Invitation and Call for Participation

Exploring Cybersecurity Challenges in Electrified Transportation:

A Focused Workshop

and IEEE Standards Coordinating Committee on Transportation (SCC42) Meeting

Wednesday, February 24, and Thursday, February 25, 2016

Howard University Interdisciplinary Research Building (HUIRB), 2201 Georgia Avenue, NW, Washington, DC 20059

http://tecworkshop.crosby.work/

Transportation electrification imposes special considerations and concerns for cybersecurity. These are in addition to widely discussed issues of connection security and vehicle-to-vehicle communication and control. The IEEE Transportation Electrification Community and the IEEE Standards Coordinating Committee on Transportation (SCC 42), with technical cooperation of the NSF Center for Power Optimization of Electro-Thermal Systems, the Information Trust Institute at the University of Illinois, Howard University, and the IEEE-USA Committee on Transportation and Aerospace Policy, will sponsor this special one-day workshop followed by a full-day meeting of IEEE SCC 42. The event will address cybersecurity issues directly associated with more-electric transportation, including propulsion system cyber vulnerabilities, cyber issues linked to human error and software bugs, vulnerabilities of active safety systems, the challenges of "always on" large battery packs, vehicle-to-grid aspects, and others. The overall goal is to characterize the cyber-security requirements for enabling transportation electrification, not including V2V and personal communications.

The workshop will include invited presentations and focused breakout discussion directed to the following objectives:

- Identify and delineate key areas of concern in cybersecurity issues directed at transportation electrification.
- Identify relevant gap areas in which fundamental engineering research and development are needed for progress.
- Set up objectives to nucleate working groups on recommended practices and standards.
- Evaluate and identify specific topics in which there is urgent need for solutions.
- Identify existing practices and advances that can be applied in the near term to cybersecurity issues in electrified transportation.

The outcomes of the discussion will provide immediate guidance and action items for IEEE SCC 42 and will lead to a published report providing guidance for near-term industry and government efforts directed at cybersecurity in transportation electrification.

Speakers and participants will address questions that include:

- How can extreme intentional operating modes be distinguished consistently from fault conditions or tamper ing?
- What are best design and validation practices to evaluate operational cybersecurity challenges in highly energy-dense systems?
- Are there strategies that lead to inherent safe modes in the event of security issues or vehicle damage?
- How do active safety systems in more-electric transportation, such as collision avoidance and positive train control, impact cybersecurity considerations?
- What are best practices for securing software and hardware update and repair processes?
- What policy and standards-related activities would be of benefit in cybersecurity issues specific to transportation electrification, including interaction of devices with power grids?

Participants are invited to this workshop, and to the subsequent SCC 42 meeting, that are designed to raise awareness of cyber-related security challenges now emerging with the growth of electric and hybrid vehicles and the trend toward more-electric energy in all forms of transportation. The workshop seeks to gather a group of experts in power electronics, systems engineering, machines and drives, and cybersecurity of devices and infrastructure.

Much of the past work on cybersecurity in transportation has emphasized vehicle-to-vehicle and vehicle-to-infrastructure communication links. Although these challenges are widely discussed and unresolved, the challenges to be addressed by this workshop are different. Issues linked to rapid energy exchange and to electric propulsion are introduced even in vehicles with minimal communication interfaces. The workshop intends to develop metrics related to key issues and develop a working plan toward policy and standards activities that could help overcome or avoid cyber-based vulnerabilities. The agenda will include invited talks by leading experts on cybersecurity in physical systems, open discussion sessions, and talks by industry participants summarizing best practices. This will be an interactive workshop.

Registration

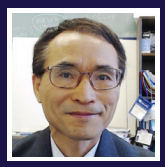
http://tecworkshop.crosby.work/

Early Registration through February 15th
One Day Fee: $150 (either day)
Student One Day Fee: $50 (either day)
Two Day Fee: $250
Student Two Day Fee: $100
Registration after February 16th and onsite:
One Day Fee: $175
Student One Day Fee: $100
Two Day Fee: $300
Student Two Day Fee: $150

Invited speakers include:

Prof. David Nicol
Director, Information Trust Institute
University of Illinois at Urbana-Champaign

Prof. Klara Narstadt
Director, Coordinated Science Laboratory
University of Illinois at Urbana-Champaign



Prof. Charles Kim
Howard University

Suggested Hotel:

Holiday Inn Central

1501 Rhode Island Ave NW,
Washington, DC 20005

http://www.inndc.com/location.php