Proceedings

AutoSec 2022

Fourth International Workshop on Automotive and Autonomous Vehicle Security

April 24, 2022
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) 1-891562-75-4

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

Table of Contents

Session 2: Autonomous Driving Security 1

DriveTruth: Automated Autonomous Driving Dataset Generation for Security Applications

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

PASS: A System-Driven Evaluation Platform for Autonomous Driving Safety and Security

Zhisheng Hu (Baidu Security), Junjie Shen (UC Irvine), Shengjian Guo (Baidu Security), Xinyang Zhang (Baidu Security), Zhenyu Zhong (Baidu Security), Qi Alfred Chen (UC Irvine) and Kang Li (Baidu Security)

WIP: On Robustness of Lane Detection Models to Physical-World Adversarial Attacks

Takami Sato (UC Irvine) and Qi Alfred Chen (UC Irvine)

Session 3: Robotic Vehicles Security

VISAS - Detecting GPS spoofing attacks against drones by analyzing camera's video stream

Barak Davidovich, Ben Nassi and Yuval Elovici (Ben-Gurion University of the Negev)

WIP: Interrupt Attack on TEE-protected Robotic Vehicles

Mulong Luo and G. Edward Suh (Cornell University)

Demo Session 2

Demo: Attacks on CAN Error Handling Mechanism

Khaled Serag (Purdue University), Vireshwar Kumar (IIT Delhi), Z. Berkay Celik (Purdue University), Rohit Bhatia (Purdue University), Mathias Payer (EPFL) and Dongyan Xu (Purdue University)

Demo: A Simulator for Cooperative and Automated Driving Security

Mohammed Lamine Bouchouia (Telecom paris – Institut Polytechnique de Paris), Jean-Philippe Monteuuis (Qualcomm), Houda Labiod (Telecom paris – Institut Polytechnique de Paris), Ons Jelassi (Telecom paris – Institut Polytechnique de Paris), Wafa Ben Jaballah (Thales) and Jonathan Petit (Qualcomm)

Demo: Identifying Drones Based on Visual Tokens

Ben Nassi (Ben-Gurion University of the Negev), Elad Feldman (Ben-Gurion University of the Negev), Aviel Levy (Ben-Gurion University of the Negev), Yaron Pirutin (Ben-Gurion University of the Negev), Asaf Shabtai (Ben-Gurion University of the Negev), Ryusuke Masuoka (Fujitsu System Integration Laboratories) and Yuval Elovici (Ben-Gurion University of the Negev)

Demo: Dynamic Time Warping as a Tool for Comparing CAN data

Mars Rayno and Jeremy Daily (Colorado State University)

Demo: Hijacking Connected Vehicle Alexa Skills

Wenbo Ding (University at Buffalo), Long Cheng (Clemson University), Xianghang Mi (University of Science and Technology of China), Ziming Zhao (University at Buffalo) and Hongxin Hu (University at Buffalo)

Demo Session 3

Demo: Understanding the Effects of Paint Colors on LiDAR Point Cloud Intensities
Shaik Sabiha, Keyan Guo, Foad Hajiaghajani, Chunming Qiao, Hongxin Hu and Ziming Zhao (University at Buffalo)

Demo: Too Afraid to Drive: Systematic Discovery of Semantic DoS Vulnerability in Autonomous Driving Planning under Physical-World Attacks
Ziwen Wan (UC Irvine), Junjie Shen (UC Irvine), Jalen Chuang (UC Irvine), Xin Xia (UCLA), Joshua Garcia (UC Irvine), Jiaqi Ma (UCLA) and Qi Alfred Chen (UC Irvine)

Demo: Attacking LiDAR Semantic Segmentation in Autonomous Driving
Yi Zhu (University at Buffalo), Chenglin Miao (University of Georgia), Foad Hajiaghajani (University at Buffalo), Mengdi Huai (University of Virginia), Lu Su (Purdue University) and Chunming Qiao (University at Buffalo)

Demo: In-Vehicle Communication Using Named Data Networking
Zachariah Threet (Tennessee Tech), Christos Papadopoulos (University of Memphis), Proyash Poddar (Florida International University), Alex Afanasyev (Florida International University), William Lambert (Tennessee Tech), Haley Burnell (Tennessee Tech), Sheikh Ghafoor (Tennessee Tech) and Susmit Shannigrahi (Tennessee Tech)

Demo: Remote Adversarial Attack on Automated Lane Centering
Yulong Cao (University of Michigan), Yanan Guo (University of Pittsburgh), Takami Sato (UC Irvine), Qi Alfred Chen (UC Irvine), Z. Morley Mao (University of Michigan) and Yueqiang Cheng (NIO)

Session 4: Intra-Vehicle Network Security 2

Detecting CAN Masquerade Attacks with Signal Clustering Similarity (L)
Pablo Moriano, Robert A. Bridges and Michael D. Iannacone (Oak Ridge National Laboratory)

GPSKey: GPS based Secret Key Establishment for Intra-Vehicle Environment (L)
Edwin Yang and Song Fang (University of Oklahoma)

Vehicle Lateral Motion Stability Under Wheel Lockup Attacks (W)
Alireza Mohammadi and Hafiz Malik (University of Michigan-Dearborn)

Session 5: Autonomous Driving Security 2

Generating 3D Adversarial Point Clouds under the Principle of LiDARs
Bo Yang (Zhejiang University), Yushi Cheng (Tsinghua University), Zizhi Jin (Zhejiang University), Xiaoyu Ji (Zhejiang University) and Wenyuan Xu (Zhejiang University)

