Guest Editors' Introduction: Secure Automotive Systems

Sandip Ray
University of Florida

Mohammad Al Faruque
University of California, Irvine

Ahmad-Reza Sadeghi
Technische Universität Darmstadt

Modern and emergent automotive systems are highly complex, dominated by a large number of integrated electronics and software components. The electronic and software components include a diversity of device functionality, ranging across infotainment, driver assistance, radio, and wireless communication. The future is expected to see an even more explosive increase in complexity with the emergence of fully automated connected cars that need to have 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 critical to ensure that these systems behave predictably, securely, and reliably, even in an 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 in 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. Many of the research works are sprinkled across the proceedings of various conferences with varying scopes and purposes. Furthermore, much of the research on automotive security is conflated with other related areas in 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.

This special issue focuses on research direction and challenges in automotive security. The aim is to facilitate an understanding spectrum of challenges, approaches, and solutions in this area, and provide an authoritative reference of the state of the art.

It is beyond the scope of a special issue to provide a comprehensive treatment of this vast area. Instead, we selected five representative articles to provide a sampling of the various facets of research challenges in this area:

- "Lessons Learned from Hacking a Car," by Miller
- "Security of Emergent Automotive Systems: A Tutorial Introduction and Perspectives on Practice," by Lopez et al.

Digital Object Identifier 10.1109/MDAT.2019.2944085
Date of current version: 31 October 2019.

- "Randomization for Safer, More Reliable and Secure, High-Performance Automotive Processors," by Trilla et al.
- "Survey of Automotive Controller Area Network Intrusion-Detection Systems," by Young et al.
- "Pass and Run: A Privacy-Preserving Delay Tolerant Network Communication Protocol for Cyber-Vehicles," by Lu et al.

Since a key goal of the special issue is to provide a comprehensive reference for different research challenges and for making progress, each article includes a detailed discussion of related research.

We express our sincere thanks to all the authors and referees for their contribution in creating this special issue. We thank the Editor-in-Chief for his encouragement and support, and the administrative staff for technical help (and friendly nudges) at different stages of this long process. We hope you enjoy this issue and that it inspires more research to identify and overcome future security challenges in our increasingly complex automotive systems and applications. ■

■ Direct questions and comments about this article to Sandip Ray, Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611 USA; sandip@ece.ufl.edu.