ASSESSING FEDERAL AND COMMERCIAL INFORMATION SECURITY NEEDS

NISTIR 4976

November 1992

David F. Ferraiolo Dennis M. Gilbert

Nickilyn Lynch

Computer Security Division

Computer Systems Laboratory

National Institute of Standards and Technology

Gaithersburg, MD

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.

unclassified sensitive information

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.

INTRODUCTION

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 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 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 information technology (IT) product users. This includes application developers, end users, and administrators. As such, security requirements can be identified based on actual existing and well understood security organizational practices.

The NIST study team used a set of topics as guidance when meeting with the various organizations. The topics are discussed in Section 2. Appendix C contains a sample of the questions asked and the issues explored during the interviews.

Development of Security Technology

The U.S. government has been involved in developing security technology for computer and communications security for some time.

Although advances have been great, it is generally perceived that the current set of security technology has, to some extent, failed to address the needs of all. This is especially true of organizations outside the Department of Defense (DoD).

The current set of security criteria, criteria interpretation, and guidelines has grown out of research and development efforts of the DoD over a period of twenty plus years. There exists one U.S. computer security standard, the Trusted Computer System Evaluation Criteria (TCSEC). It consists of security features and assurances, exclusively based on DoD security policy. The TCSEC concentrates particularly on those policies created to prevent the unauthorized disclosure of classified information. The result is a collection of security products built to TCSEC requirements that do not fully address unclassified sensitive security issues. This study indicates that these security products can be useful in providing computer security in non-DoD sectors, but they provide a partial solution at best and are used in lieu of a more appropriate set of controls.

Until recently, the government has paid little comparable attention to researching and addressing IT security needs of the government and commercial sectors that do not process classified information. During the past few years, however, managers and security officers of commercial and government organizations have paid increasing attention to IT security needs.

To help address these protection issues, NIST publishes standards and guidelines for the unclassified community. The Computer Security Act of 1987 (Public Law 100-235) assigned NIST the responsibility of developing security standards and guidelines for sensitive (non-classified) federal computer systems. The law gave NIST responsibility for developing validation procedures for cost-effective security and privacy of sensitive information in federal computer systems. The law also gave NIST the authority to perform research, conduct studies, and devise techniques appropriate to a computer system's security and privacy. To gain a better understanding of the needs of our constituents, NIST conducted this study.

Notions of Trust

As commercial and civil sectors have become increasingly dependent on complex and interconnected computer systems, trust in these systems has become an increasing concern. Examples of trust issues include: maintaining the privacy of employees, ensuring the correctness and accuracy of medical and credit records, and protecting national secrets from unauthorized disclosure or modification. The term "trusted systems" refers to systems supporting substantially increased safety, reliability, and, in particular, security mechanisms. "Security" refers to protection against unwanted disclosure, modification, or destruction of data.

To be effective, however, security must also address safeguarding system security features themselves. Security, safety, and reliability are elements of system "trustworthiness" - a level of confidence that a system will do what it is expected to do.

Conventions Used in this Document

"Federal government" refers to all government agencies, military and non-military. The "civil sector" refers to the civil "federal government" (and in some instances "state government"). DoD and military are used interchangeably, unless otherwise stated, and cover both classified and sensitive (non-classified) activities.

Document Overview

The sections following this introduction detail the study project.

Section 2, Project Approach, gives an overview of the project, discusses the project approach, profiles the organizations that were interviewed, and reviews the topics covered in the interview.

Sections 3, Findings, presents the study findings in terms of required protection policies, security, feature needs, security assurance needs, and product and application assessment.

Section 4, Conclusions, contains the study conclusions.

Appendices A - D present information not covered in the main body of the paper, including sample questions, study participants, and additional resources.

PROJECT APPROACH

Overview

The NIST study team conducted in-person discussions with key persons in 28 commercial and civil organizations between March and June 1991. Organizations were represented by 1 to 12 people. The participants came from a wide variety of perspectives, environments, applications, and system architectures. They included users and systems management, systems operations, computer security, and information resources management personnel. The study especially sought to reach people with major organizational mission responsibilities, who must react to breaches in information accuracy, availability, or privacy.

An invitational workshop was held at the beginning of the project. Numerous discussions at the workshop provided valuable input and direction. Participation in the study was strictly voluntary. The study was not part of any audit or Computer Security Act security and privacy plans review effort.

In order to encourage candor and to respect individual and organizational privacy, details are not attributed to individuals or organizations in this report

without permission. NIST sent copies of the report to study participants for comment.

Profile of the Organizations

The NIST study team met with 28 organizations - 17 federal agencies, 10 commercial organizations, and 1 state government. Fourteen of the organizations were in the Washington/Baltimore area and 14 were outside of this area, and included Arizona, California, New Jersey, New York, Pennsylvania, and Texas. Companies representing energy, financial, communications, insurance, manufacturing, computers, and service were included. Of the federal organizations, both the executive and judicial branches were represented. Activities included law enforcement, benefits delivery, nuclear/energy, space exploration, defense, tax system, information collection and dissemination, air traffic, and service center operations. Contractors participated in a number of the federal agency meetings. State functions represented included justice, transportation, lottery, franchise tax, health and welfare, motor vehicles, controllers office, and data center operations.

Appendix A provides a detailed list of the organizations. A sampling of job titles of the approximately 120 people interviewed can be found in Appendix B.

