

7th escar USA – Embedded Security in Cars Workshop

June 12 – 13, 2019, Ann Arbor Marriott Ypsilanti at Eagle Crest, Ypsilanti, MI, USA

Important Dates

Submission deadline:

February 24th, 2019

Acceptance notification:

April 15th, 2019

Final paper/presentation slides due:

May 24th, 2019

Steering Committee

Tom Forest, General Motors, tom.m.forest@gm.com

Kevin Harnett, DOT/VOLPE, kevin.harnett@dot.gov

Rob Lambert, ESCRYPT, robert.lambert@escrypt.com

André Weimerskirch, Lear Corporation, aweimerskirch@lear.com

Program Committee

Ansaf Alrabady, FCA, USA

Angela Barber, Mitsubishi, USA

Matthew Bourdua, Panasonic, USA

Lisa Boran, Ford, USA

Benedikt Brecht, VW, USA

Carsten Büttner, Germany

Justin Cappos, NYU, USA

Matt Carpenter, GRIMM, USA

Sergio Casadei, VW, USA

Andy Davis, NCC, UK

Karim El Defrawy, SRI, USA

Benjamin Glas, Porsche, Germany

Jorge Guajardo, Bosch, USA

Karl Heimer, Heimer & Associates, USA

Markus Ihle, Bosch, Germany

Di Jin, General Motors, USA

Urban Jonson, NMFTA, USA

Liron Kaneti, Argus, Israel

John Krzeszewski, Aptiv, USA

Suzanne Lightman, NIST, USA

Ira McDonald, High North, USA

Dave New, FCA, USA

Aleksey Nogin, HRL, USA

David Oswald, University of Birmingham, UK

Jonathan Petit, Onboard Security, USA

Neal Probert, Nissan, USA

Anuja Sonalker, STEER Auto Cyber, USA

Alan Tatourian, Intel, USA

Eric Thayer, AIS, USA

Alexander Tschache, VW, Germany

Mike Westra, Ford, USA

Lars Wolleschensky, Lear Corporation, USA

Xin Ye, Ford, USA

Program and Registration Information

Complete program and registration information will be available soon on www.escar.info.

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 of ideas on all aspects of vehicle cybersecurity and privacy. As in previous years, the program will include invited talks, but we will accept submitted papers and talks in automotive cybersecurity, including but not limited to the following areas:

- Cybersecurity-related engineering, formal methods, software assurance, development & validation, and security standardization
- Cybersecurity of sensors and cyber-physical systems
- Design of resilient vehicle architectures and applications
- Privacy and data protection issues in vehicular settings
- Vehicular hardware security and hardware security modules
- 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., event data recorder, tachograph)
- Security of automotive cloud-based infrastructure
- 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 self-driving vehicles sensing systems
- Security implications of AI used in a vehicle context
- Cybersecurity of commercial vehicles and medium- and heavy-duty trucks
- Vehicle-related information sharing and vulnerability coordination
- Automotive reverse engineering and penetration testing
- Security of vehicle-driven business, maintenance, and service models
- Legal aspects of automotive cybersecurity
- Research around bug bounty programs and vulnerability disclosure

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).**

Important Note 3: Please ensure that you are able to provide the final presentation slides by the deadline listed above.

Submissions must be in PDF format and will be accepted at escar's submission site: <https://www.easychair.org/conferences/?conf=escarusa2019>