Journal of Computer Security 19 (2011) 365
DOI 10.3233/JCS-2011-0425
IOS Press

Preface

This issue of the *Journal of Computer Security* comprises of three papers presented at the 22nd IFIP 11.3 Working Group Conference on Data and Application Security, which was held in London, UK, in July 2008. The primary objective of this annual conference is to disseminate original research results and the development efforts in the area of data and application security and privacy, and to provide a platform for researchers and practitioners to share their knowledge and experience.

The three papers in this special issue were invited submissions that were substantially extended for journal publication and were reviewed through a normal review process of the *Journal of Computer Security*.

These three papers address different aspects of data protection: efficient search on encrypted data, access control for spatio-temporal data, and preventing the leakage of private information when performing a combined analysis of data from multiple sources.

The first paper, "Shared and searchable encrypted data for untrusted servers", by Changyu Dong, Giovanni Russello and Naranker Dulay, proposes a novel technique for keyword searches over outsourced encrypted data. The proposed solution is based on the combined use of proxy-encryption and keyword search, that allows each user to keep one secret key only. This makes key revocation operations highly efficient since it does not require re-encryption. Unlike prior approaches, this proposed model supports both read and write operations of the outsourced data.

The second paper, "On the formalization and analysis of a spatio-temporal role-based access control model", by Manachai Toahchoodee and Indrakshi Ray, proposes a new spatiotemporal role-based access control model for use in mobile applications. It supports the notions of spatial temporal inheritance, Separation of Duties and delegation of roles, permissions and delegation chain. It employs color Petri nets to perform automated analysis in order to verify the consistency and correctness of the proposed model.

The third paper, "Secure construction and publication of contingency tables from distributed data", by Xiaoyun He, Haibing Lu, Jaideep Vaidya and Nabil Adam, presents a set of techniques for privacy preserving construction of contingency tables over data collected from multiple sources. Contingency tables are often used to study the relationship between two or more related variables. When there are multiple sources of the original data, these contingency tables must be constructed in a privacy preserving manner to avoid any leakage of private information. The paper presents approaches for both horizontally and vertically partitioned data.

Vijay Atluri