IEEE Design&Test

Call for Contributions

Special Issue on Secure Automotive Systems

Aim and Scope

Modern and emergent automotive systems are highly complex, dominated by a large amount of integrated electronics and software components. The electronic and software components perform and contribute to a diversity of device functionality, ranging across infotainment, driver assistance, radio and wireless communication, etc. The future is expected to see an even more explosive increase in complexity, with emergence of fully automated connected cars that will need to have com continuous communication with a smart highway system, interact with a variety of structured and ad hoc networks with different levels of trustworthiness, and make real-time analytics in the context of an in-motion, rapidly changing environment. In this complex world, it is clearly critical to ensure that these systems behave predictably, securely, and reliably, even in the environment involving interaction with millions of other, potentially malicious computing agents. A hacked automotive system, in the world of self-driving vehicles and vehicles with automated driver assistance, can cause catastrophic consequences, including significant loss of human lives, breakdown of highway systems, and shut-down of an entire city or region. Indeed, automotive systems do (and must) require some of the most stringent levels of compliance with requirements from security. On the other hand, the high complexity of the systems makes enforcement of such standards a highly challenging exercise.

Unsurprisingly, there has been a large interest in recent years on secure and trustworthy computing systems and devices in general, and automotive systems in particular. Nevertheless, there has been little effort to unify and consolidate this research. Much of the research is sprinkled across proceedings of various conferences with varying scopes and purpose. Furthermore, much of the research on automotive security is conflated with other related areas on security assurance with analogous but different challenges, including wearables, Internet-of-Things, or even traditional hardware and software designs. This leaves a researcher getting initiated in this area with the daunting task of sifting the various challenges, complexities, and research directions, identifying approaches applicable to automotive systems in particular, and comprehending evolving challenges caused by the rising complexity of these systems through the past, present, and future.

The goal of the special issue is to highlight research directions in secure, reliable, and predictable automotive systems. The aim is to cover spectrum of challenges, approaches, and solutions in this highly complex area, and provide an authoritative reference of the state of the art.

Topics of Interest

The special issue will cover all aspects of security and trustworthiness in automotive systems. Papers highlighting synergy and distinctions between automotive systems and other current and emergent computing platforms (e.g., mobile, IoT, and cloud-based systems) in security and trustworthiness challenges and solutions will be particularly encouraged. In addition to research articles, we strongly encourage submission of papers describing state of industrial practice in this area, as well as discussions of unique problems and challenges. Topics of interest include, but are not limited to, the following:

- Automotive security models and security architecture
- Security challenges in connected cars and cooperative transportation systems
- Security in automotive/IoT interactions
- Connections between security, reliability, and predictability in automotive
- Security in context of performance, power, and thermal challenges
- Security effects on smartness and connectivity
- Relations and trade-offs between security and functional safety
- Security in automated driving and assisted driving
- Security issues in co-operative transportation systems
- Security in emergent automotive components
- Security across automotive supply-chain
- Security validation and testing techniques
- Formal methods in Automotive security
- Certification criteria and standards (e.g., Common Criteria, ISO26262)
- Industrial experience in automotive security design, architecture, and validation

Given the goal of the special issue to provide an authoritative starting point for future research, we encourage the authors to provide a comprehensive treatment of related work, both in research and state of the practice.

Important Dates

• Manuscript submission	September 30, 2017
• First round of reviews	December 31, 2017
• Second round of reviews	March 1, 2018
• Final Manuscript	April 15, 2018

Guest Editors:

1. **Sandip Ray**, NXP Semiconductors, Austin, TX, USA
2. **Mohammad Abdullah Al Faruque**, University of California Irvine, Irvine, CA, USA
3. **Ahmad-Reza Sadeghi**, Technische Universität Darmstadt, Darmstadt, Germany