Proceedings

AutoSec 2021

Third International Workshop on Automotive and Autonomous Vehicle Security

February 25, 2021
Virtual

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) 1-891562-68-1

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 AutoSec 2021 – Third International Workshop on Automotive and Autonomous Vehicle Security

Table of Contents

Message from the Program Co-Chairs
Organizing Committee

Session 1: Miscellaneous

Car Hacking and Defense Competition on In-Vehicle Network
Hyunjae Kang, Byung Il Kwak, Young Hun Lee, Haneol Lee, Hwejae Lee, and Huy Kang Kim (Korea University)

MUVIDS: False MAVLink Injection Attack Detection in Communication for Unmanned Vehicles
Seonghoon Jeong, Eunji Park, Kang Uk Seo, Jeong Do Yoo, and Huy Kang Kim (Korea University)

Object Removal Attacks on LiDAR-based 3D Object Detectors
Zhongyuan Hau, Kenneth Co, Soteris Demetriou, and Emil Lupu (Imperial College London)

CANCloak: Deceiving Two ECUs with One Frame
Li Yue, Zheming Li, Tingting Yin, and Chao Zhang (Tsinghua University)

Demo Session 1

Demo: Curricular Reinforcement Learning for Robust Policy in Unmanned CarRacing Game
Yunzhe Tian, Yike Li, Yingxiao Xiang, Wenjia Niu, Endong Tong, and Jiqiang Liu (Beijing Jiaotong University)

Demo: Sequential Attacks on Kalman Filter-based Forward Collision Warning Systems
Yuzhe Ma, Jon Sharp, Ruizhe Wang, Earlence Fernandes, and Jerry Zhu (University of Wisconsin–Madison)

Session 2: In-Vehicle Network Security

WeepingCAN: A Stealthy CAN Bus-off Attack
Gedare Bloom (University of Colorado Colorado Springs)

Securing CAN Traffic on J1939 Networks
Jeremy Daily, David Nnaji, and Ben Ettlinger (Colorado State University)

Time-Based CAN Intrusion Detection Benchmark
Deborah H. Blevins (University of Kentucky), Pablo Moriano, Robert A. Bridges, Miki E. Verma, Michael D. Iannacone, and Samuel C Hollifield (Oak Ridge National Laboratory)

Demo Session 2

Demo: Detecting Illicit Drone Video Filming Using Cryptanalysis
Ben Nassi, Raz Ben-Netanel (Ben-Gurion University of the Negev), Adi Shamir (Weizmann Institute of Science), and Yuval Elovic (Ben-Gurion University of the Negev)

Demo: Attacking Tesla Model X's Autopilot Using Compromised Advertisement
Ben Nassi (Ben-Gurion University of the Negev), Yisroel Mirsky (Ben-Gurion University of the Negev, Georgia Tech), Dudi Nassi, Raz Ben Netanel (Ben-Gurion University of the Negev), Oleg Drokin (Independent Researcher), and Yuval Elovici (Ben-Gurion University of the Negev)

Demo Session 3

Demo: Securing Heavy Vehicle Diagnostics
Jeremy Daily, David Nnaji, and Ben Ettlinger (Colorado State University)

Demo: Impact of Stealthy Attacks on Autonomous Robotic Vehicle Missions
Pritam Dash, Mehdi Karimibiuki, and Karthik Pattabiraman (University of British Columbia)

Session 3: Autonomous Driving Security I: Physical-World Attacks

WIP: Deployability Improvement, Stealthiness User Study, and Safety Impact Assessment on Real Vehicle for Dirty Road Patch Attack
Takami Sato, Junjie Shen, Ningfei Wang (UC Irvine), Yunhan Jack Jia (ByteDance), Xue Lin (Northeastern University), and Qi Alfred Chen (UC Irvine)

Model-Agnostic Defense for Lane Detection against Adversarial Attack
Henry Xu, An Ju, and David Wagner (UC Berkeley)

WIP: End-to-End Analysis of Adversarial Attacks to Automated Lane Centering Systems
Hengyi Liang, Ruochen Jiao (Northwestern University), Takami Sato, Junjie Shen, Qi Alfred Chen (UC Irvine), and Qi Zhu (Northwestern University)

Demo Session 4

Demo: Automated Tracking System For LiDAR Spoofing Attacks On Moving Targets
Yulong Cao, Jiaxiang Ma, Kevin Fu (University of Michigan), Sara Rampazzi (University of Florida), and Z. Morley Mao (University of Michigan)

Demo: Security of Camera-based Perception for Autonomous Driving under Adversarial Attack
Christopher DiPalma, Ningfei Wang, Takami Sato, and Qi Alfred Chen (UC Irvine)

Session 4: Autonomous Driving Security II: Sensor Attacks

Spoofing Mobileye 630's Video Camera Using a Projector
Ben Nassi, Dudi Nassi, Raz Ben Netanel and Yuval Elovici (Ben-Gurion University of the Negev)

Fooling Perception via Location: A Case of Region-of-Interest Attacks on Traffic Light Detection in Autonomous Driving
Kanglan Tang, Junjie Shen, and Qi Alfred Chen (UC Irvine)

Demo Session 5

Demo: Attacking Multi-Sensor Fusion based Localization in High-Level Autonomous Driving

Junjie Shen, Jun Yeon Won, Zeyuan Chen and Qi Alfred Chen (UC Irvine)

Demo: Security of Deep Learning based Automated Lane Centering under Physical-World Attack

