Guidelines for Writing Trusted Facility Manuals

Table of Contents

NATIONAL COMPUTER SECURITY CENTER
FORT GEORGE G. MEADE, MARYLAND 20755-6000
NCSC-TG-016
Library No. S239,639
Version 1

FOREWORD

Guidelines for Writing Trusted Facility Manuals provides a set of good practices related to the documentation of trusted facility management functions of systems employed for processing classified and other sensitive information. A Trusted Facility Manual (TFM) is a document written by a system vendor that describes how to configure and install a specific secure system, operate the system in a secure manner, and make effective use of the system privileges and protection mechanisms to control access to administrative functions and databases.

Guidelines for Writing Trusted Facility Manuals is the latest addition to the "Rainbow Series" of documents. These publications are the product of the Technical Guidelines Program. The National Computer Security Center designed these technical guidelines to provide insight to the Trusted Computer System Evaluation Criteria requirements and guidance for meeting each requirement.

Recommendations for revision to this guideline are encouraged and will be reviewed by the National Computer Security Center through a formal review process.

Patrick R. Gallagher, Jr. October 1992
Director
National Computer Security Center

ACKNOWLEDGMENTS

The National Computer Security Center wishes to extend special recognition and acknowledgement for their contributions to this document to Infosystems Technology, Inc., and to Dr. Virgil D. Gligor of the University of Maryland as primary author and preparer of this document. Special thanks also go to the many computer vendor representatives, and members of the National Computer Security Center (NCSC) community who enthusiastically gave of their time and technical expertise in reviewing the material and providing valuable comments and suggestions.

Special recognition goes to Leon Neufeld, NCSC, who served as project manager for the preparation and production of this document.

PREFACE

Throughout this guideline there will be recommendations made that are not included in the Trusted Computer System Evaluation Criteria (TCSEC) as requirements. Any recommendations that are not in the TCSEC are prefaced by the word "should," whereas all requirements are prefaced by the word "shall." It is hoped that this will help to avoid any confusion.

Examples in this document are not to be construed as the only implementation that will satisfy the TCSEC requirement. The examples and literature citations provided herein are merely suggestions of appropriate designs and, possibly, implementations. The recommendations in this document are also not to be construed as supplementary requirements to the TCSEC. The TCSEC is the only metric against which systems are to be evaluated.

1 INTRODUCTION

The Department of Defense Computer Security Center (DoDCSC), established in January 1981, expands on the work started by the DoD Security Initiative. In 1985, the DoDCSC became the National Computer Security Center (NCSC) to reflect its responsibility for computer security throughout the Federal Government. The Director, NCSC, has the responsibility for establishing and publishing criteria and guidelines for all areas of computer security.

The principal goal of the NCSC is to encourage the widespread availability of trusted computer systems. In support of that goal, the NCSC created a metric, known as the DoD Trusted Computer System Evaluation Criteria (TCSEC), against which computer systems could be evaluated for security. The DoDCSC originally published the TCSEC on 15 August 1983 as CSC-STD-001-83. In December 1985, the DoD adopted it, with a few changes, as a DoD Standard, DoD 5200.28-STD. DoD Directive 5200.28, Security Requirements for Automated Information Systems (AIS) requires the TCSEC to be used throughout the DoD. The TCSEC is the standard used for evaluating the effectiveness of security controls built into Automated Data Processing (ADP) systems. The TCSEC has four divisions: D, C, B, and A, ordered in a hierarchical manner with the highest division (A) being reserved for systems providing the best available level of assurance. Within divisions C, B, and A, a number of subdivisions, known as classes, are also ordered in a hierarchical manner to represent different levels of assurance in these classes.

1.1 Purpose

A Trusted Facility Manual (TFM) is one of the documents necessary to satisfy the requirements of any class in the TCSEC. The TFM is directed towards the administrators of an installation, and its goal is to provide detailed, accurate information on how to (1) configure and install a specific secure system, (2) operate the system in a secure manner, (3) make effective use of the system privileges and protection mechanisms to control access to administrative functions and databases, and (4) avoid pitfalls and improper use of the administrative functions that would compromise the Trusted Computing Base (TCB) and user security.

The importance of the TFM in supporting the operation of a secure computer system cannot be over estimated. Even if one assumes, hypothetically, that all users of a system and their applications are trusted, and that they will use all of the available protection mechanisms correctly, the system may still be administered and operated in an insecure manner. This may be especially true when administrative users lack the skill, the care, or the interest to use the system properly. Furthermore, the security damage that administrative users can cause by careless use, or deliberate misuse, of administrative authority is significantly larger than that caused by ordinary users. Although use of a detailed, accurate TFM cannot address or counter deliberate misuse of administrative authority, it can help minimize chances of misuse due to lack of awareness of proper system use. To help minimize these instances of system misuse, the TFM should include examples of both proper uses and warnings about consequences of misuse of administrative functions, procedures, privileges, and databases.

This guideline presents the issues involved in writing TFMs. Its objectives are (1) to provide guidance to manufacturers on how to document functions of trusted facility management implemented by their systems and (2) recommend a TFM structure, format, and content that would satisfy the TCSEC requirements. The recommendations made herein should not be considered as the only means to satisfy the TCSEC requirements. Additionally, this document contains suggestions and recommendations derived from the TCSEC objectives but which are not required by TCSEC in the TFM area. For example, the TFM may include documentation required by the TCSEC in the areas of System Architecture, Design Documentation, and Trusted Distribution. The inclusion of this documentation in a TFM instead of other separate documents is optional.

1.2 Scope and Contents

The TFM should give specific guidance to administrative users on how to configure, install, and operate a secure computer system, and should clearly illustrate the intended use of all security features, citing actual system commands and procedures. Although a high level of detail in illustrating key security concepts would benefit administrative users, the TFM cannot be considered to be, nor can it be, a training manual in the area of computer security in general, nor in the area of system administration in particular. Instead, the TFM user is assumed to have some familiarity with the notion of trusted systems within the realm of computer security. The TFM will provide the user with detailed information on how to administer and operate a specific trusted system in a secure manner.

Many different organizations of the TFM are possible. For example, an acceptable TFM format would provide a separate section describing specific security responsibilities of any separate administrative roles, such as those of the security administrator, auditor, system programmer, operator, that are supported in the system; available commands for each role; use of each command; parameter and default settings; specific warnings and advice regarding the use of functions, privileges and databases of that role; and the specific responsibilities of that role for TCB security. Use of this format is advisable for manuals of systems in higher security classes, namely B2, B3, and A1, where separation of administrative roles is required.

An equally acceptable TFM organization and section format would provide a separate section for each functional requirement area of the TCSEC, namely, for security policy (e.g., Discretionary Access Control (DAC), Mandatory Access Control, (MAC)), accountability, and TCB protection. Each section would include available commands, system calls, and procedures relevant to that area; use of each command (including the effects of each command when used by different administrative roles); parameter and default settings; and specific warnings and advice regarding the use of functions, privileges, and databases available to commands of that area. Use of this alternate format is advisable for lower security classes, namely C1–B1, where the TCSEC does not mandate any separation of administrative roles. Either of the two alternate TFM formats mentioned above is equally acceptable for all TCSEC security classes as long as the TFM satisfies the TCSEC requirements. Furthermore, other TFM formats would also be acceptable as long as they satisfy the stated TCSEC requirements. The TCSEC neither requires nor suggests a specific TFM format.

