Editorial ESORICS 2007

This issue of TISSEC consists of three articles that elaborate research results originally contributed to the *12th European Symposium on Research in Computer Security (ESORICS'07)* held in Dresden, Germany, September 24–26, 2007.

The conference series of ESORICS has become *the* European research event in computer security. The symposium started in 1990 and has been organized on alternate years in different European countries. Since 2002, it has taken place annually. The contributions to ESORICS present theory, mechanisms, applications, or practical experience on all traditional or emerging topics relevant for security in computing systems.

The three articles of this special issue have been selected from 39 papers presented during the symposium out of 164 submissions. The articles exemplarily demonstrate the scope of ESORICS, dealing with an advanced formal model for state-dependent access control, sophisticated language-based security for information-flow control, and security and privacy in databases employing cryptography. A common theme of the articles is to enable programmers and system administrators to reliably control the flow of information in complex computing environments.

Becker and Nanz consider state-modifying authorization policies where actually granted access requests can have effects on the current state of the access control system. They show how to efficiently organize state updates in a well-structured architecture, and they provide both thorough semantics based on Transaction Logic and a sound and complete proof system for analyzing the actual achievements of state-modifying authorization policies.

Barthe, Rezk, Russo, and Sabelfeld enhance language-based information-flow security by inspecting the subtle impact of the concept of multithreading for low-level programs as used, for example, in mobile code scenarios. In particular, they deal with the control of the timing behavior of an execution as exhibited by a security-aware scheduler. They achieve this goal by presenting a security-preserving compilation to be employed as part of the overall approach to proof carrying code.

Ciriani, De Capitani di Vimercati, Foresti, Jajodia, Paraboschi, and Samarati contribute to security on the application level. More specifically, for enforcing confidentiality constraints in the context of data outsourcing, they study how to break sensitive associations among composed data by fragmentation and to encrypt the resulting fragments such that processing of the fragmented and encrypted data still remains sufficiently efficient.

We would like to thank all the authors for following our invitation to contribute to this special issue and all the reviewers for their insightful and helpful comments. We are also grateful to Michael Reiter, former Editor-in-Chief,

for his support in making this volume possible, and to Gene Tsudik, present Editor-in-Chief, for his help in completing it.

JOACHIM BISKUP
Technische Universitaet Dortmund
JAVIER LOPEZ
Universidad de Malaga