Preface

Today most businesses and many individuals depend on the integrity of computer systems and networks. However, transactions and data can be vulnerable to assaults from both casual and malicious sources. From denial-of-service attacks to identity theft, pranksters and predators can interfere with our lives. Security measures are essential and can take many forms, from biometrics and smart cards for user identification to defenses encoded in software and hardware components.

This issue of the *IBM Systems Journal* contains nine papers on aspects of end-to-end security. We begin with papers on methods for authenticating valid users, move on to secure software, hardware, and architecture, and then return to users—how to prevent, or at least detect, the intruders. We are indebted to A. B. Lescher, IBM Server Group, for her effort in obtaining and coordinating these papers. A tenth paper, on the comparison of production database workloads with performance benchmarks, and two book reviews are also included in the issue.

The first two papers discuss ways to identify valid users. In the first, Ratha, Connell, and Bolle outline the inherent strengths of biometrics-based authentication systems, identify the weak points in these systems, and present new solutions for eliminating some of the weak points. In the second, Hamann et al. advocate the use of smart-card-based authentication schemes and transaction protocols for very sensitive business applications. They use banking applications as examples and present a high-level architecture that allows business applications to be secured, using smart cards, in an elegant and flexible way.

Public key cryptography, with its use of private and public key pairs, is an important technology for data confidentiality—a necessary aspect of user privacy. However, the proliferation of public keys needs to be controlled, and the Internet public key infrastructure provides a standard for their management. Benantar provides the background and details of this infrastructure.

Another perspective on user validation examines and categorizes user roles, based on a security principle known as the "separation of duty." Botha and Eloff assert that the workflow environment provides a context in which requirements for this separation can be studied, and that the dynamic separation required in this context can only be enforced in the run-time environment.

Smith and Safford ask what it takes to implement a server that provides access to records in a large database in a way that protects against unauthorized access, even from the operator of the server. To answer that question, the authors constructed a prototype using a commercially available secure coprocessor. Although performance improvement is needed, it appears that server privacy is both possible and practical.

IBM's mainframe operating systems have an enviable reputation for outstanding security, and those responsible are often asked to explain why. Guski et al. provide the answers, in a high-level discussion aimed at enterprise decision makers and application architects. The discussion includes some computer security history and projections of the relevant future.

Virtual private networks allow low-cost, secure communication over the Internet. A critical factor in the security of these networks involves the exchange of keys. Cheng provides an introduction to the Internet Key Exchange Protocol, a standard for generating and maintaining the Internet Protocol secur-

ity associations that form the building blocks of virtual private networks.

Can security principles consistently and effectively be applied to system development? Whitmore describes a systematic approach for defining, modeling, and documenting security functions. This approach, which has been incorporated into training for IBM Global Services architects, has its foundation in an international standard known as "Common Criteria."

In the last paper on security, Palmer explains how ethical hacking can be used to protect against criminal hacking. Ethical hackers use the same tools as those used by the intruders in order to evaluate the security of target systems. They then report back to the owners on the problems that were found and how they can be corrected.

In the last paper in the issue, Hsu, Smith, and Young examine the characteristics of production database workloads of large corporations. The authors compare actual workloads to standard benchmarks developed by the Transaction Processing Performance Council. They describe some characteristics of actual workloads that are not reflected in the benchmarks.

The next issue of the *Journal* will be devoted to papers on knowledge management.

Marilyn L. Bates
Associate Editor

John J. Ritsko
Editor-in-Chief