This guideline contains eight additional sections. Section 2 defines the security and accountability policies and mechanisms of systems. Section 3 identifies and explains the security-relevant and security-irrelevant functions of an administrator. Section 4 identifies and explains the use of TCB commands and interfaces used by administrative users. Section 5 defines day-to-day routine operations performed by administrative users and the security vulnerabilities of these operations. Section 6 identifies all TCB security and integrity responsibilities of administrative users.

Section 7 presents recommendations for writing the TFM that satisfy the requirements of the TCSEC. Section 8 is a glossary. Section 9 lists the references cited in the text. Each section consists of three parts: a statement of purpose, an explanation of how that purpose can be achieved, and an outline summarizing the recommendations made.

These guidelines apply to computer systems and products built or modified with the intention of satisfying the TCSEC requirements.

1.3 Control Objectives

The control objectives for the TFM are similar to those of other documentation areas of the TCSEC. They refer to what should be documented in a particular area, such as the trusted facility management, and how this documentation should be structured. Thus, the control objectives for writing the TFM are:

(1) the TFM shall address all the requirements specified by the TCSEC that are relevant to it; and
(2) the TFM shall provide detailed, accurate information on how to:
  - configure and install a specific secure system;
  - operate a system in a secure manner;
  - avoid pitfalls and improper use of administrative functions that would compromise system and user security.

1.4 TFM Introduction

The purpose of this section in the TFM is to explain the scope, use, and contents of the TFM of a particular system. In general, the scope of the TFM should include explanations of how to configure and maintain secure systems, administer and operate them in a secure manner, make effective use of the system's privileges and protection mechanisms for administrative use, and avoid pitfalls and misuse of administrative authority. Depending on the particular computer system, the complexity of trusted facility management may differ and thus the scope of the TFM may differ accordingly. For example, in large systems, system configuration and installation is a complex activity described in a separate system administration manual that may, or may not, include the other important areas of the TFM. In contrast, system configuration and installation is a relatively simple activity defined in a single chapter of a TFM for a small system, such as a multi-user workstation.

The introduction to the TFM should also discuss the recommended use of the manual. In particular, this section should define the skills and general computer systems and security background assumed for administrative personnel. This is necessary because different administrative functions require different levels of skill. For example, an individual in the system programming staff that configures, installs, and maintains the TCB code often needs considerably more technical skills than an individual in the accounts management staff. Similarly, a security administrator needs more detailed knowledge of the system security policy and accountability than individuals assigned to operator's roles. The definition of required skills and background is important in aiding the management of a particular organization in assigning appropriately trained individuals to various administrative tasks.

In defining the use of the TFM, the introductory section should also include a list of other system manuals that may be consulted by the administrative staff. For example, most administrators may benefit from an understanding of the Security Features User's Guide (SFUG). Most system designs use the DAC mechanisms described in the SFUG for protection of, at least, some administrative files, and may use the trusted path mechanism to prevent spoofing of administrative commands. Similarly, whenever manual sections that logically belong in the TFM are in fact provided in other manuals --- system configuration and installation manuals, and system reference manuals containing descriptive top-level specifications (DTLSs) of commands and interfaces used by administrative users---the TFM Introduction should include references to these additional manuals. The TFM should place the references to these manuals in context and provide a brief synopsis of the relevant information from the specific manual citation. This citation would help narrow the reader's focus to a few pages of the referenced manual. Furthermore, references to documents, manuals, and standards that may be beneficial to some administrative personnel, such as password management and use guidelines and standards, should be made in this section. References to educational and training documents that are helpful to administrative personnel may also be included here.

The TFM writer may also want to define the limitations of the TFM in terms of security scope. For example, some security issues such as personnel background verification, assignment and maintenance of users' trust levels, physical system and environmental security, proper use of cryptographic techniques and devices, and procedures that assign individuals to administrative roles, generally fall outside the scope of TFM definition. Explicit recognition of such limitations enables the management of a secure facility to plan countermeasures for areas of vulnerability not countered by the trusted systems.

Finally, the introductory section of the TFM should include a "road map" defining the contents of each TFM section and possibly the relationships between various manual sections. This road map may also identify the self-contained sections of the manual that can be read independently of other sections.

In summary, the introductory section of the TFM should include:

(1) Scope of the manual
- guide the configuration and installation of secure systems;
- guide the operation of a system in a secure manner;
- enable administrative personnel to make effective use of the system's privileges and protection mechanisms;
- issue warnings about possible misuse of administrative authority.

(2) Recommended use of the manual

- review skills and systems background necessary for administrative personnel;
- suggest additional manuals, reference material, and standard, needed by administrative personnel;
- specify the limitations of security scope;

(3) TFM contents
- contents of each section;
- section relationships.

2 SYSTEM SECURITY OVERVIEW

The purpose of this section of the TFM is to define the security and accountability policies and mechanisms of the system that are designed to counter a set of perceived threats. The focus of this section should be on the administrative-user functions available to counter threats, the privileges and protection mechanisms available to administrative users, and the general vulnerabilities associated with actions of administrative users. This section should also include a list of dependencies on other security measures, such as those for the maintenance of physical security, which, although not required by the TCSEC, should be taken into account by the management of the system installation and by system accreditors.

2.1 Threats

Examples of the general security threat handled by systems built to satisfy a TCSEC class is that of unauthorized disclosure of information through either unauthorized direct or indirect access to system and user objects through system failures, subversion, and TCB tampering or through use of covert channels. The manual should describe some of the common attacks that cause unauthorized disclosure of information, in the context of the specific system. These examples might include the use of Trojan horses in untrusted shared programs, the use of covert channels by untrusted users and applications, the use of known penetration methods that cause unauthorized disclosure of sensitive or proprietary information, and the misuse of access authorization to retrieve and disclose sensitive information (e.g., insider attacks).

2.2 Countermeasures Based on Security and Accountability Policies and Procedures

This section of the TFM should include a brief discussion of the protection mechanisms available in the system that help counter the threats defined in the above section. This discussion should serve as a summary of the protection philosophy used in the design and implementation of the protection mechanisms and should include a presentation of the role of security policy (both discretionary and mandatory policy, if any), accountability, and assurance (both operational and life-cycle assurance). The dependency of the system security mechanisms on administrative-user actions should be emphasized here.

This section should point out clearly the types of threats that can, or cannot, be countered by a specific policy or mechanism. For example, this section should state that DAC mechanisms cannot, and are not meant to, prevent or contain threats posed by Trojan horses implementing time bombs, trap doors, or viruses placed in shared, untrusted applications [2]. DAC mechanisms cannot, nor are they meant to, detect or prevent access performed by an authorized subject on behalf of an unauthorized subject (e.g., the surrogate access problem [3]). Furthermore, DAC mechanisms are not, nor were they ever claimed to be, capable of controlling information (as opposed to access privilege) flows. Only MAC can handle these problems.

This section should discuss, in the context of the specific system, the role of specific accountability mechanisms and policies in countering security threats not handled by access control mechanisms. An example is the use of audit mechanisms to complement access control mechanisms in the sense that they can detect attacks initiated by authorized users (i.e., by "insiders"), or that trusted-path mechanisms are required to prevent spoofing, a threat not usually countered by access control mechanisms or policies.

