The ISC Int'l Journal of Information Security
ISeCure

January 2014, Volume 6, Number 1 (pp. 1–2)
http://www.isecure-journal.org

From the Editor-in-Chief

Editorial

I am pleased to welcome you to the first issue of the sixth volume of the journal. In this issue, we publish six 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.

The **first** paper proposes an access control middleware to overcome the complexity of deployment and enforcement of Attribute-Based Access Control (ABAC) policies in Ultra-Large-Scale systems. The middleware is data-centric and consists of a Data-Distribution-Service (DDS) layer used for loosely-coupled communication among authorization components, and an upper layer used for secure configuration and reconfiguration of authorization components. The upper layer exploits the OASIS model to permit only authorized components to get the related configuration and reconfiguration information in the proposed middleware. The notions of combining ABAC policies, combining decisions, and combining information are used in the proposed middleware to achieve multi-policy, multi-decision, and multi-information capabilities. An executable model of the proposed middleware is represented using a Colored Petri net model, which has been used to analyze the behavior of the middleware.

Zorro, as a lightweight block cipher, is the main focus of our **second** paper in this issue. Zorro has been designed to reduce the side channel vulnerability of AES-type designs as well as making them lighter through reduction of the number of S-boxes per round. This paper utilizes some properties discovered by Wang *et al.* and others to present a new differential, and a new linear attack on full-round Zorro, both of which recover the full secret key with practical complexities. The theoretical results for full-round and practical results for some reduced-round versions clearly show that the block cipher Zorro cannot be regarded as a secure block cipher in any case.

Privacy concerns in Online Social Networks (OSNs) are the main concentration of the **third** paper in this issue. In this paper, a centralized privacy-preserving framework for OSNs is presented, in which users enforce confidentiality and access control on the shared data while their connections/relationships with other users are kept anonymous in OSNs. Accordingly, users create and modify their personalized privacy settings for their shared data while employing each other's privacy settings. Evaluation of the proposed framework demonstrates its advantages compared to the most analogous recent approaches.

Security of Wireless Sensor Networks is the context of the **fourth** paper in this issue. Key management systems based on public key cryptography have many favorable characteristics such as perfect resiliency, high flexibility, and full connectivity of network; while energy consumption is a heavy burden on tight resources of nodes. This paper proposes a novel PKC-based key management system that replaces checking of digital certificates with a symmetric based protocol. The proposed protocol uses broadcast messages from the base station to authenticate the public key of nodes. To foil any malicious attack a broadcast authentication mechanism based on a modified version of μTesla has been added. Simulation results demonstrates the efficacy of the proposed method.

ISSN: 2008-2045 © 2014 ISC. All rights reserved.

In the **fifth** paper, the intention, working, bandwidth scheduling, and security problems of the Tor network are described, and a new circuit scheduling for Tor is proposed. The scheduler attempts to preserve the fairness and randomness properties through making pattern and timing analysis attacks more difficult and even impractical. The scheduler distorts timing patterns and size of packets in a random way (randomness) without imposing artificial delays or paddings (fairness). Using the scheduler, one of the most powerful related attacks is debilitated and shown that analyzing traffic patterns and size of packets are more difficult to manage.

The **sixth** paper in this issue presents a density-based clustering approach using DBSCAN, Density-Based Spatial Clustering of Applications with Noises, to classify web visitors of two real large data sets. Fourteen features, two of which are new, are proposed and used to describe and distinguish web users. The difference test (T-test) is used to reduce the dimensions and surmount one of the disadvantages of the DBSCAN algorithm. The proposed method performs better than the state of the art algorithms in terms of clustering quality and accuracy based on the authors' evaluations.

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.

Rasool Jalili

Editor-in-Chief,

ISeCure