Message from the Editor

CrossMark

Dear Readers,

While writing these lines, I just received approval for our application to join COPE (Committee on Publication Ethics), a group of journal editors established in 1997 and currently with over 10,000 members worldwide. The group was founded to provide advice for maintaining a high code of conduct and best practice guidelines for its journal editor members. This confirms the commitment of our journal, Journal of King Saud University – Computer and Information Sciences, to abiding by the high international standards of ethics and professionalism in publication.

With the recent world developments related to some cyber-attacks ranging from server hacking to virus spreading, the need for a more secure Internet is more than ever both a necessity and a requirement. As the world is becoming more dependent on the communication infrastructure provided through the Internet for individuals, corporations, or governments, a war against any cyber-attacks should be fought on both the technical and the legislative fronts. While the cooperation between researchers and academics through journal and conference publications will be advantageous in the first front, nevertheless it may be fought individually throughout the world. However, for the second front, the cooperation and agreements between countries is mandatory, and probably ought to be overseen by an international entity that may resolve disputes.

All said, I believe that the technical front has to shift from the protective aspects to the forensic ones. It is almost inconceivable to allow certain group of users with some valid credentials and not allow some other vicious ones with the same valid, but stolen, credentials. The key, and possibly the only solution, is to devise tools that may follow the traces of users that may have caused damage or were not real legitimate users. These tools should be approved and satisfy some standard specifications to be used as reliable proofs of guilt.

This third issue of volume 29 contains fourteen papers. The first article is a review of recent trends in congestion control in wireless sensor networks, followed by seven articles that fall within this context of security and its various aspects. We start this group with an article presenting some quantitative means for evaluating the security performance of wireless LANs. Followed by an article that defines a trust-based framework that uses the flood factor to achieve a secure data transmission in MANETs. The third paper presents a security model for a cloud-based health care system. Then, a new watermarking tool that protects digital images is presented. In the fifth paper, different efficient FPGA hardware implementations of AES encryption algorithm are presented and compared. The last two security related papers present some security-key signature based techniques; in one for a new identity identification and in the other for an authentication protocol for mobile commerce.

The second half of this issue covers new research in other computer related fields. The two following papers are software engineering related, with the first presenting a new tool for software design, and the second, an optimization technique for improving package structure of object-oriented software. The remaining four papers are in different areas, with the first proposing an adaptive routing policy technique for selecting data centers over the cloud; the second proposing a fault tolerant approach for leader election in MANETs; the third presenting a novel technique for motion detection; and finally, the fourth proposing a performance evaluation technique for asynchronous cache on FPGAs.

Finally, we hope that you will find the topics of this issue most useful in your research and developments, and that new research horizons will be opened for some, and some answers for others.

Editor-in-Chief of JKSUCI
Prof. Nasser-Eddine Rikli

Peer review under responsibility of King Saud University.