The ISC Int'l Journal of Information Security
ISeCure

July 2014, Volume 6, Number 2 (pp. 97–98)
http://www.isecure-journal.org

From the Editor-in-Chief

Editorial

Welcome to the second issue of the sixth volume of the journal. In this issue, we publish six papers, as well as a single page per paper incorporating the translation of the title and abstract in Persian, to be used by Persian indexing centers.

Thanks to Professor Damiani and his co-authors for their invited paper focusing on "A Risk Model for Cloud Processes", which appears as the **first** paper in this issue. The paper tackles the problems through a process-oriented quantitative risk assessment methodology aimed at disclosure risks on cloud computing platforms. Key advantages of the methodology include (i) a fully quantitative and iterative approach, which enables stakeholders to compare alternative versions of cloud-based processes; (ii) non-frequency-based probability estimates, which allow analyzing threats for which a detailed history is not available; and (iii) support for quick visual comparisons of risk profiles of alternative processes even when impact cannot be exactly quantified.

Artemia as the name of a family of provably secure authenticated encryption schemes covers the **second** paper in this issue. It is an online nonce-based authenticated encryption scheme which supports the associated data. Artemia uses the permutation based mode, JHAE, that is provably secure in the ideal permutation model. The scheme does not require the inverse of the permutation in the decryption function, which provides resource efficiency. Artemia permutations have an efficient and a simple structure and are provably secure against the differential and linear cryptanalysis. In the permutations, MDS recursive layers were used that can be easily implemented in both software and hardware.

The **third** paper in this issue proposes an efficient non-repudiation billing protocol (NRBP), based on extensible authentication protocols, in heterogonous 3G-WLAN networks. The authentication scheme provides a non-repudiation property for the billing problem. The proposed scheme is analyzed based on different security features and computation overhead. In comparison with previous approaches, this protocol contains all the considered security parameters. Moreover, the computation overhead of this protocol is less than other schemes.

The **fourth** paper proposes a type of intrusion detection system for detecting attacks in both database transaction level and inter-transaction level (user task level). For this purpose, a detection method at transaction level is proposed, which is based on describing the expected transactions within the database applications. Then at inter-transaction level, a detection method is proposed that is based on anomaly detection and uses data mining to find dependency and sequence rules. The advantage of this system compared to the previous database intrusion detection systems is that it can detect malicious behaviors in both transaction and inter-transaction levels. Also, it gains advantages of a hybrid method, including specification-based detection and anomaly detection, to minimize both false positive and false negative alarms. The evaluation results demonstrate that the true positive rate (recall metric) is higher than 80%, and the false positive rate is lower than 10% per different

ISSN: 2008-2045 © 2014 ISC. All rights reserved.

data sets and choosing appropriate ranges for support and confidence thresholds. The experimental evaluation results show high accuracy and effectiveness of the proposed system.

A blind image steganalysis method in Contourlet domain is proposed as the **fifth** paper in this issue, and it is shown that the embedding process changes statistics of Contourlet coefficients. Absolute Zernike moments and characteristic function moments of Contourlet subbands coefficients of the image are used to distinguish between the stego and non-stego images, employing a nonlinear SVM classifier with an RBF kernel. Superiority of the proposed method over its counterpart steganalyzers, in cases of five popular JPEG steganography techniques, is confirmed by the experimental results.

From this issue on, ISeCure will publish “Short Papers”. Short papers are different from regular papers in terms of their length and contribution. The length of a short paper should be about 6000 words. Short papers should present some recent results, works in progress, and new ideas that can be reported briefly. In this regard, our **sixth** paper in this issue is a short paper which proposes a two-phase detection scheme to detect and prevent wormhole attacks in MANETs. The proposed scheme attends to average delay per hop and neighbor’s behavior monitoring during data packet forwarding. According to simulation results, the proposed scheme is quite well in detecting all types of wormhole attacks such as in-band and out-of-band ones in different modes such as hidden or exposed, without requiring any hardware and clock synchronization.

Finally, I would like to sincerely thank all the authors for their submitted 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