Announcement and Call for Papers

5th escar USA – Embedded Security in Cars Workshop

June 21 – 22, 2017, **Ann Arbor Marriott Ypsilanti at Eagle Crest, MI, USA**

Important Dates

Submission deadline:
March 5th, 2017
Acceptance notification:
April 24th, 2017
Final paper/presentation slides due:
June 2nd, 2017

Steering Committee

Tom Forest, General Motors, tom.m.forest@gm.com
Kevin Harnett, DOT/VOLPE, kevin.harnett@dot.gov
Christof Paar, Univ. Bochum & UMass Amherst, christof.paar@rub.de
André Weimerskirch, Lear, aweimerskirch@lear.com
Lars Wolleschensky, ESCRYPT, lars.wolleschensky@escrypt.com

Program Committee

Lisa Boran, *Ford, USA*
Benedikt Brecht, *VW, USA*
Carsten Büttner, *Opel, Germany*
Justin Cappos, *NYU, USA*
Sergio Casadei, *VW, USA*
Barbara Czerny, *ZF TRW, USA*
Andy Davis, *NCC, UK*
Karim El Defrawy, *HRL, USA*
Michael Feiri, *ZF TRW, UK*
Ryan Gerdes, *Utah State University, USA*
Benjamin Glas, *Porsche, Germany*
Jorge Guajardo, *Bosch RTC, USA*
Karl Heimer, *AutoImmune, USA*
Markus Ihle, *Bosch, Germany*
Daniel Jiang, *Mercedes Benz, USA*
Di Jin, *General Motors, USA*
Urban Jonson, *NMFTA, USA*
Suzanne Lightman, *NIST, USA*
Bill Mazzara, *FCA, USA*
Damon McCoy, *NYU, USA*
Ira McDonald, *High North, USA*
Dave New, *FCA, USA*
Aleksey Nogin, *HRL, USA*
Hisashi Oguma, *Toyota ITC Ltd., Japan*
David Oswald, *University of Birmingham, UK*
Jonathan Petit, *Security Innovation, USA*
Neal Probert, *Nissan, USA*
Vibhu Sharma, *NXP, USA*
Anuja Sonalker, *STEER Auto Cyber, USA*
Alan Tatourian, *Intel, USA*
Eric Thayer, *AIS, USA*
Alexander Tschache, *VW, Germany*
Mike Westra, *Ford, USA*
Xin Ye, *Ford, USA*

Organizing Committee

Terri Kimball, *ESCRYPT, USA,* terri.kimball@escrypt.com
Birgitte Baardseth, *isits AG, Germany,* baardseth@is-its.org

Sponsorship Opportunities

Please contact the Organizing Committee if your organization is interested in sponsoring escar USA 2017.

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. Cybersecurity can enable new innovation and business models but, as demonstrated recently by various researchers, cybersecurity issues can jeopardize those innovations and even potentially endanger safety. This is evidenced by a landmark event that occurred in 2015 – the first formal recall specifically to address an automotive cybersecurity vulnerability.

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 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)
- Security of vehicle application platforms
- 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)
- Security of emergent technologies (e.g., automated driving, electric vehicles)
- Cybersecurity of commercial vehicles and medium- and heavy-duty trucks
- Security of other transport systems (e.g., rail, aerospace)
- Vehicle-related information sharing and vulnerability coordination
- Automotive reverse engineering and penetration testing
- Security of vehicle-driven business, maintenance, and service models

Instructions for Paper Submission

Theoretical/scientific articles, case studies and descriptions of real-world experience are welcome. All submissions will be peer-reviewed. Prospective authors should contact one of steering committee members in case they have a doubt about the appropriateness of their submission for the conference. 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=escarusa2017