The emphasis in describing the above-mentioned threats and countermeasures should be on the identification of the TCB mechanisms and policies that counter a specific threat. For example, the summary of the countermeasures supported by the system should include the basic assertion (and in other design documents, the justification) that the TCB itself is non-circumventable and tamper proof. Additional points of emphasis may be that all countermeasures supported in the system require the interaction of both access control and accountability mechanisms, and that these mechanisms should be employed by both ordinary and administrative users. This section should provide examples of interaction between ordinary and administrative user decisions to illustrate both the positive and negative consequences of such interaction.

2.3 Explicit Physical Security Assumptions

The TCSEC does not include requirements for physical security of the system installation. However, the TFM should include a section or a subsection that states the physical security assumptions made by the system designers. These assumptions should be satisfied by the management of the organization responsible for deploying the system, as the evaluation of physical security is the responsibility of the system's accreditors.

The explicit inclusion of the physical security assumptions made by designers in the TFM will provide the accreditors with the necessary input for the deployment of the system in different operational environments and provide the administrative users an important input for the sound definition of the system security profile. For example, systems that do not provide trusted paths for administrative users usually assume that a set of terminal ports is reserved for the connection of administrative consoles that are physically separated from the rest of the user terminals for the entire lifetime of the system. Also, a common assumption is that the system definition of the security profile ensures that the level of trust associated with the physical environment containing a system's peripheral will always dominate the maximum sensitivity associated with that peripheral. Similarly, this section should emphasize that systems allowing legitimate users to access their components (e.g., removable media) should be used only in environments where both administrative and ordinary users are trusted to access all data in the system and are trusted not to misuse their physical access permissions. (In such environments, the use of untrusted applications may still require the use of trusted systems even though all users are trusted to access all data.) In systems that do not allow users to access the system components, or when the above level of user trust cannot be guaranteed, the TFM should suggest the physical controls necessary to counter, or deter, the potential threat of physical access to system components. The presentation of the physical security assumptions made by system designers should enable accreditors to determine the security risks and exposures assumed by system use as well as the required countermeasures.

2.4 Protection Mechanisms Available to Administrative Users

The security of any system depends directly on the security of the administrative commands, interfaces, and databases. For this reason, administrative commands, privileges, and databases shall be protected from ordinary users, and in some TCSEC security classes, shall be separated on a role basis. This section should identify the protection mechanisms available to administrative users to ensure that these users are aware of the means available to control access to their commands, privileges, and databases.

All protection mechanisms that can be manipulated by ordinary users are also usually available to administrative users. For example, all user identification and authentication, and DAC mechanisms are available to administrative users. In addition to mentioning these mechanisms, which the SFUG already defines, this TFM section should include the description of the mechanisms available only to the administrative users and the mode of their safe use. For example, the use of special trusted-path mechanisms based on physically protected, hard-wired consoles, which may allow the invocation of command processors available only to administrative users, and the use of audit mechanisms to detect potential intrusion by authorized users, are only a few of the protection mechanisms specific to administrative users [7].

2.5 Security Vulnerabilities and Warnings

This section should describe the security vulnerabilities of administrative commands and procedures, and should suggest specific ways to counter them. Reference [7] cites generic examples of common vulnerabilities of administrative roles and role-specific vulnerabilities. In addition to similar examples, this TFM section should include a discussion of system-specific vulnerabilities and countermeasures required in the assumed environments of system use.

In any system, design and implementation assumptions are made about administrative actions and their sequence of use. For example, the loading of a system during the installation phase, and the installation itself, may require the use of special administrative commands in a specific sequence. The definition of a user security profile may require that administrators do not reuse user and group identifiers, and that the definition of the system security profile prohibits the reuse of bit encodings of sensitivity levels without careful analysis of consequences. Other potential vulnerabilities, such as those resulting from mismanagement of audit logs and post processing of files (in on-line, off-line, and hard-copy form) should also be explained here. Design and implementation assumptions should be stated explicitly in this section to ensure that administrative users are aware of the negative consequences of not satisfying these assumptions.

2.6 Separation of Administrative Roles

Security classes B2-A1 of the TCSEC require that the roles of the administrative users be separated. This requirement means that the commands, procedures, privileges, and databases of the various administrative roles shall be separated by system design and shall be documented as such. Role separation of classes B3 and A1 also requires the separation of security-relevant functions from the security irrelevant ones. Reference [7] cites the rationale and the means of achieving role separation in trusted systems.

The TFM shall define each separate role supported by the system. Each role should be clearly defined in terms of the commands and TCB interfaces available to the role, the use of each command, the command effects and exceptions (whenever these are not defined in the DTLS of the TCB), parameter and default settings, specific warnings for the command use, and advice. The TFM should also define the specific security mechanisms used to protect privileged commands and data used by administrators.

In summary, the TFM section presenting the system security overview for administrative users should include the following subsections:

- 2.1 Threats to System Security
- 2.2 Countermeasures Based on Security Policy and Accountability
- 2.3 Explicit Physical Security Assumptions
- 2.4 Protection Mechanisms Available to Administrative Users
- 2.5 Security Vulnerabilities of Administrative Users and Warnings
- 2.6 Separation of Administrative Roles (for classes B2-A1)

3 SECURITY POLICY

The purpose of this section is to identify and explain the security-relevant and security-irrelevant functions of the administrators. In particular, this section should explain, in the area of security-relevant functions, the use of the TCB commands and interfaces by administrative users to initialize discretionary access privileges, to set default user accesses to system objects after user registration, and to distribute, review, and revoke access privileges on behalf of users in systems that implement DAC in a centralized way (2]. In systems that support MAC, this section also identifies and explains the use of TCB commands and interfaces by administrators to define and change the system security profile (e.g., the system-sensitivity map, sensitivity level limits for system devices, and file systems), to define and change object sensitivity levels (e.g., label imported, unlabeled data, and media), and to change the trust level of active subjects, whenever such a function is supported. This section also should define the administrator's interfaces for other functions related to the support of DAC and MAC, such as changing object ownership, restoring privileges deleted accidentally, destroying errant processes, running consistency checks on system and user security profiles, and managing user accounts.

Reference [7] outlines the role of the security administrators in support of the security policy defined in a system. The TFM should specify the commands, system calls, functions, their parameters and default settings provided for each area of security policy and support, and should provide examples of use, potential misuse, and security implications of command misuse. For example, the TFM should explain how the administrator can change the sensitivity label of an object or a subject, and cite the expected security consequences Of such action and also how the administrator may determine the consequences of such a change in the given system. Similarly, the administrator may decide to reuse a binary representation of a sensitivity level to define a new sensitivity level. For this process, the manual shall state the circumstances in which this change is allowed, if ever, and should explain the conditions under which this change is safe. All commands, system calls, and functions should be defined in terms of their effects, exceptions, and parameters. The use of commands should be illustrated by examples showing the correct settings of various command options. This section should describe the recommended reactions of the administrator to such exceptions (unless these reactions are already described in the call/command DTLS).

The administrative functions and interfaces used in supporting the security policy have potential vulnerabilities. Reference [7] outlines some of these generic vulnerabilities. The TFM shall include warnings of all known specific vulnerabilities in the given system and possibly suggest means of reducing system risk associated with such vulnerabilities. Minimally, the TFM should specify the dependencies of the administrative roles on external policies and procedures that would help reduce system risk associated with identified vulnerabilities.

