The ISC Int'l Journal of Information Security
ISeCure

January 2018, Volume 10, Number 1 (pp. 1–2)
http://www.isecure-journal.org

From the Editor-in-Chief

Editorial

Welcome the first issue of the tenth volume of the journal. It is our great pleasure to inform our respected authors, referees, and audiences especially the Iranian information Security and cryptography community that ISeCure is currently being indexed by Emerging Sources Citation Index (ESCI) database of Web of Science (ISI). Please refer to the journal website for more information. In this issue, we publish five regular papers plus a 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, the security of a family of lightweight block ciphers, named Midori, is analyzed using impossible differential cryptanalysis. The main focus of this paper is on the security of Midori64. Therefore, to account the inadequate key schedule algorithm of Midori64; various techniques such as early-abort, memory reallocation, miss-in-the-middle, and turning are used. Two new 7-round impossible differential characteristics are proposed. Based on the new characteristics, three impossible differential attacks mounted on 10, 11, and 12 rounds on Midori64 with $2^{87.7}$, $2^{90.63}$, and $2^{90.51}$ time complexity, respectively, to retrieve the master-key.

An incentive-aware lightweight secure scheme is proposed in the **second** paper of this issue in order to achieve secure, fair, and reliable data sharing in Device-to-Device (D2D) communication. The proposed protocol is stateless and does not depend on the users contextual information. The security analysis proves that the proposed protocol resists the security attacks and meets the security requirements. This protocol is claimed to be an efficient and practical solution for secure data sharing in D2D communication.

In the **third** paper of this issue, a new semi-supervised method based on graph theory is proposed to detect and classify traffic of encrypted applications. This method utilizes clustering algorithms and labels propagation techniques. The experimental results show that the proposed method has a precise and an accurate performance in classification of encrypted traffic for the network applications. It also provides desirable results for plain un-encrypted traffic classification, especially for unbalanced streams of data.

A new finite field-based public key cryptosystem (NETRU) which is a non-commutative variant of CTRU is presented in the **forth** paper of this issue. Authors extend CTRU public key cryptosystem, that is already broken by some attacks such as linear algebra attack, over finite fields $\mathbb{Z}_p$. In the NETRU, the encryption and decryption computations are non-commutative and hence the system is secure against linear algebra attack as lattice-based attacks. NETRU is designed based on the CTRU core and exhibits high levels of security with two-sided matrix multiplication.

A host-based method for detecting individual bot-infected hosts is proposed in the **fifth** paper of this issue. The method is based on botnet life-cycle, which includes common symptoms of almost all types of botnet despite their differences. Network activities of each process running on the host are analyzed and overall security risk is evaluated. To distinguish behavioral patterns of bot process from legitimate ones, some heuristics are

ISSN: 2008-2045

proposed based on statistical features of packet sequences. The results of evaluation using real botnets and popular applications show the efficiency of the bot process detection amongst other active processes in spite of the diversity of botnets.

In the **sixth** paper of this issue, a novel decentralized online sortition protocol is proposed. In this protocol the winner of the sortition is chosen with the aid of all participants. It is claimed that the proposed protocol satisfies fairness, randomness, non-repudiation, and openness which are typical properties of a real-life sortition protocol.

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