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

August 11–12, 2025, Seattle, WA, USA

Sponsored by USENIX, the Advanced Computing Systems Association

The 3rd USENIX Symposium on Vehicle Security and Privacy (VehicleSec '25) will be co-located with the 34th USENIX Security Symposium and will take place August 11–12, 2025 at the Seattle Convention Center in Seattle, WA, USA.

Important Dates

- Paper submissions due: **Thursday, February 27, 2025, 23:59 AoE (Anywhere on Earth) time**
- Notification of paper acceptance: **Thursday, April 10, 2025**
- Final papers due: **Thursday, May 15, 2025**
- Demo/Poster/Tutorial/Lightning Talk submissions due: **Thursday, May 1, 2025**
- Notification of Demo/Poster/Tutorial/Lightning Talk acceptance: **Thursday, May 15, 2025**
- Demo/Poster/Tutorial final abstracts due: **Thursday, May 22, 2025**

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, boats, watercraft), 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, unmanned 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 either a one-hour or a two-hour slot, depending on the scope and depth of the content. Proposals should clearly indicate the preferred duration and format of the tutorial.

Lightning Talk 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 a **Best Paper Award** and **Best Demo Award**. In addition, a special **AutoDriving Security Award** will be given to one of the accepted papers to recognize and reward research that makes substantial contributions to secure today's autonomous driving technology.

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
- Multi-vehicle coordination/cooperation (e.g., V2X, drone swarm) security
- Compliance with policies (e.g., legal, security, privacy, safety, and environmental policies)
- Secure integration of hardware and software systems for vehicles (e.g., ground, aerial)
- Secure software/hardware updates in vehicle settings (e.g., cars, drones, airplanes)
- Privacy challenges in vehicle settings, e.g., driver/passenger privacy, drone/car/robot spying, intellectual property stealing, etc.
- Privacy-preserving data sharing and analysis in vehicle settings
- Security/privacy in electric, medium- and heavy-duty vehicle systems
- Security/privacy in Intelligent Transportation Systems (ITS), e.g., intelligent traffic signals
- Security/privacy for vehicle-related supporting infrastructure (e.g., charging)
- Secure vehicle-related software/hardware development process (e.g., debugging tools, simulators, testbed) and their own security/privacy
- Security/privacy of any vehicle-related fundamental technologies (e.g., sensing, control, AI, location service, IoT, etc.)
- Human factors, trust, humans in the loop, and usable security related to vehicles
- Security/privacy/resilience-related metrics and risk assessment for vehicles
- GenAI-enabled attacks on vehicles and corresponding defensive approaches
- GenAI tools and frameworks for the security of vehicles

Ethical Considerations

We expect authors to carefully consider and address the potential harms associated with carrying out their research, as well as the potential negative consequences that could stem from publishing their work. Failure to do so may result in the rejection of a submission regardless of its quality and scientific value. Where relevant, papers should include a clear statement about why the benefit of the research outweighs the harms and how the authors have taken measures and followed best practices to ensure safety and minimize the potential harms caused by their research. This includes but is not limited to, considering the impact of your research on deployed systems, understanding the costs your research imposes on others, safely and appropriately collecting data, and following responsible disclosure.

Human Subjects Research

If your submitted document relates to human subjects, analyzes data derived from human subjects, may put humans at risk, or might have other ethical implications or introduce legal issues of potential concern to the VehicleSec community, authors should disclose if an ethics review (e.g., IRB approval) was conducted, and discuss in the paper how ethical and legal concerns were addressed.

Vulnerability Disclosure

If your submitted document reports a potentially high-impact vulnerability, the authors should discuss in detail the steps they have already taken or plan to take to address these vulnerabilities (e.g., by disclosing vulnerabilities to the vendors). The chairs will contact the authors in case of concerns. The Program Committee reserves the right to reject a submission if insufficient evidence was presented that ethical or relevant legal concerns were appropriately addressed.

