Journal of Computer Security 12 (2004) 1
IOS Press

Guest editor's preface

This issue of the *Journal of Computer Security* contains five papers from the second meeting of WITS, the Workshop on Issues in the Theory of Security. WITS is organized by IFIP Working Group 1.7 (Theoretical Foundations of Security Analysis and Design), which held this meeting co-located with POPL in January 2002, with sponsorship from the ACM SIGPLAN. The third and fourth WITS are co-located with ETAPS.

WITS does not have an official proceedings. This is one of the strengths of the workshop, since participants can choose whether to present polished work or early versions of material to be presented elsewhere later. With a submission-to-accept ratio of about 2 to 1, WITS'02 had a mix of new and experienced figures, with a high quotient of excellent presentations.

In this issue, we gather five varied papers. Hughes and Shmatikov use interference-like ideas to provide a remarkably flexible account of anonymity properties, while Di Pierro, Hankin and Wiklicky offer a new quantitative, probabilistic approach to non-interference. Lowe provides a treatment of guessing attacks on cryptographic protocols, not previously represented within the Dolev–Yao tradition. Micciancio and Warinschi study the relationship between the Dolev–Yao model and more cryptographically motivated approaches, extending a soundness result to completeness. Chander, Dean and Mitchell clarify the relation between naming and authorization in trust management. Thus, these five papers touch on a wide swath of concerns in theoretical information security. WITS is one of the more vibrant venues for this subject today.

Joshua Guttman
The MITRE Corporation