The ISC Int'l Journal of Information Security
ISeCure

July 2019, Volume 11, Number 2 (pp. 93–94)
http://www.isecure-journal.org

From the Editor-in-Chief

Editorial

Welcome to the second issue of the eleventh volume of the journal. In this issue, we publish six regular 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.

In the **first** paper of this issue, three different design methods using parameter adjustments in interdependent networks are proposed. The parameters include players' costs, interdependencies, and constraints to align players' incentives with a network-wide global objective. The comprehensive investigation of existence and uniqueness conditions of Nash Equilibrium in highly interconnected networks is presented, where the security of the entities are often interdependent and the network owner wants to maximize the overall network security by designing the game's parameters. Moreover, the numerical results of applying the proposed mechanisms in a sample real-world example are illustrated.

The security of SHA-3 against differential fault analysis is considered in the **second** paper of this issue, which could be important when this scheme is used as a message authentication code. The authors improved the previous results by employing the low algebraic degree of 1.5 round differential relations of SHA-3 as a basis to apply an effective fault analysis against it. Hence, using an SAT base strategy, they can recover the whole state of SHA-3, i.e. 1600 bits, with 5-8 effective faults, with a high chance of fault detection.

An efficient and secure lightweight privacy-preserving authentication scheme for a smart grid is proposed in the **third** paper of this issue. First, the authors showed that the recently proposed lightweight message authentication scheme for smart grid communications by Mahmood *et al.* has some security vulnerabilities. Then, to address these drawbacks, they proposed a new scheme which its security is evaluated and the formal security analysis and verification are introduced via the BAN logic and AVISPA tool.

Using three identical portions of GOST2 and fixed point idea, more enhanced fixed point attacks for filtration of wrong keys are presented in the **fourth** paper of this issue. The focus of the new attacks is on reducing memory complexity while keeping other complexities unchanged as well. The results show a significant reduction in the memory complexity of the attacks, while the time complexity slightly increased in comparison to the previous fixed point attacks. The authors claimed that they provided the lowest memory complexity for an attack on a full-round GOST2 block cipher.

With the advancement and development of computer network technologies, the way for intruders has become smoother; therefore, to detect threats and attacks, the importance of intrusion detection systems (IDS) as one of the key elements of security is increasing. In the **fifth** paper of this issue, a hybrid intrusion detection system using the decision tree and support vector machine (SVM) approaches is proposed. In this system, the feature selection is initially done by the C5.0 decision tree pruning, and then the features with the least predictor importance value are removed. Removing each feature, the least square support vector machine (LS-SVM) is applied. The final features are those having the highest surface area under the Receiver Operating Characteristic

ISSN: 2008-2045

(ROC) curve for LS-SVM. The experimental results on two KDD Cup 99 and UNSW-NB15 data sets show that the proposed approach improves true positive and false positive criteria and accuracy compared to the best prior work.

Detecting fake accounts in a social network is a challenging problem and recently its importance has been increased to provide security of these types of networks. The **sixth** paper of this issue addressed two problems in the identification of fake accounts; use of similarity measures which do not consider the power and strength of the mutual friends' communications and also data imbalance in the real dataset lacking of enough fake accounts. Authors proposed a method which is a combination of graph-based and machine learning methods. They used various similarity measures and applied Principal Component Analysis to each computed similarity matrix to provide a set of informative features, reducing the complexity of data. Selecting a set of highly informative eigenvectors using elbow method, a one-class classification algorithm is trained with the extracted features to identify fake accounts. Experimental results show that this method has improved accuracy and false-negative rate compared to the previous methods.

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.

Mohammad Reza Aref
Editor-in-Chief,
ISeCure