In summary, the security policy section of the TFM should include the following subsections (whose contents are discussed in more detail in reference [7]):

3.1 Discretionary Access Control
- TCB commands and interfaces used to initialize DAC privileges and defaults;
- TCB command interfaces to distribute, review, and revoke user privileges in systems that support centralized DAC;
- group membership definition and impact on DAC.
- change of object ownership (if any), restoration of accidentally deleted privileges, destruction of errant processes;

3.2 Mandatory Access Control
- TCB commands and interfaces to define and change system security profile; classify, reclassify and import objects; and change trust level of active subjects;
- consistency checking of system security and user profiles.

3.3 Management of User Accounts
- definition and deletion of user and group accounts and identifiers.

3.4 Command System Call and Function Definitions
- effects and exceptions (if not defined in DTLSs);
- parameter and default settings;
- examples of command use and potential misuse.

3.5 Warnings of Specific Vulnerabilities of Administrative Procedures and Activities Related to Security Policy.

4 ACCOUNTABILITY

4.1 Identification and Authentication Functions of Administrative Users

The purpose of this section is to identify and explain the use of TCB commands and interfaces that should be used by administrative users to set up user security profiles, and to determine authentication and authorization parameters associated with the user identification and authentication mechanism. Reference [7] defines the role of the security administrator in the identification and authentication area. The TFM shall specify the commands, system calls and functions, and their parameters and default settings that are provided by the specific system, and should provide examples of the use, or potential misuse of these commands, and the security implications of command misuse. For example, the TFM should explain how the administrator can initialize user passwords, can distribute special passwords to other administrative users, and set up account restrictions (e.g., restricted time intervals for login, account cutoff). The commands that allow the definition of user and group identifiers shall include an explanation of how these identifiers should be chosen, why they should not be reused, and what the consequences of identifier reuse are.

In most systems, the setting of the user security profile also includes the definition of some discretionary privileges associated with the user account. For example, in systems that use groups to enforce DAC policies, administrators define the group membership. The TFM shall explain the consequences of adding or deleting a user identity to a group in terms of the added or lost discretionary privileges, and provide appropriate warnings. In systems where the user security profile also includes the specification of the maximum level of trust for each user, the TFM shall also discuss the security implications of incorrect definition or change of these levels and the interactions between these levels and the sensitivity levels of various system components (defined in the system security profile). It should also include examples of and warnings about such changes. The commands available to system administrators also include those to define and change the parameters of the login/logout mechanism used by a system. Consequently, the TFM should explain how to define these parameters, which include the time-out period, multiple login attributes, maximum Iogin time, and limits on unsuccessful logins from a terminal or into an account [7] (e.g., specific commands, command options, formats, parameter ranges, and default values). Whenever the trusted path mechanisms available to administrative users require special procedures, such as use of specific hard-wired consoles, the TFM shall specify how the administrative users can use the trusted path mechanism in a secure manner.

The TFM shall also explain the implications of the system security profile definition in providing authorization data for user log ins. For example, a terminal's maximum and minimum sensitivity levels provide cutoff values for whether a certain user login level can be used and whether a certain user with a given user and group level clearance can log in at all from a given terminal. The relationship between the terminals minimum and maximum sensitivity levels and the user's clearance level shall be explained so that consistent levels can be defined for both terminal sensitivity and user level of trust.

Finally, administrator commands for temporarily terminating a user access to the system and for permanently deleting the user account shall be defined, and the implications of such actions defined. This section should also include warnings about potential vulnerabilities, such as object ownership set to the identity of an user or account that is no longer valid, or the reuse of an old identifier, that persist when a user account is not deleted correctly or completely, and examples of such vulnerabilities [7].

For all administrative commands defined in this and other system security areas, this TFM section should include an explanation of all exceptions and, possibly, a administrator's recommended response to these exceptions. (This reaction may already be described in the system call/command DTLS). All administrative data bases that are accessed by these commands should be identified showing how they are, or can be, protected. All mechanisms available for the protection of the identification and authentication data shall be clearly explained. The use of these mechanisms should be illustrated by examples.

4.2 Audit

The purpose of this section of the TFM is to familiarize administrative users with the TCB commands and interfaces of the system's audit mechanism. These commands include those that enable or disable the audit selectivity mechanism (e.g., audit-event setup and change), those that help manage the audit trails (logs), those that perform data compression and post processing analysis, and in classes B2---A1, those that set correct channel delays and randomize variables.

Some system includes a set of audit events that should always be selected for audit to ensure the consistency of subsequent events selected by the auditor and the proper functioning of the post processing tools. These events should be explicitly highlighted for special discussion in the list of auditable events supported by the system. The complete list of events shall be defined in the TFM. The audit selection mechanism should also be presented, and examples of use should be provided. Commands of the audit selectivity mechanism include those that turn on and off events on a per-user, per-process, per-terminal, per-sensitivity-level, or per-object basis. In TCSEC classes B3 and A1, the commands that turn on and off events representing accumulations of other auditable events and audit-system alarms (if any) shall also be presented.

Systems that support audit mechanisms include commands that help manage the audit files. These commands, which include those to create new and destroy old audit logs, to change audit log size and warning points, to display, format, and compress audit data, and to check the consistency of the audit database after crashes, and when these changes take effect, shall also be included in the TFM. The procedures that shall be used by auditors to ensure that the audit files do not overflow shall also be presented. The format in the audit log file of each record field and of each type of auditable event shall be presented and explained. Commands for post processing of audit logs (if any) shall also be included in the TFM. Systems designed to satisfy the B2---A1 security requirements need to have covert channels restricted to certain limits. One means of reducing covert channel bandwidths is by placement of delays and by setting of randomization variables in system kernels and trusted processes. Commands that accomplish this task should be presented in the TFM of these systems along with a description of the covert channel handling policy recommended for enforcement. These recommendations should be derived from the covert-channel analysis guideline of the TCSEC and are important because they affect not only the security policy and the accountability areas of the system, but also system performance. Reference [7] defines the administrative functions necessary to support audit activities. As suggested in the covert channel guidelines of the TCSEC, bandwidth reduction policy should be coordinated with audit policy. For this reason, the TFM should present the bandwidth reduction policy in the same section with that presenting the audit policy.

Recommendations on audit procedures should also be included in the TFM. These procedures would suggest auditing groups of specific events that may reveal misuse of access privileges, potential system-penetration attacks, and covert channel usage. They may also suggest the frequency of audit review and provide advice on how to manage audit files on-line and off-line.

For commands used by administrative users for audit, the TFM should include a description of their effects and exceptions, and should provide examples of use, potential misuse, and security implications of command misuses. Recommendations for administrator's reactions to command exceptions should also be made. Reference [7] provides examples of vulnerabilities caused by misuse of audit command and authority. These examples include loss of audit log consistency, loss of audit logs, loss of user privacy, and various forms of denial of service. Specific instances of vulnerability in a given system and possible suggestions for reducing the system's exposure to such vulnerabilities should also be included in the audit section of the TFM.

In summary, the accountability section of the TFM should include the following subsections:

4.1 Identification and Authentication
- TCB commands and interfaces for setting up user security profiles and authentication and authorization parameters of the login mechanism;
- password distribution to ordinary and administrative users, management of password generation, and protection of passwords;
- account restrictions (e.g., restricted time intervals for log in, and account cutoffs);
- choice of user and group identifiers;
- maximum levels of trust for users and groups;
- computation of the current level of trust for subjects (e.g., subject's clearance).

