SaTC: TTP: Medium: Collaborative: Exposing and Mitigating Security/Safety Concerns of CAVs: A Holistic and Realistic Security Testing Platform for Emerging CAVs

UNIVERSITY OF MICHIGAN

UCI

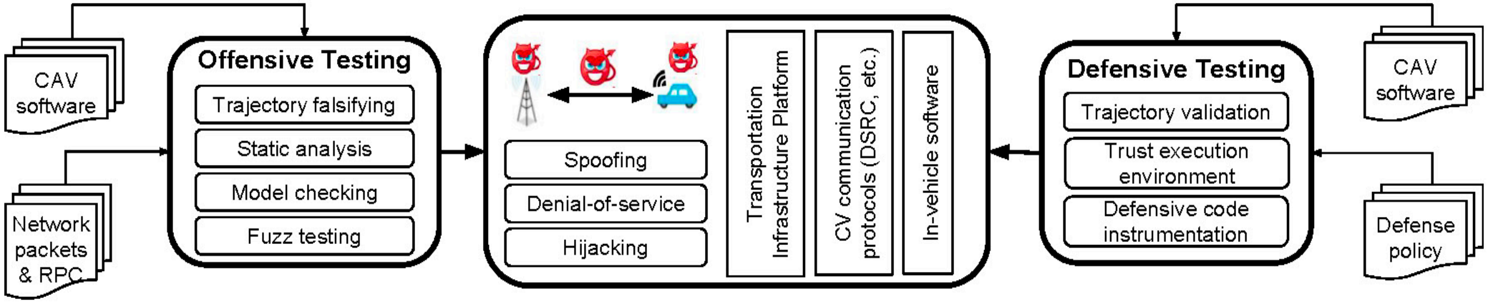
PURDUE UNIVERSITY

Challenge:

- Propose a novel CAV security/safety testing platform to address the critical needs for assessing CAV security and safety concerns in an effective & realistic manner.
- Develop, deploy, and integrate the proposed testing platform in real-world CAV testbeds and with a number of confirmed industry collaborators and early adopters.

Scientific Impact:

- The first platform to allow comprehensive evaluations of all 3 key CAV components in a unified framework
  - Necessary for systematic analysis of interdependent safety/security issues in the CAV eco-system
- Develop novel testing support by effectively combining techniques in optimization, statistical modeling, machine learning, network emulation, program analysis, & model checking.
- Build and evaluate both offensive and defensive testing support in real world environments



Solution:

- Provide both offensive & defensive testing services that cover 3 key components of CAV ecosystem: (1) transportation infra. platform, (2) CV comm. channels, (3) in-vehicle software platform.
- Highlights of new contributions:
  - Defensive testing support of detecting anomaly in localization module of autonomous vehicles (TRB'21)
  - Offensive testing support for denial-of-service vulnerabilities in connected vehicle protocols (Usenix Security'20)
  - Offensive testing support for robustness of 3D object detection sensor fusion models (ICIP'20)
  - Defensive testing support of using infrastructure-side camera for detecting CV data spoofing (under submission)

Projects: CNS-1930041, CNS-1929771

PIs: Z. Morley Mao (UMich), Qi Alfred Chen (UCI), Yiheng Feng (Purdue)

Broader Impact and Broader Participation:

- Allow hardware manufacturers, software developers, security service providers, and policymakers in the CAV industry and government to conveniently and holistically test their products against latest CAV attacks and study implications to different policies & regulations.
- Allow usage for training and education purposes for both schools and companies, and for facilitating the development of security best practices and standards in the CAV industry.
- Contributed course materials to the security and transportation courses at UMich (EECS 388), UCI (CS 134, CS 205), and Purdue (CE 299)