The ISC Int'l Journal of Information Security
ISeCure

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

From the Editor-in-Chief

Editorial

Welcome to the first 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, a certificateless signcryption (CLSC) scheme is presented, its security requirements in the standard model (without random oracles) is proved, and it is compared with some all other proposed CLSC schemes. The scheme is claimed to be robust against all existing attacks on Liu et. Al. s CLSC schemes, and to be more efficient than the all other proposed secure CLSC schemes in the standard model in the literature.

The **second** paper in this issue, investigates side channel characteristics of embedded systems and their usability in code injection attack detection. It is indicated that the architectural simulation for execution time, power usage, and temperature on benchmarks disclose meaningful and distinguishable behavior in the case of attack.

A location -based probabilistic key pre-distribution scheme is proposed in the **third** paper of this issue, which takes the location information of sensor nodes into account in order to assign keys to the nodes more efficiently. Two classes of keys (primary or secondary) are assigned to node based on its location in the network and the cell in which the node resides. Utilizing the primary key, each node forms secure links with its adjacent nodes and eventually makes a connected graph. Moreover, secondary keys are defined in order to harden the fact for the adversary to perform a successful attack in a region of the network by utilization of acquired keys from another place in the network. Compared to the existing ones, the proposed scheme has a superior scalability.

The **forth** paper in this issue proposes a new proof of continuous non-malleability of the FMNV scheme proposed by Faust et. al., while the proof results in an improved and more efficient version of this scheme. The proof also shows that one may achieve continuous non- malleability of the same security by using a leakage resilient storage scheme with (about $(k+1)(\log_2^q)$) fewer bits for the leakage bound (where k is the output size of the collision resistant hash function and q is the maximum number of tampering queries). Accordingly, the new scheme is more efficient and practical for tamper-resilient applications.

The **fifth** paper in this issue proposes a tricky aspect of code reuse techniques, called tiny code reuse attacks (Tiny-CRA) which demonstrates the ineffectiveness of the threshold based detection methods. It is shown that with bare minimum assumptions, Tiny-CRA can reduce the size of a gadget chain, so that, no distinction can be detected between normal behavior of a program and a code-reuse execution. To do so, Tiny-CRA primitives are exhibited and introduce a useful gadget set available in libc is introduced. The effectiveness of the approach is demonstrated by implementing nine different shell-codes and exploiting a real-world buffer overflow vulnerability in HT Editor 2.0.20.

ISSN: 2008-2045

An automated method for testing the implementation of access control policies in a system is proposed in the **sixth** paper in this issue. The method is able to extract test cases for evaluating the access control policies of the system under test. To generate test cases automatically, a combination of behavior model of the system and the specification of access control policies written in XACML, are used. The experimental results show that the proposed approach is able to find the failures and cover most of the code that is related to access control policies.

Finally, once again, 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