Journal of Computer Security 7 (1999) 87
IOS Press

Guest editor's preface

This issue of the *Journal of Computer Security* contains four papers selected from the 11th IEEE Computer Security Foundations Workshop (CSFW11), held in Rockport, Massachusetts, USA, 10–12 June 1998. The objective of the workshop is to bring together researchers interested in the foundations of computer security to discuss and explore issues in access-control, cryptographic protocols, database security, integrity and availability, information flow and formal methods for security. The papers in this issue were extended and revised for journal publication and subjected to the normal review process of the *Journal of Computer Security*.

The paper by Gavin Lowe titled "Towards a completeness result for model checking of security protocols" states a fundamental and useful result about the analysis of security protocols. Lowe proves that under certain sufficient conditions, if there are no attacks on a security protocol running on a small model of a system then no attack is possible on any large system running the protocol.

The paper "Proving security protocols with model checkers by data independence techniques" by A.W. Roscoe and P.J. Broadfoot considers the problem of state-space explosion when model checking security protocols that use unbounded resources such as keys and nonces. The authors describe data independence methods can be used to model-check such protocols.

In the paper "Probabilistic noninterference in a concurrent language", Dennis Volpano and Geoffrey Smith develop a type system that can be used to verify that a program is free of probabilistic timing channels. Such verification has useful applications, for example, in a mobile-code framework where hosts are trusted, a well-typed (mobile-code) program does not leak any sensitive information while running on a trusted host.

The paper "Strand spaces: proving security protocols correct" by Javier Thayer Fábrega, Jonathan Herzog and Joshua Guttman describes a new technique for analyzing and verifying security protocols. The technique is applied to two well known security protocols and provides new insights into security protocol analysis.

I would like to thank the authors for revising the initial versions of their papers and submitting them for this special issue. Thanks also to the anonymous reviewers and to the editors in chief for providing the opportunity to publish this special issue.

Simon N. Foley
Program Chair, CSFW11