Editor's Message

Welcome to this special issue of Reliability Magazine.

Just a decade ago, Internet-of-Things (IoT) was regarded as unrealistic fantasy. It was first presented as an innovative idea to stimulate the development of modern networking technologies. Within the last few years, as the maturity of tools, devices, equipment, infrastructure and services, IoT has become one of the most popular technologies in the 21st century. IoT intends to provide smart connectivity of devices on the Internet, ranging from home automation and entertainment products to industrial machinery and smart cities. It is designed to enable a variety of services by exchanging data with manufacturers, operators and consumers. Ideally, every IoT device can be uniquely identified and thus managed remotely, and is able to interconnect with other IoT devices in an automatic fashion.

Business processes can be empowered by this new technology, and various industries redesign their business models and processes along the IoT paradigm. For example, manufactures can monitor the status of things or predict when an IoT device is out of order. However, experts warn that the growing number of interconnected "thingbots" could endanger the IoT business. To maximize the social and economic benefit of the technology, security issues of interoperability, data management, platform and protocol validation have to be addressed.

In this special issue, we have collected two articles, which discuss security issues for IoT applications from different points of view.

The first article, "Secure and Safe Automated Vehicle Platooning" is by Jiafa Liu from the Computer and Information Science Department at the University of Michigan-Dearborn. This article discusses security issues when IoT is applied to automotive applications. Cyber attacks highlighted on an automated platoon system could have the most severe level of safety impact with large scale car crash and argue the importance of safety-security co-design for safety critical cyber physical systems.

The second article, "Anonymous and Secure Fault-Tolerable Routing Protocol for Overlay Networks" is by Chia-Chen Wu from the Computer Science Department at National Chiao-Tung University. The routing security is addressed for overlay networks and IoT applications. A novel protocol (SAFE) providing anonymity against adversaries is presented in the article. By randomly selecting intermediate nodes to forward data and by using layered encryption to hide an initiator from the intermediate nodes, SAFE can provide initiator and responder anonymities and fault tolerance of node failures. The fault tolerance provided by SAFE results in the reduced cost and frequency of path reconstruction, and the increased robustness of network against degradation attacks.

We hope you enjoy the articles in this issue, and that you find these contributions to the discussion of security of IoT applications within the reliability engineering profession useful. We look forward to your comments and suggestions.

Yu-Lun Huang

Professor and Director, National Chiao-Tung University (NCTU)

Editor, IEEE Reliability Special Issue on Trustworthy Computing and Cybersecurity

ylhuang@cn.nctu.edu.tw