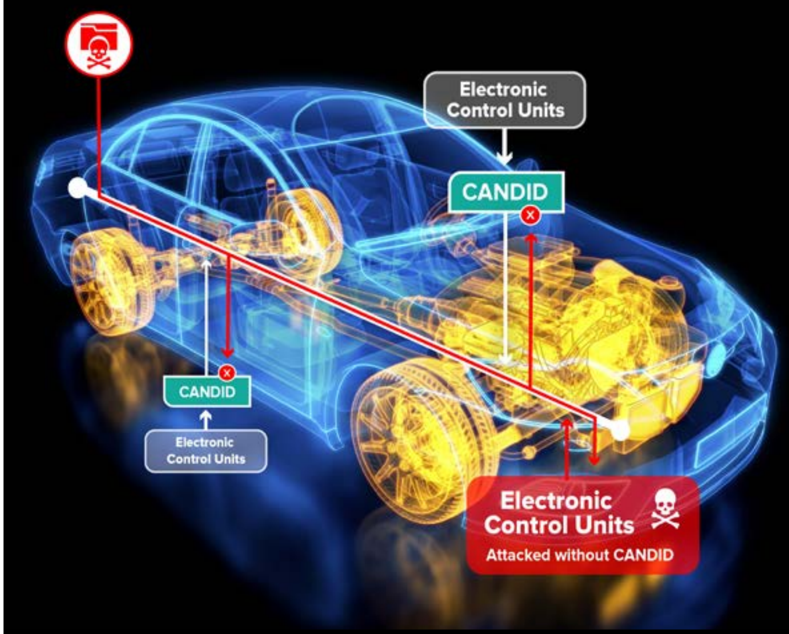
CANDID

Enhancing Vehicle Cybersecurity with Anomaly Detection

Anomaly detection for CAN systems

Charles River Analytics is developing a software/hardware solution to detect and mitigate cyberattacks on controller area networks (CANs) using advanced artificial intelligence/machine learning (AI/ML) techniques. These techniques learn what normal CAN traffic and electronic control unit (ECU) behavior looks like so they can identify anomalies as soon as they occur.

When CANDID identifies an intrusion, it handles the attack without driver input, dropping or modifying corrupt or malicious system messages without impacting vehicle operation.



Cybersecurity challenges facing intelligent vehicles

Vehicles are increasingly connected with their environment and other vehicles on the road using wireless communication tech, like Bluetooth and Wi-Fi. This greater connectivity exposes a broader attack surface. Regardless of make or model, vehicles rely on the same electronic components, made by the same manufacturers—meaning cyber vulnerabilities are widespread and quick to propagate.
We recognize that cybersecurity and vehicle protection are primary as the auto industry trends toward autonomous driving.

One particular vulnerability is the CAN. CANs have little built-in security, yet handle communications for the ECUs that are critical to the vehicle. ECUs run most essential vehicle functions, including brakes, engine, fuel injection, and tire pressure. Access to these functions makes cyberattacks on CANs and ECUs extremely dangerous, potentially resulting in a breach of confidential information or even total loss of vehicle control.

charles river analytics

Key advantages

CANDID equips your vehicles with state-of-the-art cyberattack detection and mitigation tech to keep your drivers and their data safe.

High cyberattack detection rates, including zero-day attacks

No modifications to existing protocols, systems, or components required

Flexible implementation does not require connectivity to a broader network

No added overhead; minimal size, weight, and power requirements

When CANDID identifies an intrusion, it handles the attack without driver input, dropping or modifying corrupt or malicious system messages without impacting vehicle operation.

This material is based upon work supported by the Army Contracting Command under Contract No. W56HZV-20-C-0092. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Army Contracting Command.

charles river analytics

Charles River Analytics uniquely combines agile innovation and leading-edge research with a decades-long track record of hardened engineering in austere environments to create best-in-class solutions to diverse, challenging problems.

For more information, contact

Brian Gzemski
Software Engineer,
Human-Centered AI
(617) 234-1595