Conflicts of Interest

Authors and Program Committee members are required to indicate any conflict of interest and its nature. Advisors and those that they are advising, as well as authors and PC members with an institutional relationship, are considered to share a conflict of interest. Professional collaborations (irrespective of whether they resulted in publication or funding) that occurred in the past 2 years and close personal relationships equally constitute a conflict of interest. PC members, including chairs, who have a conflict of interest with a paper will be entirely excluded from the evaluation of that paper.

A Special Note on "Fake Conflicts": Declaring conflicts of interest to avoid certain (otherwise non-conflicting) PC members is not allowed and can constitute grounds for rejection. The PC Chairs reserve the right to request additional explanation for any declared conflict. If authors have concerns about the fair treatment of their submissions, they should instead contact the chairs and provide convincing arguments for any special consideration that they are requesting.

Acknowledgment

Final versions of accepted submissions should include all sources of funding in an acknowledgments section. Authors should also disclose any affiliations, interests, or other facts that might be relevant to readers seeking to interpret the work and its implications. Authors may wish to consider the 2025 IEEE S&P Financial Conflicts Policy available at www.ieee-security.org/TC/SP2025/financial-con.html for examples.

Submission Guidelines for Papers

We accept (1) regular papers up to 13 pages and (2) short position papers or work-in-progress (WIP) papers up to 6 pages, excluding references and appendices. Short papers are suitable for position papers or original works whose descriptions fit within 6 pages. WIP papers are suitable for original yet incomplete work that is looking for middle-stage feedback from the community. We also accept Systemization of Knowledge (SoK) papers; the length of SoK papers should be similar to regular papers. Note that reviewers are not required to read the appendices or any supplementary

material. Once accepted, the camera-ready version of regular and SoK papers should be at most 18 pages, and short position papers or work-in-progress (WIP) papers should be at most 10 pages, including the bibliography and any appendices. Authors should not change the font or the margins of the USENIX format. **For regular papers, shorter papers won't be penalized; thus, authors are encouraged to submit papers of appropriate length based on the research contribution.**

Submissions should be typeset in two-column format using 10-point type on 12-point (single-spaced) leading in a text block 7" wide x 9" deep, with .33" inter-column space, formatted for 8.5" x 11" paper. Authors must use the USENIX templates and style files available at www.usenix.org/conferences/author-resources/paper-templates when preparing their paper for submission. Failure to adhere to the page limit and formatting requirements can be grounds for rejection. Submissions must be in Portable Document Format (PDF). Authors should pay special attention to unusual fonts, images, and figures that might create problems for reviewers. Documents should render correctly in Adobe Reader when printed in black and white.

Submissions should be anonymized for review; no author names or affiliations may appear on the title page, and papers should avoid revealing authors' identities in the text. When referring to their previous work, authors are required to cite their papers in the third person without identifying themselves. Acceptance of final papers may be subject to shepherd approval.

Short, WIP, and SoK papers must have the prefix "Short:"/ "WIP:"/"SoK:" in their titles. The submission form will be linked from the Call for Papers web page.

Once a paper is accepted, at least one of the authors is expected to attend the conference to present it. Alternative arrangements can be made if there are justifiable difficulties in travel and will be allowed only on a case-by-case basis with permission from the Program Co-chairs. The proceedings will be published and archived by USENIX.

Double and Concurrent Submissions

Technical papers must not substantially overlap with papers that have been published or that are simultaneously submitted to a journal or a conference/workshop with proceedings. Double-submission will result in immediate rejection. The Program Committee may share information with other conference chairs and journal editors so as to detect such cases.

Submission and Publication Process

The program committee and external reviewers are required to treat all submissions as confidential. However, the program co-chairs or designated committee members may share submissions outside the program committee to allow chairs of other conferences to identify dual submissions. Papers that do not comply with the submission requirements, including length and anonymity, or that do not have a clear application to vehicle security and privacy may be rejected without review. Papers accompanied by nondisclosure agreement forms will not be considered.

