TRUSTBLT.TXT

NCSL BULLETIN

Advising users on computer systems technology

July 1990

NCSL Bulletins are published by the National Computer Systems Laboratory (NCSL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. Bulletins are issued on an as-needed basis and are available from NCSL Publications, National Institute of Standards and Technology, B151, Technology Building, Gaithersburg, MD 20899, telephone (301) 975-2821 or FTS 879-2821.

The following bulletins are available:

Data Encryption Standard, June 1990

GUIDANCE TO FEDERAL AGENCIES ON THE USE OF TRUSTED SYSTEMS TECHNOLOGY

INTRODUCTION

Purpose. The purpose of this document is to provide initial guidance to federal departments and agencies on the use of trusted systems technology in computer systems which handle unclassified sensitive information.

Background. The National Institute of Standards and Technology (NIST) has received many inquiries from federal agencies regarding the applicability of Department of Defense (DoD) Standard 5200.28-STD, DoD Trusted Computer Systems Evaluation Criteria (TCSEC), and National Telecommunications and Information Systems Security Policy (NTISSP) Number 200, National Policy on Controlled Access Protection, to computer systems which are used to process unclassified sensitive information and which are covered by the Computer Security Act of 1987 (Public Law 100-235). The TCSEC, often called the "Orange Book," was developed by the National Computer Security Center (NCSC) of the National Security Agency (NSA). NTISSP 200 was published under authority of National Security Decision Directive (NSDD) 145 prior to the passage of the Computer Security Act, which established new federal authorities and policy on protection of unclassified computer

systems.

Authority -- NIST Responsibilities under Computer Security Act. The Computer Security Act of 1987 assigns NIST the responsibility for developing security standards and guidelines for federal computer systems, with the exception of classified and a specified category of Department of Defense unclassified systems (referred to as "Warner Amendment" systems). NIST is therefore responsible for advising all federal agencies on the use of trusted systems technology in most unclassified computer systems.

Objectives. Specific objectives of this document are to:

- provide guidance to federal agencies on the use of trusted systems technology;
- clarify the applicability of the TCSEC and NTISSP Number 200; and
- describe NIST's long-range plans for the development of additional policy, guidance, and technical recommendations on the use of trusted system technology.

Definition. Trusted Systems Technology - The technical methods and mechanisms that are used to develop trusted systems, are used to assure the enforcement of a security policy in such systems, and are contained within the trusted systems. Examples of trusted systems are trusted operating systems, trusted networks, trusted databases, and trusted applications. Examples of methods are modeling, software engineering, and automated evaluation. Examples of mechanisms include identification, authentication, auditing, and access control.

Applicability. This guidance applies to those federal computer systems defined in the Computer Security Act of 1987.

POLICY GUIDANCE

Use of Trusted Systems Technology. Each agency should select computer security controls, including trusted systems technology, for its systems which are commensurate with the estimated risk and magnitude of potential loss of confidentiality, integrity or availability. The selection should be based upon an analysis of the security risks for each system within its particular environment. Trusted systems technology can be particularly useful for agencies

with significant requirements for confidentiality of computer-based information. It can also provide basic access control protection to help meet information integrity requirements.

Applicability of NTISSP Number 200. There is no binding national policy on the applicability and use of trusted systems technology in federal computer systems which process unclassified information. In particular, NTISSP Number 200 does not apply to unclassified systems covered by the Computer Security Act of 1987.

USE OF TRUSTED SYSTEMS TECHNOLOGY

Value of Trusted Systems. NIST recommends the use of trusted systems technology when such technology satisfies requirements for adequate and cost-effective access control protection. Such requirements exist when there is a need for safeguarding the confidentiality and integrity of information. In addition, the assurance process which is a part of trusted systems technology can help support system availability requirements. All these requirements should be planned for and validated by a formal risk management procedure. As an integral part of the planning process required by the Computer Security Act, the first step in risk management is the conduct of a thorough risk analysis. The second step in risk management is selection of appropriate security controls based on the analysis of the security risks for the environment involved. This risk management process should balance security and performance requirements and provide for cost-effective security and privacy of sensitive information in the system. Effective use of trusted systems technology, like any other security control, should substantially increase the protection relative to the additional acquisition, operating and maintenance costs of the security mechanisms obtained.

Computer Security Planning and Protection Strategy. A security protection strategy consists of a mix of physical, administrative, and technical safeguards, including trusted systems technology. The use of trusted system technology can be an effective part of a larger computer security protection strategy for satisfying confidentiality, integrity, and availability requirements. As with other types of protection mechanisms, the benefits attainable from trusted systems technology can only be realized if these mechanisms are used properly in a complementary fashion.

Use of Evaluated Products. Agencies with a need for systems with trusted technology features should select those systems from NSA's Evaluated Products List (EPL). If EPL products are not available, then agencies may select or design systems that best meet their security requirements using the TCSEC as a guide. NSA's Information Systems Security Products and Services Catalog contains the EPL, which lists evaluated products, those systems that are currently undergoing evaluation, and the current status of such evaluations.

