The ISC Int'l Journal of Information Security
ISeCure

July 2010, Volume 2, Number 2 (pp. 67–68)
http://www.isecure-journal.org

From the Editor-in-Chief

Editorial

Welcome to the second issue of the second volume of ISeCure, the ISC International Journal of Information Security. After two years of voluntary cooperation in handling of submitted papers and publishing of ISeCure, on behalf of the Editorial Board, I would like to express our sincere appreciation to paper editors, reviewers, editorial assistants, administrative assistant, English editor, authors, and readers.

During the course of publication of this issue, we received a substantial number of manuscripts. Among them, several were the extended version of some selected papers from the ISCISC'09 conference. Unfortunately, due to our rigid review process, no ISCISC'09 paper found its way into this issue. We are looking forward to receiving and reviewing the extended papers from the ISCISC'10 conference, as well as any other related conference. It is expected that the respectable conference authors extend their papers in terms of both contribution and the length (see `http://isecure-journal.org/Form/GeneralInformation.aspx?CT=Guide#author-guide` for more information), before submitting it to ISeCure. As always, any comment, feedback, submission, and contribution from our dear readers is welcome.

This issue of ISeCure includes four papers. Our sincere gratitude goes to Professor Ed Dawson, who accepted to submit his invited paper to ISeCure. The **invited paper** investigates whether the current authorization models are able to adapt with the required flexibility and scalability of the emerging business models based on the concept of virtual organizations. The authors discuss the motivation and requirement for a new flexible access control model that addresses such needs through an explicit specification of the objectives of the system. In their proposed Objectives-Based Access Control concept, access decisions are made based on a late trade-off analysis between those explicit objectives.

The **second paper** focuses on establishing pairwise keys among sensors in wireless sensor networks considering the limited computation power in such networks. As available key establishment schemes suffer from either weak performance, or high resource consumption in the sensor side, the authors propose using symmetric polynomials as the basis for their key establishment protocol. The performance is improved through distributing polynomial shares among the sensors. It is possible to tune the proposed protocol based on the required performance, security, and resource consumption.

The **third paper** investigates hiding a considerable amount of secret information into Arabic text cover media using the extension character "Kashida" in the Arabic language. The implemented system, called MSCUKAT, utilizes several algorithms proposed in this paper. Increasing the capacity of cover media to hide more secret information, reducing the file size growth after hiding the secret, enhancing the security of the encoded cover media, and outperforming the previous works in this special context are the improvements done in the paper.

The **fourth paper** presents a steganalysis method for detection of Perturbed Quantization (PQ) steganography scheme. It is shown that the PQ method deforms the dependencies of DCT coefficient values, especially changes much lower than significant bitplanes. To perform steganalysis, feature extraction from the empirical matrix is proposed. The features are exploited within an empirical matrix of DCT coefficients having some most-significant bit planes deleted. Four empirical matrices are obtained and combined into the resulting features from these matrices to be used in steganalysis. This technique can detect PQ embedding on stego images with 77 percent detection accuracy on mixed embedding rates between 0:05 - 0:4 bits per non-zero DCT AC coefficients (BPNZC).

Rasool Jalili

Editor-in-Chief,

ISeCure