The ISC Int'l Journal of Information Security
ISeCure

January 2011, Volume 3, Number 1 (pp. 1–1)
http://www.isecure-journal.org

From the Editor-in-Chief

Editorial

We are publishing the third volume of ISeCure, the ISC International Journal of Information Security, while the world encountering serious challenges on the cyber war as well as the security of the cyber space. The affirmation of the emergence and propagation of the new generation of intelligent malwares (such as Stuxnet in industrial infrastructures) around the world in 2010, leads us to look after the future of cyber space security, which is described in the invited paper of this issue.

On behalf of the editorial board, I express my genuine appreciation for the very challenging topic selected by Professor Matt Bishop to write an invited paper on. He articulated several aspects of the past and future of computer security, considering the fact that computer security affects all aspects of our daily life in all ingredients of society. Professor Bishop hypothesizes about the future of the field of Computer Security. He integrated all his thoughts/experiences presented in several conferences and published in various journals, as well as the feedbacks/comments he received therein, into this valuable paper.

The second paper in this issue proposes an efficient and cost-effective lattice-based public-key cryptosystem using non-commutative quaternion algebra. The authors proved that such a cryptosystem is more secure than some existing lattice-based ones, and with a dimension of 41, it has security equal to NTRU-167. The underlying algebraic structure, key generation, key security, message security, and the process of encryption and decryption are described in detail.

In the third paper, the authors propose an e-voting scheme based on Asadpour *et al.*'s scheme, which is one of the most recent results trying to resolve issues with Mu-Varadharajan's e-voting scheme. The scheme, which is based on a special structure, directly uses the identity of the voter, hides it in that structure, and reveals it after double voting. The security of the scheme depends on the hardness of the RSA cryptosystem, Discrete Logarithm problem, and Representation problem.

In the fourth paper of this issue, the authors treat the problem of robust image watermarking against DWT-based image compression algorithms, using genetic algorithms. The experimental results on the proposed algorithm confirm its strength against some attacks as well as its appropriateness for secure and progressive image transmission applications over the Internet.

Rasool Jalili
Editor-in-Chief,
ISeCure

ISSN: 2008-2045