Topics Covered

The following topics were addressed at each meeting:

- Key, significant information protection requirements - those elements that were the driving force in establishing the protection requirements, e.g. legal or regulatory, business practices, organization policy regarding customer and employee privacy, fear of litigation, etc.
- Organizational information processing environment - in general terms, such things as centralization vs. distribution of resources, management and administration, and issues regarding networking, connectivity, interoperability, and homogeneity.
- Organizational information protection objectives - the concerns regarding system trustworthiness including confidentiality, integrity, availability, safety, and reliability.
- Important information protection features and assurances - what type of computer security products, features, and mechanisms were used, desired, or sought? This included discussion of the organization's baseline protections including design, development, and operational controls for providing confidence that the security features exist and work as intended.
- Needed confidence level in protection mechanisms - the degree of confidence in the protection mechanisms required by the organization.
- Methods to achieve confidence - what methods the organization uses, would like to use, or have available to achieve the desired confidence.

- Addressing evolving protection requirements of the 1990s -how the organization sees its situation and environment changing over the next few years and how that impacts its protection requirements.

Each organization was also invited to make additional comments or ask additional questions. Because of the free-form "discovery" nature of the meetings not all of the topics were covered in the same level of detail at every meeting.

The questions used at each meeting are in Appendix C. They served as background as well as guidance to the team during the meetings with the organizations. The questions represent the types of information sought, but were not necessarily asked during the sessions.

FINDINGS

Each organization interviewed exhibited unique security characteristics. Security was often described in terms of the organization's missions and goals. Security objectives were also different from system to system within an organization. For example, the requirements (security features and types of assurance) for the financial and administrative system within a hospital were drastically different from those for the computer resources devoted to the clinical treatment of patients within that hospital.

System and organizational security requirements are based on a higher set of environmental and policy factors and conditions. These factors and conditions are referred to in this document as "basis for protection" and discussed below.

At the system level, representatives from each organization generally described their security requirements in terms of the following control objectives:

- identification and authentication,
- access control, and
- user accountability.

The emphasis and specifics of each area were largely different. This was particularly true for the control objective access control. The TCSEC C2 class was often cited as a practical baseline for referencing applicable requirements. While C2 does provide many baseline requirements, it falls short in both security features, (e.g., password complexity, resource access control, and system access control) and assurances.

In addition, the need for a variety of access controls was noted. The TCSEC label-based mandatory policy was commonly viewed as inappropriate for the protection of commercial and civil sector data.

Specifics of these computer security approaches are described in Subsection 3.3, Organizational Security Approach.

Basis for Protection

Significant and broadly sweeping security requirements were found to exist within all organizations. Such requirements included protecting the integrity, availability, and confidentiality of key software systems, databases, and data networks.

Driving Requirements

Both federal government and corporations were found to rely heavily on information processing systems to meet their individual operational, financial, and information technology requirements. The corruption, unauthorized disclosure, or theft of resources could disrupt operations and have immediate serious financial, legal, human safety, personal privacy and public confidence impacts. Computers must also be protected against misuse by an individual committing such acts as data interchange fraud, harassment or personal terrorism, and pornography.

Organizations processing and storing classified information focus on preventing unauthorized observation/disclosure of data as the basis for protection. For these organizations, the unauthorized flow of information from a high level to a low level was the principal concern.

For the federal government, requirements exist for protecting the privacy of personal information. These requirements come from the Privacy Act of 1974. The Act provides privacy safeguards by requiring federal agencies to protect the personal information it collects, maintains, uses, and disseminates. Additionally, when an agency contracts for services, the contractor must protect the information subject to the Act's requirements.

Protecting the privacy of personal information was also relevant to commercial sector organizations. The need to protect sensitive data from unauthorized access resulted from operational environment (including threats) and data sensitivity factors. These factors include legal obligations and self-imposed requirements including confidentiality of salary, performance, and health (mental, drug, and alcohol related illness), as well as data involving legal incidents.

Privacy issues were perceived as particularly critical in medical and insurance applications. Educational, employment and personnel, banking and financial institutions, and credit bureaus also acknowledged protecting the privacy of individuals as a high organizational priority.

The need to preserve customer, insurer, and stockholder confidence was also cited as a basic security objective for many organizations. The vice president of a major bank described the need to "provide a good service at a reasonable cost"

as an important capability of most savings and financial institutions but described the need for "maintaining a general sense of customer confidence" as critical.

The basis for protection takes on a specific meaning for those organizations, such as banks, credit companies, and insurance companies, concerned with preventing unauthorized distribution of financial assets. These businesses are subject to federal regulatory requirements of the Federal Trade Commission and the Federal Reserve Board under the Fair Credit Billing Act, Equal Credit Opportunity Act, and Truth-in-Lending Act.

Security issues can also be unique to a specific industry. Of all the organizations interviewed, only PACBELL and BELLCORE were concerned with preventing unauthorized use of long-distance telephone circuits. Only hospitals and those who develop hospital systems were concerned with preventing unauthorized distribution of prescription drugs.

Professional standards, health and safety, prevention of embezzlement, good business practices, and profit were also stated as key factors in an organization's basis for protection.

Types of Information

In general, the interviews focused on the protection of information that a user may entrust to a system. During the course of the interviews, two other types of information were noted as requiring protection. These two types were:

- system-operating information (software, tables, etc.); and
- system-generated information (user activity data, general traffic data, audit information, etc.).

Each type of information was found to have its own security policy requirements. In the case of system-operating information and system-generated information, the system itself was perceived as the owner and primary custodian of the information. The system owner/operator sets the policy requirements for protecting information. The owner of system-generated information is the system owner/administrator, who also sets its policy.

