The ISC Int'l Journal of Information Security
ISeCure

July 2017, Volume 9, Number 2 (pp. 1–2)
http://www.isecure-journal.org

From the Editor-in-Chief

Editorial

Welcome to the second issue of the ninth 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, the computational complexity of finding a minimal basis for the Guess-and-determine (GD) attack through finding a reduction between this problem and finding the maximum uniquely restricted matching in a bipartite graph is studied. GD attack is a general cryptanalysis technique for evaluating security of symmetric cryptosystems. In particular, GD attacks have been a favorite tool for evaluating strength of many prominent stream ciphers during the past decade. The effectiveness of this attack is based on the number of unknown bits which will be guessed by the attacker to break the cryptosystem.

The **second** paper in this issue, proposes a new framework for joint encryption encoding scheme based on polar codes, namely, an efficient and secure joint secret key encryption channel coding scheme. The issue of using a new coding structure, i.e. polar codes, in Rao-Nam (RN) like schemes is addressed. Cryptanalysis methods indicate that the proposed scheme has an acceptable level of security with a relatively smaller key size in comparison with the previous works. The authors claimed that the proposed scheme is appropriate for high-speed communications.

The **third** paper of this issue, proposes a software implementation of symmetric ciphers in order to smooth their consumed powers by defining a new coding scheme and equivalent basic operations, namely AND and XOR. This method decreases data dependency between processed data and its corresponding consumed power which leads to more immunity against chosen-plaintext attack (CPA). Also, this method is practically evaluated on SIMON cipher for the purpose of studying the implementation overheads and resistance improvements against CPA.

A cipher-text only attack on permutation-only multimedia ciphers is proposed in the **forth** paper in this issue. It is shown that permutation-only multimedia ciphers can completely be broken in a chosen-plaintext scenario which models a very resourceful adversary and does not hold in many practical situations. It is shown that efficient use of redundancies of speech signal in time and frequency can pave the path for both successful cipher-text only attack and estimation of the parameters of scrambler systems. Conducted tests showed that the proposed method achieves higher accuracy and descrambles samples with higher intelligibility than previous method.

The specialists of information technology are not agreed on the definition of discriminative features characterizing the phishing websites. Therefore, there are limited number of reliable training samples in phishing detection problems. Furthermore, available training samples suffer from abnormal samples which cause classification error. To solve these problems, a supervised feature extraction method, called weighted feature line embedding

ISSN: 2008-2045 © 2017 ISC. All rights reserved.

(WFLE), is proposed in the **fifth** paper of this issue. The features extracted by WFLE improve the performance of phishing website detection particularly by using small training sets.

The application of machine learning techniques in detecting malicious web pages is investigated in the **sixth** paper of this issue.. In order to detect malicious web pages, a novel set of features including HTML, JavaScript (jQuery library) and XSS attacks is proposed and analyzed. The proposed features are evaluated on a data set that is gathered by a crawler from malicious web domains, IP, and address black lists.

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