(2020 USENIX)Plug-N-Pwned: Comprehensive Vulnerability Analysis of OBD-II Dongles as A New Over-the-Air Attack Surface in Automotive IoT

1 Summary

A large number of OBD-II dongles have been deployed in various automobiles, which provide the driver of the car capacities to monitor and operate the car remotely combined with the mobile apps. However, these widely used dongles and apps have quilt a lot vulnerabilities which can be exploited by the attacker to cause severe consequence, such as privacy leakage, emergency brake, etc. In this paper, the author devise an analyze tool to detect some common vulnerabilities in OBD-II dongles and conduct real experiments to prove the existence of these vulnerabilities.

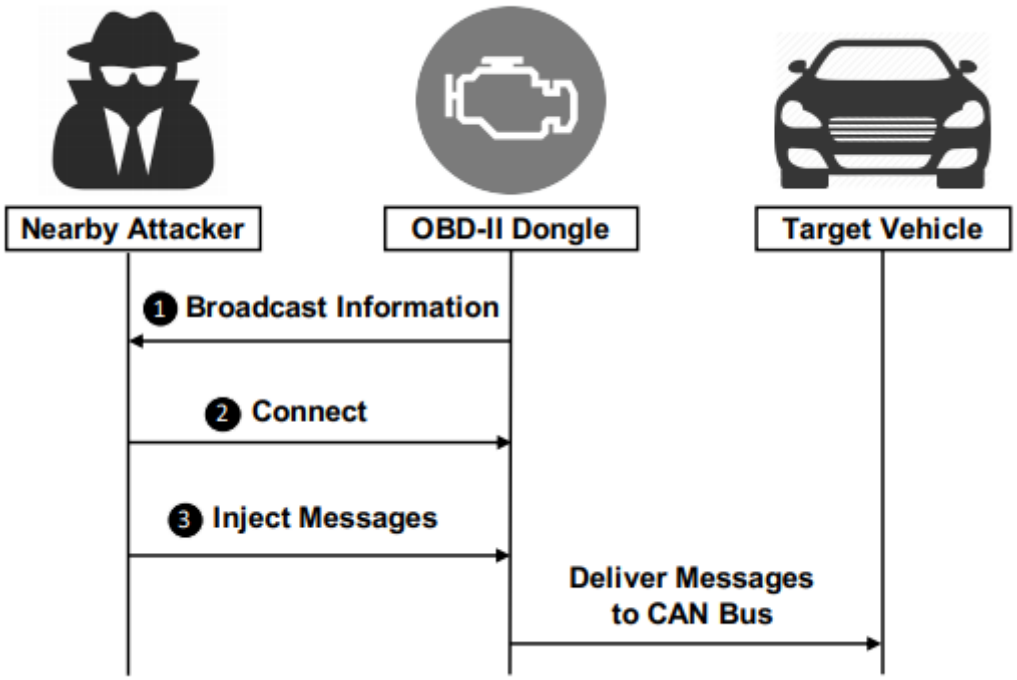
2 Challenge

The main challenge in this work is the diversity of dongles. First, different dongles communicate with corresponding apps using different protocols, such as Wi-Fi or BLE. Second, the OBD-II port is not a strict standard and there are many customize implementation on them. So, it non-trivial to propose a generic method to identify the vulnerabilities.
Another challenge comes from the fact that almost all messages provided by the dongles just perform some query request and these messages can't affect the vehicles significantly. So it's a requirement to devise undefined messages to perform attack and the analyze tool must also detect these situations.

3 Main Idea

3.1 Attack Model and Surface

In this paper, the author focused on the wireless OBD-II dongle, because it can offer attackers the ability to perform remote attack. The attack model is illustrated below:



First, the attacker tries to capture the broadcasting signals emitted by the target dongle, then he tries to build connection with it. Once the connection is constructed, the attacker can send message to the dongle to try to get information of the vehicle or manipulating some aspects of it.
The attack surface reside in the three phase of the three phases:

1. Broadcast Stage, in which the dongles emit identification information.
2. Connection Stage, with some possible verification steps.
3. Communicating Stage.

3.2 Vulnerability Analysis

The main goal of the analyze is trying our best to find vulnerabilities reside in the three phases. The author proposed a detection framework, DONGLE-SCOPE to perform the analyze. The workflow of the DONGLE-SCOPE is shown below.

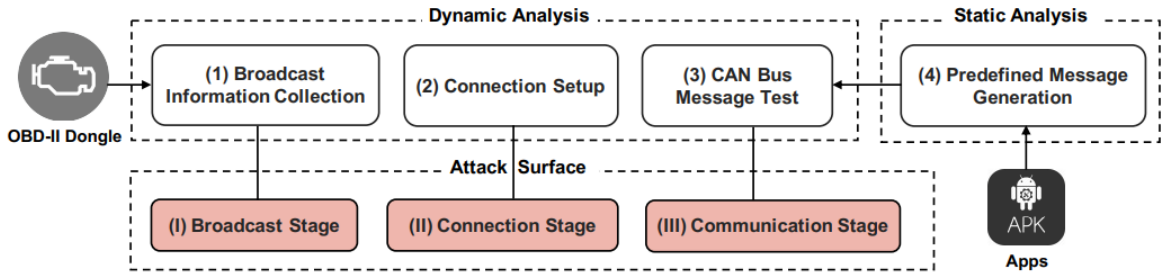


Figure 4: Design Overview of DONGLESCOPE.

