Journal of Computer Security 5 (1997) 1–2
IOS Press

Guest editors' preface

The four papers included in this special issue of the *Journal of Computer Security* are extended versions of papers originally presented at the 1996 European Symposium on Research in Computer Security (ESORICS '96). The ESORICS Symposia have been held every two years since 1990 in different European countries. The last edition was held in Rome, Italy, on September 1996. This symposium is the main European forum for security research.

The selected papers have been subjected to the normal review process of the journal. The first two deal with theoretical foundations of security. The other two deal with two areas of great topical interest: mobile computing systems and electronic commerce.

The paper "Merging heterogeneous security orderings" by P.A. Bonatti et al. deals with the problem of integrating multiple heterogeneous legacy databases when they do not share the same security ordering. This assumption is often true as the databases may have been developed independently by different agencies at different points in time. The authors present techniques by which multiple security orderings can be merged into a single unified ordering that preserves the security relationships between orderings. A logic programming based approach and a graph-theoretic one are proposed.

In the paper "Threat scenarios as a means to formally develop secure systems", V. Lotz introduces a new method for the formal development of secure systems that closely corresponds to the way secure systems are developed in practice. It is based on "FOCUS", a general-purpose approach to the design and verification of distributed, interactive systems. The method utilizes threat scenarios resulting from threat identification and risk analysis, and models those attacks that are of importance in the system's security. The author shows the usefulness of the proposed approach by developing an authentication server component, thereby analysing two simple authentication protocols.

In the paper "Digital payment systems with passive anonymity-revoking trustees", J. Camenisch et al. deal with the protection of user's anonymity in electronic payment systems. Because anonymity could be in conflict with law enforcement, for instance in cases of blackmailing or money laundering, it has been proposed to design systems in which a trusted third party (a trustee) or a set of trustees can selectively revoke the anonymity of the participants involved in a suspicious transaction. In the paper the authors present an anonymous digital payment system such that the trustees are neither involved in payment transactions nor in the opening of a customer new account, but only in case of a justified suspicion.

In the paper "Server-supported signatures", N. Asokan et al. present a novel non-repudiation technique, called *server-supported signatures*, S^3. The authors'

main motivation arises from the typical mobile computing environments where the mobile entities have considerably less computing power than do static entities. S^3 is based on one-way hash functions and traditional digital signatures. However, for ordinary users, S^3 limits the use of asymmetric cryptographic techniques to signature verification. All signature generations are done by third parties, called signature servers. S^3 uses only verifiable third parties (i.e., third parties whose cheating can be proved to an arbitrator).

The guest editors would like to acknowledge the efforts of the referees who have critically reviewed the manuscripts and provided the authors with useful comments and advice for improving the papers. They would also like to thank the authors for extending the initial versions of their papers and going through the revision cycles according to the referees' comments. Finally, the guest editors are grateful to the editors in chief of the journal for giving the opportunity of organizing this special issue.

Elisa Bertino, Emilio Montolivo and Helmut Kurth