Journal of Computer Security 13 (2005) 1–2
IOS Press

Guest editor's preface

There is an increasing interest in the use of formal methods for security analysis and design purposes, which is witnessed by the success of some workshops and conferences devoted to this topic. In particular, this special issue of the *Journal of Computer Security* is devoted to a selection of papers from the *Third International Workshop on Issues in the Theory of Security* (WITS), that was held in Warsaw (Poland) on April 5–6, 2003.

WITS is the official meeting organized by the IFIP Working Group 1.7 on *Foundations of Security Analysis and Design* (FOSAD) and for the 2003 edition was organized in cooperation with ACM SIGPLAN and GI FoMSESS. WITS was established to promote the investigation on 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.

WITS 2003 was held as a satellite event of ETAPS (the Joint European Conferences on Theory and Practice of Software) and attracted about 55 participants.

WITS 2003 received 35 submissions, out of which 15 have been selected for presentation (see http://www.dsi.unive.it/IFIPWG1_7/wits2003.html for more details) by the Programme Committee that I chaired. This special issue contains six of those contributions, which have passed the standard journal refereeing procedure. They cover a large spectrum of topics, ranging from models for security protocol analysis to trust management, from non-interference proof techniques to secure operating systems. The list of accepted papers is the following:

- "Relating Multiset Rewriting and Process Algebras for Security Protocol Analysis" by S. Bistarelli, I. Cervesato, G. Lenzini and F. Martinelli.
- "Checking Security Policies through an Enhanced Control Flow Analysis" by C. Bodei, P. Degano and C. Priami.
- "Non-Interference Proof Techniques for the Analysis of Cryptographic Protocols" by M. Bugliesi and S. Rossi.
- "Verifying Information Flow Goals in Security-Enhanced Linux" by J.D. Guttman, A.L. Herzog, J.D. Ramsdell and C.W. Skorupka.
- "Decidability of Context-Explicit Security Protocols" by R. Ramanujam and S.P. Suresh.
- "Reputation-Based Trust Management" by V. Shmatikov and C. Talcott.

I thank the authors for their efforts in preparing good contributions and all the referees for their careful work and helpful assistance in selecting the papers.

Roberto Gorrieri
University of Bologna, Italy