Use of Class "C2" Systems. Systems designed to meet "C2" or higher classes of the TCSEC should first be considered when acquiring multi-user computer systems with a requirement to control user access to information according to "need to know" and authorization. The "C2" and other TCSEC criteria were designed to achieve confidentiality through improved access control. The same access control mechanisms can also be beneficial for helping to maintain information integrity. While it should be recognized that access controls are a necessary part of achieving integrity and availability, there are other requirements for integrity and availability not covered by the TCSEC. NIST recommends that federal departments and agencies consider using "C2" functionality as a minimum to help protect their multi-user systems having confidentiality or integrity control requirements.

Use of Division "B" Systems. When acquiring multi-user computer systems with a requirement for mandatory separation of sensitive information and for which security labels can be established, systems designed to meet the criteria of the "B" division of the TCSEC can be useful. Systems in that division are designed to enforce a mandatory access control or multi-level security policy. However, the cost benefit considerations discussed earlier are of particular importance when considering the use of "B" division level systems. In the context of this guidance document, the term "security label" is used to denote confidentiality, integrity, or availability categories established pursuant to a larger organizational information security policy. Security labels are a generalization of the "sensitivity labels" used in the TCSEC.

NIST PLANS FOR DEVELOPMENT OF TRUSTED SYSTEMS GUIDANCE

NIST recognizes that federal agencies in their unclassified computer security programs will require additional guidance

on the use of trusted systems technology as it evolves. NIST has an active program to develop such guidance. This section describes some of the current activities designed to provide this guidance over the next few years.

National Evaluation Criteria. NIST plans to publish guidance on information and system integrity, focusing first on technical methods of achieving effective integrity controls in computer and telecommunications systems. NIST recognizes the benefits of TCSEC evaluated products and will work closely with NSA and other private and public sector organizations to create a set of national evaluation criteria that will emphasize integrity and availability to complement the TCSEC. NIST will work with NSA to extend NSA's evaluation program to incorporate these methods into trusted systems.

Security Criteria for Distributed Systems. NIST and NSA are studying the need for security criteria in distributed computer systems to address integrity, availability and confidentiality of unclassified information.

Security Labels. NIST also plans to work with government organizations and industry in developing suggested standard categories of data to which security labels, which would control the handling of that data, can be applied. The labels can be applied to categories of unclassified government and commercial information that require protection for confidentiality, integrity and availability purposes. These labels can then be used with "B" division trusted systems. Note that any security labeling scheme should complement an organization's information protection policy.

Guide to Use of Trusted Systems Technology. NIST is preparing additional guidance to assist federal agencies in deciding how to use trusted systems technology to protect computer systems containing unclassified sensitive information. This guide will include more detailed information on the extent to which that technology provides system-level confidentiality, integrity and availability protection for unclassified systems. The guide will stress the key point that the risk analysis-based process of identifying valid information protection requirements is an essential prerequisite for determining the full set of protection mechanisms (trusted systems included) to be effectively applied to computer systems. This guide can be viewed as complementing the NSA's "Yellow Book" (CSC-STD-004-85, Guidance for Applying the DoD Trusted Computer System

Evaluation Criteria in Specific Environments, June 25, 1985), which addresses the use of trusted technology in systems processing classified information.

International Evaluation Criteria. NIST is participating in international computer security standards activities that are specifying a wide range of security services and mechanisms in information technology. NIST recognizes the efforts and contributions of numerous international organizations presently developing security architectures, profiles, and criteria. Specifically, NIST is reviewing the Information Technology Security Evaluation Criteria (ITSEC) that have been proposed for European Community use and is preparing comments on their utility for U.S. Government unclassified applications.

REFERENCE DOCUMENTS

Computer Security Act. The Computer Security Act of 1987 was signed into law on January 8, 1988, therefore superseding NTISSP Number 200 for systems processing sensitive unclassified information. It established NIST's authority to develop uniform technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in federal computer systems, except those systems processing classified or Warner Amendment information. The Act also prescribed a process whereby agencies are required to prepare plans for the security and privacy of federal computer systems containing sensitive information.

NSDD-145. National Security Decision Directive (NSDD) 145, National Policy on Telecommunications and Automated Information Systems Security, was issued on September 17, 1984. NSDD-145 required federal agencies to establish policies, procedures, and practices to protect national security related information in computer systems. NSDD-145 established the National Telecommunications and Information Systems Security Committee (NTISSC) to develop and issue national system security operating policies.

NTISSP Number 200. The NTISSC issued NTISSP Number 200 on July 15, 1987. NTISSP 200 required multi-user computer systems containing classified or unclassified sensitive information operated by federal agencies and their contractors to have "controlled access protection" as a minimum level of security protection. Controlled access

protection is technically defined in the TCSEC as the "C2" class of trust. Further, NTISSP 200 required federal agencies and contractors to provide this controlled access protection in automated information systems containing sensitive information within five years (hence the well-known phrase "C2 by '92").

NIST'S COMPUTER SECURITY PROGRAM

For further information regarding other aspects of NIST's computer security program, including NIST's federal agency assistance program, please contact:

Computer Security Division
National Computer Systems Laboratory
Building 225, Room A216
National Institute of Standards and Technology
Gaithersburg, MD 20899
Telephone (301) 975-2934