Demo: Too Afraid to Drive: Systematic Discovery of Semantic DoS Vulnerability in Autonomous Driving Planning under Physical-World Attacks

Ziwen Wan Junjie Shen Jalen Chuang Xin Xia† Joshua Garcia Jiaqi Ma† Qi Alfred Chen
University of California, Irvine †University of California, Los Angeles
{ziwenw8, junjies1, jzchuang, joshua.garcia, alfchen}@uci.edu
†{x35xia, jiaqima}@ucla.edu

I. Introduction

In high-level Autonomous Driving (AD) systems, behavioral planning is in charge of making high-level driving decisions such as cruising and stopping [1], and thus highly security-critical. In this work, we perform the first systematic study of semantic security vulnerabilities specific to overly-conservative AD behavioral planning behaviors, i.e., those that can cause failed or significantly-degraded mission performance, which can be critical for AD services such as robo-taxi/delivery. We call them semantic Denial-of-Service (DoS) vulnerabilities, which we envision to be most generally exposed in practical AD systems due to the tendency for conservativeness to avoid safety incidents. To achieve high practicality and realism, we assume that the attacker can only introduce seemingly-benign external physical objects to the driving environment, e.g., off-road dumped cardboard boxes.

To systematically discover such vulnerabilities, we design *PlanFuzz*, a novel dynamic testing approach that addresses various problem-specific design challenges. Specifically, we propose and identify planning invariants as novel testing oracles, and design new input generation to systematically enforce problem-specific constraints for attacker-introduced physical objects. We also design a novel behavioral planning vulnerability distance metric to effectively guide the discovery. PlanFuzz can effectively discover 9 previously-unknown semantic DoS vulnerabilities.

II. Problem Formulation

Attack goal: Semantic Denial-of-Service (DoS) of BP. In this paper, we target an attack goal of causing *semantic Denial-of-Service (DoS)* on BP, which we define as causing it to change a normal driving decision to an *overly-conservative* one so that the victim AD vehicle will have a *failed* or *significantly-degraded* mission performance (e.g., never reach the destination). Specifically, we focus on 2 concrete types of such DoS in an AD context: (1) causing an emergency/permanent stop, and (2) causing the victim to give up a mission-critical driving decision, such as necessary left/right turns and lane changing on the route. To achieve this goal, in this paper we target *physical-world attack vectors* in the AD context (e.g., adding seemingly-benign static/dynamic physical road objects) for high practicality and realism.

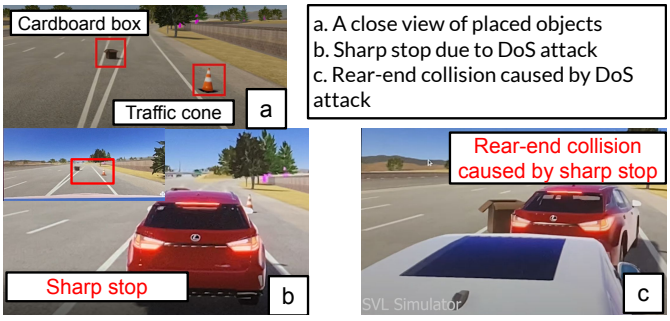

Fig. 1. An example of semantic DoS vulnerability in Autoware lane following.

III. Demonstration Plan

As mentioned earlier, we build a novel dynamic testing approach, *PlanFuzz*, to systematically discover such vulnerabilities. In the demo, we will show the end-to-end attack consequences of lane-following DoS vulnerability, one of the discovered vulnerabilities of PlanFuzz in Autoware [2] (a full-stack AD system), in a production-grade AD simulator, LGSVL [3]. More demo videos (more driving scenarios in both Autoware [2] and Apollo [4]) are available on our project website: **https://sites.google.com/view/cav-sec/planfuzz**.

Lane-following DoS attack on Autoware. In this scenario, we will demonstrate that attacker can use two off-road static objects to trigger fully stop decision and this could lead to rear-end collision in the highway off-ramp. Fig. 1 is a demonstration of this vulnerability and the consequence.

Acknowldgments

This research was supported in part by the NSF under CNS-1850533, CNS-1932464, CNS-1929771, and CNS-2145493.

References

[1] B. Paden, M. Čáp, S. Z. Yong, D. Yershov, and E. Frazzoli, "A Survey of Motion Planning and Control Techniques for Self-driving Urban Vehicles," *IEEE Transactions on intelligent vehicles*, 2016.
[2] "Autoware.AI." https://www.autoware.ai/.
[3] LG, "LGSVL Simulator." https://github.com/lgsvl/simulator.
[4] "Apollo." https://github.com/ApolloAuto/apollo.

Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2022
24 April 2022, San Diego, CA, USA
ISBN 1-891562-75-4
https://dx.doi.org/10.14722/autosec.2022.23046
www.ndss-symposium.org