Journal of Computer Security 12 (2004) 313–315
IOS Press

Guest editor's preface

This issue of the *Journal of Computer Security* contains nine papers selected from the 15th Computer Security Foundations Workshop (CSFW15) held on 24–26 June 2002, in Canada at the Keltic Lodge, in Nova Scotia. 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 15th workshop attracted a record number of submissions, resulting in a very high quality programme, and this is reflected in the unusually high number of papers selected for this special issue. These papers were extended and revised for journal publication, and subjected to the normal review process of the *Journal of Computer Security*.

In "Model checking SPKI/SDSI", Jha and Reps establish a connection between the public key infrastructure standard SPKI/SDSI and pushdown systems. In particular, they show how a set of SPKI/SDSI name and authorization certificates can be used to define a pushdown system, in effect providing a pushdown system semantics for SPKI/SDSI. This enables a wide variety of authorization problems on certificate sets to be solved efficiently using established model checking techniques on pushdown systems.

In his paper "Probabilistic analysis of an anonymity system", Shmatikov makes use of the probabilistic model checker PRISM to analyse the Crowds system for anonymous web browsing. He demonstrates how to model the peer-to-peer group communication system, which is based on random message routing, using a discrete-time Markov chain. The chain can then be analysed with respect to particular anonymity requirements expressed in Probabilistic CTL. The paper reports two subtle ways in which the level of anonymity can degrade, both of which were exposed by the process of model checking. One of these issues was previously unknown.

In "Embedding agents within the intruder to detect parallel attacks", Broadfoot and Roscoe build on previous work concerned with the incorporation of data independence techniques into the CSP approach to model checking cryptographic protocols. This paper is concerned with modeling systems in which agents can execute arbitrarily many concurrent protocol runs in such a way that the model can be verified by means of a finite FDR check. The authors show how an agent modeled as an oracle 'internally' within the intruder naturally describes multiple concurrent runs for that agent. They identify a 'just-in-time' property on values generated by protocol agents, which provides a bound on the intruder without losing any attacks, and thus establishing conditions that enable FDR analysis.

Guttman's paper "Authentication tests and disjoint encryption: a design method for security protocols" proposes a protocol design method built on the author's previous work on authentication tests. That work showed how agents could make use of encryption together with randomly generated values such as nonces to achieve authentication guarantees. The current paper shows how the design of a protocol can be based around the authentication tests appropriate to ensure the protocol's desired properties. The approach is illustrated with the design of a protocol ATSPECT for e-commerce transactions. The protocol is correct by construction, by ensuring that an authentication test is incorporated for each security goal, and that the authentication tests do not interfere.

"Types and effects for asymmetric cryptographic protocols" by Gordon and Jeffrey extends their earlier work on typing for authenticity to the case of asymmetric cryptography. The main contribution of the paper is a new type and effect system appropriate for asymmetric cryptographic protocols. In particular, it deals with the additional phenomena that arise in asymmetric cryptography (where trusted items might be public or secret) in contrast to symmetric cryptography. Separation of trust and secrecy is dealt with by separating the notion of public message type from that of 'tainted' message type. The more dynamic notion of trust is dealt with through 'trust effects', which track trust information for a data item through an execution. Finally, the wider range of nonce handshake styles (which are similar to Guttman's authentication tests) are supported via a corresponding range of challenge/response types. The result is a type and effect system which handles the way asymmetric cryptography is used in authentication protocols.

In "Type-based cryptographic operations", Duggan shows how cryptographic types can be used to express secrecy and integrity guarantees for a network programming language. The types keep track of values encrypted and signed using keys associated with principals. The paper provides syntax and types to ensure that cryptography is used correctly in trusted code, eliminating the need for some run-time cryptographic checks, and resulting in more efficient programs.

The paper "A formal model of rational exchange and its application to the analysis of Syverson's protocol" by Buttyán, Hubaux and Čapkun, uses game theory to provide a model of exchange protocols as sets of strategies for protocol parties. The paper shows how properties of exchange protocols, such as rational exchange and fairness, can be formally defined and analysed within this model. The approach is illustrated with a protocol proposed by Syverson, which is shown to be rational in the presence of a reliable communication medium, but not otherwise.

In "Polynomial liveness", Backes, Pfitzmann, Waidner and Steiner consider the problem of establishing liveness properties of cryptographic protocols. In order to allow analysis with finite protocol runs, they introduce the notions of polynomial fairness, which requires that messages will be scheduled after a polynomial number of steps; and polynomial liveness, which requires that something good will happen after a polynomial number of steps. This avoids the traditional need to characterise liveness and fairness properties on infinite runs. They identify circumstances under

which their liveness properties are preserved by simulatability, and hence when they hold for protocol implementations.

Finally, Lowe's paper "Defining information flow quantity" is concerned with extending notions of information flow to allow quantification of the information passed, and thus give a formal definition of the capacity of covert channels. The novelty of this approach is in its pessimistic, rather than probabilistic, treatment of nondeterminism. The paper uses the discrete-time model of CSP, and defines channel capacity in terms of the maximum rate of information that could be obtained by a Low level testing process about the behaviour of some high-level user.

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, CSFW15