Journal of Computer Security 10 (2002) 211
IOS Press

Guest editors' preface

This issue of the *Journal of Computer Security* contains three papers that were originally presented at the 7th ACM Conference on Computer and Communications Security (CCS 2000), which took place on 1–4 November 2000 in Athens, Greece. The papers were revised to include additional material; they also underwent the normal rigorous review process for inclusion in the *Journal of Computer Security*.

All three papers focus in their own way, on privacy. Collectively, anonymity, privacy-enhancing technologies, and certificate management accountability form the cornerstone of each paper.

In the first paper entitled "Hordes: a multicast based protocol for anonymity" B.N. Levine and C. Shields focus their paper, on maintaining *anonymity* in a network environment. The protocol they developed, called *Hordes*, uses forwarding mechanisms for sending data and the anonymity inherent in multicast routing to receive data. The authors propose definitions of anonymity and *unlinkability* (with respect to a single entity) and also quantify both terms. Based on these definitions, the authors perform a detailed comparison of Hordes with existing protocols, thus demonstrating the performance advantages of Hordes as well as trade-off in the use of multicast routing to reduce the network latency of communication.

In the second paper, entitled "A uniform framework for regulating service access and information release on the Web", P.A. Bonatti and P. Samarati address *privacy-enhancing technologies*. The authors propose a uniform formal framework for regulating both service access and information disclosure over large-scale networks. The framework is based on a language for access/release policies and a policy-filtering mechanism. The paper provides users with a means to communicate their requirements and also preserve the appropriate level of privacy.

A. Buldas, P. Laud and H. Lipmaa, in their paper entitled "Eliminating counterevidence with applications to accountable certificate management", focus on *accountability*. The authors suggest a primitive called *undeniable attester*, which allows a user to commit to a set of bit-strings by publishing a short digest of this set and to give attestations for any bit-string that is or is not a member of the set. *Untractability* of creating two contradictory proofs for the same candidate bit-string and digest is the important feature of this primitive. The aim of the paper is to increase the accountability of certificate management by making it untractable to the Certification Authority to create contradictory statements about the validity of a certificate.

We would like to express our appreciation to all reviewers for providing insightful and constructive comments to the authors.

Sushil Jajodia
George Mason University
USA

Dimitris Gritzalis
Athens University of Economics and Business
Greece