Journal of Computer Security 21 (2013) 779–780
DOI 10.3233/JCS-130488
IOS Press

Preface

This Special Issue is devoted to *Security and Trust Principles*. The issue took inspiration from the conference on Principles of Security and Trust (POST), held in Tallinn, Estonia during March, 2012. The Special Issue contains six papers, greatly extended from their original form and that have been accepted for publication after a rigorous review process and revisions.

Two papers are devoted specifically to symbolic analysis of security protocols. "Verification of security protocols with lists: From length one to unbounded length", by M. Paiola and B. Blanchet, extends the message structures that can be used in the ProVerif system for symbolic protocol analysis. The list structures that they add are useful for understanding group protocols, in which messages often grow in concert with the set of group members. By contrast, "Provably repairing the ISO/IEC 9798 standard for entity authentication", by D. Basin, C. Cremers and S. Meier, focuses on a specific collection of standardized protocols. The authors show that a surprising number of problems arise in these protocols, and that the Scyther automated tool can verify corrected versions. It thus provides a strong argument for systematically using the best available formal tools when standardizing protocols.

One paper, "Privacy-supporting cloud computing by in-browser key translation", by M. Arapinis, S. Bursuc and M. Ryan, proposes a novel protocol. This protocol establishes through the ProVerif system that a certain type of cloud-based service can be carried out using enough encrypted data that a malicious cloud provider cannot undermine the privacy of the participants.

"Verified indifferentiable hashing into elliptic curves", by G. Barthe, B. Grégoire, S. Heraud, F. Olmedo and S. Zanella-Béguelin, is the specifically cryptographic paper in the *STP* issue. It documents a rigorous proof of a recently proposed cryptographic technique, carried out in the Coq proof system, and confirms the value of mechanized proof within cryptography.

The remaining two papers are focused on programming language security. "A core calculus for provenance", by U.A. Acar, A. Ahmed, J. Cheney and R. Perera, develops a core calculus to clarify the power of provenance in computing. Secure provenance is increasingly important with multiple, partially suspicious principals sharing access to important data objects. "Type-based analysis of key management in PKCS#11 cryptographic devices", by M. Centenaro, R. Focardi and F.L. Luccio, uses a type system to determine whether key management methods are secure in the context of hardware security tokens.

These papers thus provide a broad snapshot of the foundational methods and issues in security and trust.

We are deeply grateful to the reviewers who worked hard to referee these papers and lead them to their current forms.

Pierpaolo Degano
Dipartimento di Informatica
Universita' di Pisa
Pisa, Italy

Joshua D. Guttman
Department of Computer Science
Worcester Polytechnic Institute
Worcester, MA, USA