The ISC Int'l Journal of Information Security
ISeCure

July 2018, Volume 10, Number 2 (pp. 77–78)
http://www.isecure-journal.org

**From the Editor-in-Chief**

# Editorial

Welcome to the second issue of the tenth volume of the journal. In this issue, we publish five regular papers plus a review 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 which is an invited paper, anomaly detection approaches and systems specific for IoT is analyzed, evaluated and classified. Authors analyzed anomaly detection systems and approaches from three perspectives including engine architecture, application position and detection method. Moreover, approaches are investigated considering the associated classification.

The first impossible differential cryptanalysis of Deoxys-BC-256 is presented in the **second** paper of this issue. This model is used in Deoxys, final-round candidate of the CAESAR competition, as an internal tweakable block cipher. The paper contributions include impossible differential attacks on up to 8-round Deoxys-BC-256 in the single-key model. Their attack reaches 9 rounds in the related-key related-tweak model which has a slightly higher data complexity than the best previous results obtained by a related-key related-tweak rectangle attack presented at FSE 2018, but requires a lower memory complexity with an equal time complexity.

In the **third** paper of this issue, distributed contingency logic, a proper extension of contingency logic is proposed. Secret sharing scheme and a man in the middle attack to a weak protocol is formalized in the proposed logic. Moreover, a condition where disclose a secret may hide another one for ever is illustrated. It is proved that the proposed protocol satisfies soundness and completeness which are the main theorems of every logics. In addition, it is proven that the distributed contingency logic is more expressive than the classical contingency logic and the epistemic logic.

Determining the common information privately and efficiently between two mutually mistrusting parties have become an important issue in social networks, in recent years. Many Private Set Intersection (PSI) protocols have been introduced to address this issue. The **forth** paper of this issue, showed that Abadi et al protocols, two protocols in this context, are vulnerable to eavesdropping attack. Accordingly, they proposed a solution to secure the protocols. Moreover, the performance of both O-PSI and modified O-PSI protocols are analyzed and it is shown that the proposed scheme is comparable with the O-PSI protocol.

The **fifth** paper of this issue proposed an approach to enforce RBAC policies on encrypted data outsourced to the service provider. Authors utilize Chinese Remainder Theorem (CRT) for key management and role/permission assignment. Efficient user revocation, support of role hierarchical structure updates, availability of authorized resources for users of newly added roles, and enforcement of write access control policies as well as static separation of duties (SSD), are advantages of the proposed solution. In addition, the ciphertext size is linearly proportional to the plaintext size, regardless of the number of roles and users.

ISSN: 2008-2045 

A methodology to detect malicious URLs and the type of attacks based on multi-class classification is presented in the **sixth** paper of this issue. Authors proposes 42 new features of spam, phishing and malware URLs like URL features, URL Source features, domain name features and Short URLs features. To evaluate the proposed approach, the state of the art supervised batch and online machine learning classifiers are used in this paper. Experiments are performed on the binary and multi-class dataset using the aforementioned machine learning classifiers. Using the proposed URL features, confidence weighted learning classifier achieves the best average accuracy of 98.44% in identification of attack types using multi-class setting and highest accuracy of 99.86% in detection of malicious URLs using binary setting.

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