Guest Editor's Preface

The second issue of the Journal of Computer Security is drawn from papers presented at the IEEE Computer Security Foundations Workshop IV, Franconia, New Hampshire, USA, June 18-20, 1991. This series of annual workshops was founded in 1988 by Jonathan Millen. The objective of the workshops is to explore fundamental issues and current theories of security for computer systems. Particular attention is focussed on the underlying system models, and how security is verified with respect to its definition in these theories.

Several papers presented at the 1991 Workshop were invited for submission to the Journal. Submitted papers were revised for journal publication and subjected to the normal rigorous review process of the Journal. This issue contains two papers selected for publication through this process.

"Towards a Theory of Penetration-Resistant Systems and its Applications," by Sarbari Gupta and Virgil Gligor, presents a formal model for penetration-resistant systems to be used at the system call and detailed code level. The paper seeks to move penetration detection beyond the Flaw Hypothesis Methodology towards a more rigorous discipline. This is somewhat analogous to the manner in which verification takes error detection beyond testing. The authors' model addresses the class of penetration patterns caused by unprivileged users' code interactions with the system. This paper should encourage development of similar models for other classes of penetration patterns, such as caused by system failures, administrative errors, and improper installation for example.

Simon Foley, in "Aggregation and Separation as Noninterference Properties," introduces a model for information flow between security classes which allows aggregation, separation, and non-transitive exceptions to the normal flows in a lattice. The paper shows how complex policies based on these exceptions can be constructed by combining simpler policies. It develops a notion of noninterference for these policies, and proves an unwinding theorem for aggregation policies. These concepts are developed in context of a deterministic state machine model. The author suggests that extensions to other models should be possible.

A third paper, "A Logical View of Secure Dependencies" by Pierre Bieber and Frédéric Cuppens, from the 1991 Foundations Workshop was published in the previous issue of the Journal.

This issue also contains a paper by Amihai Motro, "A Unified Model for Security and Integrity in Relational Databases," selected from the regular contributions to the Journal. This paper deals with discretionary access controls in relational databases, and their interaction with integrity constraints. In the author's model all protective restrictions—whether stemming from security concerns or from integrity constraints—are expressed in terms of database views. The enforcement mechanism then reduces to an application of the view inference problem. The author presents algebraic and logical approaches for this purpose. Finally, the author discusses how a more general concept of integrity, based on soundness and completeness constraints, can be enforced by these mechanisms.

In conclusion, I would like to thank the authors, committee members, and panelists of the 1991 Computer Security Foundations Workshop, as well as the

reviewers of papers invited for the Journal. Their interest and hard work has established a valuable forum for foundational research in Computer Security.

Ravi Sandhu