Journal of Computer Security 11 (2003) 449–450
IOS Press

Guest editor's preface

This issue of the *Journal of Computer Security* contains five papers selected from the 14th Computer Security Foundations Workshop (CSFW14) held at Keltic Lodge, Nova Scotia, 11–13 June 2001. 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, intrusion detection, 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 "Authenticity by typing for security protocols", Gordon and Jeffrey propose a novel method of using type-checking for verifying authenticity properties. This approach builds on the spi-calculus, introducing correspondence assertions into the language to express authenticity properties on authentication protocols, and then proposing a type and effect system which can be used to verify them statically.

The paper "Logical relations for encryption" by Sumii and Pierce proposes an extension of the λ-calculus with cryptographic primitives to describe security protocols. The properties required of such protocols are expressed in terms of behavioural equivalences, so that programs which differ only in terms of their secrets should be equivalent. The authors propose a proof technique based on logical relations for establishing equivalences, and illustrate their approach with the Needham–Schroeder public-key protocol.

In "Some attacks upon authenticated group key agreement protocols", Pereira and Quisquater are concerned with the Cliques suite of protocols, which extend Diffie-Hellman key-exchange to a group setting. They formulate the security properties required of such protocols, and identify different ways in which properties in the two-party setting might extend to the multi-party situation. The authors propose a model for analysing these protocols, which considers the problem of whether an attacker can obtain a secret in terms of whether a linear system of equations is consistent, which is straightforward to check. The paper shows how consistency of the equations can identify attacks, and uses the method to identify a number of previously unpublished attacks on the Cliques protocols.

Halpern and van der Meyden give semantics to the public key infrastructure standard SPKI in their paper "A logical reconstruction of SPKI". They extend their earlier work on a Logic of Local Name Containment to a (monotonic) logic which deals with the SPKI features of certificate expiry and revocation. They examine the standard SPKI reduction rules in the light of this logic. The paper shows that the rules are complete with respect to concrete certificates – whether a particular principal is permitted to perform particular actions – but that additional rules are required for more general reasoning about certificates.

In “A unifying approach to the security of distributed and multi-threaded programs”, Mantel and Sabelfeld are concerned with the problem of establishing secure information flow in the context of multi-threaded programs, and in establishing a connection between language-based security and noninterference-like properties. The paper uses a multi-threaded while language and a strong timing-sensitive security specification which implies security in the presence of any particular scheduler. A translation is given for programs into state-event systems so that they can be considered against noninterference properties. The paper establishes a very strong relationship between security in the two settings: the translation is sound and complete, meaning that a program is secure in the language sense if and only if its translation is secure as a state-event system. Since the language-based approach allows global security of a system to be derived from the security of each individual thread, this enables compositional verification of noninterference system properties.

Finally, “A compositional logic for protocol correctness” by Durgin, Mitchell and Pavlovic presents a logic, built around a process language, for reasoning about security protocols. Assertions are attached to protocol actions: they describe what must hold in any run containing the associated action, against any attack, enabling reasoning about all possible protocol runs. The logic provides axioms and inference rules for reasoning about assertions. Unlike BAN-style logics which also associate assertions with protocol actions, the semantics of this logic is based around traces. The notion of *cords* is introduced for describing traces. Cords are based on strands, but crucially give an explicit account of variable binding and substitution. The overall result of this paper is a compositional logic enabling natural proofs of protocol correctness in terms of the guarantees available at each stage of a protocol's execution.

I would like to thank the authors for revising the initial versions of their papers and submitting them for inclusion in this special issue. I am also grateful to the anonymous reviewers and to the Editors-in-Chief for providing the opportunity to publish this special issue.

Steve Schneider
Program Chair, CSFW14