

# **Automotive and Autonomous Vehicle Security Workshop 2021 (AutoSec 2021)**

Online  
25 February 2021

ISBN: 978-1-7138-3764-0

**Printed from e-media with permission by:**

Curran Associates, Inc.  
57 Morehouse Lane  
Red Hook, NY 12571



**Some format issues inherent in the e-media version may also appear in this print version.**

Copyright© (2021) by The Internet Society  
All rights reserved.

Printed with permission by Curran Associates, Inc. (2021)

For permission requests, please contact The Internet Society  
at the address below.

The Internet Society  
11710 Plaza America Drive, Suite 400  
Reston, VA 20190  
U.S.A.

Phone: (703) 439-2120  
Fax: (703) 326-9881

[www.internetsociety.org](http://www.internetsociety.org)

**Additional copies of this publication are available from:**

Curran Associates, Inc.  
57 Morehouse Lane  
Red Hook, NY 12571 USA  
Phone: 845-758-0400  
Fax: 845-758-2633  
Email: [curran@proceedings.com](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

## **Table of Contents**

### **Message from the Program Co-Chairs Organizing Committee**

#### **Session 1: Miscellaneous**

- 1 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)*
- 7 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)*
- 13 Object Removal Attacks on LiDAR-based 3D Object Detectors  
*Zhongyuan Hau, Kenneth Co, Soteris Demetriou, and Emil Lupu (Imperial College London)*
- 17 CANCloak: Deceiving Two ECUs with One Frame  
*Li Yue, Zheming Li, Tingting Yin, and Chao Zhang (Tsinghua University)*

#### **Demo Session 1**

- 23 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)*
- 24 Demo: Sequential Attacks on Kalman Filter-based Forward Collision Warning Systems  
*Yuzhe Ma, Jon Sharp, Ruizhe Wang, Earlene Fernandes, and Jerry Zhu (University of Wisconsin–Madison)*

#### **Session 2: In-Vehicle Network Security**

- 25 WeepingCAN: A Stealthy CAN Bus-off Attack  
*Gedare Bloom (University of Colorado Colorado Springs)*
- 31 Securing CAN Traffic on J1939 Networks  
*Jeremy Daily, David Nnaji, and Ben Ettlinger (Colorado State University)*
- 38 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**

- 44 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)*
- 45 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**

- 46 Demo: Securing Heavy Vehicle Diagnostics  
*Jeremy Daily, David Nnaji, and Ben Ettlinger (Colorado State University)*
- 47 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**

- 48 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)*
- 52 Model-Agnostic Defense for Lane Detection against Adversarial Attack  
*Henry Xu, An Ju, and David Wagner (UC Berkeley)*
- 58 WIP: End-to-End Analysis of Adversarial Attacks to Automated Lane Centering Systems  
*Hengyi Liang, Ruo Chen Jiao (Northwestern University), Takami Sato, Junjie Shen, Qi Alfred Chen (UC Irvine), and Qi Zhu (Northwestern University)*

## **Demo Session 4**

- 62 Demo: Automated Tracking System For LiDAR Spoofing Attacks On Moving Targets  
*Yulong Cao, Jiayang Ma, Kevin Fu (University of Michigan), Sara Rampazzi (University of Florida), and Z. Morley Mao (University of Michigan)*
- 63 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**

- 64 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)*
- 68 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**

- 72 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)*
- 73 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**

- 74 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)*
- 80 Denial-of-Service Attacks on C-V2X Networks  
*Natasa Trkulja, David Starobinski (Boston University), and Randall A. Berry (Northwestern University)*
- 86 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**

- 92 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)*
- 98 Trusted Verification of Over-the-Air (OTA) Secure Software Updates on COTS Embedded Systems  
*Anway Mukherjee, Ryan Gerdes, and Tam Chantem (Virginia Tech)*