Journal of Computer Security 4 (1996) 1–2
IOS Press

Guest-editors' preface

This issue of the *Journal of Computer Security* contains five papers, whose preliminary versions were presented at the 1994 European Symposium on Research in Computer Security (ESORICS'94), held in Brighton, UK, November, 1994. The ESORICS symposia have been held every two years since 1990 and represent the main European forum for security research.

The papers in this special issue are invited submissions that were revised for journal publication and subjected to the normal review process of the journal. We believe that the selected papers cover various aspects of computer security and, therefore, they are highly complementary to each other.

Bruno d'Ausbourg and Christel Calas in the paper "Controlling causal dependencies over a secure network" address security issues in a LAN-based environment. The goal of their work is to design a practical multilevel system offering full security. The approach they propose is based on a control of causal dependencies, concerning basic events in the distributed system, that exhaustively enforces all information flow. Formal definitions and security conditions are presented in the paper, providing a formal basis for the subsequent discussion. An architecture is then proposed in the paper and a secure-medium access control protocol is defined. The paper also reports results on the protocol performance, by discussing three different cases, and presents an example of use of this protocol for a secure distributed file system.

One classical problem of some security requirements such as information flow controls is the difficulty of modelling them as abstract specifications that can be preserved through refinements. In "Non-interference through determinism", A.W. Roscoe, J.C.P. Woodcock and L. Wulf propose a solution where the abstract specifications are first translated in a process-algebraic model (CSP) and then expanded to include security specifications. An example is given where the first abstract specifications are written in Z.

In "A calculus for security bootstrapping in distributed system", Ueli Maurer and Pierre Schmid propose an attractive and simple model to describe the production of security properties in communications from basic initial properties. They build a calculus allowing one to analyse and compare cryptographic protocols.

Azad Jiwa et al. pick up on an idea of Rabin to show how a central service delivering certified nonces can simplify authentication dialogues. The central service has to be trusted to behave properly (e.g., by not repeating itself) and not to publish its private key, but that is a modest price for the simplicity generated.

Ralf Hauser and colleagues address a matter which receives rather little attention in the literature – how to change keys or passwords in a secure and robust way. They propose a novel technique and argue convincingy for its correctness.

As a concluding remark, we would like to thank the authors, for extending the initial versions of their papers and going through several revision cycles according to the referees' comments. Special thanks are due to the anonymous referees for their invaluable help in assessing both contents and presentation of each paper. Finally, we would like to thank the editors in chief of the journal for giving the opportunity of organizing this special issue.

Elisa Bertino, Gérard Eizenberg and Roger M. Needham