The ISC Int'l Journal of Information Security
ISeCure

January 2013, Volume 5, Number 1 (pp. 1–3)
http://www.isecure-journal.org

From the Editor-in-Chief

Editorial

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

My sincere thanks and appreciation to Professor Akhaee and Professor Marvasti for their deep and comprehensive invited survey paper investigating the concepts and criteria of information hiding, its traits, requirements, and applications. In particular, HAS (Human Auditory System) and HVS (Human Visual System) are briefly reviewed to find out the amount of data, which can be embedded into an audio or image due to the weaknesses in these systems. A classification of well-known audio and image data hiding schemes is proposed along with their general comparison. Finally, the authors review the steganalysis methods for testing the watermarking algorithms.

The **second paper** in this issue presents a new broadcast encryption scheme based on threshold secret-sharing and secure multiparty computation. The scheme is fair and dynamic. Henceforth, a broadcaster can broadcast a message to any dynamic group of users in the system while no cheater is able to gain an unfair advantage over the other users. The scheme is collusion-resistant, as well. By taking advantage of secure multiparty computation, a traitor needs k cooperators in order to create a decryption machine. Broadcasters can compromise on communication complexity and collusion resistance by choosing a proper value of k. Comparisons with the other similar schemes indicate performance and complexity improvements by the proposed scheme. The scheme is modeled using the applied pi calculus, and its security is verified using ProVerif.

Our **third paper** in this issue proposes an identity-based key agreement protocol among users of different networks using elliptic curves. The security proof of the proposed protocol in the random oracle model confirms that it satisfies all the desired security attributes. Evaluation of the proposed protocol in comparison with some related protocols indicates 10% less execution time and 50% less communication cost than the competitor protocols.

The **fourth paper** in this issue proposes an approach to extract features from executable files to find their run-time behavior. It is assumed that the behavior of a binary file can be represented by the value of its registers. Comparing such values before and after an API invocation in an original executable and those in a doubtful possibly malware-injected version, can help to detect malicious files. The authors' experiment indicates a high level of accuracy and a low level of false positive in the proposed approach.

Back to the watermarking topic, our **fifth paper** in this issue proposes a robust multiplicative video watermarking scheme. In this scheme, video signals are segmented into 3-D blocks and the 3-D wavelet transform is applied on them. The low frequency components of the wavelet coefficients are used to make the process robust against malicious and unintentional attacks. The watermark extraction in the scheme relies on a maximum

ISSN: 2008-2045

likelihood-based procedure, observing the distribution of the watermarked coefficients. Evaluation of the proposed scheme indicates its superiority to some other well-known similar methods.

Finally, the **sixth paper** in this issue proposes an algorithm for image encryption using chaotic tent maps and the desired key image. The first part of the algorithm, works in the frequency domain, changes the phase of the plain image, which in turn results in changes in the pixel values, and shuffles the pixel locations in the time domain. Simulation-based evaluation with respect to the well-known criteria indicates higher performance and security than similar published algorithms.

The editorial is concluded by the list of our faithful reviewers. On behalf of the editorial board, I acknowledge all the following volunteer researchers and scientists, who have reviewed manuscripts published in ISeCure during the past years. We greatly appreciate their tireless and largely unseen work. The list is ordered alphabetically by surnames:

Abadi, Mahdi
Tarbiat Modares University, Iran.

Abbasi, Sedigheh
Universitá degli Studi di Milano, Italy.

Abdollahzadeh Barforoush, Ahmad
Amirkabir University of Technology, Iran.

Ahmadian Attari, Mahmoud
K.N. Toosi University of Technology, Iran.

Akhaee, Mohammad Ali
University of Tehran, Iran.

Alaghband, Mahdi
Sharif University of Technology, Iran.

Alizadeh, Mahdi
Sharif University of Technology, Iran.

Amini, Morteza
Sharif University of Technology, Iran.

Asadpour, Masoud
University of Tehran, Iran.

Azmi, Reza
Alzahra University, Iran.

Bagheri, Nasour
Shahid Rajaee Teacher Training University, Iran.

Behnia, Sohrab
Urmia University of Technology, Iran.

Berenjkoub, Mehdi
Isfahan University of Technology, Iran.

Boorghany, Ahmad
Sharif University of Technology, Iran.

Damiani, Ernesto
Universitá degli Studi di Milano, Italy.

Daneshgar, Amir
Sharif University of Technology, Iran.

Dorri Nogoorani, Sadegh
Sharif University of Technology, Iran.

Dousti, Mohammad Sadeq
Sharif University of Technology, Iran.

Eghlidos, Taraneh
Sharif University of Technology, Iran.

Fakhredanesh, Mohammad
Amirkabir University of Technology, Iran.

Farhadi, Hamid
The University of Tokyo, Japan.

Firouzmand, Mohammad
Iranian Research Organization for Science & Technology, Iran.

Ghaemmaghami, Shahrokh
Sharif University of Technology, Iran.

Ghanbari, Mohammad
Sharif University of Technology, Iran.

Ghayoori, Majid
Imam Hussein University, Iran.

Gholampour, Iman
Sharif University of Technology, Iran.

Hadavi, Mohammad Ali
Sharif University of Technology, Iran.

Rasool Jalili
Editor-in-Chief,
ISeCure