Die Fakultät für Informatik an der Universität Wien lädt Sie herzlich ein zum

CS-Colloquium

Automotive Cybersecurity: an Industry Perspective and Research Challenges

mit Dr. Zhendong Ma (Bosch)

Wann?	27. November, ab 15:00 Uhr
Wo?	Hörsaal 3 (HS3), Fakultät für Informatik Währinger Straße 29 1090 Wien

Abstract

The Automotive systems have undergone a profound technological transformation in recent years due to the industry trends towards electrification, connectivity, and autonomy. Cybersecurity becomes a challenging issue because cars are turning into computers-on-wheels and running largely on software. This talk briefly reviews the history of car hacks and provides an insight of the challenges and solutions from an industry perspective. It then describes the research challenges to secure automotive systems in the era of Internet of Things, and proposes possible research directions.

Bio

Dr. Zhendong MA is a security expert in automotive security engineering, threat analysis, security architecture design and technology development in and around intelligent and connected cars. Since August 2019, he works as an automotive security engineer at Bosch Engineering in Vienna. From October 2017 to July 2019 he worked as a senior security engineer at AVL in Graz, where he participated in the build-up of automotive security engineering capabilities from security analysis, design, development to testing. He also lead security R&D projects and established strategic research efforts and partnerships. Prior to joining AVL, he led innovation and research projects on information security and privacy in various areas including cloud computing, digital identity, video surveillance system, industrial control systems, embedded and cyber-physical systems at Austrian Institute of Technology from 2010 to 2017. He holds a doctorate degree from Ulm University while researching on the emerging vehicular communication system security and privacy in EU FP6 project SEVECOM and PRECIOSA. His current

research interests are in the defense and offense of automotive systems and embedded systems in general, and the theories and practices of securing Internet of Things.