4.2 Definition and Change of System Parameters of the Log in Mechanism and when they take effect
- timeout interval;
- multiple login attributes;
- maximum login time;
- limits on unsuccessful logins from a terminal or to an account;
- use of special trusted path mechanisms for administrative users.

4.3 Audit Mechanisms
- audit-event selection mechanisms (e.g., audit-event setup and change);

- management of audit logs (e.g., protections of audit logs);
- functions for formatting, compressioning, and postprocessing of audit files;
- interfaces for setting of covert channel delays and randomization of variables;
- description of audit log and event formats.

4.4 Commands, System Calls and Function Definition

- effects and exceptions of each command of the accountability area (if not defined in DTLSs);
- parameter and default settings;
- examples of use and potential misuse.

4.5 Warnings of Specific Security Vulnerabilities of Administrative Activities and Procedures Related to Identification, Authentication, Trusted Path and Audit

5 ROUTINE OPERATIONS

The purpose of this section of the TFM is to define the routine operations performed by administrative users, describe the operation's security, describe the vulnerabilites associated with these operations, and provide appropriate warnings. These operations are carried out, in most cases, by execution of appropriate commands from a system console. However, in some instances, these operations involve manipulation of physical devices, such as printers, storage devices, removable media, communication switches, and modems. For this reason, this TFM section may differ from the rest of the TFM. It should contain not only definitions of specific commands and TCB interfaces, but also procedures and policies for secure use and manipulation of hardware devices.

Routine operations of administrative personnel include both security-relevant and security-irrelevant operations. Security-relevant functions include those that boot and shut down the system, set system clocks, identify damaged user volumes and files, perform TCB backups and on-line device tests, run system integrity tests, and respond to user requests to mount/unmount volumes. Routine security- irrelevant operations include those that perform system metering, and that require operator response to various user requests [7]

This section the TFM should include a description of each command used for routine operations, including its effects and exceptions, and should provide examples of use, potential misuse, and security implications of command misuse. Examples of vulnerabilities of security-relevant, routine operations include the booting of an old version of the TCB, causing inconsistency problems for users; system shutdown while still in normal operation causing loss of files and file system inconsistencies; and inadequate use of devices and device interfaces (e.g., printers).

This section the TFM should also include descriptions of administrative commands that perform security-irrelevant routine operations. These commands include those traditionally performed by account administrators, such as commands used for maintenance of accounting files, for turning on and off accounting, for running accounting tools, for collecting statistics of system and resource usage, and billing information.

Administrative policies and procedures that define security-relevant handling of devices shall also be included in the TFM. For example, procedures to install, activate, and set the current sensitivity level of a printer within the pre-defined range should be defined, and examples of the installation procedure should be given. In summary, the TFM section defining the routine administrative operations and procedure in the following subsections:

5.1 Security-Relevant Procedures and Operations
- running of system diagnostics;
- system boot and shutdown;
- setting of system clocks;
- identification of damaged user files and volumes;
- routine backup of TCB files;
- on-line device testing;
- response to user requests to mount/unmount volumes;
- handling of peripheral devices, removable storage, and output (e.g., printers, printer output, diskpacks, tape reels).

5.2 Security-Irrelevant Procedures and Operations
- back-up of user volumes;
- system metering;
- response to various user requests;
- user account administration;

5.3 Commands, System Calls and Function Definitions
- effects and exceptions of each command of the routine operations area (unless defined in the DTLSs);
- parameter and default settings;
- examples of use and potential misuse.

5.4 Warning of Specific Security Vulnerabilities of Routine Operations

6 SECURITY OF THE TCB

The two purposes of this TFM section are to identify and explain all aspects of TCB security and integrity that become the responsibility of administrative users. Because the security of all user programs, data, and application subsystems is provided by the TCB, the maintenance of TCB security and integrity is one of the most sensitive administrative functions.

Maintenance of TCB security spans the entire system life cycle. It includes procedures for strict configuration management during system development and use, and for secure system distribution, installation, and local maintenance. In some cases, administrative users are allowed and required to generate another evaluated version of the TCB from source code (e.g., make changes to the TCB source code and regenerate the TCB on site). In such cases, the TFM shall include detailed descriptions of procedures that generate a new TCB version from source code, the necessary system commands, the list of approved tools (e.g., compilers, linkers, loaders) for TCB generation, examples of command use, warnings of possible problems in generating a new TCB, vulnerabilities that may affect TCB security, and configuration management.

The TFM shall also provide, or reference a separate document that provides, a description of command exceptions, appropriate warnings, and possible exception handling advice. The TFM should also provide, or reference a separate document that describes, the configuration management tools. The TFM shall include descriptions of the procedures that must be followed by site administrators to install new releases of the TCB.

TCB security may be violated during installation and maintenance (see [7]). For this reason, the TFM shall provide a description of the TCB installation procedures, including the required commands, exceptions, parameter settings, required system configuration, warnings, and advice. The installation procedures should contain descriptions of the TCB data structures that must be initialized by the user, and of the TCB loading. Also, the installation procedures should include a list of tools (e.g., editors, loaders) approved for TCB installation and an appropriate description of secure installation assumptions (e.g., administrative procedures, such as those that require physical audit of the installation procedure by independent personnel).

All TCB maintenance procedures shall be defined in the TFM. These procedures should include analyzing system "dumps" after crashes, conducting crash-recovery and restart actions, performing consistency checking of TCB files and directories, changing system configuration parameters (e.g., table sizes, devices, and device drivers), running periodic system integrity checks, and repairing damaged labels. A list of the approved tools for TCB maintenance, relevant commands, exceptions, warnings, and advice should also be included in this section.

The ability to install and maintain a system's TCB in a secure manner requires that administrative users be cognizant of all TCB modules. Administrators should especially be cognizant of those hardware modules containing the reference monitor mechanism, and of all the of default file protections for TCB files or objects. If available, the command needed to run a tool that checks the correct privilege and sensitivity-level initialization for TCB files or objects shall be identified and its use illustrated. Thus, either the TFM itself shall provide a list of all TCB modules, including their interfaces, and shall specify the TCB file or object privileges necessary to protect the TCB or the TFM shall list a separate document that does.

The TFM shall include warnings and advice on how to handle both generic and system-specific vulnerabilities (if any) of TCB installation and maintenance. For example, administrative users should be warned that interchanges of dedicated- console and user-terminal communication lines can cause potential loss of trusted path for administrative users, that placement of extraneous code in the TCB configuration may result from using an unapproved tool, and that running a borrowed untrusted program under administrative identity may cause an untold number of TCB security problems [7].

Finally, the TFM shall include a description of policies and procedures that define the distribution procedures for a trusted system (i.e., a class A1 requirement). These policies and procedures shall be used to maintain the integrity of the mapping between the master copy defining the current version of the TCB and the on-site installed copy.

In summary, the TFM section that defines the security measures necessary for protection of the TCB should include the following subsections:

6.1 The Generation of the TCB Source Code
- list of TCB code modules, module interface and data (including modules of the reference monitor);
- list of approved tools for TCB generation
- procedures for TCB generation;
- vulnerabilities.

6.2 Configuration Management Policy (if required, reference to a separate configuration management document)

6.3 Ratings-maintenance Plan (if applicable, reference to a separate rating maintenance document)

6.4 TCB Installation Procedure
- TCB generation from source code (whenever allowed by the system manufacturer);
- TCB hardware installation;
- TCB data structure initialization;
- TCB loading;
- setting of TCB file protection;
- list of approved tools.

