Guest Editors' Preface

This issue of the Journal of Computer Security contains four papers presented at the 1992 IEEE Symposium on Research in Security and Privacy, Oakland, California, USA, May 1992. These annual symposia have been sponsored since 1980 by the IEEE Computer Society Technical Committee on Security and Privacy. The Symposium is a forum for reporting research results in computer security from academic, industrial, and government laboratories.

The papers contained in this special issue were invited submissions that were revised for Journal publication and subjected to the normal review process of the Journal.

Jon Millen's "A Resource Allocation Model for Denial of Service Protection" introduces the concept of a Denial-of-Service Protection Base (DPB), which is similar to a reference monitor, but whose function is to guarantee, rather than deny, access. A DPB is made up of a resource monitor, a waiting time policy, and a user agreement. Its purpose is to assume that each benign process will make progress in accordance with the waiting time policy and that no non-CPU resource is revoked from a benign process until its time requirement is zero. This paper presents a formal model of a resource monitor and gives an example of a DPB that enforces a Maximum Waiting policy.

In "Authorization in Distributed Systems: A Formal Approach" Thomas Woo and Simon Lam present a formal language with a precise semantics for specifying access control policies independently of their implementations. The generality of the language, which allows it to capture a wide variety of authorization policies, stems from its ability to capture three structural properties inherent in an authorization policy: closure properties, default properties, and inheritance properties. The authors show that the specifications within the language can be translated into extended logic programs to assist in policy evaluation.

Virgil Gligor, Shyh-Wei Luan, and Joseph Pato's "On Inter-Realm Authentication in Large Distributed Systems" states and justifies a policy for propagating authentication trust across realm boundaries. The policy is analogous to the policy for identity and signature authentication in national and international law. The design helps limit global security exposures that may result from a realm authentication server being penetrated and can operate either transparently with respect to inter-realm path selection and acceptance or allow clients to choose paths from a set offered by a server. As an example, the paper presents a simple protocol that selects inter-realm authentication paths that satisfy the policy.

In "A High Assurance Window System Prototype" Jeremy Epstein, Hilarie Orman, John McHugh, Rita Pascale, Martha Branstad, and Ann Marmor-Squires describe the security policy, architecture, and operation of Trusted X (TX), a prototype multilevel secure windowing system based on the X Window System. TX is an application, not a complete system, and uses the TMach 2.5 prototype as an operating system platform. Although TX does not satisfy all of the TCSEC's certification requirements for B3, the architecture was designed to satisfy the B3 structuring and minimization criteria.

In conclusion, we thank the authors and reviewers of the papers for their hard work. We also thank the editors of the Journal for encouraging us to compile this special issue.

John McLean and Richard Kemmerer