

## Guest editor's preface

This Special Issue of the *Journal of Computer Security* comprises of three papers presented at the 13th IFIP 11.3 Working group conference on Database Security, which was held in Seattle, Washington, in July 1999. The primary objective of this annual conference is to disseminate original research results and development efforts in the area of database security, 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 subjected to the customary review process of the *Journal of Computer Security*.

These three papers address different levels of data protection: access control to prevent access by unauthorized users, preventing leakage of sensitive information through legitimate access to non-sensitive data via inference, and detection of malicious activity by either authorized or unauthorized users.

The first paper, "Intrusion confinement by isolation in information systems" by Peng Liu, Sushil Jajodia and Catherine D. McCollum, presents an approach to limit the damage caused by intrusions and minimize detection latency. The key idea is to isolate the suspicious users and allow them to access a copy of the database, instead of the main database. When a suspicious user turns out to be malicious, the corresponding copy is discarded. On the other hand, if the suspicious user turns out to be innocent, the corresponding copy is merged into the main database. The merging techniques are adopted from the replicated database literature to resolve mutual inconsistency.

The second paper, "Using sample size to limit exposure to data mining" by Chris Clifton shows how lower bounds from pattern recognition theory can be used to determine sample sizes where data mining tools cannot obtain reliable results to infer sensitive data from non-sensitive data. This knowledge can thus be used to state and enforce clear limits on what can be learned from systematic data mining.

The third paper, "Temporal authorization bases: From specification to integration" by Elisa Bertino, Piero Andrea Bonatti, Elena Ferrari and Maria Luisa Sapino presents a flexible authorization mechanism in which authorizations can be specified with temporal validity. Moreover, it allows subjects and objects to have hierarchical relationships where authorizations can be inherited from general to specific subjects and objects. It provides a means to deal with inconsistencies that arise due to the specification of both positive and negative authorizations that are valid during cer-

tain time intervals when coupled with inheritance. It also presents approaches for integrating authorizations as well as multiple subject/object hierarchies in heterogeneous distributed environments.

Vijay Atluri and John Hale