Message from the Editor

With the fast growth of IoT technology, new reliability concerns also emerged. Among the new concerns, we will study two particularly interesting topics in this issue including IoT critical infrastructure and computer security education.

On the first topic, P. A. Laplante of Penn State University presents an article *"Critical Infrastructure Systems and the Internet of Things"* to discuss the considerations for IoT applications that involve or interact with critical systems. In the forthcoming IoT age, traditional security concerns have been extended to threaten new kinds of devices and systems. Fu-Hau Hsu introduces in his article *"Is Your Vehicle Controlled by You?"* that the new threat can be physically harmful when a vehicle is hijacked given that hacking is done against vehicular computers. Wireless networks are part of the critical infrastructure in the IoT age. To illustrate an applicable testbed for security analysis, Borting Chen and Yu-Lun Huang's article *"Launching a Security Testbed for Wireless Networks with Extensibility to Support Mobile Experiments"* presents relevant concepts, case studies, performance measurement, and war-driving experiments.

Computer security education has been a hot topic for decades. Foreseeing the trend, computer security becomes even more important in the IoT age since the large-quantity and the heterogeneity of devices make security and reliability problems more and more complex. An article "*Tool, Technique, and Tao in Computer Security Education.*" provided by Zhenkai Liang and Jian Mao discusses fundamental concepts and the right methodology for computer security education. It points out a good direction for the students who are facing the fast-changing security landscape. "*CTF: Alternative Training for Offensive Security*", the last article in this issue written by Chung-Kuan Chen and myself, describes an alternative way for computer security education. Traditional security education is insufficient for offensive security. Most security courses are designed from the defender's perspective, and have a big gap from the real world problems in practice. The emerging contest Catch-The Flag (CTF) can complement the traditional education for security training. In a CTF contest, competitors will try to solve security problems that are close to real world problems, or attack competitors' systems with a wide range of knowledge of skills.

I sincerely invite you to read the interesting articles in this issue, and provide us with your comments and feedback. Happy reading.

Shiuhpyng Winston Shieh
Editor-in-Chief, IEEE Reliability