Sector Protection Requirements

Some similarities and differences of security needs within the commercial, civil, and military sectors were noted. Security objectives were specified and governed by many independent levels of authority, from general legislation, to organizational rules of operation, to rights and needs of the individual. Standards of due care were different in each environment, just as controlling laws differ in each state. Each organization had its own objectives and rules for computer

access privileges. The U.S. DoD confidentiality policy was unique in applying a single set of security services across a large number of applications.

Common Notions of Protection

"Conventional wisdom" holds that the military is concerned only with protecting the confidentiality of classified information. Similarly, a policy of integrity and reliability is associated primarily with commercial and civil sectors. The study team found those view points to be over-simplified.

Integrity issues are critical to the commercial and civil sectors, as well as the military sector. For example, integrity takes on a critical meaning within a military Nuclear Command and Control (NC2) system. The NC2 system may disseminate a critical message from a top command tier of a tactical network down to a field terminal associated with a weapon. This dissemination must occur in a timely and unaltered manner. The knowledge of the contents of such a message during a nuclear exchange would have little or no value to an adversary. However, the ability of an adversary to alter the contents of, or to deny or delay the delivery of, such a message could alter the course of a war.

The study team found that a computerized hospital support system, whether in a VA or commercial hospital, also imposes stringent integrity controls. The integrity controls of such a system must provide for the ethics and laws associated with the clinical treatment of patients. Prior diagnoses can never be destroyed or altered; only doctors can perform a diagnosis and prescribe medicine. Protecting the accuracy of patients medical records may be critical if there is an accident where the patient becomes unconscious. The correctness of information including the patient's reaction to medications, pre-existing ailments, blood type, or medication currently being prescribed can all prove to be health-threatening or even life-threatening.

Integrity issues, in general, were found to address a richer and more dynamic facet of security than confidentiality. These issues often pertained not only to who can access what data (which is common to most confidentiality access control models) but also how and when the data is accessed. The more commonly agreed upon objectives of integrity include:

- Ensuring the consistency of data values within a computer system;
- Recovering to a known consistent state in the event of a system failure;
- Ensuring that data is modified only in authorized ways, whether by users or by the system;
- Maintaining consistency between information internal to the computer system and the realities of the outside world.

Integrity issues were particularly relevant to applications such as funds transfer, clinical medicine, environmental research, air traffic control, and avionics, as well

as many classified and sensitive (non-classified) . DoD applications. For some systems, integrity was closely related to the issue of system safety. Two examples are maintaining the safe operation of a manned space vehicle and a doctor relying on the correct results of a medical diagnostic machine.

While usually associated with the military sector, the commercial and civil sectors are also concerned with protecting the confidentiality of their information. Examples include the protection of personnel data, marketing plans, product announcements, formulas, and manufacturing and development techniques.

Commercial and civil sector organizations are obligated to protect the results of mandatory medical exams and substance abuse tests from unauthorized disclosure. The compromise of a preliminary agricultural report could provide an unfair advantage within the futures market. The knowledge of the thresholds used by IRS computers to flag tax returns for subsequent audits could have great financial benefits.

Distinguishing Protection Characteristics

Although a common core of high-level security needs have been found to exist across all sectors, some basic differences exist. These differences are in the way information is handled and where the emphasis is placed on security within the commercial, civil, and military sectors.

The military emphasizes strong access controls placed between users and classified information. These controls must be highly resistant to bypass and alteration. To achieve this and other requirements, the operating environment is designed around a requisite security architecture.

Because of the potential consequences, organizations that process classified information are willing to go through greater expense than the rest of the federal government in terms of dollars, system development time, and computer performance, to mitigate risk. Where add-on security products are not available, the military has designed and developed secure systems from the ground up to meet its security needs. Such expenses are normally not justified in the commercial and civil sectors.

On the other hand, the commercial and civil sectors have traditionally emphasized auditing techniques, along with basic access control methods. This was based on (1) the belief that a user who knows he or she is being watched is less likely to violate security and (2) the average user knowing little about computers. In contrast, the military has always placed less emphasis on auditing since it is concerned with threats from malicious software, such as Trojan Horses and trap doors, that can be designed to bypass ordinary auditing mechanisms. However, since the average person is more knowledgeable and comfortable with computers, the threat to commercial systems has increased. Consequently, the

difference between the security threats to commercial computer systems and those of the military is becoming less extreme.

The study team found that most commercial organizations take a carefully measured and cost-effective approach to computer and communications security issues. Each commercial organization interviewed described computer security as an important and necessary capability of their computer systems. However, such statements were quickly caveated with the reality that a business case is also presented regarding the merits of such capabilities. This business case was described as balancing the:

- cost to implement, maintain, and administer security;
- benefits gained by imposing security; and
- impact on the user.

The costs associated with security are absorbed as part of overhead, resulting in reduced profits and a potential loss of competitiveness. On the other hand, by neglecting security, an organization becomes more vulnerable to attack. An attack could result in an unexpected and direct cost to the company through a loss of confidence in the organization by its customers, or legal actions. These factors can affect profits.

Another consideration is how security effects the user. The goal is to make security features as transparent as possible to the user. If a user's ability to utilize the system is impeded due to security constraints, then the organization is that much less efficient. An organization risks becoming less competitive due to higher overhead cost or absorbing the added operational cost through lower profits.

A great deal of importance is placed on being in-step with other organizations of like size and function in terms of a security program. This provides confidence that the organization is staying within the norm of generally accepted business practices, thereby reducing risk in terms of incurred liability. Such considerations, along with more traditional risk analysis, are used as the basis for determining requirements and implementing safeguards. Within the commercial sector, there is a trade-off between the cost associated with potential loss and the cost associated with implementing security mechanisms.

