Proceedings

The Inaugural Symposium on Vehicle Security & Privacy

February 27, 2023
San Diego, CA, USA

Hosted by the

Internet Society
11710 Plaza America Drive
Suite 400
Reston, VA 20190

Address your correspondence to: NDSS Program Manager, Internet Society, 11710 Plaza America Drive, Suite 400, Reston, VA 20190 USA, tel. +1 703 439 2120, fax +1 703 326 9881, ndss@elists.isoc.org.

ISBN Number (Digital Format) 1-891562-88-6

Additional copies may be ordered from:

Internet Society
11710 Plaza America Drive
Suite 400
Reston, VA 20190
tel +1 703.439.2120
fax +1 703.326.9881
http://www.internetsociety.org

Proceedings of VehicleSec 2023 – The Inaugural Symposium on Vehicle Security & Privacy

Table of Contents

Short: Rethinking Secure Pairing in Drone Swarms
Muslum Ozgur Ozmen (Purdue University), Habiba Farrukh (Purdue University), Hyungsub Kim (Purdue University), Antonio Bianchi (Purdue University) and Z. Berkay Celik (Purdue University)

CableAuth: A Biometric Second Factor Authentication Scheme for Electric Vehicle Charging
Jack Sturgess (University of Oxford), Sebastian Köhler (University of Oxford), Simon Birnbach (University of Oxford) and Ivan Martinovic (University of Oxford)

WIP: The Feasibility of High-performance Message Authentication in Automotive Ethernet Networks
Evan Allen (Virginia Tech), Zeb Bowden (Virginia Tech Transportation Institute), Randy Marchany (Virginia Tech) and J. Scot Ransbottom (Virginia Tech)

Session 3: Connected Autonomous Vehicle Security & Privacy

Towards Privacy-Preserving Platooning Services by means of Homomorphic Encryption
Nicolas Quero (Expleo France), Aymen Boudguiga (CEA LIST), Renaud Sirdey (CEA LIST) and Nadir Karam (Expleo France)

VASP: V2X Application Spoofing Platform
Mohammad Raashid Ansari (Qualcomm Technologies, Inc.), Jonathan Petit (Qualcomm Technologies, Inc.), Jean-Philippe Monteuuis (Qualcomm Technologies, Inc.) and Cong Chen (Qualcomm Technologies, Inc.)

Location Spoofing Attacks on Autonomous Fleets
Jinghan Yang (Washington University in St. Louis), Andew Estornell (Washington University in St. Louis) and Yevgeniy Vorobeychik (Washington University in St. Louis)

Session 4: Automotive and Autonomous Driving Privacy and Situational Awareness

Reminding Drivers of the Stalking Vehicles on the Road
Wei Sun (The Ohio State University) and Kannan Srinivsan (The Ohio State University)

On the Feasibility of Profiling Electric Vehicles through Charging Data
Ankit Gangwal (IIIT Hyderabad), Aakash Jain (IIIT Hyderabad) and Mauro Conti (University of Padova)

Human Drivers' Situation Awareness of Autonomous Driving Under Physical-world Attacks
Katherine Zhang (Purdue University), Claire Chen (Pennsylvania State University) and Aiping Xiong (Pennsylvania State University)

Guess Which Car Type I Am Driving: Information Leak via Driving Apps
Dongyao Chen (Shanghai Jiao Tong University), Mert D. Pesé (Clemson University) and Kang G. Shin (University of Michigan, Ann Arbor)

Efficient Privacy-Preserved Processing of Multimodal Data for Vehicular Traffic Analysis
Reza Arablouei (Data61, CSIRO), Meisam Mohammady (Iowa State University) and Jerome Le Ny (Polytechnique Montreal)

Session 5A: Automotive and Autonomous Driving Defense

WIP: Augmenting Vehicle Safety With Passive BLE
Noah T. Curran (University of Michigan), Kang G. Shin (University of Michigan), William Hass (Lear Corporation), Lars Wolleschensky (Lear Corporation), Rekha Singoria (Lear Corporation), Isaac Snellgrove (Lear Corporation) and Ran Tao (Lear Corporation)

Formally Verified Software Update Management System in Automotive
Jaewan Seo (Korea University), Jiwon Kwak (Korea University) and Seungjoo Kim (Korea University)

Short: Certifiably Robust Perception Against Adversarial Patch Attacks: A Survey
Chong Xiang (Princeton University), Chawin Sitawarin (University of California, Berkeley), Tong Wu (Princeton University) and Prateek Mittal (Princeton University)

Non-Interactive Privacy-Preserving Sybil-Free Authentication Scheme in VANETs
Mahdi Akil (Karlstad University), Leonardo Martucci (Karlstad University) and Jaap-Henk Hoepman (Radboud University Nijmegen)

