CyCAR'2013: First International Academic Workshop on Security, Privacy and Dependability for CyberVehicles

Arslan Munir
Rice University
Houston, TX, USA
arslan@rice.edu

Farinaz Koushanfar
Rice University
Houston, TX, USA
farinaz@rice.edu

Hervé Seudié
Robert Bosch GmbH
Darmstadt, Germany
herve.seudie@de.bosch.com

Ahmad-Reza Sadeghi
Intel CRISC & TU Darmstadt
Darmstadt, Germany
ahmad.sadeghi@trust.cased.de

ABSTRACT

The next generation of automobiles (also known as CyberVehicles) will increasingly incorporate electronic control units in novel automotive control applications. Recent work has demonstrated vulnerability of modern automotive control systems to security attacks that directly impact CyberVehicles' physical safety and dependability. The First International Academic Workshop on Security, Privacy and Dependability for CyberVehicles (CyCAR'13) focuses on security and privacy topics in CyberVehicles that are within the scope of ACM Conference on Computer and Communications Security (CCS). Specifically, the workshop targets issues related to security and privacy issues in computerized, complex, and connected modern vehicles as well as their complex supply chains. This workshop offers an opportunity to trigger the transfer of the accumulated knowledge by the ACM CCS community to the car industry while taking into account typical automotive constraints such as interoperability, reliability, dependability, quality, resource constraints and/or complex supply chain.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*Security and Protection (e.g., firewalls)*; C.3 [**Computer Systems Organization**]: Special-Purpose and Application-Based Systems—*Real-time and embedded systems*; C.4 [**Computer Systems Organization**]: Performance of Systems—*Design studies, modeling techniques*; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection (e.g., firewalls)

General Terms

Performance, Reliability, Security

CCS'13, November 4–8, 2013, Berlin, Germany.

Keywords

Automotive, security, dependability, privacy, cybervehicles, embedded systems

1. INTRODUCTION

Modern automotive systems integrate a multitude of embedded hard real-time control functionalities, and a host of advanced information and entertainment (infotainment) features. The true paradigm shift for future automotive (CyberVehicle) systems and other transportation systems, i.e., avionics, maritime, and rails, is not only a result of this increasing plurality of subsystems and functions, but is also driven by the unprecedented levels of intra- and inter-CyberVehicle system connections and communications as well as networking with external entities, such as smart mobile devices and the cloud. The emergence of new generations of intelligent transportation systems that are fully connected to their surrounding objects, environments, and networks poses various design challenges for the automotive/transportation industry, such as interoperability, reliability, dependability, quality and security.

The development of CyberVehicles is both necessary and inevitable, as it opens up both several business opportunities and user comfort. For example, traffic congestion avoidance mitigation services that take advantage of connectivity to the cloud and global perspective of route conditions can alleviate the rising business losses due to traffic jam in metropolitan areas. Such services ought to consider safety and security as a top objectives as attacks to one subsystem or network component could impact a larger portion of the connected system.

The First International Academic Workshop on Security, Privacy and Dependability for CyberVehicles (CyCAR'13) brings together researchers and practitioners in security domain related to modern and next generation automotive systems. The workshop solicited two types of original papers: full papers and short/work-in-progress/position-papers. The goal of this workshop is to bring together academic and automotive industry researchers to discuss, identify and address the challenges related to achieving secure, dependable and privacy-preserving cybervehicle systems.

2. FORMAT

CyCAR'2013 will be a full-day workshop program on the first day of CCS 2013. The workshop will begin with an invited talk from Ulrich Huber, Associate principal of McKinsey & Company, responsible for automotive solutions. In his talk "Mobility of the future", Ulrich will present his views on the roadmap of future applications in the area of cyber vehicles and their impact on security and privacy. The workshop will also have accepted paper sessions. Each paper session will conclude with a discussion led by a pre-chosen workshop participant. These discussions will tie together common themes of the presentations and hopefully lead to insightful discussions about future research directions. The program will end with a panel discussion where panelists will discuss the current state of the art, focus areas, and opportunities for future research.

3. TOPICS OF INTEREST

In terms of author audience, we solicited paper submissions related to the following (but not limited to) research topics:

- Security engineering and life-cycle management in the automotive and transportation domain
- Security management in automotive supply chain
- Design methodologies and development, validation, and automation tools for secure vehicle components
- Secure and dependable intra- and inter-vehicle communication
- Secure theft protection mechanisms for the automotive domain
- Anonymous credentials in the automotive domain
- Automotive security research challenges
- Dependable and secure automotive use-cases
- Architecture and implementation technologies for automotive trusted platform
- Limitations, alternatives, and tradeoffs regarding automotive trusted computing
- Secure wireless and mobile technologies in vehicles
- Secure localization and location privacy
- Mobile (smart) device integration in vehicles and transport systems
- Intrusion detection systems for the automotive domain
- Secure interaction between cloud and vehicular network
- Secure software update and feature activation on car components
- IP protection in vehicle components
- Secure software update and feature activation on car components
- Secure remote update
- Remote attestation of automotive trusted devices
- Secure hardware for low cost automotive devices
- Virtualization in automotive components

4. PROGRAM COMMITTEE

We are grateful to the following program committee members for contributing their expertise in selection of the papers for the workshop program:

- Arslan Munir, Rice University, Houston, TX, USA
- Frank Kargl, Ulm University, Germany
- Elmar Schoch, AUDI, Germany
- Wenyuan XU, University of South Carolina, USA
- Sdrjan Capkun, ETH Zurich, Switzerland
- Matthias Schunter, Intel, Germany
- Flavio D. Garcia, University of Birmingham, England
- Tom Forest, General Motors Research & Development, USA
- Gang Qu, University of Maryland, USA
- Ivan Martinovic, University of Oxford, England
- Christoph Paar, University of Bochum, Germany
- Gene Tsudik, University of California, USA
- Alexandra Dmitrienko, Fraunhofer SIT, Germany
- Steffen Schulz, Intel, Germany
- Lujo Bauer, Carnegie Mellon University, USA
- John Kenney, Toyota InfoTechnology Center, USA
- Kevin Snow, University of North Carolina at Chapel Hill, USA

5. WORKSHOP ORGANIZERS

- Ahmad-Reza Sadeghi, Intel CRISC & TU Darmstadt, Germany, ahmad.sadeghi@trust.cased.de
- Cliff Wang, Army Research Office, USA, cliff.wang@us.army.mil
- Hervé Seudié, Robert Bosch GmbH, Germany, herve.seudie@de.bosch.com
- Farinaz Koushanfar, Rice University, USA, farinaz@rice.edu
- Albert Held, Daimler AG, Germany, albert.held@daimler.com