Computer security programs of the federal government, in general, look at different cost factors than those of the commercial sector. The concerns in federal government, like the commercial sector, are budgetary, "regulatory," and reputation. The difference is that the federal government is not profit-oriented, nor does it worry about market share. Of more concern is maintaining public confidence, complying with new regulations, and keeping a good reputation with the public. A major security incident can impact all three factors.

Organizational Security Approach

The NIST study team discussed with each organization the type of computer security products, features, and mechanisms that were used, desired, or sought. This included the organization's approach to providing confidence that the security features exist and work as intended. These include design, development, and operational control aspects. These approaches will only consider information technology and not discuss other safeguards, such as physical and procedural controls.

Identification and Authentication

Identification and authentication were critical to every system the NIST study team reviewed. The most common method of authentication was passwords. Passwords can also be required at the data file level.

Passwords are considered by many to be a relatively weak security mechanism. Users tend to use easily guess passwords (e.g., spouse's name, birth date, sport team, etc.). A randomly generated password is difficult to remember, causing the user to write it down and creating the possibility of loss or disclosure. Other vulnerabilities include spoofing users, users stealing passwords through observing key strokes, and users sharing passwords. The unauthorized use of passwords by hackers or insiders is a primary concern.

Those interviewed felt that NIST should encourage vendors to provide a strong password management capability at the operating system level that would be tailorable to specific environmental needs.

Along with the availability of a strong password management capability, they felt NIST should continue to promote research on improving the integrity of the identification and authentication process. Technologies such as smart cards, signature verification, and voice authentication were mentioned as having a potential place in an overall approach to security. However, for organizations with large numbers of users, only a low-cost solution would be practical.

Access Control

The access control needs and control policies of each organization interviewed varied. Many of these policies consider site, organizational, industry, or agency-unique factors.

Access control policies are context-dependent; it is not possible to know the environment in which such control will be applied. Not all stated access control policies can be easily mapped and implemented using the existing access control framework of the TCSEC. The TCSEC specifies two types of controls: Discretionary Access Controls (DAC) and Mandatory Access Controls (MAC).

Since the TCSEC's appearance in December of 1983, DAC requirements have been perceived as being technically correct for commercial and civil security needs, as well as for single-level military systems. MAC is used for multi-level secure military systems, but its use in other applications is rare. The need for access controls more appropriate to the commercial and civil sector, than that of DAC, was found to exist. There is a need for DAC, but DAC falls short when implemented alone in solving the wide breath of security problems facing sensitive processing environments.

The remainder of this section describes the applicability of DAC and MAC, as well as other access control approaches, to the policy needs of those organization interviewed.

Discretionary Access Control

DAC plays an important role in supporting security requirements of many organizations, especially within engineering and research environments where the discretionary sharing of access and exchange of information is important. For many organizations, users must be able to specify what access other users have to resources that they control, without the intercession of an administrator. This makes the controls discretionary. Within a true DAC environment, the ability for a user to access information is dynamic and changes rapidly over short periods.

Organizations expressed concerns about relying solely on DAC as the primary means of protection. Specifically, they were concerned with the propagation of access rights, reliance on the cooperation of users, and, to a lesser extent, DAC's vulnerabilities to a Trojan Horse.

Some organizations expressed concern over exactly who has the capability to specify group membership. By granting membership to a group, user access rights to protected data can dynamically change without the knowledge of the owner of that data. For some organizations, the ability to specify group membership was described as appropriately placed at the project level, while for other organizations, group membership was more appropriately placed at the security officer level. The organizations were concerned with this capability and would like the option of specifying control over group ownership within their computer systems. In addition, the ability to list group membership before granting access privileges to that group was considered by some as a necessary part of this capability.

The most common approach to implementing DAC is through access control lists (ACLs). The TCSEC encouraged ACLs as appropriate for user-controlled access rights. However, when centrally administered, ACLs can become clumsy and difficult to maintain. In centrally administrating DAC, the system administrator assumes responsibility for ownership of all resources, determining what resources and modes of access are needed for the performance of each user's

function within the organization. For each new user or every change in responsibility, the central administrator establishes the appropriate access rights within the system. Additionally, when a person leaves the organization, the central administrator deletes the person from all ACLs within the system. Many of the organizations felt ACLs were difficult for the central control and management of access rights.

Role-Based Controls

Many organizations preferred a centrally administered, non-discretionary set of controls to meet their security policies and objectives. During the course of this study, organizational policies and objectives have included maintaining and enforcing the rules and ethics associated with a judge's chambers, and the laws and respect for privacy of diagnosing ailments, treating of disease, and administering of medicine within a VA hospital. To support such policies, a capability to centrally control and maintain access rights is needed. The security administrator is responsible for enforcing policy and represents the organization as the "owner" of system objects. Access control decisions were found to be based on the roles individual users take on as part of an organization. This includes the specification of duties, responsibilities, obligations, and qualifications. For example, the roles included doctor, nurse, clinician, or pharmacist associated with a VA hospital; or teller or loan officer associated with a banking system. The doctor's role includes privileges to perform diagnoses, prescribe medication, or add a entry to (not simply modify) a record of treatments performed on a patient. The privileges defined for the role of pharmacist include those to dispense (not prescribe) prescription drugs.

The determination of membership and the allocation of privileges to a role is not so much in accordance with discretionary decisions on the part of a system administrator, but rather in compliance with organization-specific protection guidelines. These guidelines derive from existing laws, ethics, regulations, or generally accepted practices. The guidelines are non-discretionary in the sense that they are unavoidably imposed on users. For example, a doctor can prescribe medication, but cannot pass that privilege on to a nurse.

