The ISC Int'l Journal of Information Security
ISeCure

July 2013, Volume 5, Number 2 (pp. 117–118)
http://www.isecure-journal.org

From the Editor-in-Chief

Editorial

On behalf of the ISeCure editorial board, I am pleased to welcome you to the second issue of the fifth 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 in this issue proposes an access control model, named Semantic-Aware Role-Based Access Control Model (SARBAC) for Pervasive Computing Environments (PCEs). The model is context aware with partial context information, exceptions, and default policies. Furthermore, it recognizes the non-monotonicity requirement for access control in PCEs. Description Logic (DL) and Answer Set Programming (ASP) are appropriate tools for context modeling and addressing non-monotonic requirements, respectively. Therefore, $MKNF^+$ is used as a formal basis to combine the strengths of both DL and ASP in SARBAC. The expressive power of the proposed model is demonstrated through a case study.

The **second** paper in this issue presents a computational model and convergence theorem for spreading rumor in social networks. The focus of this paper is on the relation between the homogeneity of the society and rumor convergence in it. The result shows that the homogeneity of the society is a necessary condition for convergence of the spread rumor.

The **third** paper in this issue proposes a new trust model called GTrust, in which trust is considered as a collective and shared feature of all group members. In GTrust, not only different possible kinds of trust relations between individuals and groups are considered, but also the transition of trust from a group to a person and vice versa is introduced. Hence, GTrust is partially different from other trust models which only consider the trust among individuals, and is more suited to the nature of trust in emerging virtual environments.

The **fourth** paper in this issue introduces a trust calculation method, which utilizes user similarities to predict trust values without any need for direct ratings. The method is based on socio-psychological studies, and calculates user similarities based on their profile information and their shared texts via text-mining techniques. The benefits of using context in inferring trust is studied, which shows an improvement of 72 percent in the precision of the predictions. The proposed technique can be used in any direct rating mechanism to evaluate the correctness of trust values assigned by users. It increases the robustness of trust and reputation mechanisms against dishonest feedbacks.

The **fifth** paper in this issue presents a generic construction of convertible limited verifier signature (CLVS) into which the existing secure CLVS schemes fit. The construction is extended to address the unsolved question of designing an efficient construction with more than two limited verifiers. It presents two generic convertible limited multi-verifier signature (CLMVS) constructions. In the first construction, each limited verifier checks the validity of the signature; whereas in the second one, all limited verifiers have to cooperate. Based on the second generic construction, a pairing-based CLMVS scheme is presented which is secure in the standard model, and has a strong confirmation property. The scheme is employed with one limited verifier (CLVS) to design a new electronic voting protocol.

The **sixth** paper of this issue focuses on using Artificial Immune Systems (AIS) in the field of computer security, and especially in Intrusion Detection Systems (IDS). The paper extends the TLR algorithm of the danger theory, to identify the antigens based on a simple identifier. The extension is called STLR (structural TLR), and attempts to model the interaction of adaptive and innate biological immune systems, while simultaneously considering the structure of the antigens. The experimental results show that by the use of the structural aspects of an antigen, STLR leads to a considerable increase in the detection rate and accuracy.

I would like to sincerely thank all the authors for their high-quality 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