Journal of Computer Security 6 (1998) 1
IOS Press

Guest editors' preface

This issue of the *Journal of Computer Security* contains four papers selected from the 10th IEEE Computer Security Foundations Workshop (CSFW10), held in Rockport, Massachusetts, USA, 10–12 June 1997. 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*.

In "On SDSI's linked local name spaces", Abadi proposes a logic and semantics to describe local name spaces in SDSI (Rivest and Lampson's Simple Distributed System Infrastructure). By providing rules that map compound names to their meanings, the logic contributes to our understanding of local naming and provides a basis for a formal foundation for SDSI and related systems such as Simple Public Key Infrastructure (SPKI).

The paper "Provable security for cryptographic protocols – exact analysis and engineering applications" by Gray, Ip and Lui, shows, in a provable security style, how the security of a protocol can be related to the security of its underlying cryptographic primitives. The authors use this relationship to replace loose asymptotic arguments by concrete recommendations on the bit-lengths of cryptographic keys and how often principles should re-key.

The detailed specification of a security protocol using the CSP process algebra can be tedious and error-prone. In "Casper: A compiler for the analysis of security protocols", Lowe describes a compiler that translates abstract security protocol specifications to CSP. This CSP can be, in turn, analysed for attacks using the FDR model checker. The protocol notation proposed is similar to the convention used to describe security protocols in publications and is easy to use.

In "The inductive approach to verifying cryptographic protocols", Paulson presents an original formal approach to the mechanical verification of cryptographic protocols. Protocols are specified inductively as sets of traces and the Isabelle/HOL theorem proving environment is used to guide and check proofs of relevant security properties. The technique supports reasoning about protocols with infinite state, multiple and concurrent protocol runs and compromised keys.

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, CSFW10