CALL FOR PAPERS - VCSS 2021

The 3rd International Workshop on Vehicle Communication and Software Security (VCSS 2021) - https://qrs21.techconf.org/workshops/VCSS
Co-located with the IEEE International Conference on Software Quality, Reliability, and Security (QRS 2021) - https://qrs21.techconf.org
December 6-10, 2021, Hainan Island, China.

The last decade has witnessed an increased level of sophistication in embedded vehicle software. Connected and autonomous vehicles (CAV) are classified as critical systems, as their failure could directly impact human safety or lead to loss of valuable assets. Hence, their security is a major concern for users as well as designers. Connected vehicles are primarily software controlled and communicate with each other, the cloud, and the intelligent transportation infrastructure via wireless networks. Given that, the underlying software that controls vehicles' operations and the integrated communication technologies must be designed and deployed with a higher level of security and safety assurance than traditional systems.

The VCSS workshop seeks to bring together researchers and practitioners working toward the improvement of security of communication and software solutions in the automotive sector. The workshop provides the leaders in the field with an excellent opportunity to discuss emerging security challenges and exchange their research findings and experience. We welcome papers and presentations reflecting the latest advances in theory and technology related to the security of intelligent vehicles.

The list of topics includes, but is not limited to:

- Vehicular network and software vulnerability assessment and security risk analysis
- Architecture, design, and implementation of secure and safe vehicle software
- Design of in-vehicles secure information systems and software applications
- Vehicle operating system security
- V2V, V2I and V2X communication security
- Secure in-vehicle communications and CAN bus
- Availability, reliability, and fault tolerance in VANETs communication
- Secure vehicular fog and vehicle-to-cloud communications
- New methodologies for attack and threat modeling in vehicle communication and software
- Malware analysis and detection in vehicle software and in-vehicle network
- Vehicle software testing, verification, and validation
- Security and safety evaluation methodologies and metrics in CAV
- Vehicle software standardization, certification, and interoperability
- Artificial Intelligence and machine learning for CAV security
- Penetration testing, forensics, events monitoring and auditing of vehicle software
- Practical experiences, empirical studies, and testbeds for intelligent vehicle security
- Industrial experiences and best practices for secure vehicle software development

Workshop Chair:
Mohammad Zulkernine, Queen's University, Canada

Program Chairs:
Talal Halabi, University of Winnipeg, Canada
Ryo Kurachi, Nagoya University, Japan
Dennis Kengo Oka, Synopsys, Inc., USA

Program Committee:
TBD

Important Dates:

Submission of papers due: September 20, 2021
Author notification: October 20, 2021
Camera-ready papers due: November 1, 2021
Workshop dates: December 6-10, 2021

More information can be found here: https://qrs21.techconf.org/workshops/VCSS
Questions regarding the workshop should be emailed to t.halabi@uwinnipeg.ca