Once roles are established within the system, the privileges associated with these roles remain relatively constant or change slowly over time. The administrative task is then to grant and revoke user membership to the set of specified roles within the system. The capability of an administrator to simply grant and delete membership to existing roles has been described as desirable. When a user's function changes within the organization, the user's membership to existing roles should be easily deleted and new ones granted. Finally, when a person leaves the organization, all of that person's memberships to all roles are deleted. For an organization that experiences a large turnover of personnel, a role-based implementation security policy is the only logical choice.

The NIST study team talked with several organizations that felt role-based access or access based on function was a control more suited to their needs than DAC or MAC. While add-on packages will give an organization access based on function for their systems, role-based access control should be generally promoted as are DAC and MAC. Currently no standard exists to promote the wide availability of role-based access control.

Separation of Transactions

Separation of transactions is a design and implementation approach which partitions a task-oriented set of programs and data. This set is available to a specific user who is allowed access only to these resources. A group of available transactions define a particular task that can be assumed by a user. Although similar, separation of transactions differs from role-based control in that creation of roles and the granting of membership to roles are an administrative function while the underlying access control rules enforced through separation of transactions is achieved through a combination of administrative and transaction-design decisions.

Because of the stable functionality and the deterministic characteristics of transactions within some organizations, security engineers or those knowledgeable of security issues facing an organization (i.e., privacy, data integrity, etc.) play an important role in specifying access-control decisions during the design and development of the system. For example, for one organization, transactions were designed to retrieve an entire customer record minus the customer's social security number. In addition, design-time access control decisions can consider aggregation problems that are difficult to address within conventional run-time access control environments. Security guidelines are addressed by the designer and developers of a transaction or by direct involvement in the design and development effort of proposed transactions.

Once a transaction has been developed and introduced into the operational environment, a security administrator may assign the named transaction to specific users or user groups. The importance of control over transactions, as opposed to simple read and write access, can be seen by considering a simple banking transaction. Tellers may execute a savings deposit transaction, requiring read and write access to specific fields within a savings file and a transaction log file. An accounting supervisor may be able to execute correction transactions, requiring exactly the same read and write access to the same files as the teller. The difference is the process executed and the values written to the transaction log file.

A major insurance company enforces its corporate policy through the use of separation of transactions. Within the organization, each unit (performing a specified task) is assigned a collection of transactions to perform an assigned task or function. A unit security administrator determines "what users get access

to what transactions," within that unit. The security administer can add and delete users to the unit, but cannot assign transactions to individuals outside the unit.

Separation of Related Duties

Although more of a policy than a mechanism, separation of related duties is used in deterring fraud within financial systems. Such duties can include authorizing, approving, and recording transactions, issuing or receiving assets, and making payments. Separation of related duties refers to the situation where different users are given distinct, but often interrelated tasks such that a failure of one user to perform as expected will be detected by another. For separation of related duties to be effective, computer capabilities must be partitioned. These capabilities must be accessible only to users or processes associated with specific tasks.

Several organizations described the need for an add-on capability of separation of related duties. One example would be a program or device to separate users who authorize or commit the expenditure of funds from those authorized to place orders for services and equipment. The IRS has used this policy as a requirement from the outset and a system with this capability was developed especially for them.

Principle of Least Privilege

The principle of least privilege was described by some of those interviewed as an important control approach in meeting security policies and objectives. This principle gives the user no more privilege then is necessary to perform a job. Implementing least privilege requires identifying what the user's job is, determining the minimum set of privileges required to perform that job, and restricting the user to a domain with those privileges. Least privilege allows a user to have different levels of privilege at different times, depending on what task is being performed. By denying access to transactions and privileges that are not necessary for the performance of their duties, those privileges cannot be used to circumvent the organizational protection policy. Least privilege is particularly important for those systems where there is a "privileged user" or "superuser" capability that would otherwise grant a wide set of privileges to users that need only a subset of those privileges.

The principle of least privilege is similar to separation of transactions. It differs in that separation of transactions restricts the set of programs that can access data and places restrictions on which users can execute what programs. Least privilege restricts a user's access to data by denying users privileges that are not necessary to do their job.

Several organizations would like an operating system capability that supports the principle of least privilege. This capability is currently supported in upper end

secure systems (B2 and above), but many organizations expressed the desire to see this capability at a more basic level.

Label-Based Mandatory Access Controls

The other form of access control specified in the Orange Book is label-based mandatory access control. MAC is a non-discretionary access control, restricting users in their access to data on levels implemented through labels. These are (1) the level associated with the trust of the user, i.e., clearance, and (2) the level associated with the sensitivity of the data.

Forming an alliance among companies that are otherwise competitors was cited as a reason to enforce a confidentiality policy. For such an alliance to exist, the ability to isolate and share information on a non-discretionary, formal "need-to-know" basis is required.

The formal "need-to-know" has primary emphasis on categories and, to a lesser extent, on hierarchical levels. The term "category" is used to describe non-hierarchical separation. Outside the DoD, few organizations operate using hierarchical levels. Most non-DoD organizations have employees and users belonging to one level, but with different responsibilities, i. e., in different categories.

For example, a commercial organization recently formed strategic alliances with some of its competitors. Although this organization has always allowed access to some of its most sensitive proprietary information by outside consultants, this access was narrow and limited. Because of the frequency and scope of past access requirements, physical and procedural measures could provide the necessary isolation. However, the physical and procedural controls of the past have become impractical with current information needs. The only practical solution is label-based mandatory categorization. This type of access would allow limited partnership between competitors.

