The ISC Int'l Journal of Information Security
ISeCure

July 2012, Volume 4, Number 2 (pp. 95–96)
http://www.isecure-journal.org

From the Editor-in-Chief

Editorial

Welcome to the second issue of the fourth volume of ISeCure. In this issue, we publish six papers, along with a single page per paper including the translation of the title and the abstract in Persian, for the utilization of Persian indexing centers.

Our **first paper** of this issue introduces an analytical and robust approach to detect stego images, based on the analysis of the eigenvalues of the cover correlation matrix. The method uses the LSB plane of images in spatial domain, extendable to transform domain, to detect low embedding rates. The proposed method is evaluated through simulation, whose results demonstrated outperformance of the method over some well-known LSB steganalysis methods, especially at low embedding rates.

The **second paper** analyzes some weaknesses of the GSM Encryption Algorithm A5/1 as well as an improvement to an attack and investigation of the A5/1 state transition. A method is proposed to identify and eliminate useless states from the pre-computed tables. An approach is also proposed to improve the time complexity and the required memory in the online phase of the attack. Another weakness of A5/1 is also discussed, focusing on its internal state transition and keystream sequence period. The model is verified using a variety of simulations, whose results are shown to be consistent with the theoretical ones.

The **third paper** combines cryptography and information hiding methods, and uses chaos theory to improve the security of Double Random Phase Encoding (DRPE). In particular, a chaotic map and a fractal image are used to generate the encryption/decryption keys of the plain image. In this way, there is no need to transfer the keys through a secure channel, and sending the key generation parameters is sufficient. In order to watermark the encrypted image, its real and imaginary parts are embedded into an enlarged normalized host image. Experimental results demonstrate the higher security and resistance of the method against the commonplace attacks.

The **fourth paper** proposes a causal alert correlation method aimed to detect attack scenarios in real-time Intrusion Detection Systems (IDSs). The knowledge base of the attack patterns is represented in a Causal Relations Graph. For each received alert, its correlations with the previously received alerts are found by performing a search only in a corresponding Queue tree, which significantly reduces the processing time of each alert. The proposed method is claimed to be immune against deliberately slowed attacks. Experimental results of the implementation and tests against the DARPA2000 dataset show the correctness of the proposed method as well as its efficiency with respect to the running time.

The **fifth paper** attempts to analyze the digital forensics involved in the creation of counterfeit documents, with specific focus on determining whether a graphic design application has been installed, whether the application has been used, and determining whether an association can be made between the application's actions and such a digital crime. The subsequent phase involves analyzing files associated with these applications for file

ISSN: 2008-2045

signatures and metadata. Subsequently, it will be possible to determine whether a system has been used for creating counterfeit documents.

Our **last paper** in this issue introduces a framework for an integrated representation of trust and confidence using intervals. The framework introduces a multiplication operator for trust intervals to compute the propagated trust and confidence, as well as a summation operator to aggregate different trust opinions. In addition, a time-variant method is proposed that comprises freshness, expertise level, and two similarity measures to estimate the confidence. The model is studied on two well-known datasets and the results are compared to other existing methods to show its accuracy.

I would like to sincerely thank all the authors for their high-quality research papers, and acknowledge our reviewers for their valuable and critical reviews, which helped us to keep the quality of ISeCure and its current standard.

Rasool Jalili
Editor-in-Chief,
ISeCure