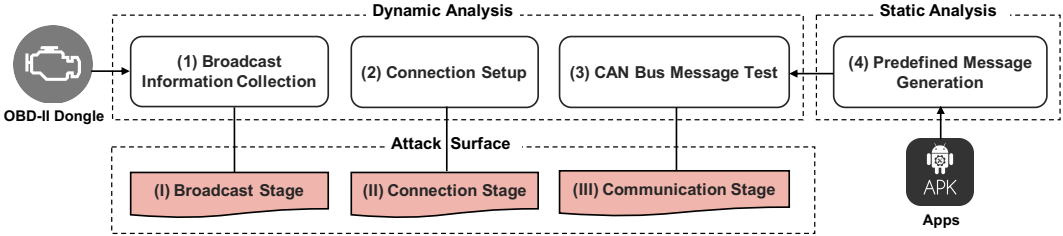


Countermeasures

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]).



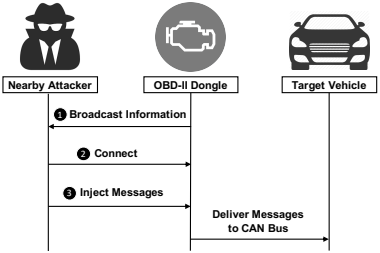
Takeaway



DongleScope

- Comprehensive security analysis
- Automatic testing tool DongleScope

Takeaway



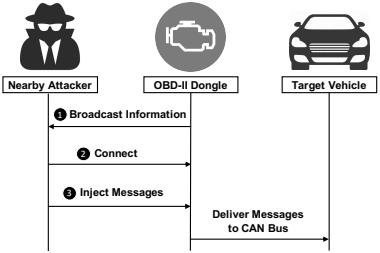
DongleScope

- Comprehensive security analysis
- Automatic testing tool DongleScope

Vulnerability Analysis

- Uncovered and quantified 5 vulnerabilities
- Constructed 4 concrete attacks

Takeaway



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.

References I

Shi-Huang Chen, Jeng-Shyang Pan, and Kaixuan Lu, *Driving behavior analysis based on vehicle obd information and adaboost algorithms*, Proceedings of the International MultiConference of Engineers and Computer Scientists, vol. 1, 2015, pp. 18–20.

Miro Enev, Alex Takakuwa, Karl Koscher, and Tadayoshi Kohno, *Automobile driver fingerprinting*, Proceedings on Privacy Enhancing Technologies **2016** (2016), no. 1, 34–50.

Douglas S Eisinger and Peter Wathern, *Policy evolution and clean air: The case of us motor vehicle inspection and maintenance*, Transportation Research Part D: Transport and Environment **13** (2008), no. 6, 359–368.

Fca secure gateway module, `https://diag.net/msg/m1fsoznwl3nndqti9pxq9k4nz0`.

Bogdan Groza, Stefan Murvay, Anthony Van Herrewege, and Ingrid Verbauwhede, *Libra-can: a lightweight broadcast authentication protocol for controller area networks*, International Conference on Cryptology and Network Security, Springer, 2012, pp. 185–200.

Ryo Kurachi, Yutaka Matsubara, Hiroaki Takada, Naoki Adachi, Yukihiro Miyashita, and Satoshi Horihata, *Cacan-centralized authentication system in can (controller area network)*, 14th Int. Conf. on Embedded Security in Cars (ESCAR 2014), 2014.

Alexei Kovelman, *A Remote Attack on the Bosch Drivelog Connector Dongle*, `https://argus-sec.com/remote-attack-bosch-drivelog-connector-dongle`, 2017.

Dennis K Nilsson, Ulf E Larson, and Erland Jonsson, *Efficient in-vehicle delayed data authentication based on compound message authentication codes*, Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th, IEEE, 2008, pp. 1–5.

openxc-android, `https://github.com/openxc/openxc-android`, 2019.

References II

Andreea-Ina Radu and Flavio D Garcia, *Leia: A lightweight authentication protocol for can*, European Symposium on Research in Computer Security, Springer, 2016, pp. 283–300.

Anthony Van Herrewege, Dave Singelee, and Ingrid Verbauwhede, *Canauth-a simple, backward compatible broadcast authentication protocol for can bus*, ECRYPT Workshop on Lightweight Cryptography, vol. 2011, 2011.