Journal of Computer Security 5 (1997) 269–270
IOS Press

# Guest editors' preface

This issue of the *Journal of Computer Security* contains three papers presented at the 1996 IFIP 11.3 Working Conference on Database Security, which was held in Como, Italy, July 1996. This yearly Working Conference, at its tenth event, has the purpose of presenting and disseminating original results in database security research and development and establishing a framework for researchers and practitioners to discuss their experience.

The papers contained in this special issue were invited submissions that were revised for Journal publication and subjected to the normal review process of the Journal.

The three papers touch different aspects of database security but have a common theme: the specification and enforcement of authorizations. This theme is studied in the context of federated systems in the first paper, of workflow systems in the second paper, and of object-oriented systems in the third paper. All these three contexts represent recent and active areas in which there are many security problems to be investigated.

In the first paper "Automated derivation of global authorizations for database federations", Silvana Castano, Sabrina De Capitani di Vimercati, and Maria Grazia Fugini present an approach to designing and enforcing authorizations in federated database systems. The approach derives authorizations at the federation level on the basis of authorizations defined at the different component systems. The proposed process, based on the concepts of similarity and abstraction, produces authorizations which allow federated users to execute on remote objects the same accesses they can exercise on "similar" local objects. This derivation can be enforced at the time the federated schema is designed or a posteriori.

In the second paper "Enforcing mandatory and discretionary security in workflow management systems", Vijayalakshmi Atluri and Wei-Kuang Huang address the problem of specifying and enforcing security constraints in workflow management systems. The paper addresses both multilevel mandatory and discretionary authorization-based security constraints. Mandatory constraints are enforced by assigning security labels to each task. The proposed approach detects task dependencies which cannot be enforced because of security constraints. Discretionary access control is based on authorizations whose assignment and revocation are synchronized with the workflow so that a subject can gain access to objects only during execution of tasks. Both mandatory and discretionary policies are modeled by means of Petri nets.

Steve A. Demurjian and T.C. Ting present an approach to specifying and enforcing authorizations in object-oriented systems in the paper "Towards a definitive paradigm for security in object-oriented systems and applications". The approach, strongly based on the use of encapsulation, embeds security constraints in application code. The authors address the problem of generating application code enforcing security constraints starting from specified authorizations. Authorizations are stated in terms of user roles and of profiles describing the elements of the data model. The paper illustrates the different design and analysis phases necessary to state security specifications and produce the application code enforcing them.

Pierangela Samarati and Ravi Sandhu