6.5 TCB Maintenance Procedures
- analysis of system dumps;
- crash recovery and restart;
- changes of configuration parameters;
- repair of damaged TCB data structures;
- consistency-checking procedures;
- running of periodic system-integrity checks

6.6 Trusted Distribution of the TCB
- policies and procedures;
- correspondence between master copy and installed copy

6.7 Commands, System Calls, and Function Definitions for TCB Generation from Source Code, Installation, Maintenance, and Trusted Distribution
- effects and exceptions (unless defined in DTLSs);
- parameter and default settings;
- examples of use and potential misuse.

6.8 Warnings of Specific Security Vulnerabilities of TCB Generation, Installation, Maintenance, and Distribution

7 SATISFYING THE TCSEC REQUlREMENTS

This section of the TFM should contain the definition of the TFM requirements on a TCSEC class basis. All of the requirements listed below derive from corresponding documentation requirements and objectives of the TCSEC. Although similar TFM requirements appear in multiple classes, the contents of TFM sections shall reflect the complexity of policy, accountability, assurance, and documentation of the evaluation class. Consequently, this section should contain suggestions and recommendations that may not be found in the TFM requirements area but that derive from other TCSEC areas. These suggestions and recommendations illustrate the added complexity of various TCSEC classes.

7.1 Requirements and Recommendations for Security Class C1

The TFM of a C1 class system may have the following structure:

7.1.1 TFM Introduction

The TFM introduction may include the following topics:

Scope of the TFM
- guide to configure and install secure systems;
- guide to operate a system in a secure manner;
- enable administrative personnel to make effective use of the system's privileges and protection mechanisms;
- issue warnings about possible misuse of administrative authority.

Recommended use of the TFM
- review skills and systems background necessary for administrative personnel, suggest additional manuals, reference material, and standards needed by administrative personnel;
- specify the limitations of security scope;

Contents of the TFM
- contents of each section;
- section relationships.

(For specific DAC requirements, the reader should refer to [2].)

7.1.2 System Security Overview

This section of the TFM shall include a brief description of the system administration vulnerabilites specific to the given system, warnings, and advice on how to counter these vulnerabilities.

> "A manual addressed to the ADP administration shall present cautions about the function and privileges that should be controlled when runninga sucure facility [6]."

The above TCSEC requirement sugguest that the administrative functions and privileges that need to be controlled when running a sucure facility shall be identifies, and the vulnerabilities associated with those functgions and privileges shall be determined. Warnings relatiing to thes vulnerabilites shall be presented.

The administrative functions and privileges that need to be controlled when running a class C1 secure facility include those supporting security policy (i.e., DAC), accountability (i.e., identification and authentication), and operational assurance (i.e., system integrity).

Security Policy

This section of the TFM shall include descriptions of the TCB commands, interfaces, and procedures to:

- initialize discretionary access privileges and defaults for individual users and groups;
- distribute, review, and revoke privileges on an individual user or group basis;

- change object ownership (if any), restore accidentally deleted privileges, and kill errant processes;
- define and change group membership (whenever groups are supported), and explain the effect of such action on DAC;
- explain the implications of creating and deleting user and group accounts on DAC.

7.1.3 Accountability

Identification and Authentication

This section of the TFM shall include descriptions of the TCB commands, interfaces and procedures to perform the following functions:

- conduct setup of user/group security profiles, and authentication and authorization parameters of the login mechanism;
- conduct password management distribution to ordinary and administrative users or groups (see [4]);
- define account restrictions (e.g., time intervals for login, account cutoff time).

This section shall also include descriptions of the definition and change of log in mechanism parameters. These parameters include:

- types of terminals supported and terminal; interface initialization;
- time---out interval;
- multiple log in attributes (if supported);
- maximum login time;
- limits on unsuccessful logins from a terminal or to an account.

7.1.4 Routine Operations

Although the TCSEC does not cite specific requirements in this area, the TFM should include commands and procedures for the following activities:

- perform system boot and shut down;
- set system clocks;
- conduct on-line device testing;
- perform backup of user volumes;
- perform system metering;
- response to various user requests.

7.1.5 Security of the TCB

This section of the TFM shall include descriptions of the TCB command procedures that are provided "to validate periodically the correct operation of the on-site hardware and firmware elements of the TCB."[6]

In all areas of the TFM, and for all security classes where TCB commands and interface descriptions are required, the TFM shall include:

- effects and exceptions of each command (if not already defined in the DTLS);
- parameter and default setting;

- examples of potential use and misuse.
- In all areas of the TFM, and for all security classes, warnings (i.e., cautions) shall be provided for specific security vulnerabilities of the relevant administrative commands, interfaces, and procedures. Any modification to the TCB, for all security classes, may invalidate the systems rating [5].

7.2 Requirements and Recommendations for Security Class C2

Security class C2 includes all the TFM requirements of security class Cl. In addition, the following documentation requirements are added.

7.2.1 TFM Introduction

No Additional Requirements/Recommendations (NAR)

7.2.2 System Security Overview

The first design documentation requirement of TCSEC is that:

> "Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB."[6]

The above requirement suggests that the system security overview section should include an additional subsection on security philosophy. This section should contain a discussion of the security threats that could be countered by the use of this system, and of specific countermeasures based on security policy and accountability.

7.2.3 Security Policy

(NAR)

7.2.4 Accountability

The second documentation requirement is: "The procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event shall be given [6]. This requirements implies that the following sections should be added to the accountability area:

7.2.4.1 Identification and Authentication

(NAR)

7.2.4.2 Audit

The TFM should include a section describing the audit mechanisms, TCB commands, interfaces, and procedures for the following activities:

- determine audit selection mechanisms; these mechanisms include the commands and procedures necessary to display all security-relevant auditable events, to select the required and the optional audit events, and to turn on and off events selectively on a per-user and per-process

basis;
- conduct audit log management; this activity includes commands and procedures to create, save, and destroy saved audit logs; to change audit log size and warning point for audit log overflow; to format, compress and display audit logs;
- protect audit commands and databases;
- ensure maintenance of audit consistency;
    - perform post processing of audit data; this is an optional feature of a system and of the TFM, and includes mostly application-specific commands and procedures for intrusion detection. (However, all of these commands and procedures, and also the available tools and their protection from unauthorized user access, should be described whenever they are provided);

    The audit section of the TFM shall include a detailed description of the audit record structure for each type of audit event and of the entire audit log. (For specific details of audit requirements, the reader should refer to [1]).

7.2.5 Routine Operations

(NAR)

7.2.6 Security of the TCB

Additional requirement that is relevant to TCB protection is included here.

7.3 Requirements and Recommendations for Security Class B1

All TFM requirements of a class C2 system are included here. The documentation requirements of class B1 suggest significant additions to the TFM contents beyond those implied by the TCSEC requirements of security policy and accountability.

The TFM of a class B1 system should include the following additional documentation:

7.3.1 TFM Introduction

(NAR)

7.3.2 System Security Overview

This section should include any additional requirement referring to the system security overview. That is, this section of the TFM "shall provide guidelines on the consistent and effective use of the protection features of the system; [and] how they interact." [6] This suggests that the TFM should include a discussion of the interaction between the protection mechanisms and functions available to administrative users and those available to ordinary users. As mentioned in Section 2 above, this interaction is particularly important in the areas of security policy and accountability.

