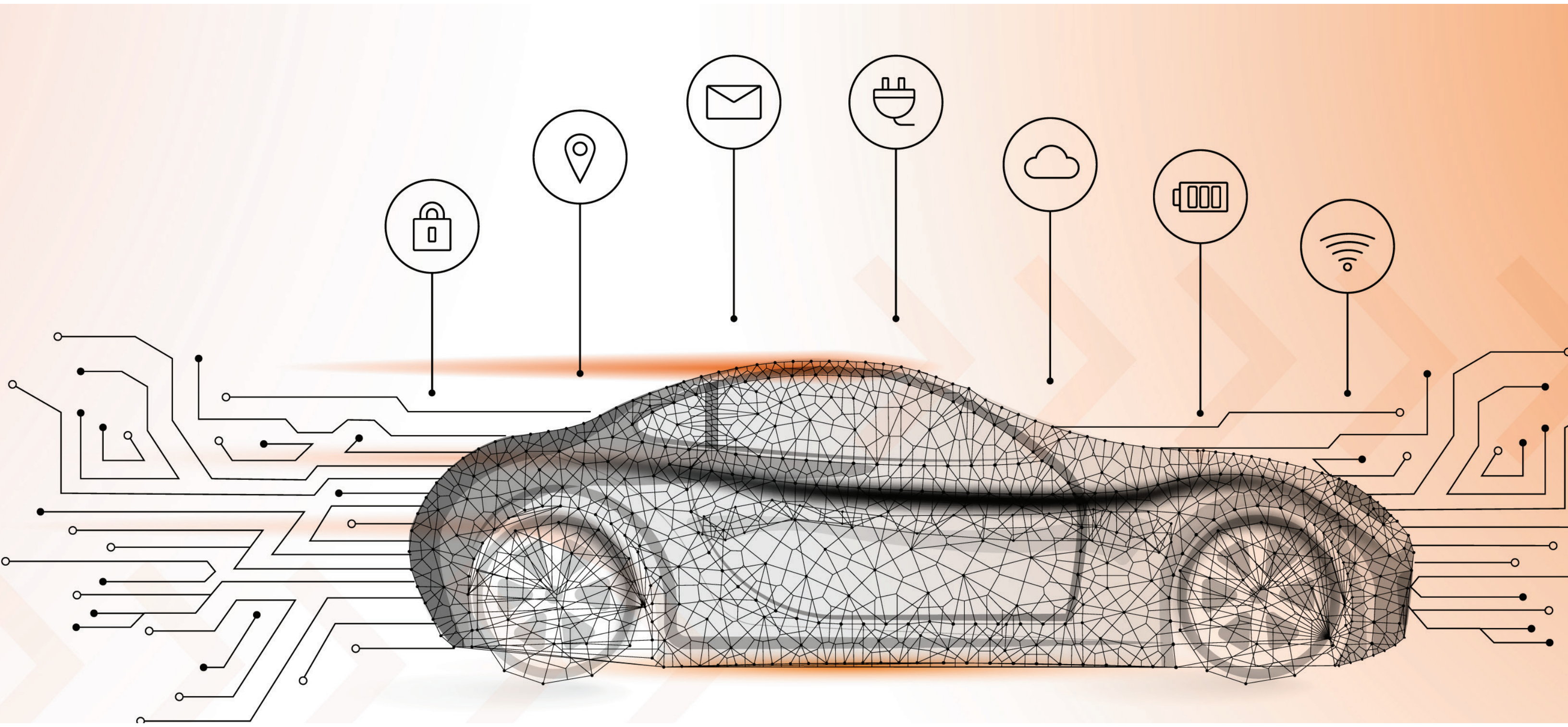
SJSU SAN JOSÉ STATE UNIVERSITY

CALIFORNIA STATE UNIVERSITY
LONG BEACH

Protecting Our Community from the Hidden Vulnerabilities of Today's Intelligent Transportation Systems

Project 2132
May 2022

Shahab Tayeb, PhD



Introduction

This project highlights the security vulnerabilities and attack surface of Controller Area Network (CAN) protocol, a common in-vehicle network standard found in all automobiles. Due to CAN's widespread use, any security vulnerabilities would have potentially catastrophic consequences for the public. Such vulnerabilities range from eavesdropping, where the attacker can read the raw data traversing the vehicle, to spoofing, where the attacker can place fabricated traffic on the network.

Study Methods

Through a simulation of the CAN, the researchers established the CAN data baseline and performed a closed-circuit analysis of penetration testing. The team then used a direct connection to the OBDII port for the hardware implementation component. Due to the obscure nature of CAN, the team reverse-engineered the missing parameters through a series of passive sniffing attacks on the network.

Findings

This project supplemented simulation findings with hardware implementation of event triggers on an actual vehicle. The team demonstrated the lack of confidentiality of the communication medium by eavesdropping on the traffic and its analysis. The lack of integrity was made visible through the placement of the spoofed CAN frames. These findings demonstrate the vulnerabilities of CAN and the need for increased cybersecurity protections.

Policy Recommendations

The findings suggest the necessity of a layered defense mechanism covering the fundamental pillars of cybersecurity from confidentiality to integrity, to authentication and non-repudiation. There are established guidelines on the best practices for each of these security requirements for non-vehicular networks. The transportation industry, and specifically the automotive industry, can adapt those best practices to better fit the requirements of such a robust system as a running vehicle along with its time-sensitive and lightweight requirements.

About the Author

Dr. Shahab Tayeb

Dr. Shahab Tayeb is a faculty member with the Department of Electrical and Computer Engineering in the Lyles College of Engineering at California State University, Fresno. Dr. Tayeb's research expertise and interests include network security and privacy, particularly in the context of the Internet of Vehicles. His research incorporates machine learning techniques and data analytics approaches to tackle the detection of zero-day attacks. Through funding from the Fresno State Transportation Institute, his research team has been working on the security of the network backbone for Connected and Autonomous Vehicles over the past two years. He has also been the recipient of several scholarships and national awards, including a US Congressional Commendation for STEM mentorship.

To Learn More

For more details about the study, download the full report at **transweb.sjsu.edu/research/2132**

MTI is a University Transportation Center sponsored by the U.S. Department of Transportation's Office of the Assistant Secretary for Research and Technology and by Caltrans. The Institute is located within San José State University's Lucas Graduate School of Business.