As business alliances become a corporate reality for many U.S. companies, label-based mandatory access controls will become more important. Currently, label-based MAC is not generally available as part of an operating system, but it can be added.

Object-Label Association

The ability to associate a label (not necessarily used in access decisions) with an object was described as a needed capability by several organizations interviewed. These labels would carry warning, advisory, and other information associated with an object and would not be used for making mandatory access control decisions. For example, within a hospital system, a label would associate a warning with a prescription drug, i.e., "not for use if person has high blood

pressure". The association between a drug and a warning is an important relationship. For medical systems in general, the capability to associate an information label describing the quality of an x-ray, CATscan, sonogram, or any other image shared among medical professionals, can be a vital capability. Currently, object-label association is neither a capability available within most systems nor encouraged through security standards.

User Accountability

User accountability means holding individual users responsible for their actions. Imposing a policy of accountability on system users was described by organizations as both a detection and deterrent mechanism. This implies that an individual is knowledgeable of some standard of conduct and answerable to a higher authority who may impose penalties on those who fail to adhere to this standard. Also, making users aware that their actions are being monitored is thought to prevent a would-be violator from committing a breach of security.

Individual accountability is accomplished through:

- uniquely identifying and authenticating the individual user;
- authorizing access to the system;
- generating an audit trail of security relevant events; and
- reviewing the database of security relevant events for deviations from some specified standard of conduct.

Although acknowledging vulnerabilities with the process of identifying and authenticating an individual, organizations are aware that technological solutions are available, but not yet affordable. In addition, they recognize that existing administrative interfaces are inadequate for an effective review of the database of security-relevant events. This was especially true for environments doing distributed processing.

A related issue raised in a few interviews was intrusive employee monitoring/surveillance. A few organizations indicated employees or their representatives had expressed concern about potential misuses of increasingly sophisticated data gathering and analysis tools.

NIST should promote incorporating computer security auditing standards in products. Those interviewed expressed frustration with various aspects of auditing computer security events. Current auditing features, although sufficient in meeting evaluation criteria, are of limited practical use in distributed and networked environments. There was limited understanding of what events should be audited, what information should be collected, what form that information should be in, and how to compare and consolidate the information from one system to another. Interoperability and a common format for auditing security-relevant events is needed. Common formats would facilitate the central collection

and reduction of security-relevant events. This is integral to achieving security in the heterogeneous, distributed environment many organizations are facing.

Electronic Data Interchange (EDI)

EDI is the computer-to-computer interchange of messages representing business documents. Most organizations expect EDI to become a common part of their business practices. They recognize that while EDI can provide an opportunity for improved efficiency, it has the potential for additional risk.

Some expressed concern that by using EDI technology, original hard-copy evidence of obligation and commitment by concerned parties would not be available. For EDI to be a practical alternative to paper, specific assurances must be provided that EDI messages are authentic and properly authorized. The goal of EDI technology is to provide the same capabilities as traditional paper-based administrative functions with more efficiently and the same level of trust.

Assurance and Quality

Assurance gives a user or system owner a degree of reliability that claims of security functionality and policy support can be relied on with confidence. Assurance is gained through various methods using evaluation criteria as a metric. Some people felt that part of confidence was an effective user interface, with quality equating to ease of use.

Security assurance is an important factor in any secure system development effort and an important element of an existing or emerging security standard. The desired level and types of specific assurance requirements are, at best, difficult to assess. Most of those interviewed felt that, at a minimum, security features should be implemented with the same level of confidence, quality, and robustness as other non-security-related operating environment system features.

Some interviewees said that they saw a general increase in the level of quality in computer products and felt a higher degree of confidence in those products. However, they could not report comparable improvements in the security features associated with new system releases or versions of systems, or the confidence they had in them. One aspect of quality notably missing from security features is a friendly user and administrator interface. This is particularly apparent when managing ACLs, reviewing audit reports, and administering passwords. Several interviewees felt that resolving such problems would enhance the effectiveness of security.

A sizable segment of those interviewed felt that the current assurance and evaluation process is not cost-effective. The security associated with many systems and applications should not be viewed any differently than any other aspect of the system. It should be subject to the same cost-benefit analysis as

other features. In regard to assurance levels, a basic level needs to accommodate the notion of generally accepted commercial practices.

For the majority of organizations interviewed, a moderate level of assurance was described as appropriate. However, there is a class of software/hardware systems where it is necessary that the system be shown to be probably correct with respect to some aspects of its trusted operation. As noted, maintaining the confidentiality of classified data within a military system may warrant such a confidence level. However, critical systems exist outside the military. Security functionality is critical to electronic funds transfer systems, as is safety within avionic and transportation control systems. In addition, with the increased use of embedded computers in medical systems, improved methods of assuring their correct operation becomes increasingly important.

Evaluation

The process of security evaluation validates the functionality of the features as well as assurances of a system.

The current process of evaluation was described to those interviewed by the NIST study team as being an adjunct to the assurance process. The evaluation process is not without its costs in terms of product development costs, development delays, and its availability. The development costs included the production of evaluation evidence (which in many cases is not necessarily a byproduct of normal system development), additional phases and activities added to the system design and development, and enhanced architectural requirements. The availability and development delays included evaluation time and evidence preparation time.

Those interviewed were almost uniformly concerned with the cost. Some interviewees expressed concerns about vendors passing along the added design and development cost to the customer. Another concern was the availability of evaluated products. Most noted that the products they were currently using were not the same version as the product that was evaluated.

Even with the visibility and concern over the costs associated with evaluation, most organizations recognized a need for an independent and faster evaluation. Surprisingly, there was not strong support for vendor self-assertion with respect to evaluations. Most organizations possessed a basic distrust for vendors based on past experiences.

