The ISC Int'l Journal of Information Security
ISeCure

July 2011, Volume 3, Number 2 (p. 67)
http://www.isecure-journal.org

From the Editor-in-Chief

Editorial

Welcome to the second issue of the third volume of ISeCure. From this issue on, ISeCure enjoys several new advisory board members, whom I wish to first acknowledge: Respected professors (in alphabetical order) Wan Fokkink, Keith Martin, Carles Padro, and Philip Rogaway. They are among the leaders of security research over the world, and I wish ISeCure will promote its academic excellence with their advice.

In this issue, we published four papers. Our special thanks to Professor Philip Rogaway who submitted the manuscript of his invited talk in the ISCISC'11 conference as an invited paper. In the paper, Professor Rogaway puts together and exemplifies some cryptographic definitions. The approach is focused on two themes: First, the security definitions are man-made, and therefore not carved into the stone. Second, the definitions are too important to be taken lightly. It is claimed that the approach has the potential of being applied to other fields.

The second paper proposes an unsupervised method in attack-plan recognition as an alert correlation system. The system consists of an Attack Scenario Extraction Algorithm (ASEA), and a Hidden Markov Model (HMM)-based correlation method of intrusion alerts. ASEA mines the stream of alerts for attack scenarios and combines prior knowledge as well as statistical relationships. The HMM is used to predict the next attack class, a process known as plan recognition. This component operates independently of network topology, system vulnerabilities, and system configurations, while it is more robust against over-fitting. The proposed system was applied to a well-known related dataset and the results are satisfactory.

The third paper focuses on access control requirements of new computational environments such as web services. The paper proposes the Constrained Policy Graph (CPG) as a new model to specify Access Control Policies (ACPs) and their composition, as well as verification of conflict or incompatibility among ACPs. The way of using the CPG to model and verify the composition of web service ACPs is shown. The paper also illustrates the application of CPG for modeling policies in BPEL processes.

The fourth paper proposes a distributed scheme for database outsourcing. In this scheme, shares of data are stored on different servers, and indexes are separated from data. In order to distribute data among different servers, Shamir's secret sharing scheme is used. A B^+-tree index is also utilized on the order-preserved encrypted values for each searchable attribute. The proposed approach is secure against different database attacks, yet it supports exact match, range, aggregation, and pattern-matching queries efficiently. Simulation results show the prominence of the approach.

Rasool Jalili
Editor-in-Chief,
ISeCure

ISSN: 2008-2045