



## 8<sup>th</sup> escar USA – Embedded Security in Cars Workshop

May 20 – 21, 2020, The Inn at St. John's, Plymouth, MI, USA

### Important Dates

Submission deadline extended:

March 9, 2020

~~March 1<sup>st</sup>, 2020~~

Acceptance notification:

April 20<sup>th</sup>, 2020

### Steering Committee

Tom Forest, General Motors  
Kevin Harnett, DOT/VOLPE  
Rob Lambert, ESCRYPT  
André Weimerskirch, Lear Corporation

### Program Committee

Ansaf Alrabady, FCA  
Angela Barber, Mitsubishi  
Matthew Bourdua, Panasonic  
Lisa Boran, Ford  
Benedikt Brecht, VW  
Justin Cappos, NYU  
Matt Carpenter, GRIMM  
Sergio Casadei, VW  
Qi Alfred Chen, University of California,  
Irvine  
Jeremy Daily, Colorado State University  
Andy Davis, NCC  
Karim El Defrawy, SRI  
Michael Feiri, ZF  
Sebastian Fischmeister, University of  
Waterloo  
Benjamin Glas, Porsche  
Jorge Guajardo, Bosch  
Karl Heimer, Heimer & Associates  
Markus Ihle, Bosch  
Di Jin, General Motors  
Urban Jonson, NMFTA  
Liron Kaneti, Argus  
John Krzeszewski, Aptiv  
Suzanne Lightman, NIST  
Di Ma, University of Michigan-Dearborn  
Morley Mao, University of Michigan  
Ira McDonald, High North  
Dave New, FCA  
Aleksy Nogin, HRL Laboratory  
Hisashi Oguma, Toyota ITC  
David Oswald, University of Birmingham  
Jonathan Petit, Qualcomm  
Neal Probert, Nissan  
Anuja Sonalker, STEER  
Alan Tatourian, Intel  
Eric Thayer, AIS  
Alexander Tschache, VW  
Mike Westra, Ford  
Lars Wolleschensky, Lear Corporation  
Xin Ye, Ford

### Overview and Topics

Information technology has become the driving force behind most innovation in the automotive industry, supporting connectivity, infotainment, and automation applications. The situation is similar for commercial vehicles.

A crucial aspect of most automotive electronic applications is cybersecurity. The escar series of workshops, held annually in Europe, the USA, and Asia, has established itself as the premier forum for information, discussion and exchange cybersecurity and privacy ideas between academia, industry, and government, and we invite researchers to present their ideas for industry feedback. As in previous years, the program will include invited talks, and we request submitted papers and talks on automotive cybersecurity, including but not limited to the following areas:

- Cybersecurity-related engineering, formal methods, software assurance, development & validation, and security standardization
- Cloud security, as it relates to the vehicle's cybersecurity
- Automotive manufacturing security, including supply-chain security
- The overlap of functional safety and cybersecurity
- Design of resilient vehicle architectures and applications
- Privacy and data protection issues in vehicular settings
- Vehicular hardware security and hardware security modules
- Vehicle applications of virtualization, isolation, trusted execution environments, etc.
- Security of vehicular communications (on-board, passenger, and V2X)
- Vehicle cyber intrusion detection systems, forensics, and incident response
- Security of legally mandated applications (e.g., ELD, EDR and tachograph)
- Security economics
- Security of road pricing, restricted areas access and vehicle monitoring
- Security of vehicle theft prevention and theft response solutions
- Security of vehicular rights control and audit (e.g., feature activation)
- Electric vehicle charging security
- Security aspects of automated driving and ADAS, including sensing and AI
- Cybersecurity of commercial vehicles and medium- and heavy-duty trucks
- Vehicle-related information sharing, vulnerability coordination, and bug-bounty programs
- Automotive reverse engineering and penetration testing
- Security of vehicle-driven business, maintenance, and service models
- Legal aspects of automotive cybersecurity

### Instructions for Paper Submission

Theoretical/scientific articles, case studies and descriptions of real-world experience are welcome. All submissions will be double-blind peer-reviewed. Two types of submissions will be accepted:

*Full papers of up to 15 pages:* This can be, for example, new research results, case studies, or state-of-the-art reports. The value to the escar community should be clearly demonstrated.

*Extended abstracts of 3 or more full pages:* This category is geared towards contributions from industry and government. These will consist of a presentation only - no full paper will be required. The abstract must be at least 3 full pages and should clearly outline the content of the planned presentation and its value to the escar community.

**Important Note 1:** Extended abstracts of less than 3 full pages will be rejected without review. Marketing driven submissions and submissions that lack details to enable a review were not well received and almost always rejected in the past.

**Important Note 2:** For both submission types the text must be in English with a font size of at least 10pt. **Submissions must be anonymous with no identifying features on the submissions (such as obvious references).**

Submissions must be in PDF format and will be accepted at escar's submission site:

<https://www.easychair.org/conferences/?conf=escarusa2020>

### Program and Registration Information

Complete program and registration information will be available soon on [www.escar.info](http://www.escar.info).