Semi-Automated Synthesis of Driving Rules
Diego Ortiz (University of California, Santa Cruz), Leilani Gilpin (University of California, Santa Cruz) and Alvaro A. Cardenas (University of California, Santa Cruz)

GPS Spoofing Attack Detection on Intersection Movement Assist using One-Class Classification
Jun Ying (Purdue University), Yiheng Feng (Purdue University), Qi Alfred Chen (University of California, Irvine) and Z. Morley Mao (University of Michigan)

Session 5B: Automotive and Autonomous Driving Attacks

Enhanced Vehicular Roll-Jam Attack using a Known Noise Source
Zachary Depp (The Ohio State University), Halit Bugra Tulay (The Ohio State University) and C. Emre Koksal (The Ohio State University)

Exploiting Transport Protocol Vulnerabilities in SAE J1939 Networks
Rik Chatterjee (Colorado State University), Subhojeet Mukherjee (Colorado State University) and Jeremy Daily (Colorado State University)

WIP: Practical Removal Attacks on LiDAR-based Object Detection in Autonomous Driving
Takami Sato (University of California, Irvine), Yuki Hayakawa (Keio University), Ryo Suzuki (Keio University), Yohsuke Shiiki (Keio University), Kentaro Yoshioka (Keio University) and Qi Alfred Chen (University of California, Irvine)

Evaluations of Cyber Attacks on Cooperative Control of Connected and Autonomous Vehicles at Bottleneck Points
H M Sabbir Ahmad (Boston University), Ehsan Sabouni (Boston University), Wei Xiao (Massachusetts Institute of Technology), Christos G. Cassandras (Boston University) and Wenchao Li (Boston University)

WIP: Towards the Practicality of the Adversarial Attack on Object Tracking in Autonomous Driving

Chen Ma (Xi'an Jiaotong University), Ningfei Wang (University of California, Irvine), Qi Alfred Chen (University of California, Irvine) and Chao Shen (Xi'an Jiaotong University)

Demo Session

Demo: Discovering Faulty Patches in Robotic Vehicle Control Software

Hyungsub Kim (Purdue University), Muslum Ozgur Ozmen (Purdue University), Z. Berkay Celik (Purdue University), Antonio Bianchi (Purdue University) and Dongyan Xu (Purdue University)

Demo: Ransom Vehicle through Charging Pile

Shangru Song (Tsinghua University), Hetian Shi (Tsinghua University), Ruoyu Lun (State Key Laboratory of Science and Engineering Computing), Yunchao Guan (Tsinghua University), Xiang Li (Tsinghua University), Jihu Zheng (Tsinghua University) and Jianwei Zhuge (Tsinghua University, Zhongguancun Laboratory)

Demo: Real-time System Availability for Cyber-physical Systems using ARM TrustZone

Jinwen Wang (Washington University in St. Louis), Ao Li (Washington University in St. Louis), Haoran Li (Washington University at St. Louis), Chenyang Lu (Washington University at St. Louis) and Ning Zhang (Washington University at St. Louis)

Demo: Physically Hijacking Object Trackers

Raymond Muller (Purdue University), Yanmao Man (University of Arizona), Z. Berkay Celik (Purdue University), Ming Li (University of Arizona) and Ryan Gerdes (Virginia Tech)

WIP: Infrared Laser Reflection Attack Against Traffic Sign Recognition Systems

Takami Sato (University of California, Irvine), Sri Hrushikesh Varma Bhupathiraju (University of Florida), Michael Clifford (Toyota InfoTech Labs), Takeshi Sugawara (The University of Electro-Communications), Qi Alfred Chen (University of California, Irvine) and Sara Rampazzi (University of Florida)

VASP: V2X Application Spoofing Platform

Mohammad Raashid Ansari (Qualcomm Technologies, Inc.), Jonathan Petit (Qualcomm Technologies, Inc.), Jean-Philippe Monteuuis (Qualcomm Technologies, Inc.) and Cong Chen (Qualcomm Technologies, Inc.)

Exploiting Transport Protocol Vulnerabilities in SAE J1939 Networks

Rik Chatterjee (Colorado State University), Subhojeet Mukherjee (Colorado State University) and Jeremy Daily (Colorado State University)

Poster Session

Poster: Effects of Knowledge and Experience on Drivers' Intention to Use CAVs

Zekun Cai (Pennsylvania State University) and Aiping Xiong (Pennsylvania State University)

Poster: Practical Swarm Attestation using Probabilistic Program Integrity Verification

Sanket Uppin (Indian Institute of Technology, Delhi), Mehreen Jabbeen (Indian Institute of Technology, Delhi), Rijurekha Sen (Indian Institute of Technology, Delhi) and Vireshwar Kumar (IIT Delhi)

