The ISC Int'l Journal of Information Security
ISeCure

January 2016, Volume 8, Number 1 (pp. 1–2)
http://www.isecure-journal.org

From the Editor-in-Chief

Editorial

Welcome to the first issue of the eighth 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.

Our invited authors in the **first** paper of this issue review two formal approaches in verification of security protocols; model checking and theorem proving. In this paper, Scyther operational semantics is explained as a model checking approach, and some of the famous security protocols are modelled and verified using this method. Moreover, the notion "Glass Pipe" is discussed to describe the meaning of authentication, and a deduction system is provided to formally define the notion. Finally, using this deduction system, some of famous protocols are verified, and the results are compared with the results of Scyther model checker.

A lattice-based threshold secret sharing scheme (TSSS) is introduced in the **second** paper of this issue, in which secret reconstruction is based on the Babais nearest plane algorithm. In a post-quantum world, there should be no quantum threat to secret sharing schemes. A solution to this problem is the utilization of lattice-based cryptosystems to design lattice-based TSSSs. In this paper, the effect of lattice dimension is investigated on the security and correctness of the proposed scheme. It is proved that for a fixed value of lattice dimension, the proposed scheme is asymptotically correct; while a quantitative proof of security from the information theoretic viewpoint is also provided.

The **third** paper in this issue focuses on the vulnerabilities of smartphones. Code Reuse Attack (CRA) techniques are introduced as a powerful attack model that enables attackers to launch any arbitrary malicious behaviour on a victims device. Moreover, some unique aspects of ARM architecture are considered to provide a general model for code reuse attacks, called Patulous Code Reuse Attack (PCRA). The attack applies all of the available machine instructions that change Program Counter (PC), as well as indirect branches to any other register, in order to deploy the principles of ROP convention. The effectiveness of the proposed approach is demonstrated by defining five different sub-models of PCRA, explaining the algorithm of finding PCRA gadgets, introducing a useful set of gadgets, and providing a sample proof of concept exploit on Android 4.4.

Secure transmission of configuration information to FPGAs is the focus of the **forth** paper in this issue. In this paper, a "Self-authentication" methodology is presented, in which the originality of sub-components in the bitstream is authenticated in parallel with the intrinsic operation of the design. In the case of discovering violation, the normal data flow is obfuscated and the circuit would be locked. Experimental results indicate that this methodology improves the IP security against malicious updates with reasonable overheads.

The **fifth** paper in this issue, proposes an efficient method to detect unauthenticated events based on the more, the safe, the less the unsafe (MSLU) policy in wireless sensor networks (WSNs). The proposed method tends to forward event occurrence reports with more separate sources. MSLU policy comes from the network

ISSN: 2008-2045

co-coverage and redundancy. The evaluation results show that the proposed method detects unauthenticated events effectively.

In the **sixth** paper of this issue, authors propose a new method to reduce the time complexity of impossible differential attack. The method can be applied for a variety of block cipher designs, especially those with weak diffusion layer. The method has also been applied on LBlock resulting into an impossible differential attack better than known previous attacks on this lightweight block cipher.

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. Last but not least, I would like to sincerely thank Dr. Rasool Jalili for seven years of acting as the journal Editor-in-Chief.

Mohammad Reza Aref
Editor-in-Chief,
ISeCure