WIP: Infrastructure-Aided Defense for Autonomous Driving Systems: Opportunities and Challenges
Yunpeng Luo (UC Irvine), Ningfei Wang (UC Irvine), Bo Yu (PerceptIn), Shaoshan Liu (PerceptIn) and Qi Alfred Chen (UC Irvine)

Session 6: Connected Autonomous Vehicle Security & Privacy

Towards a TEE-based V2V Protocol for Connected and Autonomous Vehicles
Mohit Kumar Jangid and Zhiqiang Lin (Ohio State University)

Drivers and Passengers Maybe the Weakest Link in the CAV Data Privacy Defenses
Aiping Xiong (Pennsylvania State University), Zekun Cai (Pennsylvania State University) and Tianhao Wang (University of Virginia)

Message from the Program Co-Chairs

On behalf of the AutoSec 2022 Steering Committee and Organizing Committee, we welcome you to the Fourth International Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2022. As ground and aerial vehicles such as cars, buses, trucks, airplanes, and drones make the whole world increasingly convenient and connected, security and privacy problems pose direct threats to passengers, owners, operators, as well as the environment. Since 2019 the AutoSec workshop has been an impactful venue for new theories, technologies, and systems related to security and privacy challenges in all kinds of current and emerging vehicles, and their supporting infrastructures, especially on the emerging technologies such as autonomy, driver assistance, and connectivity.

AutoSec 2022 received many high-quality submissions. In total, 23 regular papers, 9 short/work-in-progress papers, and 17 demo papers were reviewed by the Technical Program Committee (TPC). The TPC of AutoSec 2022 comprised researchers and industry practitioners. Each regular/short paper received at least three reviews, and each demo paper received at least one review. After the careful review process, the TPC had a virtual meeting to discuss three boundary papers. Consequently, the TPC selected 9 regular papers, 6 short/work-in-progress papers, and 15 demo papers to be presented in the workshop.

All accepted papers and demos are considered for the Best Paper Award, Best Short Paper Award, and Best Demo Award. The winners and runners-up win cash prizes, sponsored by UCI CS. 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.

The workshop was held in one day at the Catamaran Resort Hotel & Spa, San Diego, CA, USA as one of the Network and Distributed System Security Symposium (NDSS) 2022's co-located workshops. Beyond the technical program of the research papers, the workshop was enriched by many other items. The workshop program featured keynotes from Prof. Dongyan Xu (Samuel Conte Professor of Computer Science at Purdue University) and Mr. Kell Rozman (Toyota Motor North America). AutoSec 2022 also featured a demo session to allow academic researchers and industry companies to share demonstrations of their latest attacks, defenses, tools, or systems on automotive and autonomous vehicles. In addition, this year a new "community shout-out" session was introduced 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. AutoSec 2022 also had a community discussion on the future of AutoSec.

The organization of a workshop requires the collaboration of many individuals. First, we would like to thank the authors for submitting to the workshop. Second, we thank the TPC for their efforts in reviewing the papers, providing valuable feedback to authors, and attending online discussions. Third, we thank the Steering Committee for the guidance. We are indeed thankful to the NDSS organizers for coordinating this successful event. We hope that you will find this program interesting and that the workshop will provide you with a valuable opportunity to interact with other researchers and practitioners in automotive and autonomous vehicle security.

Qi Alfred Chen
UC Irvine

Z. Berkay Celik
Purdue University

Ziming Zhao
University at Buffalo

Program Co-Chairs

Qi Alfred Chen, *University of California, Irvine*
Ziming Zhao, *University at Buffalo*
Z. Berkay Celik, *Purdue University*

Technical Program Committee

Houssam Abbas, *Oregon State University*
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*
Michael Clifford, *Toyota*
Jeremy Daily, Colorado State University
Soteris Demetriou, *Imperial College London*
Sriharsha Etigowni, *Purdue University*
Tom Forest, *GM*
Ryan Gerdes, *Virginia Tech*
Guofei Gu, *Texas A&M University*
Shengjian Guo, Baidu Security
Xiali Hei, *University of Louisiana at Lafayette*
Bardh Hoaxa, *Toyota Research Institute North America*
Hongxin Hu, *University at Buffalo*
Shalabh Jain, *Bosch Research*
Xiaoyu Ji, *Zhejiang University*
Zbigniew T. Kalbarczyk, *University of Illinois at Urbana-Champaign*
Chung Hwan Kim, *University of Texas at Dallas*
Taegyu Kim, *Purdue University and Pennsylvania State University*
Vireshwar Kumar, *IIT Delhi*
Ming Li, *University of Arizona*
Zhiqiang Lin, *Ohio State University*
Peng Liu, *Pennsylvania State University*
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 Pesé, *University of Michigan*
Jonathan Petit, *Qualcomm*
Sara Rampazzi, *University of Florida*

Indrakshi Ray, *Colorado State University*
Kemal Tepe, *GM*
Dave (Jing) Tian, *Purdue University*
Yuan Tian, *University of Virginia*
André Weimerskirch, *Lear Corporation*
Luyi Xing, *Indiana 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, *SRI International*
Chunming Qiao, *University at Buffalo*
Mani Srivastava, *University of California, Los Angeles*
Gene Tsudik, *University of California, Irvine*