3rd USENIX Symposium on Vehicle Security and Privacy (VehicleSec'25)

Seattle, Washington, USA
11-12 August 2025

ISBN: 979-8-3313-3699-8

Printed from e-media with permission by:

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571



Some format issues inherent in the e-media version may also appear in this print version.

Copyright© (2025) by Usenix Association
All rights reserved.

Printed with permission by Curran Associates, Inc. (2026)

For permission requests, please contact Usenix Association
at the address below.

Usenix Association
2560 Ninth Street, Suite 215
Berkeley, California, 94710

https://www.usenix.org/

Additional copies of this publication are available from:

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: 845-758-0400
Fax: 845-758-2633
Email: curran@proceedings.com
Web: www.proceedings.com

3rd USENIX Symposium on Vehicle Security and Privacy (VehicleSec '25)

August 11–12, 2025
Seattle, WA, USA

Monday, August 11

Vehicle Network Security

Stateful Behavior Inference and Runtime Enforcement for Vehicle Network Security 1
Achintya Desai, *UC Santa Barbara;* Ruochen Dai, *University of Florida;* Yanju Chen, *UC Santa Barbara;* Ky Ho, *Oceanit Laboratories;* Austin Kee, *University of Florida;* Sophie Bulatovic, *Oceanit Laboratories;* Md Shafiuzzaman, *UC Santa Barbara;* Ken (Yihang) Bai, *University of Florida;* Il Ung Jeong and David Siu, *Oceanit Laboratories;* Tuba Yavuz, *University of Florida;* Tevfik Bultan, *UC Santa Barbara*

WIP: Intrusion Detection and Localization for CAN by Extracting Propagation Delay Features from Message Intervals 19
Zhaozhou Tang, *Georgia Institute of Technology;* Khaled Serag, *Qatar Computing Research Institute;* Saman Zonouz, *Georgia Institute of Technology;* Z. Berkay Celik and Dongyan Xu, *Purdue University;* Raheem Beyah, *Georgia Institute of Technology*

CANdid - An Open-Access Annotated Dataset of Vehicle CAN Bus Traffic 27
Tomas Howson, *CSSM, School of Physics, Chemistry and Earth Sciences, University of Adelaide;* Alexander Rohl, *Defence Science and Technology Group, Australia;* Matthew Roughan, *School of Computer and Mathematical Sciences, University of Adelaide;* Martin White and James Zanotti, *CSSM, School of Physics, Chemistry and Earth Sciences, University of Adelaide*

Drone Security

ConfuSense: Sensor Reconfiguration Attacks for Stealthy UAV Manipulation 45
Alessandro Erba, *KASTEL Security Research Labs, Karlsruhe Institute of Technology;* John H. Castellanos, *Hitachi Energy Research, Germany;* Sahil Sihag, *CISPA Helmholtz Center for Information Security;* Saman Zonouz, *Georgia Institute of Technology;* Nils Ole Tippenhauer, *CISPA Helmholtz Center for Information Security*

WIP: Hijacking Attacks on UAV Follow-Me Systems in Realistic Scenarios 63
Jiarui Li, Joseph Brewington, Qingzhao Zhang, and Z. Morley Mao, *University of Michigan*

WIP: Evaluating the End-to-End Impact of False Localization Attacks on vSLAM-Based Autonomous Drones . . . 73
Yuga Ebine, *Waseda University;* Kazuki Nomoto and Yuna Tanaka, *Waseda University, Deloitte Tohmatsu Cyber LLC;* Ryunosuke Kobayashi and Go Tsuruoka, *Waseda University;* Tatsuya Mori, *Waseda University, RIKEN AIP, NICT*

Electric Vehicle Charging Security 1

EmuOCPP: Effective and Scalable OCPP Security and Privacy Testing 81
Soumaya Boussaha, *SAP, EURECOM;* Victor Fresno Gómez, *EURECOM, UPM;* Thomas Barber, *SAP SE;* Daniele Antonioli, *EURECOM*

Short: Breaking the Charge: Exploiting State Manipulation in EV Charging 99
Ce Zhou and Qiben Yan, *Michigan State University;* Zhiyan Yu, *Washington University in Saint Louis;* Eshan Dixit, *Michigan State University;* Ning Zhang, *Washington University in Saint Louis;* Huacheng Zeng, *Michigan State University;* Alireza Safdari Ghanhdari, *Rectrix Inc*

Autonomous Vehicle Privacy

You Can Drive But You Cannot Hide: Detection of Hidden Cellular GPS Vehicle Trackers 109
Moshe Chaim Satt, Donghan Hu, Patrick Zielinski, and Danny Yuxing Huang, *New York University*

WIP: Blurred Lines – A GDPR-Compliant Framework for Anonymising Automotive Video Data 125
Rithwik Vinod and Luca Arnaboldi, *University of Birmingham*

Secure FLOATING - Scalable Federated Learning Framework for Real-time Trust in Mobility Data using Secure Multi-Party Computation and Blockchain 133
Junaid Ahmed Khan, *Western Washington University;* Kaan Ozbay, *New York University*

