Call for Papers: ISOC Symposium on Vehicle Security and Privacy (VehicleSec 2024)

Co-located with NDSS 2024, San Diego, CA

A vehicle is a machine that transports people and/or cargo 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), underwater (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, as well as the environment. Recent improvements in vehicle autonomy and connectivity (e.g., autonomous driving, drone delivery, vehicle-to-everything (V2X) communication, intelligent transportation, drone swarm), have only served to exacerbate security and privacy challenges and thus require urgent attention from academia, industry, and policy-makers. To meet this critical need, the ISOC (Internet Society) VehicleSec symposium aims at bringing 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, underwater, 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, real-time computing, edge computing, location service, simulation, digital twin, multi-agent protocol/system design, and human-machine interaction).

The **Second ISOC Symposium on Vehicle Security and Privacy** (VehicleSec 2024) will take place February 26, 2024 in conjunction with the Network and Distributed System Security Symposium (NDSS) 2024 in San Diego, CA.

Community Reception. VehicleSec will host a reception as a community social event on the night of the symposium (February 26, 2024), with refreshments such as food and drinks.

Keynote Speech: Following the model of VehicleSec 2023 and its predecessor, AutoSec workshops, we intend to feature **two keynotes**, one from academia and another from the industry, aiming at offering VehicleSec attendees a broader and more diverse perspective on the problem space.

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

Lightning Talk Session: The symposium will feature a Lightning Talks session with short and engaging 5-minute "live" presentations on any topics that can be worth a timely shout-out to the VehicleSec community, which includes but 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/Poster Award**. The winner and runner-up will receive cash prizes. In addition, a special **AutoDriving Security Award**, with a cash prize, 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.

Travel Grants: Selected students will be provided with support to attend the symposium in person.

Submission Guidelines for Papers/Demos/Posters:
We accept (1) **regular papers up to 10 pages,** (2) **short position papers** or **work-in-progress (WIP) papers up to 6 pages**, and (3) **demo/poster papers up to 1 page**, all in double-column NDSS format and including references and appendices. We also accept **Systemization of Knowledge (SoK) papers**; in this case, the paper length can be **up to 10 pages**, excluding references and well-marked appendices. Note that reviewers are not required to read the

appendices or any supplementary material. Authors should not change the font or the margins of the NDSS 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.

Papers must be formatted for US letter size (not A4) paper in a two-column layout, with columns no more than 9.25 in. high and 3.5 in. wide. The text must be in Times font, 10-point or larger, with 11-point or larger line spacing. Authors must use the NDSS templates. The NDSS 2024 templates are available at https://www.ndss-symposium.org/ndss2024/submissions/templates/. 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' identity in the text. When referring to their previous work, authors are required to cite their papers in the third person, without identifying themselves.

Short/WIP/SoK/demo/poster papers must have the prefix "Short:"/"WIP:"/"SoK:"/"Demo:"/"Poster:" in their titles. The submission portal for Papers/Demos/Posters is at:

https://submit.vehiclesec.io/

Once accepted, at least one of the authors should 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 PC Chairs. The proceedings will be published and archived by the Internet Society (ISOC).

Submission Guidelines for Lightning Talks:

We solicit short and engaging 5-minute "live" (in-person) presentations on any topics that can be worth a timely shout-out to the VehicleSec community, which includes but 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. A good lightning talk should be to present an (outrageous) idea to engage the community and spark future research.

Please submit your Lightning Talk title and abstract (200 words or less) for full consideration via the Lightning Talk submission form by **January 11, 2024**. Lightning Talk abstracts will be published on the symposium website.

- All 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.
- Time limits will be strictly enforced.
- For additional information regarding Lightning Talks, do not hesitate to contact the Lightning Talk Chair Ming Li at lim@arizona.edu.

