J Autom Reasoning (2011) 46:223–224
DOI 10.1007/s10817-010-9184-z

Preface of Special Issue on "Computer Security: Foundations and Automated Reasoning"

Lujo Bauer · Sandro Etalle · Jerry den Hartog · Luca Viganò

Received: 15 June 2010 / Accepted: 17 June 2010 / Published online: 30 June 2010

The papers in this volume form a special issue on "Computer Security: Foundations and Automated Reasoning". This special issue is part of a series of special issues, traditionally associated with the ARSPA workshop on Automated Reasoning for Security Protocol Analysis. The 2008 ARSPA workshop was organized in conjunction with WITS, the Workshop on Issues in the Theory of Security, and with FCS, the workshop on Foundations of Computer Security.

ARSPA was set up to bring together researchers and practitioners working on developing and applying automated reasoning techniques and tools for the formal specification and analysis of security protocols. WITS is the official annual workshop organized by the IFIP Working Group 1.7 on "Theoretical Foundations of Security Analysis and Design", established to promote the investigation of the theoretical foundations of security, discovering and promoting new areas of application of theoretical techniques in computer security and supporting the systematic use of formal techniques in the development of security related applications. Finally, the workshop FCS continues a tradition, initiated with the Workshops on Formal Methods and Security Protocols (FMSP) in 1998 and 1999, continued with the Workshop on Formal Methods and Computer Security (FMCS) in 2000, and finally with the LICS

L. Bauer
Carnegie Mellon University, 5000 Forbes Avenue,
Pittsburgh, PA 15213, USA

S. Etalle · J. den Hartog
Technical University of Eindhoven, 5612AZ Eindhoven,
The Netherlands

L. Viganò (✉)
Dipartimento di Informatica, Università di Verona, strada le Grazie 15,
37134 Verona, Italy
e-mail: luca.vigano@univr.it

satellite Workshop on Foundations of Computer Security (FCS) in 2002 through 2005, of bringing together the formal methods and the security communities.

This issue is the result of a selection of the papers that were submitted to an open call that was issued after the joint ARSPA-WITS-FCS 2008 workshop. We received 28 submissions and, after two rounds of reviews, six papers were selected for publication. The accepted papers are on the topics of formal analysis of cryptographic primitives ("A Survey of Symbolic Methods in Computational Analysis of Cryptographic Systems", "Automated Proofs for Asymmetric Encryption", and "Encoding Cryptographic Primitives in a Calculus with Polyadic Synchronisation"); formal analysis of protocols ("Reducing Protocol Analysis with XOR to the XOR-free Case in the Horn Theory Based Approach" and "Multi-Attacker Protocol Validation"); and formal analysis of system correctness ("Collaborative Planning with Confidentiality").

Given the high number and the high quality of the submissions we had to be very selective. We would like to thank the reviewers who made the selection work possible. We also thank Tobias Nipkow, the Editor-in-Chief of this journal, as well as all the members of its publishing staff, for their support and for making this issue possible.