Poster: 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

Abstract

In high-level Autonomous Driving (AD) systems, behavioral planning is in charge of making high-level driving decisions such as cruising and stopping, 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. We evaluate PlanFuzz on 3 planning implementations from practical open-source AD systems, and find that it can effectively discover 9 previously-unknown semantic DoS vulnerabilities without false positives. We find all our new designs necessary, as without each design, statistically significant performance drops are generally observed. We further perform exploitation case studies using simulation and real-vehicle traces. We discuss root causes and potential fixes.

I. REFERENCE

This work will appear at NDSS 2022:

Ziwen Wan, Junjie Shen, Jalen Chuang, Xin Xia, Joshua Garcia, Jiaqi Ma, and Qi Alfred Chen.“Too Afraid to Drive: Systematic Discovery of Semantic DoS Vulnerability in Autonomous Driving Planning under Physical-World Attacks”. In Proceedings of the Network and Distributed System Security Symposium (NDSS), 2022, 24 - 28 April. San Diego, CA: ISOC.

II. DOI

Network and Distributed Systems Security (NDSS) Symposium 2022
24 - 28 April, San Diego, CA, USA
ISBN 1-891562-74-6https://dx.doi.org/10.14722/ndss.2022.24177
www.ndss-symposium.org

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

To appear in NDSS 2022

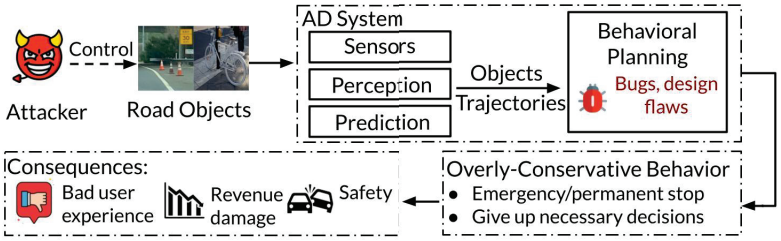
Ziwen Wan, Junjie Shen, Jalen Chuang, Xin Xia†, Joshua Garcia, Jiaqi Ma†, Qi Alfred Chen

University of California, Irvine, †University of California, Los Angeles

Take a picture for attack demo & more information!

Problem Formulation

- **Attack target:** Behavior Planning (BP) in Autonomous Driving (AD)
  - Making driving decisions (e.g., cruising, stopping) → ***highly security-critical***
- **Attack vector:** Attacker-controllable common road objects
  - E.g., dumped cardboard boxes, parked bikes on the road side
- **Attack goal**: Semantic Denial-of-Service (DoS) of BP
  - Emergency/permanent stop, give up critical driving decisions
- **Attack consequence:**
  - Damage the availability of AD-enabled commercial services and thus ruin the user experience, reputation, and also revenues
  - Possible safety problem, e.g., rear-end collisions due to emergency stop

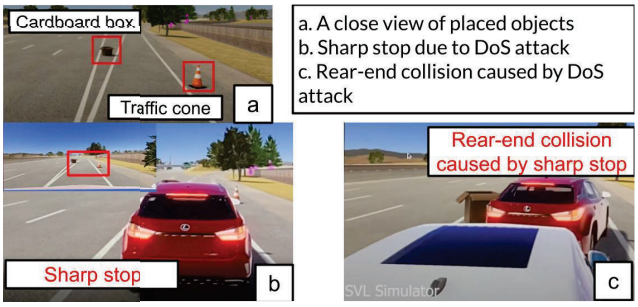


Summary

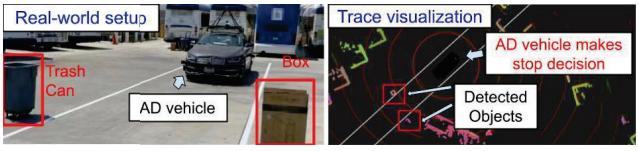
- *First* to perform **AD planning-specific** semantic vuln discovery
  - Focus: Semantic *DoS* vulnerabilities in Behavioral Planning (BP)
- Design **PlanFuzz**, which discovered 9 new vuln from Apollo & Autoware
  - Novel problem-specific designs on (1) *testing oracle*, (2) *input generation*, & (3) *effective code-level fuzzing guidance*
- Vuln exploit demo via simulation & real vehicle-based experiments

Exploitation Demonstration

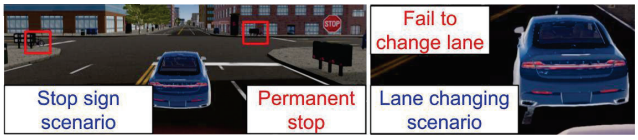
- Demo: DoS attack on Autoware lane following



- Demo: DoS attack on Autoware lane following demonstrated with real vehicle-based exp.



- See **our website** for demos of ***more discovered vulnerabilities*** in other scenarios (lane change, intersection, ...)



PlanFuzz: Novel Dynamic Testing Approach for Semantic DoS Vulnerabilities in AD BP