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 consumer electronics 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 (H-CPS) making smart healthcare, agriculture CPS (A-CPS) making smart agriculture, and transportation CPS (T-CPS) making smart transportation and energy CPS (E-CPS) making smart energy. Similarly, at a smaller scale smart homes and autonomous vehicles can have serious cybersecurity issues.

With the above thoughts, we invited perspective authors to contribute to the current Special Section that presents state-of-art of cybersecurity solutions for consumer electronics and consumer technology. 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 (RKE)

systems which can be integrated in facilities like smart homes and smart vehicles.

The guest editors sincerely believe that this Special Section will be a good reading for Consumer Technology 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.

Guest Editors Bio:

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

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