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-preservin g 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 light
- 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
- Attacks leveraging GenAI (e.g., large language model) technologies and defense in response to GenAI technologies

Important Dates

- Paper/Poster/Demo Submission Deadline: **Anywhere-on-earth (AOE) December 15, 2023**
- Lightning Talk Submission Deadline: January 11, 2024
- Notification of Acceptance: January 25, 2024
- Camera Ready Submission: February 10, 2024
- Symposium Date: February 26, 2024
- Community Reception Date: February 26, 2024 (at night)

General Chairs

Alfred Chen, University of California, Irvine
Z. Berkay Celik, Purdue University

Program Chairs

Ziming Zhao, University at Buffalo
Aiping Xiong, The Pennsylvania State University

Lightning Talk Chair

Ming Li, University of Arizona

Demo/Poster Chair

Sara Rampazzi, University of Florida

Web Chair

Mert Pesé, Clemson University

Publications Chair

Ryan Gerdes, Virginia Tech

Publicity Chair

Ning Zhang, Washington University at St. Louis

Travel Grant Chair

Hyungsub Kim, Purdue University

Sponsorship Chair

Luis Garcia, University of Utah

Technical Program Committee (Pending finalization)

Houssam Abbas, Oregon State University
Antonio Bianchi, Purdue University
Gedare Bloom, U of Colorado Colorado Springs
Yulong Cao, University of Michigan
Alvaro Cardenas, University of California Santa Cruz
Dongyao Chen, Shanghai Jiao Tong University
Andrew Clark, Washington University at St. Louis
Michael Clifford, Toyota
Mauro Conti, University of Padova
Jeremy Daily, Colorado State University
Jiarun Dai, Fudan University
Bruce DeBruhl, Cal Poly
Soteris Demetriou, Imperial College London
Georgios Fainekos, Toyota Research Institute of N. America
Habiba Farrukh, UC Irvine
Yiheng Feng, Purdue University
Tom Forest, General Motors
Daniel Fremont, UC Santa Cruz
Guofei Gu, Texas A&M
Luis Antonio Garcia, University of Utah
Mohammad Hamad, Technical University of Munich
Xiali Hei, University of Louisiana at Lafayette
Hongxin Hu, University at Buffalo
Shengtuo Hu ByteDance
Sashidhar Jakkamsetti, Bosch
Shalabh Jain, Bosch Research
Murtuza Jadliwala, U of Texas at San Antonio
Xiaoyu Ji, Zhejiang University
Justin Kappos, NYU
Huy Kang Kim, Korea University
Chung Hwan Kim, University of Texas at Dallas
Taegyu Kim, Pennsylvania State University
Hyungsub Kim, Purdue University
Vireshwar Kumar, IIT Delhi
Wenchao Li, Boston University
Ming Li, University of Arizona
Xiaojing Liao, Indiana University
Zhiqiang Lin, Ohio State University
Peng Liu, Pennsylvania State University
Wenjing Lou, Virginia Tech
Mulong Luo, Cornell University
Scott Moore, Ford Motor Company
Ivan De Oliveira Nunes, Rochester Institute of Technology
Christos Papadopoulos, University of Memphis
Karthik Pattabiraman, University of British Columbia
Mert Pesé, Clemson University
Jonathan Petit, Qualcomm
Hang Qiu, UC Riverside
Hanif Rahbari, Rochester Institute of Technology
Prashanth Rajivan, University of Washington
Sara Rampazzi, University of Florida
Indrakshi Ray, Colorado State University
Kui Ren, Zhejiang University
Neetesh Saxena, Cardiff University
Arman Sargolzaei, University of South Florida
Yasser Shoukry, University of California, Irvine
David Starobinski, Boston University
Dave (Jing) Tian, Purdue University
Yuan Tian, University of California, Los Angeles
Lan Wang, University of Memphis
André Weimerskirch, Lear Corporation
Luyi Xing, Indiana University
Qiben Yan, Michigan State University
Kun Yang, Zhejiang University
Min Yang, Fudan University
Kentaro Yoshioka, Keio University
Ning Zhang, Washington University at St. Louis
Qi Zhu, Northwestern University
Saman Zonouz, Georgia Tech

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

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.

Ethical Considerations

Human Subjects Research: If a paper 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 the paper reports a potentially high-impact vulnerability, the authors should discuss their plan for responsible disclosure. 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.