

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

Submitted by Zhuoqing Mao on Mon, 07/06/2020 - 12:18pm

Project Details

Lead PI

[Zhuoqing Mao](#)

Co-PIs

[Yiheng Feng](#)

Performance Period

Oct 01, 2019 - Sep 30, 2023

Institution(s)

Regents of the University of Michigan - Ann Arbor

Sponsor(s)

National Science Foundation

Award Number

[1930041](#)

Ranked 573 out of 2290 Group Projects.
94 related hits.

Connected and Automated Vehicle (CAV) technologies enable real-time information sharing and driving automation, with the potential of significantly improving safety and efficiency of the transportation system. However, cyber-security threats may compromise the efficiency of infrastructure operations and the safety of passengers, posing a significant challenge for CAV deployment. This collaborative project develops a novel CAV testing platform to address the critical needs for assessing the security and safety concerns of the CAV system in an effective and realistic manner. Hardware manufacturers, software developers, and security service providers in the CAV industry can all leverage such a platform to conveniently and holistically test their products. Moreover, the testing platform can be used for training and education in both academia and industry, and facilitate the development of security best practices and standards in industry.

The testing platform provides both offensive and defensive testing services covering three parts of the CAV ecosystem: (1) transportation infrastructure, (2) connected vehicle communication channels, and (3) in-vehicle software platform. It is the first CAV security testing platform supporting cross-component offensive and defensive testing services designed to capture the inter-relationships among the three key components. The project develops testing support by effectively combining techniques in optimization, statistical modeling, machine learning, network emulation, program analysis, and model checking, while supporting innovative use of known defense solutions, including trusted computing hardware, access control policy enforcement, and anomaly detection. The project implements and deploys the testing platform in real-world CAV testbeds and collaborates with industry partners for early adoption.



[Zhuoqing Mao](#)

Related Artifacts

No related artifacts found.



[TTP Medium Collaborative Division of Computer and Network Systems \(CNS\)](#)