This framework test the OBD-II dongle on a vehicle and conduct static program analyze simultaneously. According to three phases, the framework can be divided into four main components. For each component in the dynamic analyze, a corresponding measurement is proposed to judge the existence of vulnerabilities.
During the broadcasting stage, it collects the broadcast information. In the connection stage it examine not only the feasibility to build a connection but also the possibility to build multi connections

while the user is using the dongle. In the communication stage, it tests whether predefined and undefined messages can pass the filter of the dongle and cause the desirable effect.

3.3 Experiment

The author collected 77 most popular OBD-II dongles on Amazon and 21 companion apps on Google Play to conduct the experiment. The author exerted DONGLE-SCOPE on these dongles and apps to find if they have the five identified vulnerabilities:

- Connection layer authentication.
- Application layer authentication.
- Multi access capability.
- Filter out undefined messages.
- Over-the-air firmware subverting and extraction.

With the experiments, the author found that all of these dongles have at least two types of vulnerabilities.

3.4 Case Study

To reveal the severity of these vulnerabilities, the author designed four concrete types of attacks which exploit one or more vulnerabilities each, as shown in the table below:

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%)

These attacks can cause very severe consequence, such as leakage of information or even some safety-critical hazard. A lot of dongles on the shelf can be used as attack surfaces to perform the attack.

4 Strength

1. Conduct extensive experiments on Wireless OBD-II dongles and apps.
2. Combine dynamic analysis and static analysis to find vulnerabilities.

5 Weakness

1. The analysis need a real car, which is expensive to find.
2. Without enough summary on some total pattern behind these devices

(2020 NDSS)Automated Cross-Platform Reverse Engineering of CAN Bus Commands From Mobile Apps

1 Solved Problem

In this paper, the author proposed a new method to perform reverse engineering on CAN bus messages. Compared to previous methods, the new method doesn't need a real car and human intervene, which lead to low cost and high efficiency.

2 Main Idea

Recent years, with the evolution of Iot and its application in automobiles, a lot of mobile apps have be generated to provide various functions about the car, such as remote diagnosis and operation. However, such apps have to use CAN messages to communicate with the vehicles too, either by itself or its companion dongles. This provides us a new way to revert engineering the CAN messages by analyzing the logic that they generate a message.

3 Highlights Worth Learning

1. The idea to analyze the bus commands generation process to get the syntactic and semantic of the CAN messages.
2. Using backward slicing to get the semantic.

(2020 MobiCom)Renovating Road Signs for Infrastructure-to-Vehicle Networking

1 Solved Problem

Current researches on perception of automobiles mostly concentrate on the vehicle side, such as more powerful sensors and more effective algorithms. However, some dynamic conditions on the road may be difficult for on-vehicle sensors to detect. So there is a requirement to deploy infrastructures along the road. However, most of the road side infrastructures are very expensive to deploy. In this paper, the author proposed a novel method that use the traffic signs to convey dynamic information about the road but keep their origin functions.

2 Main Idea

In this paper, the author propose RetroI2V, which exploits the visible light backscattering communication schemes(VLBC) to carry information between vehicle and road sign.

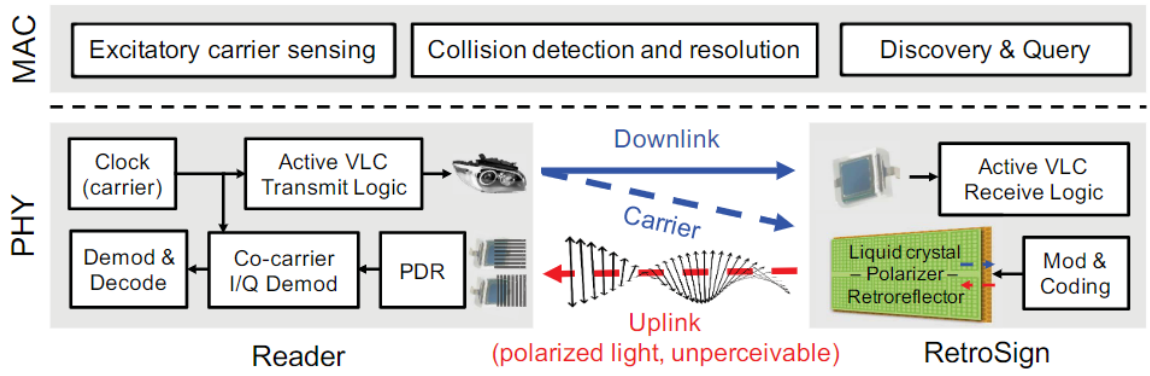


Figure 1: RetroI2V system architecture.

The picture above show the high-level design of RetroI2V. The architecture of RetroI2V consists of two main layers, the PHY layer and MAC layer. The PHY is designed to deal with emit and sense of the light. The MAC layer is designed to avoid collision cases.
To apply the VLBC in the road scenarios, the author renovated the structure of the LCD used to generate information signals and excitatory carrier sensing(ECS) to avoid in-band interference.

3 Highlights Worth Learning

1. The idea to use light to carry information between vehicle and the road side.
2. The method proposed to deal with multi-access, long distance and flicker.