Takami Sato, Junjie Shen, Ningfei Wang (UC Irvine), Yunhan Jack Jia (ByteDance), Xue Lin (Northeastern University), and Qi Alfred Chen (UC Irvine)

Session 5: Connected Vehicle Security

Impact Evaluation of Falsified Data Attacks on Connected Vehicle Based Traffic Signal Control Systems

Shihong Huang (University of Michigan, Ann Arbor), Yiheng Feng (Purdue University), Wai Wong (University of Michigan, Ann Arbor), Qi Alfred Chen (UC Irvine), Z. Morley Mao and Henry X. Liu (University of Michigan, Ann Arbor)

Denial-of-Service Attacks on C-V2X Networks

Natasa Trkulja, David Starobinski (Boston University), and Randall A. Berry (Northwestern University)

Vision-Based Two-Factor Authentication & Localization Scheme for Autonomous Vehicles

Anas Alsoliman, Marco Levorato, and Qi Alfred Chen (UC Irvine)

Session 6: Electric Vehicle Security

Low-risk Privacy-preserving Electric Vehicle Charging with Payments

Andreas Unterweger, Fabian Knirsch, Clemens Brunner, and Dominik Engel (Center for Secure Energy Informatics, Salzburg University of Applied Sciences, Puch bei Hallein, Austria)

Trusted Verification of Over-the-Air (OTA) Secure Software Updates on COTS Embedded Systems

Anway Mukherjee, Ryan Gerdes, and Tam Chantem (Virginia Tech)

Message from the Program Co-Chairs

It is our great pleasure to welcome you to the 3rd International Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2021. This workshop is organized to contribute to new theories, technologies, and systems related to security and privacy challenges in automotive and autonomous vehicles and their supporting infrastructures. Ground and aerial vehicles, such as cars, buses, trucks, airplanes, and drones make the whole world convenient and connected. Due to their wide usage and high safety criticality, any security and privacy problems in them pose direct threats to users and stakeholders in transportation. With the recent global interest in substantially increasing their autonomy and connectivity, including autonomous driving, drone delivery, vehicle-to-everything (V2X) communication, intelligent transportation, and drone swarm technologies, such problems become more critical than ever and thus require immediate attention and discussion in both academia and industry.

In addition to the regular session that presents regular papers and short position/work-in-progress research papers, AutoSec 2021 also features 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. All accepted papers and demos are considered for Best Paper Award and Best Demo Award. The winner and runner-up win cash prizes, sponsored by UCI CS and UB CSE. In addition, a special Baidu Security AutoDriving Security Award is given to one of the accepted papers to recognize and reward research that makes substantial contributions to secure today's emerging autonomous driving technology.

In response to the call for papers of AutoSec 2021, 21 regular papers, five short/work-in-progress papers, and 10 demo papers were submitted. Each regular/short paper received at least three reviews, and each demo paper received at least one review. Consequently, the program committee selected 12 regular papers, and accepted all short and demo papers to broaden the community. These papers cover a variety of topics, ranging from various new contributions to in-vehicle network security (including new attacks, defenses, and also benchmarks), to new attack discovery and defense designs for emerging autonomous driving systems security, to connected vehicle infrastructure and protocol security, and to electric vehicle security and trusted software updates for embedded systems. Among them, the papers receiving the highest and second highest average review scores are the Best Paper Award winner and runner-up. In addition, among the short/work-in-progress papers, the ones receiving the highest and second highest average review scores are the Best Short Paper Award winner and runner-up. Among the papers studying autonomous driving security, the highest-scored regular one received the Baidu Security AutoDriving Security Award. Best Demo Award winner and runner-up are decided based on the voting results during the workshop.

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 program committee members for their efforts in reviewing the papers and providing valuable feedback to authors. 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, USA

Ziming Zhao
University at Buffalo, USA

Gail-Joon Ahn
Arizona State University, USA and Samsung Research, South Korea

Organizing Committee

Program Co-Chairs

Qi Alfred Chen, *University of California, Irvine*
Ziming Zhao, *University at Buffalo*
Gail-Joon Ahn, *ASU and Samsung Research*

Program Committee

Gedare Bloom, *University of Colorado Colorado Springs*
Alvaro Cardenas, *University of California Santa Cruz*
Stephen Checkoway, *Oberlin College*
Dongyao Chen, *Shanghai Jiao Tong University*
Jeremy Daily, *Colorado State University*
Sriharsha Etigowni, *Purdue University*
Thomas Forest, *General Motors*
Ryan Gerdes, *Virginia Tech*
Xiali Hei, *University of Louisiana at Lafayette*
Hongxin Hu, *Clemson University*
Zbigniew T. Kalbarczyk, *University of Illinois at Urbana-Champaign*
Taegyu Kim, *Purdue University*
Karl Koscher, *University of Washington*
Sekar Kulandaivel, *Carnegie Mellon University*
Kang Li, *Baidu, Inc.*
Chung-Wei Lin, *National Taiwan University*
Zhiqiang Lin, *The Ohio State University*
Peng Liu, *Pennsylvania State University*
Morley Mao, *University of Michigan*
Karthik Pattabiraman, *University of British Columbia*
Mert Pesé, *University of Michigan*
Jonathan Petit, *Qualcomm*
Hanif Rahbari, *Rochester Institute of Technology*
Indrakshi Ray, *Colorado State University*
David Starobinski, *Boston University*
Yuan Tian, *University of Virginia*
André Weimerskirch, *Lear Corporation*
Shengzhi Zhang, *Boston University*
Fengwei Zhang, *Southern University of Science and Technology*
Ning Zhang, *Washington University at St. Louis*