7.3.3 Security Policy

The additional security policy requirements of MAC and labeling suggest that additional administrative responsibilities should be documented in the TFM. The TFM requirement that the "manual shall describe the operator and administrator functions related to security,"[6] suggests that the TFM should include a description of all TCB commands, interfaces and procedures to perform the following functions:

- define and change system security profiles;
- classify, reclassify, import, and export objects;
- perform consistency checks on system and user security profiles.

7.3.4 Accountability

7.3.4.1 Identification and Authentication

The B1 requirements mandate the identification and authentication recommendations of classes Cl and C2 (i.e., they mandate the identification and authentication on a per-individual-user basis). In addition, it requires that the TFM includes TCB commands and procedures to define and change the user (and, possibly, group) levels of trust. It also requires that the computation of a subject's login level of trust be included in the TFM.

7.3.4.2 Audit

The additional B1 requirements that shall be included in the TFM documentation include:

- a description of how the audit mechanism records any override of output markings;
- a description of how the TCB commands, interfaces, and procedures support audit on a per-object sensitivity level basis

7.3.5 Routine Operations

(NAR)

7.3.6 Security of the TCB

The additional TFM requirement in this area is that the TFM "shall provide guidelines on [...] how to securely generate a new TCB" [6].

This requirement suggests that the TFM include:

- a list of approved tools for TCB generation;
- a description of procedures for TCB generation;
- a description of the vulnerabilities in generating a new TCB.

The B1 requirements of the TFM also state that the TFM "shall provide guidelines on [...] privileges needed to be controlled in order to operate the facility in a secure manner" [6]. This implies that the settings and the defaults for the protection privileges of the TCB files should be specified. Warnings about the improper setting of such privileges should be included.

7.4 Requirements and Recommendations for Security Class B2

All TFM requirements of the class B1 are included here. The documentation requirements of class B2 suggest additions to the TFM contents beyond those implied by the TCSEC requirements of security policy, accountability, and operational assurance.

The TFM of a B2 system should include the following additional documentation.

7.4.1 Introduction

(NAR)

7.4.2 System Security Overview

The only additional requirement for inclusion in this section is the separation of administrative functions into two roles, namely that of the administrator and that of the operator. Section 3 discusses the documentation requirements for B2 role separation.

7.4.3 Security Policy

The two additional security-policy requirements that should be documented in the TFM address the areas of subject sensitivity and device labels. The TFM shall include the TCB commands and procedures to:

- change the security label of an active subject (if this function is provided);
- assign and change the device sensitivity levels.

This section of the TFM shall also include a discussion of the security vulnerabilities associated with change of trust level of an active subject. Also it shall include a discussion of the relationship between the device sensitivity levels and the level of trust associated with the physical environment in which the devices are located.

7.4.4 Accountability

7.4.4.1 Identification and Authentication

The only additional TFM requirement here is that of documenting the trusted path mechanisms available to administrative users whenever this mechanism differs from that available to ordinary users (and documented in the SFUG).

7.4.4.2 Audit

The only additional TFM requirement of the audit area is that of defining the TCB commands and interfaces for auditing covert channels, for setting delays in covert channels, and for randomizing covert-channel variables.

7.4.5 Routine Operations

The routine operations performed by administrative users should be presented according to the separation of roles required by the trusted facility management area of the TCSEC and suggested by [7].

7.4.6 Security of the TCIB

The additional TFM requirements for this section include:

- the list of TCB modules shall identify the modules of the reference monitor mechanism;
- "[...] the procedures for secure generation of a new TCB from source after modification of any modules in the TCB shall be described" [6]. (This requirement implies that configuration management shall be in place. References to additional documents defining these procedures and plans could be included in the TFM).

7.5 Requirements and Recommendations for Security Class B3

The only additional requirements of class B3 that shall be included in the TFM are in the areas of system overview, audit, routine operations, and security of the TCB.

7.5.1 TFM Introduction

(NAR)

7.5.2 System Overview

The TFM should include a discussion of the physical security assumptions made by the system designers and implementators that must be satisfied by the installed system. Also, this section shall include a discussion of the separation between the security-relevant and security-irrelevant functions of the administrators and operators (see [7]).

7.5.3 Security Policy

(NAR)

7.5.4 Accountability

7.5.4.1 Identification and Authentication

(NAR)

7.5.4.2 Audit

The TFM should describe the TCB commands and interfaces available to the auditor that enable him or her to monitor the accumulation of auditable events and to respond effectively to such event signals.

7.5.5 Routine Operations

The additional routine operations carried out by secure and ordinary operators should be specified in the TFM. These should include:

- the identification of damaged user files and volumes;
- the routine backup of TCB files;
- the mounting and unmounting of volumes.

Security-irrelevant administrator and operator actions, such as handling user requests and managing the accounting system, should also be documented here.

7.5.6 Security of the TCB

Two additional TFM requirements are included here. The first is that "[The TFM] shall include procedures to ensure that the system is initially started in a secure manner" [6]. This requirement suggests that the TFM must document procedures for:

- TCB hardware installation (using the list of approved hardware modules);
- TCB loading; TCB data structure initialization;
- initialization of privileges for TCB file
- use of approved initialization tools.

The second requirement is that "procedures shall also be included to resume secure system operation after any lapse in system operation" [6].

This requirement suggests that the TFM should document procedures for:

- analysis of system dumps;
- crash recovery and restart in a secure state;
- repair of damaged TCB data structures (e.g., labels);
- changes of configuration parameters (e.g., table sizes);
- consistency checking procedures.

7.6 Requirements of Security Class A1

Although no additional explicit TFM requirements beyond that required for B3 are included here, the TFM should define procedures for trusted distribution consistent with the [6] requirements.

GLOSSARY

Access -
A specific type of interaction between a subject and an object that results in the flow of information from one to the other.

Account Administrator -
An administrative role or user assigned to maintain accounting files, tools, user accounts, and system statistics.

Administrative User -
A user assigned to supervise all or a portion of an AIS system.

Approval Accreditation -
The official authorization that is granted to an AIS system to process sensitive information in its operational environment, based upon comprehensive security evaluation of the system's hardware, firmware, and software security design, configuration, and implementation and of the other system procedural, administrative, physical, TEMPEST, personnel, and communications security controls.

Audit -
To conduct the independent review and examination of system records and activities.

Audit Event Selection -
Selection, by authorized personnel, of the auditable events that are to be recorded on the audit trail.

Audit Mechanism -
The part of the TCB used to collect, review, and/or examine system activities.

Audit Post Processing -
Processing, by authorized personnel, of specified events that had been recorded on the audit trail.

Audit Trail -
A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in transaction from its inception to final results.

Auditable Event -
Any event that can be selected for inclusion in the audit trail. These events should include, in addition to security-relevant events, events taken to recover the system after failure and any events that might prove to be security relevant at a later time.

Auditor -
An authorized individual, or role, with administrative duties, which include selecting the events to be audited on the system, setting up the audit flags that enable the recording of those events, and analyzing the audit. trail

Authenticate -
(1) To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system. (2) To verify the integrity of data that has been stored, transmitted, or otherwise exposed to possible unauthorized modification.

Authenticated User -
A user who has accessed an AIS system with a valid identifier and authenticator.

Automated Information System (AIS) -

An assembly of computer hardware, firmware, and software configured to collect, create, communicate, compute, disseminate, process, store, and /or control data or information.

