VehicleSec '26: 4th USENIX Symposium on Vehicle Security and Privacy

August 10–11, 2026, Baltimore, MD, USA

Sponsored by USENIX, the Advanced Computing Systems Association

The 4th USENIX Symposium on Vehicle Security and Privacy (VehicleSec '26) will be co-located with the 35th USENIX Security Symposium and will take place August 10–11, 2026 in Baltimore, MD, USA.

Important Dates

- Paper submissions due: Tuesday, February 24, 2026, 23:59 AoE (Anywhere on Earth) time
- Notification of paper acceptance: Tuesday, April 7, 2026
- Final papers due: Wednesday, June 10, 2026
- Demo/Poster/Tutorial/Lightning Talk submissions due: ~~Tuesday, May 5, 2026~~ Tuesday, May 12, 2026
- Notification of Demo/Poster/Tutorial/Lightning Talk acceptance: Tuesday, May 26, 2026
- Demo/Poster/Tutorial final abstracts due: Wednesday, June 3, 2026

Overview

A vehicle is a machine that transports people and/or goods in one or more physical domains, such as on the ground (e.g., cars, bicycles, motorcycles, trucks, buses, scooters, trains), in the air (e.g., drones, airplanes, helicopters), in the water (e.g., ships, submarine), and in space (e.g., spacecraft). Due to their safety and mission-critical nature, the security and privacy of vehicles can pose direct threats to passengers, owners, operators, and the infrastructure. Recent improvements in vehicle autonomy and connectivity (e.g., autonomous driving, uncrewed aerial vehicles (UAVs), vehicle-to-everything (V2X) communication, intelligent transportation systems, and swarm robotics) have also served to exacerbate security and privacy challenges and thus require urgent attention from academia, industry, and policy-makers. To meet this critical need, VehicleSec aims to bring together an audience of university researchers, scientists, industry professionals, and government representatives to contribute new theories, technologies, and systems on any security/privacy issues related to vehicles (e.g., ground, aerial, in/on water, space), their sub-systems (e.g., in-vehicle networks, autonomy, connectivity, human-machine interfaces), supporting infrastructures (e.g., transportation infrastructure, charging station, ground control station), and related fundamental technologies (e.g., sensing, control, AI/ML/DNN/LLM, wireless communication, real-time computing, edge computing, location service, simulation, digital twin, multi-agent protocol/system design, and human-machine interaction).

Demo/Poster Session

VehicleSec will feature a demo/poster session to allow academic, governmental, and industry participants to share demonstrations and/or present posters of their latest practical attacks, defenses, and security/privacy tools or systems related to vehicles.

Tutorial Session

The symposium will also feature a tutorial session with an in-depth learning experience on one or more state-of-the-art topics in vehicle privacy and security presented by researchers or practitioners within the field. A tutorial should focus on its topic in detail and include references to the "must-read" papers or materials within its domain. Tutorials in which participants actively engage in exercises or hands-on work are particularly welcome. We encourage tutorials to include hands-on elements, live demonstrations, or interactive discussions. Each tutorial will be allocated a one-hour slot. Proposals should clearly indicate the format of the tutorial, prerequisites for participating in the tutorial (e.g., background knowledge, program languages), required materials (e.g., hardware, datasets, virtual machine images, wifi access), including (if any) material provided by the applicant (e.g., hardware, documentation).

Lightning Talks Session

The symposium will feature a Lightning Talks session with short and engaging 5-minute in-person presentations on any topics that can be worth a timely shout-out to the VehicleSec community, which include but are not limited to emerging hot topics, preliminary research results, practical problems encountered, lessons learned, the introduction of tutorials and education materials, tips and tricks, simulators/simulations, data and visualizations (e.g., autonomous driving datasets), or other (interdisciplinary) topics related to vehicles.

Awards

Accepted papers and demos/posters will be considered for Best Paper Award and Best Demo Award. Accepted artifacts will be considered for the Distinguished Artifact Award.

Areas of Interest

Topics of interest include, but are not limited to:

- Embedded/sensor/analog/actuator security, privacy, and forensics in vehicle settings
- Vehicle-related malware/firmware analysis
- Secure/resilient/trustworthy/privacy-preserving perception, localization, planning, and control in autonomous/automated vehicles
- Security/safety/robustness verification related to vehicles
- Intra- and inter-vehicle network (e.g., CAN bus, V2X, remote operator channel) security