NISTIR 4976

Assessing Federal and Commercial Information Security Needs

David F. Ferraiolo
Dennis M. Gilbert
Nickilyn Lynch

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Computer Security Division
Computer Systems Laboratory
Gaithersburg, MD 20899

NIST

NISTIR 4976

Assessing Federal and Commercial Information Security Needs

David F. Ferraiolo
Dennis M. Gilbert
Nickilyn Lynch

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Computer Security Division
Computer Systems Laboratory
Gaithersburg, MD 20899

November 1992

U.S. DEPARTMENT OF COMMERCE
Barbara Hackman Franklin, Secretary

TECHNOLOGY ADMINISTRATION
Robert M. White, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
John W. Lyons, Director

ABSTRACT

In a cooperative effort with government and industry, the National Institute of Standards and Technology (NIST) conducted a study to assess the current and future information technology (IT) security needs of the commercial, civil, and military sectors.

The primary objectives of the study were to:

- determine a basic set of information protection policies and control objectives that pertain to the secure processing needs of organizations within all sectors; and

- identify protection requirements and technical approaches that are used, desired or sought so they can be considered for future federal standards and guidelines.

The findings of this study address the basic security needs of IT product users, including system developers, end users, administrators, and evaluators. Security needs have been identified based on actual existing and well-understood security organizational practices.

EXECUTIVE SUMMARY

The federal government and private industry rely heavily on information processing systems to meet their individual operational, financial, and information technology requirements. Corruption, unauthorized disclosure, or theft of resources have the potential to disrupt operations and could have financial, legal, human safety, personal privacy, and public confidence impact.

Each organization interviewed exhibited unique security characteristics described in terms of the organization's missions and goals. Security needs were further characterized from system to system within an organization.

System and organizational security requirements were found to be based on a higher set of environmental and policy factors and conditions. Computer security technology is applied uniquely in each situation even though there are common concerns.

Because each organization has unique security needs, security products have been applied on a case by case basis to meet individual security threats and concerns. Products should be flexible enough to serve a broad spectrum of security needs at the operating system level, the application level, the organizational level, and the site level. Organizational security requirements also change over time and cannot be totally specified at the time of product acquisition.

For organizations that process unclassified sensitive information, the availability of a greater variety of trusted products that go beyond C2 in terms of functionality and flexibility is needed. There is a demand to address data integrity in a more direct and user friendly manner. Vendors should consider new mechanisms that directly address discretionary and non-discretionary controls, such as role-based access controls, separation of duties, separation of transactions, and user-oriented least privilege.

Most organizations felt security standards should include a wide range of assurances including a "generally accepted commercial practice" level. This new level should minimize the cost of developing new systems or retro-fitting new security functionality in existing systems.

Nearly all of those interviewed expressed the desire to have an independent third party give a "stamp of approval" with regard to the trustworthiness of the systems they were buying. However, the current evaluation and certification process (i.e., with respect to a TCSEC class) was not perceived by users as meeting their needs for a variety of reasons.

Those interviewed felt that security standards have not emerged

that will allow integrating security across a multi-vendor environment. A system should provide a single user view of security services across a wide range of operating systems. Security features should inter-operate with other security services on both local and remote machines, without the need to train users in new security products. Security technology must support users working effectively together, sharing information, resources and network applications from whatever desktop device they choose within their authority, while providing a common set of security services.

This study has attempted to identify basic security needs of information technology product users, administrators, developers, and evaluators based on actual organizational practices. Although the findings of this study should not be considered conclusive, it is hoped that they will be considered in the development of future protection requirements, standards, guidelines and evaluation programs.

TABLE OF CONTENTS

PAGE

LIST OF APPENDICES