Short: Certifiably Robust Perception Against Adversarial Patch Attacks: Today and Tomorrow

Chong Xiang (Princeton University), Chawin Sitawarin (University of California, Berkeley), Tong Wu (Princeton University) and Prateek Mittal (Princeton University)

Analysing Adversarial Threats to Rule-Based Local-Planning Algorithms for Autonomous Driving

Andrew Roberts (Tallinn University of Technology), Mohsen Malayjerdi (Tallinn University of Technology), Mauro Bellone (Tallinn University of Technology), Olaf Maennel (Tallinn University of Technology) and Ehsan Malayjerdi (Tallinn University of Technology)

WIP: AMICA: Attention-based Multi-Identifier model for asynchronous intrusion detection on Controller Area networks

Natasha Alkhatib (Télécom Paris), Lina Achaji (INRIA), Maria Mushtaq (Télécom Paris), Hadi Ghauch (Télécom Paris) and Jean-Luc Danger (Télécom Paris)

CANtropy: Time Series Feature Extraction-Based Intrusion Detection Systems for Controller Area Networks

Md Hasan Shahriar (Virginia Polytechnic Institute and State University), Wenjing Lou (Virginia Tech) and Y. Thomas Hou (Virginia Tech)

Cooperative Perception for Safe Control of Autonomous Vehicles under LiDAR Spoofing Attacks

Hongchao Zhang (Washington University in St. Louis), Zhouchi Li (Worcester Polytechnic Institute), Shiyu Cheng (Washington University in St. Louis) and Andrew Clark (Washington University in St. Louis)

Reminding Drivers of the Stalking Vehicles on the Road

Wei Sun (The Ohio State University) and Kannan Srinivsan (The Ohio State University)

Message from the Symposium Chairs

On behalf of the VehicleSec 2023 Steering Committee and Organizing Committee, we welcome you to the Inaugural ISOC (Internet Society) Symposium on Vehicle Security and Privacy (VehicleSec) 2023. 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), under water (e.g., ships, boats, watercraft), and in space (e.g., spacecraft). Due to their safety-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 policymakers. To meet this critical need, building upon the continuous four-year growth of the AutoSec (Automotive and Autonomous Vehicle Security) Workshop, the ISOC 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, real-time computing, edge computing, location service, simulation, digital twin, multi-agent protocol/system design, and human-machine interaction).

VehicleSec 2023 received many high-quality submissions. In total, 71 papers (49 regular papers and 22 short/work-in-progress papers), six demos, and six posters were reviewed by the Technical Program Committee (TPC) comprising 58 world-leading researchers and industry practitioners in the area of vehicle security and privacy. After the careful review process and discussions, the TPC selected 28 papers (20 regular papers and eight short/work-in-progress papers), four demos, and two posters to be presented in the symposium. Along with additional poster/demo presentations we invited from the accepted papers, in total seven demos and eight posters were presented in the demo/poster sessions in the symposium. In addition, this year we continued to have a “lightning community shout-out” session for interested attendees to give lightning talks on their ongoing efforts or new ideas that they feel eager to broadcast and seek feedback at the community level. After careful review and discussion among the organizing committee, we accepted six interesting and impactful lightning talks out of 13 submitted from academia and industry.

In this inaugural VehicleSec event, we have attracted a total of eight sponsors, including General Motors, NSF, University of Tennessee, Knoxville (UTK), Zoox, ETAS, Arizona State University (ASU), CyberTruck Challenge, and Qualcomm, which totals $38,500 in support. We used sponsorship funds for student travel grants, paper awards, trophies, community reception, and souvenirs. All accepted papers and demos are considered for the Zoox Best Paper Award, ETAS Best Short Paper Award, and Qualcomm Best Demo Award. In addition, a special General Motors AutoDriving Security Award is given to one of the accepted papers to recognize and reward research that makes substantial contributions to securing today’s emerging autonomous driving technology. We also recognized 5 TPC members with superior contributions to the review process this year with Outstanding Reviewer Awards. With the received sponsorship support from NSF, University of Tennessee, Knoxville (UTK), and CyberTruck Challenge, we were able to provide student travel grant awards for the first time. In total, we received 63 student travel grant

applications, and selected 25 awardees with priorities given to students from underrepresented groups in the community.

The symposium was held in one day at the Catamaran Resort Hotel & Spa, San Diego, CA, USA as one of the co-located events with Network and Distributed System Security Symposium (NDSS) 2023. Beyond the technical program of the research papers, the symposium was enriched by two keynotes (one from academic and one from industry), demo/poster sessions, lightning community shout-outs, industry exhibition tables, and the first-ever community reception at the night of the symposium day as a social event for the vehicle security and privacy community. Specifically, the symposium program featured an academia keynote from Prof. Kang G. Shin (Kevin and Nancy O'Connor Professor at the University of Michigan, ACM Fellow, IEEE Fellow, member of Korean Academy of Engineering) and an industry keynote from Mr. Michael Westra (In-Vehicle Cyber Security Technical Manager, Ford Motor Company).