Many organizations also took exception with the current format of evaluations and viewed them as limited in scope. It was suggested that evaluations include other security-related aspects such as performance, ease of use, compatibility with existing applications and hardware, and interoperability issues. Some even suggested that a "Consumer Report"-style product assessment would be useful.

Such a report would support their procurement needs as well as provide incentives for vendors to develop a quality set of user and administrator interfaces rather than meeting minimum requirements.

Most organization representatives viewed the performance of evaluations in a stand-alone laboratory environment as unrealistic for their actual operating environments. Of all the organizations interviewed, not one processed in a stand-alone environment. Almost all organizations had intelligent workstations directly or remotely connected through a local-area network.

Current Criteria Not Keeping Pace

Although advances have been great, several organizations stressed that the current state of security technology has failed to address the needs of all. This is especially true of organizations outside the DoD who felt little attention has been paid to current criteria in addressing their security requirements.

Trusted technology has also failed to keep pace with technological advances in information processing. Existing security theory and criteria are founded on the multi-user stand-alone computing environment, such as the mainframe computer. However, the trend is toward distributed storage, processing, and communication functions, on low-cost specialized machines on a network. The network is becoming the computer. Current product evaluations exclude general network facilities, while many computers are installed in networks.

The Trusted Network Interpretation (TNI) of the TCSEC was developed to address the security network issue. It provides security evaluation and design criteria for networks of systems that are developed, installed, and administered as though they were a single time-sharing system. However, most organizations procure systems in an evolutionary fashion with new computer resources added, replaced, deleted, and added again. The system may be connected to another network which may be connected to still another network. The TNI does not address this evolution.

Need for Security in Open Systems

Those interviewed felt that security standards which allow the comprehensive implementation to integrate security across a multi-vendor environment have failed to emerge. It should be possible to:

- interface many systems, both present and future;
- provide a single user view of security services across a wide range of operating systems; and
- have security features interoperate with other security services on both local and remote machines, without the need to train users in new security products.

The need to implement security should not limit an organization in choosing the best solution and integrating it into their existing system. Security technology must support users working effectively together.

Owner-Custodian Relations

Organizations assume a certain risk when they permit their information to be transmitted over a commercial or public network and used by computer systems they do not control. They are aware that simply connecting to a network can increase the vulnerability of their own computer system to hackers or malicious software. Some users conclude that, in addition to providing mechanisms to protect information on their own systems, they need to consider the security implications of sharing resources with subscribers on other systems. When an information owner passes information to another system for use on that system, the user wants assurance that information is protected in accordance with the owner's protection criteria.

In an owner-custodian relationship, there is a transfer of responsibility for safeguarding information from one party to another. In practical terms, the owner of the information defines what protection it requires; any system that processes the information must ensure that the system security policy satisfies the owner's protection policy.

An example is a military contractor who protects classified information using DoD policy. Another example is the Financial Intelligence Center (FINCEN) of the Department of the Treasury. To be effective in its counter-narcotic efforts, FINCEN must interact and share information with other law enforcement organizations, such as the Coast Guard, IRS, Secret Service, postal inspection, gambling commissions, banks, etc. FINCEN, as a custodian of information belonging to a large number of organizations, must provide security services that can be demonstrated effective at meeting a variety of security policies.

Security Policies and Environments Can Change Over Time

For many organizations, security requirements cannot always be considered at the outset of system procurement, or service or custodial establishment. For these organizations, the ability to integrate security into existing processing environments in an evolutionary fashion is critical. All of the organizations interviewed reported significant changes in their environments, as new computer and information technologies are acquired. In some cases, the changes are new customers or new alliances with other organizations. Some of the organizations interviewed became custodians of others' data, in some instances data of their competitors, as well as their own data. In some situations, organizations faced changing requirements regarding with whom they exchange data.

In addition, threats can change over time. For example, attackers can devise new techniques. Hidden vulnerabilities can be discovered after system deployment. Vulnerabilities can also be missed during system evaluation and discovered in operational use.

CONCLUSIONS

The NIST study team concluded that computer security is applied uniquely in each situation even though there are common concerns in all sectors. Because each organization has unique security needs, security products have been applied on a case-by-case basis to meet individual computer security threats. Security at the operating system level, the application level, the organizational level, and the site level must be considered. Products need to be flexible enough to serve a broad spectrum of security needs.

Considerations must be made for the reality that security requirements evolve and cannot be totally specified at the time of product acquisition. Security capabilities need to include new system and network connections. Security managers need to be aware of changing laws and regulations.

At the operating system level, basic capabilities need to be adaptable to a variety of organizational policies and applications. These capabilities should include security extensions that allow more security to be added at a later date. These extensions can include trivial password checkers, system built options, and enhanced system administrative capabilities, such as setting minimum-length password, creating roles, granting and revoking access and capabilities).

More classes of operating systems beyond C2 with more flexibility within the classes are needed. Users are concerned with computer security issues beyond confidentiality and disclosure. There is a need to address data integrity in a more direct and user-friendly manner. Vendors should consider new mechanisms that more directly address such things as role-based access controls, separation of duties, separation of transactions, and user-oriented least privilege.

Minimum Security Requirements

A majority of those interviewed wanted a baseline of computer security controls in the systems they purchase. These would include a more flexible DAC, role-based non-discretionary access controls, and principle of least privilege. While acknowledging their responsibility in determining security requirements, they saw value in knowing that their systems met a pre-existing computer security baseline.

