March 5th, 2020

Towards Secure Cyber-Physical Systems for Autonomous Vehicles

Morteza Biglari-Abhari
Department of Electrical and Computer Engineering, University of Auckland in Auckland, New Zealand

Abstract

Cyber-Physical systems have become ubiquitous. These systems integrate different functionalities to satisfy the performance requirements and take advantage of the available processing power of multi-core systems. Safety critical applications such as autonomous vehicles or medical devices rely not only on proving correct functionality of cyber-physical systems as essential certification criteria but they must also satisfy other design constraints such as energy efficiency, low power consumption and reliability. Their need to connect to the internet have created new challenges which means addressing the security vulnerabilities has become as the first-class design concern.

In this talk, first a hardware/software co-design approach for two critical tasks, real-time pedestrian and vehicle detections, which are essential in advanced driving assistance systems (ADAS) and autonomous driving systems (ADS) is presented. We use partial dynamic reconfiguration on FPGA for adaptive vehicle detection. In the second part of

this talk, a system-level security-aware design approach is presented to avoid or confine the impact of security compromises on the critical components of the cyber-physical systems implemented in multiprocessor systems on chip. Our system-level security approach considers the described system architecture for a specific application and analyzes its security vulnerability based on the specified security rules to generate an impact analysis report. Then, it creates a new system architecture configuration to protect the critical components of the system by providing isolation of tasks without the need to trust a central authority at run-time for heterogeneous multiprocessor system. This approach allows safe use of shared IP with direct memory access, as well as shared libraries by regulating memory accesses and the communications between the system components.

Short bio

Morteza Biglari-Abhari received the M.Sc. degree in electrical and electronic engineering from Sharif University of Technology, Tehran, Iran, and Ph.D. degree from the University of Adelaide, Australia. He joined the Department of Electrical and Computer Engineering, University of Auckland in Auckland, New Zealand in 2001. He has been Director of Computer Systems Engineering program from December 2015 to January 2020 and previously member of the Academic Program Committee in Faculty of Engineering for eight years.

His current research interests include Security Enhanced Computer Architecture (secure and reliable architecture for multiprocessor systems on chip for automotive applications and autonomous vehicles), Embedded Computer Vision Systems (hardware/software co-design for object detection and tracking using smart distributed cameras, convolutional neural networks and machine learning) and real-time low power reconfigurable multiprocessor systems on chip. He has been a reviewer for many conferences in the embedded systems research area and several journals, including the IEEE Transactions on Computers, IEEE Transactions on Circuits and Systems for Video Technology, IEEE Transaction on Industrial Informatics, IEEE Embedded Systems Letters, ACM Transactions on Embedded Computing Systems, Journal of Microprocessors and Micro Systems, Journal of Real Time Image Processing, and Journal on Embedded Systems.