Accepted submissions will be treated as confidential prior to publication on the VehicleSec '25 website; rejected submissions will be permanently treated as confidential.

As part of USENIX's open-access policy, all papers will be available online before the conference. If your accepted paper should not be published prior to the event, please notify production@usenix.org after you submit your final accepted paper. USENIX also allows authors to retain ownership of the copyright in their works, requesting only that USENIX be granted the right to be the first publisher of that work. See our sample consent form available at www.usenix.org/sites/default/files/consent_author_proceedings.pdf for the complete terms of publication. If the conference registration fee will pose a hardship for the presenter of an accepted paper, please contact conference@usenix.org.

If you have any other questions related to the submission process, please email the program co-chairs at vehiclesec25chairs@usenix.org. Please reach out as soon as possible, as it may not be possible to answer late questions prior to the submission deadline.

Submission Guidelines for Demos and Posters

We accept demos and posters of up to 2 pages, including references and appendices. Submissions should be typeset in two-column format using 10-point type on 12-point (single-spaced) leading in a text block 7" wide x 9" deep, with .33" inter-column space, formatted for 8.5" x 11" paper. Authors must use the USENIX templates and style files available at www.usenix.org/conferences/author-resources/paper-templates when preparing their demo and poster for submission. Submissions must be in Portable Document Format (PDF). Authors should pay special attention to unusual fonts, images, and figures that might create problems for reviewers. Documents should render correctly in Adobe Reader when printed in black and white.

Submissions can be anonymized for review, but it is not mandatory. Demo and Poster papers must have the prefix "Demo:" or "Poster:" in their titles. The submission portal for Demos and Posters will be linked from the Call for Papers web page.

To allow attendees to better learn and experience practical vehicle-related attacks, defenses, and tools, VehicleSec will structurally encourage authors to submit Demos. Specifically, all accepted demos will be provided a demo table and a poster easel (so a superset of the setup for an accepted Poster, which will be provided only a poster easel). At the presentation time, each demo should have (1) exhibitions, slides, videos, and/or interactive/live demos to showcase on the table and (2) a poster presentation of the demo to be put on the easel. All the accepted demos will be considered for the Best Demo Award. Note that although the setup of a demo includes a poster during the presentation, authors only need to submit a demo paper. For additional information regarding demos and posters, please do not hesitate to contact the Demo/Poster Chair Qiben Yan at vehiclesec25-demos-posters@usenix.org.

Submission Guidelines for Tutorials

We invite tutorial proposals to be a part of the tutorial sessions taking place during the symposium on August 11, 2025. Tutorials aim to offer participants an in-depth and practical understanding of emerging topics in vehicle security and privacy, spanning research advancements, industry practices, and critical policy issues. We welcome proposals from researchers, practitioners, and educators in academia, industry, and government.

We encourage tutorials to include hands-on elements, live demonstrations, or interactive discussions. Each tutorial will be allocated either a one-hour or two-hour slot, depending on the scope and depth of the content. Proposals should clearly indicate the preferred duration and format of the tutorial.

We accept tutorial submissions of up to 2 pages, including references and appendices. Tutorial proposals must include:

- **Title:** A concise and descriptive title.
- **Abstract:** A brief summary (up to 500 words) outlining the tutorial's scope, objectives, and intended audience.
- **Presenter(s):** Names, affiliations, and a short bio (a maximum of 250 words each) highlighting relevant expertise and experience.
- **Target Audience:** Specify the expected audience, required prior knowledge, and estimated number of attendees.
- **Content Outline:** Detailed breakdown of topics to be covered and expected learning outcomes.
- **Format and Duration:** Proposed session length (one-hour or two-hour) and preferred mode of delivery (e.g., lecture, hands-on, hybrid).
- **Special Requirements:** Any technical or logistical needs (e.g., software, hardware, internet connectivity). Note that requirements will be reviewed along with the submission and, if accepted, submitters will be notified of what needs can and cannot be fulfilled.
- **Supporting Material:** Any existing slides, reference materials, or prerequisites (optional).

