Journal of Computer Security 9 (2001) 1–2
IOS Press

Guest editor's preface

This issue of the *Journal of Computer Security* contains five papers selected from the 12th IEEE Computer Security Foundations Workshop (CSFW12), held in Mordano, Italy, 28–30 June 1999. Though it has grown slightly over the years to around 50 participants, CSFW has kept its general character: a small group of researchers meets in a relatively isolated spot to exchange ideas at the foundations of security. The enclosed papers are based upon the recommendation of the program committee. The authors revised their original papers and the results were reviewed according to the usual standards for *JCS*. (Editor-in-Chief Jon Millen graciously agreed to take over editorial duties for me where there was potential for conflict of interest.)

Two main areas of interest for CSFW over the years have been the formal analysis of security protocols and the mathematical characterization of information flow security. These continued to be well represented. Two of the papers were on the formal analysis of security protocols. "Fault-preserving simplifying transformations for security protocols" by Hui and Lowe describes techniques that allow the simplification of an actual protocol specification without removing any security faults in the process. This oddly desirable result is useful for analyzing the large protocols encountered in practice today, which are often too unwieldy to be easily amenable to formal analysis. The techniques in this paper allow the transformation of protocols into something more manageable while preserving the correctness of the analysis, and these techniques are illustrated in application to a large commercial protocol. In "Athena: a novel approach to efficient automatic security protocol analysis" Song, Berezin, and Perrig describe an automated verification tool, Athena, that is based on the Strand Space Model. This model was described in the special issue of *JCS* from CSFW11 and is proving to be very influential on the field as a whole. In this paper, Song et al. expand that model and design an associated logic and tool that also combines in techniques of theorem proving and model checking. In the area of of information flow security, Ryan and Schneider present "Process algebra and noninterference", a careful study of non-interference properties from the standpoint of process algebra. A central thesis of the paper is that much of the dispute over different formulations of noninterference can be fruitfully viewed as a dispute over different formulations of process equivalence. Ryan and Schneider show how one can gain insight into the nature of noninterference by recasting its various formulations within the framework of the process algebra CSP.

In "A logic for SDSI's linked local name spaces", Halpern and van der Meyden present a logic for local names in Rivest and Lampson's Simple Distributed System Infrastructure (SDSI). SDSI's name spaces have been considered logically before, notably by Abadi; however, the logic and semantics in this paper more directly respects SDSI's name resolution algorithm. Also, Abadi speculated that his logic was

incomplete; whereas Halpern and van der Meyden prove both soundness and completeness for their axiomatization.

An area of security that has been very much in the news but not had much foundational analysis is denial of service. In “A cost-based framework for analysis of denial of service in networks”, Meadows develops a model of denial of service specifically in the context of authentication. While authentication protocols serve to protect against unauthorized access and thus limit denial of service, the act of authenticating is resource intensive and can thus itself be used as a means to deny service. Meadows examines denial of service by constructing a framework for weighing the cost to the defender against the cost to an attacker.

I would like to thank the program committee of CSFW12 for recommending these papers and the anonymous reviewers for their reviews. Thanks to the Editors-in-Chief for the opportunity to produce this special issue. Finally, thanks especially to the authors for preparing the revisions of their original papers.

Paul F. Syverson
Program Chair, CSFW12