Baseline Capabilities

While DAC was considered useful, that capability was not flexible enough for group membership. A number of organizations were administering access control policies based on the roles or job functions of its staff. However, these policies were implemented by mechanisms, such as access control lists, that were not designed to facilitate a role-based world view.

Organizations felt that role-based or access-based functions were controls more suited to their needs than DAC or MAC. While there are add-on packages that provide this function, this type of access control should be as widely promoted as are DAC and MAC. Lack of standards for role-based access control contributes to the problem.

Within DAC environments, organizations need control over group ownership within their computer systems. In addition, the ability to list group membership before granting access privileges to that group was considered to be necessary.

Several organizations described the need for an operating system capability that supports the principle of least privilege. This capability is currently supported in upper-end secure systems (B2 and above), but many organizations expressed the desire to see this capability at a more basic level.

Computer Security Features Enabled by Default

Vendors should deliver computer security systems with the security features turned on or enabled. This would provide an initial security state and enforce a disciplined consideration of those features to be disabled. A very small minority wanted computer systems delivered with the security features turned off. They wanted the choice of turning on only those features they needed in order to not excessively inhibit system performance.

Assurance

Most organizations felt evaluation criteria should include a wide range of assurance levels. This includes a "generally accepted commercial practice" level which minimizes the cost of developing systems and the length of time associated with evaluation. Evidence used in the assurance process should be founded on a sound base of experience and observations. Evidence should be limited to that which has shown to be beneficial in the past, not that which, in theory, should be beneficial.

Evaluation

The current evaluation and certification process (i.e., with respect to TCSEC) is not perceived by users as meeting their needs for a variety of reasons. One reason cited was the time lag between new product releases and formal certification. Another reason was that the existing certification process does not

address other issues associated with operational environments, such as effectiveness of mechanism, performance, version compatibility, adaptability, and ease of integration.

Each organization felt that the products they acquired needed to be evaluated regarding security features and assurances. None felt that vendor self-certification or vendor representation were adequate. While a few wanted to do a portion of the evaluation themselves, the vast majority wanted an independent third party evaluation. A federal government-operated or commercial government-accredited process was the most desirable. Many factors contributed to each organization's attitude toward certification, including sensitivity of the applications, corporate culture, time and cost considerations, mission criticality, past experience with vendors, and availability of assessment sources.

Administration

The vast majority of the organizations interviewed felt that administering computer security, particularly access control, was burdensome in a heterogeneous, distributed environment. Given their other responsibilities, this function took more time and effort than they felt was appropriate.

Interviewees wanted computer security-related products that would easily implement organization security policy and manage security functions. These functions included centralized network security administration and single logon for network data and services. Organizations felt that improved security administrator interfaces were essential to balance the increasing need for protection and limitations on the staff resources devoted to it.

Password Management

Most organizations felt that vendors should provide a strong password management capability at the operating system level and it should be tailorable to specific environmental needs. Along with that, most felt NIST should continue to promote research on improving the integrity of the identification and authentication process. Technologies such as smart cards, signature verification, and voice authentication have a potential place in an overall approach to security. However, for most organizations, only a low-cost solution would be practical due to a large number of users.

EDI Capabilities

For EDI to be a practical alternative to the exchange of paper, organizations want specific assurances that EDI messages are authentic and properly authorized. The goal of EDI technology is to provide the same capabilities as traditional

paper-based administrative functions with more efficiently and the same level of trust. This requires EDI standards that are part of the baseline operating system.

Add-on Packages

Several organizations described the need for a variety of add-on products. In some cases, these products are available, but do not interface with the already-purchased computer systems. In those cases, organizations felt that the add-on packages should be capable of working with a wider variety of machines.

An add-on package that provides separation of related duties is needed. Currently, this feature must be contracted out. Object-label association is neither a capability available within most systems nor is it encouraged through security standards. Organizations were interested in add-on products that would meet this need. They also felt that security standards for object-label association should be developed.

Currently, label-based mandatory access controls are not generally available as part of the operating system, but as an add-on. Since this type of access control will be used more and more by companies forming alliances with competitors, the capability to isolate and share information on a non-discretionary, formal "need-to-know" basis will be required.

Current Criteria

Although advances have been great, several organizations stressed that the current state of security technology criteria has failed to keep pace with technological advances in information processing. Computer security criteria needs to be kept current. In addition, criteria which addresses the evolving technology of networked computers is needed.

Current criteria also does not address procurement in an evolutionary fashion with computers interconnected to networks.

Security Standards for Multi-Vendor Systems

Those interviewed felt that security standards that allow comprehensive implementation of security across a multi-vendor environment have failed to emerge. The possible standards would provide for:

- interfacing many systems, both present and future;
- a single user view of security services across a wide range of operating systems; and
- security features inter-operating with other security services on both local and remote machines, without the need to train users in new security products.

The need to implement security should not limit an organization in choosing the best solution and integrating it into their existing system. Security technology must support users working effectively together.

Closing Thoughts

Because each organization has unique security needs, security products have been applied on a case-by-case basis in meeting individual computer security threats. Security at the operating system level, the application level, the organizational level, and the site level must be considered. Products need to flexible enough to consider a broad spectrum of security needs.

At the operating system level, basic capabilities that are adaptable to a variety of organizational policies and applications need to be part of a computer security baseline. These capabilities would be extensions so that more security can be inserted, such as a trivial password checker, or system build-in options, as well as enhanced system administrative capabilities, such as setting minimum-length password, creating roles, granting and revoking access and capabilities.

Security requirements evolve and cannot be totally specified at the time of product acquisition. Security capabilities need to include new system and network connections, while security managers need to be aware of changing laws and regulations.