Submissions should be typeset in two-column format using 10-point type on 12-point (single-spaced) leading in a text block 7" wide x 9" deep, with .33" inter-column space, formatted for 8.5" x 11" paper. Authors must use the USENIX templates and style files available at www.usenix.org/conferences/author-resources/paper-templates when preparing their tutorial for submission. Submissions must be in Portable Document Format (PDF). Authors should pay special attention to unusual fonts, images, and figures that might create problems for reviewers. Documents should render correctly in Adobe Reader when printed in black and white.

Submissions can be anonymized for review, but it is not mandatory. Tutorial submissions must have the prefix "Tutorial:" in their titles. The submission portal for tutorials will be linked from the Call for Papers web page.

Tutorial proposals will be evaluated based on:

- Relevance to the symposium themes.
- Clarity and comprehensiveness of the proposal.
- Practicality and accessibility of the tutorial content.
- Presenter expertise and experience.

We encourage diversity in topics and presenters to provide participants with a broad range of learning opportunities. For additional information regarding tutorials, do not hesitate to contact the Tutorial Chair, Mert Pesé, at vehiclesec25-talks-tutorials@usenix.org.

Submission Guidelines for Lightning Talks

We will host a Lightning Talks session at the symposium. We solicit 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, work-in-progress research ideas, and preliminary results, practical problems encountered, lessons learned, tips and tricks, simulators/simulations, data and visualizations (e.g., autonomous driving datasets), or other (interdisciplinary) topics related to vehicles.

Note that the lightning talks **are not** intended for self-promotion or commercial advertisement. Specifically, share concepts, methodologies, or findings that can be broadly applied or spark meaningful discussions. Focus on the work itself rather than promoting your product, service, or organization. Avoid sales pitches, advertisements, or excessive emphasis on personal or corporate achievements.

Please submit your Lightning Talk title and abstract (200 words or less) for full consideration via the Lightning Talk submission form linked from the Call for Papers web page. Lightning Talk abstracts will be published on the symposium website.

All lightning talk submissions must include the presenter's name, affiliation, and contact information. Please note that the presenter must make all submissions. Submissions from PR firms will be rejected without review. A time limit for lightning talks will be strictly enforced. For additional information regarding Lightning Talks, do not hesitate to contact the Lightning Talk Chair, Mert Pesé, at vehiclesec25-talks-tutorials@usenix.org.

Symposium Organizers

General Chairs

Z. Berkay Celik, *Purdue University*
Ning Zhang, *Washington University at St. Louis*

Program Co-Chairs

Sara Rampazzi, *University of Florida*
Aiping Xiong, *The Pennsylvania State University*

Program Committee

Houssam Abbas, *Oregon State University*
Sri Hrushikesh Varma Bhupathiraju, *University of Florida*
Antonio Bianchi, *Purdue University*
Gedare Bloom, *University of Colorado Colorado Springs*
Alvaro Cardenas, *University of California, Santa Cruz*
Stephen Checkoway, *Oberlin College*
Dongyao Chen, *Shanghai Jiao Tong University*
Hanlin Chen, *Oak Ridge National Laboratory*
Andrew Clark, *Washington University in St. Louis*
Michael Clifford, *Toyota*
Mauro Conti, *University of Padova*
Jiarun Dai, *Fudan University*
Jeremy Daily, *Colorado State University*
Ivan De Oliveira Nunes, *Rochester Institute of Technology*
Divanilson Rodrigo de Sousa Campelo, *Federal University of Pernambuco*
Bruce DeBruhl, *California Polytechnic State University*
Thomas Forest, *General Motors*
Daniel Fremont, *University of California, Santa Cruz*
Xing Gao, *University of Delaware*
Luis Antonio Garcia, *The University of Utah*
Ryan Gerdes, *Virginia Tech*
Sheikh Mahbub Habib, *Continental AG*
Mohammad Hamad, *Technical University of Munich*
Xiali Hei, *University of Louisiana at Lafayette*
Bardh Hoaxa, *Toyota Research Institute of North America (TRINA)*
Hans-Joachim Hof, *The Technical University Ingolstadt of Applied Sciences*
Hongxin Hu, *University at Buffalo*
Shengtuo Hu, *ByteDance*
Murtuza Jadliwala, *The University of Texas at San Antonio*
Shalabh Jain, *Bosch*
Sashidhar Jakkamsetti, *Bosch*
Xiaoyu Ji, *Zhejiang University*
Justin Kappos, *New York University*

