Editors' Preface

This issue contains five papers. The first three papers were nominated from papers presented at the 8th IEEE Computer Security Foundations Workshop which was held June 13-15, 1995 in Kenmare, Ireland. The nominated papers were later revised and then went through the regular JCS review process for which Li Gong, the program chair of the 1995 workshop, was responsible.

The first paper, entitled "Specifying Security for Computer Supported Collaborative Working", by Simon N. Foley and Jeremy J. Jacob, shows how to specify confidentiality requirements in applications that facilitate cooperation between multiple users. It suggests a trace-based notation for specifying activities and for stating properties to limit information flow among the users who engage in them.

In "Distributing Trust amongst Multiple Authentication Servers", Chen et al. propose a protocol in which multiple untrusted servers generate candidate keys for the clients and the clients use a cross checksum scheme to verify these candidate keys. No individual server is trusted, but the scheme is secure if more than half of them behave correctly.

The third paper, entitled "The Composability of Non-Interference", by Zakinthinos and Lee, concerns a form of non-interference for event systems, similar to McCullough's generalized non-interference. This property is not generally composable, but this paper shows that it is preserved by compositions in which any feedback is interrupted by a delay.

In "Theft of Information in the Take-Grant Model", Bishop looks at an extension of the take-grant protection model, a simple model of propagation of access rights in which safety is decidable in linear time. The extension has rules for implicit reads resulting from information flow, determining who can "know" object contents. This paper provides a procedure to test whether a subject can "snoop" information by obtaining an implicit read without the cooperation of a subject who currently has explicit read access.

In the last paper "Multiple Key Distribution Maintaining User Anonymity via Broadcast Channels", Blundo et al. consider how a trusted authority can broadcast a message in such a way that each member of a specified privileged subset of users can decrypt the message to compute a session key. The particular advantage of their approach is that it allows for user anonymity.

Sushil Jajodia and Jonathan Millen