Journal of Computer Security 22 (2014) 201–202
DOI 10.3233/JCS-140497
IOS Press

Preface

Foundational aspects of security

This Special Issue of the *Journal of Computer Security* focuses on foundational aspects of security, which in recent years have helped change much of the way we think about and approach system security. The volume features three outstanding papers, each devoted to one of the pillars of security theory: logic, model checking and types.

- Joshua Guttman in "Establishing and preserving protocol security goals" proposes a model-theoretic approach to the verification of security properties, where the models are executions, and the security goals are implications over the geometric fragment of predicate logic. This methodology also leads to a new reading of protocol refinement and transformation, and offers the possibility of reasoning about these concepts in semantic terms.
- "Effective verification of confidentiality for multi-threaded programs", by Tri Ngo, Mariëlle Stoelinga and Marieke Huisman, focuses on the verification of confidentiality properties in concurrent systems via model checking. More specifically, it studies observational determinism (a property that ensures secure information flow) in multi-threaded programs, under a given scheduler. The latter guarantees robustness with respect to refinement attacks. Moreover, it proposes a counter-example generation technique which allows to extract an actual attack when the verification of a program fails.
- Finally, in "Union, intersection and refinement types and reasoning about type disjointness for secure protocol implementations", Michael Backes, Cătălin Hriţcu and Matteo Maffei present a new type system for verifying the security of cryptographic protocol implementations, where the main novelty is the capability to check statically the disjointness of types. The increased expressivity enables the analysis of protocol classes that were previously out of reach for the type-based approach, such as signatures of private data and encryptions of authenticated data. The proposed system and parts of the soundness proof are formalized in Coq.

This collection pays homage to the recent decision by the European Joint Conferences on Theory and Practice of Software (ETAPS) to add a conference on security to the confederation, and to the enthusiastic response of the security theory community to this initiative. We believe that this alliance will be highly beneficial for all communities involved.

The last decades had witnessed an increasing interest in formal approaches to the design, analysis and verification of security protocols, which had lead, on one hand, to a proliferation of workshops and colloquia on security theory and, on the other hand, to the decision by the ETAPS community to add security to their cluster of interests. In 2011 the joint workshops ARSPA and WITS became the first security event associated to ETAPS, under the name of TOSCA (Theory of Security and Applications). In 2012 the workshops SecCo (Security Issues in Concurrency) and FAST (Formal Aspects of Security and Trust) joined in, thus providing the critical mass to form a new conference, which took the name of POST (Principles Of Security and Trust). POST has been one of the ETAPS sister conferences since then.

We would like to thank all anonymous reviewers who have greatly helped us in the production of this Special Issue.

Konstantinos Chatzikokolakis
CNRS
France

Sebastian Alexander Mödersheim
DTU Informatics
Denmark

Catuscia Palamidessi
INRIA
France

Jun Pang
University of Luxembourg
Luxembourg