Ameer Kashani, *Denso*
Chung Hwan Kim, *The University of Texas at Dallas*
Huy Kang Kim, *Korea University*
Taegyu Kim, *The Pennsylvania State University*
Yongdae Kim, *Korea Advanced Institute of Science and Technology (KAIST)*
Vireshwar Kumar, *IIT Delhi*
Xiaojing Liao, *Indiana University*
Zhiqiang Lin, *Ohio State University*
Peng Liu, *The Pennsylvania State University*
Wenjing Lou, *Virginia Tech*
Li Lu, *Zhejiang University*
Mulong Luo, *Cornell University*
Muslum Ozgur Ozmen, *Arizona State University*
Christos Papadopoulos, *University of Memphis*
Karthik Pattabiraman, *University of British Columbia*
Jonathan Petit, *Qualcomm*
Hang Qiu, *University of California, Riverside*
Hanif Rahbari, *Rochester Institute of Technology*
Prashanth Rajivan, *University of Washington*
Indrakshi Ray, *Colorado State University*
Kui Ren, *Zhejiang University*
Takami Sato, *University of California, Irvine*
Neetesh Saxena, *Cardiff University*
Yasser Shoukry, *University of California, Irvine*
Ruoyu Song, *Purdue University*
Takeshi Sugawara, *The University of Electro-Communications*
Dave (Jing) Tian, *Purdue University*
Jinwen Wang, *Washington University in St. Louis*
Lan Wang, *University of Memphis*
Ningfei Wang, *University of California, Irvine*
André Weimerskirch, *Block Harbor Cybersecurity*
Luyi Xing, *Indiana University*
Xiangru Xu, *University of Wisconsin—Madison*
Carter Yagemann, *Ohio State University*
Kun Yang, *Zhejiang University*
Min Yang, *Fudan University*
Kentaro Yoshioka, *Keio University*
Zhiyuan Yu, *Washington University in St. Louis*
Xugui Zhou, *Louisiana State University*
Shuguo Zhuo, *Zhejiang University*
Saman Zonouz, *Georgia Institute of Technology*

Poster/Demo Program Chair
Qiben Yan, *Michigan State University*

Poster/Demo Program Committee
Noah T. Curran, *University of Michigan*
Pedram MohajerAnsari, *Clemson University*
Amir Salarpour, *Clemson University*
Yazhou Tu, *Auburn University*
Guangjing Wang, *University of South Florida*
Jinwen Wang, *Washington University in St. Louis*
Qiben Yan, *Michigan State University*
Zhiyuan Yu, *Washington University in St. Louis*
Ce Zhou, *Michigan State University*

Lightning Talk and Tutorial Chair
Mert Pesé, *Clemson University*

Publications Chair
Yiheng Feng, *Purdue University*

Publicity Chair
Hyungsub Kim, *Indiana University*

Program Committee Local Arrangements Chair
Habiba Farrukh, *University of California, Irvine*

Sponsorship Chair
Luis Garcia, *The University of Utah*

Travel Grant Chair
Nidhi Rastogi, *Rochester Institute of Technology*

Steering Committee
Gail-Joon Ahn, *Arizona State University*
David Balenson, *USC Information Sciences Institute*
Chunming Qiao, *University at Buffalo*
Kang Shin, *University of Michigan*
Mani Srivastava, *University of California, Los Angeles*
Gene Tsudik, *University of California, Irvine*
Dongyan Xu, *Purdue University*