Guest Editors' Introduction

Novel Cybersecurity Paradigms for Consumer Technology

Fernando Pescador
Universidad Politécnica de Madrid

Saraju P. Mohanty
University of North Texas

Almost all the current generation consumer electronics (CE) and consumer technology (CT) have the feature of Internet connectivity. This connectivity comes with the major challenge of cybersecurity. Cybersecurity threats in for CE devices and systems have multiple forms including software, hardware, and communications networks. The cybersecurity attacks can come from remote locations through Internet. The cybersecurity threats can be local as built-in as trojans, which can be remotely exploited.

In general, a variety of consumer devices are integrated in the Internet-of-Things (IoT) and cyber–physical systems (CPS) making large smart components. For example, healthcare CPS making smart healthcare, agriculture CPS making smart agriculture, and transportation CPS making smart transportation, and energy CPS making smart energy. Similarly, at a smaller scale, smart homes and autonomous vehicles can have serious cybersecurity issues.

With the previous thoughts, we invited perspective authors to contribute to the current special section that presents state-of-the-art of cybersecurity solutions for CE and CT. We briefly present the accepted papers in the following paragraphs.

The article titled "Evolution of Wi-Fi Protected Access: Security Challenges" presents various weaknesses Wi-Fi network security along with the possible solutions. It identifies where these weaknesses originated in the previous versions of Wi-Fi network security and discusses how the new version fixed those.

The article titled "Reliable IoT Data Management Platform Based on Real-World Cooperation Through Blockchain" introduces a blockchain-based data management platform to verify the integrity big sensor data received through IoT-integrated devices, such as camera, personal assistant device, air-conditioning control, or smart meter.

The article titled "A Reverse Hash Chain Path-Based Access Control Scheme for a Connected Smart Home System" presents a blockchain-based solution for security of smart and connected homes.

The article titled "A Defense Mechanism Against Replay Attack in Remote Keyless Entry Systems Using Timestamping and XOR Logic" introduces a robust remote keyless entry systems, which can be integrated in facilities, such as smart homes and smart vehicles.

The guest editors sincerely believe that this special section will be a good reading for CT researchers around the globe. The guest editors would like to thank all the authors for their excellent contributions and the reviewers for their help in reviewing the manuscripts.

Fernando Pescador,
Guest Editor
Universidad Politécnica de Madrid, 28040 Madrid, Spain
Saraju P. Mohanty,
Guest Editor
University of North Texas, Denton, TX 76203 USA

Digital Object Identifier 10.1109/MCE.2020.3032206
Date of current version 4 December 2020.

Published by the IEEE Consumer Technology Society

Fernando Pescador is currently an Assistant Professor with the Department of Computer Science and Electronic Engineering, Universidad Politécnica de Madrid, Madrid, Spain. Contact him at fernando.pescador@upm.es.

Saraju P. Mohanty is currently a Professor with the Department of Computer Science and Engineering, University of North Texas, Denton, TX, USA. Contact him at saraju.mohanty@unt.edu.