The organization of a symposium, especially the inaugural one, requires the collaboration of many individuals. First, we would like to thank all the authors for submitting to the symposium. Second, we thank all the TPC members for their efforts in reviewing the papers, providing valuable feedback to authors, and attending online discussions. Third, we thank all the sponsors for their generous support for this inaugural event. Furthermore, we sincerely thank the Steering Committee for the guidance, and the numerous ISOC staff and NDSS organizers for their tremendous help in coordinating this successful event. Last but not least, we thank the student volunteers who helped with the symposium program and local arrangements. We hope that you will find this program interesting and that the symposium will provide you with a valuable opportunity to interact with other researchers and practitioners in the growing area of vehicle security and privacy.

Qi Alfred Chen	**Ziming Zhao**	**Z. Berkay Celik**	**Ryan Gerdes**
UC Irvine	***University at Buffalo***	***Purdue University***	***Virginia Tech***

Organizing Committee

General Chairs

Qi Alfred Chen, *University of California, Irvine*
Ziming Zhao, *University at Buffalo*

Program Chairs

Z. Berkay Celik, *Purdue University*
Ryan Gerdes, *Virginia Tech*

Lightning Talk Chair

Ming Li, *University of Arizona*

Demo/Poster Chair

Sara Rampazzi, *University of Florida*

Web Chair

Mert Pesé, *Clemson University*

Publication Chair

Aiping Xiong, *Penn State University*

Travel Grant Chair

Hyungsub Kim, *Purdue University*

Technical Program Committee

Houssam Abbas, *Oregon State University*
Qadeer Ahmed, *Ohio State University*
Antonio Bianchi, *Purdue University*
Dongyao Chen, *Shanghai Jiao Tong University*
Michael Clifford, *Toyota*
Jeremy Daily, *Colorado State University*
Bruce DeBruhl, *Cal Poly*
Soteris Demetriou, *Imperial College London*
Georgios Fainekos, *Toyota Research Institute of N. America*
Yiheng Feng, *Purdue University*
Earlence Fernandes, *University of California, San Diego*
Tom Forest, *General Motors*
Xiali Hei, *University of Louisiana at Lafayette*
Bardh Hoaxa, *Toyota Research Institute North America*
Hongxin Hu, *University at Buffalo*
Shalabh Jain, *Bosch Research*
Murtuza Jadliwala, *University of Texas at San Antonio*
Xiaoyu Ji, *Zhejiang University*
Yongdae Kim, *KAIST*
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*
Ming Li, *University of Arizona*
Zhiqiang Lin, *Ohio State University*
Peng Liu, *Pennsylvania State University*
Gedare Bloom, *University of Colorado Colorado Springs*
Yulong Cao, *University of Michigan*
Alvaro Cardenas, *University of California, Santa Cruz*
Wenjing Lou, *Virginia Tech*
Mulong Luo, *Cornell University*
Eleonora Losiouk, *University of Padua*
Xiapu Luo, *Hong Kong Polytechnic University*
Ben Nassi, *Ben-Gurion University of the Negev*
Miroslav Pajic, *Duke University*
Karthik Pattabiraman, *University of British Columbia*
Mert D. Pesé, *University of Michigan*
Jonathan Petit, *Qualcomm*
Sara Rampazzi, *University of Florida*
Indrakshi Ray, *Colorado State University*

Neetesh Saxena, *Cardiff University*
Khaled Serag, *Purdue University*
Weisong Shi, *Wayne State University*
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*
Aiping Xiong, *Pennsylvania State University*
Luyi Xing, *Indiana University*
Qiben Yan, *Michigan State University*
Min Yang, *Fudan University*
Fengwei Zhang, *Southern University of Science and Technology*
Ning Zhang, *Washington University at St. Louis*
Qi Zhu, *Northwestern University*

Steering Committee

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

Student Volunteers

Mehmet Ali Acikbas, *Clemson*
Fayzah Alshammari, *UC Irvine*
Trishna Chakraborty, *UC Irvine*
Bulut Gozubuyuk, *Clemson*
Yunpeng Luo, *UC Irvine*
Yanmao Man, *University of Arizona*
Raymond Muller, *Purdue University*
Takami Sato, *UC Irvine*
Xi Tan, *University at Buffalo*
Bhupathiraju Sri Hrushikesh Varma, *University of Florida*
Ziwen Wan, *UC Irvine*
Chenyi Wang, *University of Arizona*
Ningfei Wang, *UC Irvine*
Katherine Zhang, *Purdue University*