The ISC Int'l Journal of Information Security
ISeCure

July 2016, Volume 8, Number 2 (pp. 91–92)
http://www.isecure-journal.org

From the Editor-in-Chief

Editorial

Welcome to the second issue of the eight 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, a technique is proposed to hinder the reverse engineering against theft and trust during the chip fabrication. Special standard cells are designed, injected into the related library, and inserted in the design netlist at physical level. The duty of the cells is to encrypt net interconnections, which needs the corresponding key to be realized. As a result, the probability of extracting the right topology and therefore accurate functionality with the absence of the key is practically zero in a scrambled design. The experiments and analyses demonstrate the feasibility of automating this easily at the physical design flow.

The **second** paper in this issue focuses on providing the security and privacy of RFID-based applications. Respected authors in this paper, analyzed the privacy of a new protocol, proposed by Yu-Jehn in 2015, which is based on the Electronic Product Code Class 1 Generation 2 (EPC C1 G2) standard. It is shown that the protocol is vulnerable to secret parameter reveal attack, traceability attacks, and forward traceability attack, and also it does not provide the privacy of RFID users. Moreover, Aan improved version of the protocol is proposed which eliminates the existing weaknesses.

Security challenges of deploying low cost sensor nodes with restricted energy resources are investigated in the **third** paper of this issue. The paper proposes integration of the sensor nodes position as part of their identity for key management of heterogeneous sensor networks. The position of is used for authentication and dedicating the key to all network links. The results of evaluation show that the proposed scheme is superior in terms of scalability, security, and reliability, while utilizes thewith less memory complexity.

Multiplicative spread spectrum watermarking for images is the focus of the **forth** paper in this issue. An information bit is spread into middle-frequency Discrete Cosine Transform coefficients of each block of an image using a generated pseudo-random sequence. Despite the conventional signal modeling, both signal and noise are distributed with the Laplacian distribution. The optimum decoder for the proposed embedding method is derived based on the maximum likelihood decoding scheme. The watermarking system is analyzed in the presence of noise while analytical evaluations and several simulations are provided. The results are satisfactory in terms of performance and transparency.

The aim of the **fifth** paper in this issue is to consider uncertainty in the software security evaluation process. The Dempster-Shafer theory is used as evidence to formulate the uncertainties in input parameters and to determine their effects on the output measures . Security attacks are expressed using UML diagrams (i.e., misuse case and mal-activity diagrams), and security parameters are specified using the SecAM profile. UML/SecAM models are then transformed into attack trees, which allow quantifying the probability of security breaches. The applicability of the method has been validated through a case study on an online marketing system.

ISSN: 2008-2045

Our **sixth** paper in this issue provides an evidence to indicate that any RFID -protocol based on a few calls to a short PRNG function is vulnerable to common attacks in the context, such as secret disclosure attack. The authors present efficient attacks against two recent improved protocols published in ISeCure . Their attacks are efficient and have high success probability. They also suggested to use lightweight block ciphers instead of short PRNGs to design a secure protocol for constrainconstrained environments.

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