Preface

The papers presented in this issue address the subject of security. They were selected from a technical symposium conducted in October 1977 by the *IBM Systems Journal* and the IBM Systems Research Institute. The objective of the symposium was to examine systems security from the viewpoints of controllability, auditability, recoverability, protectability, and the interrelationships among them.

A prominent feature of security is protection or securing something against loss or misuse. When we look at this aspect of security in relation to data processing, we most frequently think of data and the procedures that turn data into useful information. Protection becomes more and more important as modern technology makes information readily available through distributed data and distributed processing. It is necessary to have protection not only within the confines of the computer system, but also throughout the whole communications network of an enterprise.

The growing interest in methods of protecting data has led to the development of advanced cryptographic techniques. Cryptography is a method of protecting data by making it meaningless to anyone who does not have authorized access to it. This is accomplished by an algorithm that alters the data using a complex series of transformations and substitutions. The algorithm is tailored to specific users by means of individual keys. Such a key-driven cryptographic scheme was accepted as a Data Encryption Standard (DES) by the National Bureau of Standards in 1977 and became effective on July 15, 1977. Products are available that employ both software and hardware implementations of the DES algorithm to encipher and decipher data. The first three papers discuss a key-driven cryptographic system using DES.

The effectiveness of any cryptographic system is highly dependent on the techniques used for selecting, handling, and protecting the cryptographic keys used in the ciphering process. The security of data depends on the security of the cryptographic keys, so the protocol for managing keys in a cryptographic system becomes vital. After discussing the concept of cryptography in a data processing environment, the first paper describes a scheme for key management. The generation, distribution, and installation of cryptographic keys in this key management scheme is the subject of the second paper.

Control functions are required to ensure that the use of cryptography is not disruptive to the normal activities of data processing. The aim is to include cryptography in the architecture of a system. The third paper discusses changes in Systems Network Architecture that allow the use of cryptography in a communications environment. The control of functions has become a logical part of the network architecture. Architectural similarities for the file environment are also discussed.

Control is vital to any security mechanism. External administrative control of the resources of a computing system is becoming increasingly complex. The paper on administrative control of computing service describes a method of cooperation between the internal and external control environments. Administrative procedures can be interfaced to system software through operating system components to enhance security. The computer shares responsibility for maintaining a secure, controlled environment. Automation of resource administration helps data processing management control access to resources, thereby helping to prevent willful or accidental misappropriation.

Control of processing itself is as important as control of the computing resources used in processing. With data processing being distributed over multiple nodes, the concepts of auditability and controllability grow as security concerns. Introducing the concept of spheres of control within the active elements of a process, the final paper provides a framework for understanding the audit and control aspects of modern data processing applications.

I wish to acknowledge the assistance of R. H. Courtney in the preparation of this issue; and thank also the participants of the security symposium, where so many good ideas were generated.

Connie Thiel
Editor