The ISC Int'l Journal of Information Security
ISeCure

January 2015, Volume 7, Number 1 (pp. 1–2)
http://www.isecure-journal.org

From the Editor-in-Chief

Editorial

Welcome to the first issue of the seventh volume of the journal. In this issue, we publish five regular papers plus one short paper 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.

In the **first** paper of this issue an Optimistic Fair Exchange (OFE) protocol is proposed. OFE protocols are a good way for two parties to exchange their digital items in a fair way. But, there is a security problem in OFE protocols if the arbitrator acts dishonestly and colludes with the verifier, then the arbitrator can complete the transaction without getting signer's agreement. This paper proposes a traceable optimistic fair exchange protocol to trace the dishonest signer. The presented scheme is the first generic accountable OFE protocol that is secure in the standard model.

A novel local search method for microaggregation is the **second** paper in this issue. The paper proposes an effective microaggregation algorithm to produce useful protected data for privacy preserving data publishing. Microaggregation is mapped to a graph problem with two constraints. The algorithm iteratively satisfies the constraints in order to minimize Sum of within-group Squared Error (SSE). Experimental results on different real and synthetic data sets show the superiority of the method in comparison with recent microaggregation algorithms.

The **third** paper in this issue proposes a combinatorial model for access control in virtual organizations (VOs). In this model, organizations make their access control decisions based on the enhanced ABAC model and their VOs make their decisions based on the enhanced SBAC model. By ABAC, organizations can make fine-grain decisions and by SBAC, VOs can make their decisions in more abstract level by considering the semantic relationships of subjects and resources.

The **fourth** paper proposes a combination of steganography and cryptography for hiding information into digital images. In the first step, secret data is encrypted using the mono-alphabetic substitution cipher method and then it is embedded inside an image using a novel algorithm. The embedding algorithm utilizes a combination of random patterns based on Space Filling Curves (SFC) and the optimal pair-wise LSB matching method. Since finding the suboptimum adjustment list in the used LSB matching method has been defined as a discrete problem, therefore the modified version of Imperialist Competitive Algorithm using Genetic Algorithm operations is applied. The increase of visual quality obtained by this method shows that the performance of it is better than the previous methods belonged to the both LSB replacement approach and LSB matching approach.

A Grouped Gossip-based Reputation Aggregation Algorithm (GGRA) is proposed as the **fifth** paper in this issue. In GGRA, GossipTrust is executed in each group between group members and between groups instead of executing in the whole network. Due to the reduction in the number of nodes and using strongly connected graph instead of a weakly one, gossip algorithm in GGRA executes quickly. With grouping, not only reputation

ISSN: 2008-2045

aggregation is expected to be more scalable, but also because of the decrement in the number of errors of the gossiped communication, the results get more accurate.

Our **sixth** paper in this issue is a short paper which proposes a method for preventing Hardware Trojan Horse in ICs. For this aim, a cell placement algorithm is provided in which the algorithm places cells such a way that insertion of extra flip flop would be impossible. Also by using a clock skew, as one of the most important factors of circuits, and placing cells such a way that insertion of extra flip flop results differences in clock skew, the adversary cannot reach to his goals.

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

Rasool Jalili

Editor-in-Chief,

ISeCure