Journal of Computer Security 19 (2011) 485–486
DOI 10.3233/JCS-2011-0427
IOS Press

Introduction

This issue of the *Journal of Computer Security* comprises of four papers presented at the 23rd IFIP Working Group 11.3 Working Conference on Data and Applications Security, which was held in Montreal, Canada, in July 2009. The primary objective of this annual conference is to disseminate original research results, development efforts and innovative ideas in the area of data and applications security, and to provide a platform for researchers and practitioners to share their knowledge and experience.

The four papers in this Special Issue were invited submissions that were substantially extended for journal publication and subjected to the customary review process of the *Journal of Computer Security*.

These four papers address different levels of data protection: enabling inference proof view updates and view refreshes, enabling efficient protection of privacy in outsourced databases, presenting a semantics-based automated reasoning approach for detecting security threats, and enabling efficient enforcement of spatiotemporal access control when the precise locations cannot be stated.

The first paper, "Inference-proof view update transactions with forwarded refreshments" by Joachim Biskup, Christian Gogolin, Jens Seiler and Torben Weibert, examines the problem of making view updates inference proof. It provides a formal specification of the goal of inference-proofness in terms of indistinguishability, and extends the inference control method of controlled query evaluation with lying (which only applies to static information systems) to correctly handle view updates and view refreshes. The key idea is to only allow updates that do not cause consistency or confidentiality problems. The update is denied if it causes a consistency problem but the denial does not lead to inference. However, when the update can create consistency problems and a denial would lead to confidentiality problems, the server lies and notifies the client that the update is successful, without actually carrying it out. The server may also lie and claim that the update is already compatible with the database, if that is necessary to guarantee confidentiality. The paper also develops protocols that can handle view update transactions.

The second paper, "Selective data outsourcing for enforcing privacy" by Valentina Ciriani, Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi and Pierangela Samarati, presents an approach for preserving privacy requirements in an outsourced database. The approach taken in the paper is based on fragmentation of tables/relations in the database. However, unlike existing approaches, the paper does not require encryption of sensitive attributes in the different fragments to prevent association attacks. Rather, the paper relies on the data owner to store a fragment of the relation locally, ensuring that at least one of the attribute in the confidentiality constraint is stored locally, thus breaking the association with

other attributes in the constraints. Since finding a minimal fragment is an NP-hard problem, the paper models this as a constrained hyper-graph 2-coloring problem and uses heuristic approaches to solve the problem.

The third paper, "Management of security policy configuration using a Semantic Threat Graph approach" by Simon Foley and William Fitzgerald, presents a semantics-based approach for testing whether the security configuration of a network has adequate counter measures to guard against known threats and vulnerability exploits. Threat graphs extend the traditional threat tree with explicit categorization of system components and modeling of the semantic relationships amongst them. Now, ontology based reasoning can be used for automatic security analysis. A case study based on Network Access Controls demonstrates how threats can be analysed and how automated configuration recommendations can be made based on catalogues of countermeasures drawn from best-practice standards.

The fourth paper, "Efficiently enforcing spatiotemporal access control under uncertain location information" by Heechang Shin, Vijayalakshmi Atluri and June-suh Cho, considers the problem of access control can be efficiently enforced in spatiotemporal context when the location estimates are uncertain. The proposed solution grants an access request efficiently if the confidence level of the location predicate exceeds the predefined uncertainty threshold level specified in the policy. The paper proposes strategies to compute the upper bound and lower bound values on a region that can be used to filter out moving objects, such that these moving objects will be discarded upon evaluating location predicates, thus ensuring that the entire moving object database does not have to be evaluated.

Jaideep Vaidya
Ehud Gudes