Bandwidth -

A characteristic of a communication channel that is the amount of information that can be passed through it in a given amount of time, usually expressed in bits per second.

Category -

A restrictive label that has been applied to classified or unclassified data as a means of increasing the protection of the data and further restricting access to the data.

Channel -

An information transfer path within a system. May also refer to the mechanism by which the path is effected.

Covert Channel -

A communication channel that allows two cooperating processes to transfer information in a manner that violates the system's security policy. Synonymous with Confinement Channel.

Covert Storage Channel -

A covert channel that involves the direct or indirect writing of a storage location by one process and the direct or indirect reading of the storage location by another process. Covert storage channels typically involve a finite resource (e.g., sectors on a disk) that is shared by two subjects at different security levels.

Covert Timing Channel -

A covert channel in which one process signals information to another by modulating its own use of system resources (e.g., Central Processing Unit time) in such a way that this manipulation affects the real response time observed by these second process.

Data -

Information with a specific physical representation.

Data Integrity -

The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction.

Descriptive Top-Level Specification (DTLS) -

A top-level specification that is written in a natural language (e.g., English), an informal program design notation, or a combination of the two.

Discretionary Access Control -

A means of restricting access to objects based on the identity and need-to-know of the user, process, and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.

Formal Security Policy Model -

A mathematically precise statement of a security policy. To be adequately precise, such a model shall represent the initial state of a system, the way in which the system progresses from one state to another, and a definition of a "secure" state of the system. To be acceptable as a basis for a TCB, the model shall be supported by a formal proof that if the initial state of the system satisfies the definition of a "secure" state. If all assumptions required by the model hold, then all future states of the system will be secure. Some formal modeling techniques include state transition models, temporal logic models, denotational semantics models, and algebraic specification models.

Formal Top-Level Specification (FTLS) -

A top-level specification that is written in a formal mathematical language to allow theorems showing the correspondence of the system specification to its formal requirements to be hypothesized and formally proven.

Functional Testing -

The portion of security testing in which the advertised features of a system are tested, under operational conditions, for correct operation.

Least Privilege -

The principle that requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

Mandatory Access Control -

A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e., clearance) of subjects to access information of such sensitivity.

Multilevel Device -

A device that is used in a manner that permits simultaneous processing of data of two or more security levels without risk of compromise. To accomplish this, sensitivity labels are normally stored on the same physical medium and in the same form (i.e., machine-readable or human-readable) as the data being processed.

Multilevel Secure -

A class of system containing information with different sensitivities that, simultaneously permits access by users with different security clearances and need-to-know, but prevents users from obtaining access to information for which they lack authorization.

Object -

A passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Examples of objects are records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, and network nodes.

Operator -

An administrative role or user assigned to perform routine maintenance operations of the AIS system and to respond to routine user requests.

Output -

Information that has been exported by a TCB.

Password -

A private character string that is used to authenticate an identity.

Process -

A program in execution. It is completely characterized by a single current execution point (represented by the machine state) and address space.

Read -

A fundamental operation that results only in the flow of information from an object to a subject.

Read Access (Privilege) -
Permission to read information.

Security Administrator -
An administrative role or user responsible for the security of an AS and having the authority to enforce the security safeguards on all others who have access to the AIS (with the possible exception of the Auditor).

Security Level -
The combination of a hierarchical classification and a set of non-hierarchical categories that represents the sensitivity of information.

Security Policy -
The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

Security Policy Model -
A formal (informal.in the case of B1) presentation of the security policy enforced by the system. It must identify the set of rules and practices that regulate how a system manages, protects, and distributes sensitive information.

Security-Relevant Event -
Any event that attempts to change the security state of the system (e.g., change the DAC, change the security level of the subject, change user password). Also, any event that attempts to violate the security policy of the system, (e.g., too many attempts to log in, attempts to violate the MAC limits of a device, attempts to downgrade a file).

Security Testing -
A process used to determine that the security features of a system are implemented as designed and that they are adequate for a proposed application environment.

Sensitive Information -
Any information, the loss, misuse, modification of, or unauthorized access to, that could affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, U.S. Code, but that has not been specifically authorized under criteria established by an Executive order or act of Congress to be kept classified in the interest of national defense or foreign policy.

Sensitivity Label -
A piece of information that represents the security level of an object and that describes the sensitivity (e.g., classification) of the data in the object. Sensitivity labels are used by the TCB as the basis for MAC decisions.

Subject -
An active entity, generally in the form of a person, process, or device that causes information to flow among objects or changes in the system state. Technically, a process/domain pair.

Subject Security Level -
A subject's security level that is equal to the security level of the objects to which it has both read and write access. A subject's security level shall always be dominated by the clearance of the user associated with the subject.

System Programmer -
An administrative role or user responsible for the trusted system

distribution, configuration, installation, and non-routine maintenance.

System Security Map -
A map defining the correspondence between the binary and ASCII formats of security levels (e.g., between binary format of security levels and sensitivity labels).

Top-Level Specification (TLS) -
A non-procedural description of system behavior at the most abstract level; typically, a functional specification that omits all implementation details.

Trap Door -
A hidden software or hardware mechanism that can be triggered to permits system protection mechanisms to be circumvented. It is activated in some innocent-appearing manner (e.g., special "random" key sequence at a terminal).

Trojan Horse -
A computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security; for example, making a "blind copy" of a sensitive file for the creator of the Trojan horse.

Trusted Computer System -
A system that employs sufficient hardware and software assurance measures to allow its use for simultaneous processing a range of sensitive or classified information.

Trusted Computing Base (TCB) -
The totality of protection mechanisms within a computer system -`including hardware, firmware, and software --- the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a TCB to enforce a security policy correctly depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user's clearance) related to the security policy.

Trusted Path -
A mechanism by which a person at a terminal can communicate directly with the TCB. This mechanism can only be activated by the person or the TCB and cannot be imitated by untrusted software.

User -
Person or process accessing an AS either by direct connections (i.e., via terminals), or indirect connections (i.e., prepare input data or receive output that is not reviewed for content or classification by a responsible individual).

Verification -
The process of comparing two levels of system specification for proper correspondence (e.g., security policy model with top-level specification, TLS with source code, or source code with object code). This process may or may not be automated.

Write -
A fundamental operation that results only in the flow of information from a subject to an object.

Write Access (Privilege) -
Permission to write an object.

REFERENCES

[1]
National Computer Security Center, A Guide to Understanding Audit in Trusted Systems, NCSC-TG-001, Version 2, June 1988.

[2]
National Computer Security Center, A Guide to Understanding Discretionary Access Control in Trusted Systems, NCSC-TG-003, version-I, September 1987.

[3]
Gligor V. D., J. C. Huskamp, S. R. Welke, C. J. Linn, W. T. Mayfield, Traditional Capability-Based Systems: An Analysis of their Ability to Meet the Trusted Computer Security Evaluation Criteria, Institute for Defense Analyses, IDA Paper PI 935, February 1987.

[4]
Department of Defense, Password Management Guideline, CSC-STD-002-85, April 1985.

[5]
National Computer Security Center, The Rating Maintenance Phase, NCSC-TG-013-89, 23 June 1989.

[6]
National Computer Security Center, Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200. 28-STD, 1985.

[7]
National Computer Security Center, Guidelines for Trusted Facility Management, NCSC-TG-015-89, 18 October 1989.