Hardware Security

CarPlay at Risk: Unveiling Security Threats of Third-Party Infotainment Adapters 143
Jun Yeon Won, Wenzhuo Wang, Keith Redmill, and Zhiqiang Lin, *Ohio State University*

SoK: Stealing Cars Since Remote Keyless Entry Introduction and How to Defend From It 161
Tommaso Bianchi and Alessandro Brighente, *University of Padova;* Mauro Conti, *University of Padova, Delft University of Technology;* Edoardo Pavan, *University of Padova*

Threat Analysis and Detection in In-Vehicle Infotainment System Leveraging MITRE ATT&CK and Suricata. . . .179
Yeonjae Kang and Huy Kang Kim, *Korea University*

Tuesday, August 12

Autonomous Vehicle Security

Beyond the Glow: Understanding Luminescent Marker Behavior Against Autonomous Vehicle Perception Systems 195
Arkajyoti Mitra, *University of Texas at Arlington;* Pedram MohajerAnsari, *Clemson University;* Afia Anjum and Paul Agbaje, *University of Texas at Arlington;* Mert D. Pesé, *Clemson University;* Habeeb Olufowobi, *University of Texas at Arlington*

WIP: Understanding the Mechanisms Behind NDT-Based Localization Vulnerabilities in Autonomous Driving 211
Yuna Tanaka and Kazuki Nomoto, *Waseda University, Deloitte Tohmatsu Cyber LLC;* Ryunosuke Kobayashi and Go Tsuruoka, *Waseda University;* Tatsuya Mori, *WasedaUniversity, NICT, RIKEN AIP*

Electric Vehicle Charging Security 2

Oblivious Plug&Charge: A Privacy-Preserving EV Charging Scheme based on ORAM 221
Timm Lauser, *Darmstadt University of Applied Sciences;* Nergiz Yuca, *University of Passau;* Dustin Kern, *Darmstadt University of Applied Sciences;* Nikolay Matyunin, *Honda Research Institute Europe GmbH;* Stefan Katzenbeisser, *University of Passau;* Christoph Krauß, *Darmstadt University of Applied Sciences*

DrainDead: Emptying Batteries of Parked Electric Vehicles. 233
Jakob Löw and Dominik Bayerl, *Technische Hochschule Ingolstadt;* Kevin Mayer, *Friedrich-Alexander Universität Erlangen-Nürnberg;* Hans-Joachim Hof, *Technische Hochschule Ingolstadt*

Short: PIBuster: Exploiting a Common Misconfiguration in CCS EV Chargers 243
Marcell Szakály, Sebastian Köhler, and Ivan Martinovic, *University of Oxford*

Human Aspects of Vehicle Security and Privacy

Human Drivers' Awareness of Utility and Privacy Risks of Vehicle-to-Everything Communication: A Driving Simulator Study 251
Zekun Cai, Rao Li, and Aiping Xiong, *The Pennsylvania State University*

Short: Unencrypted Flying Objects: Security Lessons from University Small Satellite Developers and Their Code 269
Rachel McAmis and Gregor Haas, *University of Washington;* Mattea Sim, *Indiana University;* David Kohlbrenner and Tadayoshi Kohno, *University of Washington*

Vehicle Security Analysis

WIP: QKSAN: Towards Multiple Sanitizers for In-vehicle COTS OS Kernels. 279
Yalong Zou, Ziqiu Cheng, and Dongliang Mu, *Huazhong University of Science and Technology*

Short: APSFuzz: Simulation-Based Fuzzing Testing for Automated Parking Systems 289
Tong Bu, Jiarun Dai, Jiaqi Luo, Songyang Peng, Zongan Huang, and Min Yang, *Fudan University*

WIP: A Black Box System for Automotive Digital Forensics 297
Muhammad Yusuf Bambang Setiadji, Eirini Anthi, and Theodoros Spyridopoulos, *Cardiff University;* Gareth Davies, *Thales UK*

AI-Based Attacks and Defenses

WIP: Evaluation of Threats and Impacts of HD Map Tampering Attacks in Autonomous Driving 307
Miyu Sato and Ryunosuke Kobayashi, *Waseda University;* Kazuki Nomoto and Yuna Tanaka, *Waseda University, Deloitte Tohmatsu Cyber LLC;* Go Tsuruoka, *Waseda University;* Tatsuya Mori, *Waseda University, NICT, RIKEN AIP*

WIP: From Detection to Explanation: Using LLMs for Adversarial Scenario Analysis in Vehicles 315
David Fernandez, Pedram MohajerAnsari, Cigdem Kokenoz, Amir Salarpour, Bing Li, and Mert D. Pesé, *Clemson University*

Lightweight Deep Learning for Cyber-Resilient Heavy Vehicles: Efficient Signal Reconstruction on Embedded Systems 325
Maxwel Bar-on, *Colorado State University;* Hossein Shirazi, *San Diego State University;* Indrakshi Ray and Jeremy Daily, *Colorado State University*

WIP: Learning Adversarial Attacks on Adaptive Traffic Signal Control Systems Under Cooperative Perception. . . 343
Wangzhi Li, Tianheng Zhu, and Yiheng Feng, *Purdue University*