NCSC-TG-026
Library No. 5-237,294
Version 1

FOREWORD

The National Computer Security Center is publishing A Guide to Writing the Security Features User's Guide for Trusted Systems as part of the "Rainbow Series" of documents our Technical Guidelines Program produces. In the Rainbow Series, we discuss in detail the features of the Department of Defense Trusted Computer System Evaluation Criteria (DoD 5200.28-STD) and provide guidance for meeting each requirement. The National Computer Security Center, through its Trusted Product Evaluation Program, evaluates the security features of commercially-produced computer systems. Together, these programs ensure that organizations are capable of protecting their important data with trusted computer systems.

A Guide to Writing the Security Features User's Guide for Trusted Systems expands on the Trusted Computer System Evaluation Criteria requirement for a Security Features User's Guide by discussing the intent behind the requirement and the relationship it has to other requirements in the Trusted Computer System Evaluation Criteria. The guide's target audience is the author of the Security Features User's Guide for a specific trusted system undergoing evaluation as a trusted product; however, many of the recommendations apply to any system that must satisfy the Trusted Computer System Evaluation Criteria requirements.

As the Director, National Computer Security Center, I invite your recommendations for revision to this technical guideline. We plan to review and update this document periodically in response to the needs of the community. Please address any proposals for revision through appropriate channels to:

National Computer Security Center
9800 Savage Road
Ft. George G. Meade, MD 20755-6000

Attention: Chief, Standards, Criteria, and Guidelines Division

Patrick R. Gallagher, Jr. September 1991
Director
National Computer Security Center

ACKNOWLEDGEMENTS

The National Computer Security Center expresses appreciation to David M. Chizmadia as project manager and principal author of this document.

We also thank the evaluators, vendors and users in the United States computer security community who contributed their time and expertise to the review of this document.

CONTENTS

1. INTRODUCTION

1.1 PURPOSE

This guideline explains the motivation and meaning of the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) requirement for a Security Features Users Guide (SFUG), which reads as follows:

> "A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another." [TCSEC;x.x.4.1]

The reader is assumed to be the potential author of a SFUG; to be familiar with the basic principles of technical writing, computer science, and trusted systems; and to have a detailed understanding of the specific trusted system that will be described in the SFUG.

1.2 SCOPE

This guideline identifies and discusses the considerations that influence the development and evaluation of a SFUG, such as its audience, content, and organization. It is intentionally descriptive, as opposed to prescriptive, in its discussion of the SFUG requirement. That is, it describes the various approaches to writing a SFUG that have been accepted by trusted product evaluators in the past, without making judgments about the "correct" ones to choose - although preferred approaches may be noted.

Throughout this guideline there will be statements made that are not included in the TCSEC as requirements. These statements will fall into three categories. First, some describe a strongly recommended course of action: these statements will be prefaced by the word "should." Second, others describe one of several equally appropriate recommended courses of action: these statements will be prefaced by the word "could." Finally, a few suggest an optional course of action: these statements will be prefaced by the word "can."

1.3 ORGANIZATION

The remainder of this guideline presents information that may be useful to a writer developing a SFUG. Chapter 2 discusses the developmental aspects of writing the SFUG, including the audience and possible packaging options, presentation styles, and the security topics that should be addressed in the SFUG (as derived from TCSEC feature requirements). Chapter 3 contains two example annotated outlines of SFUGs to illustrate some of the topics discussed in the body of the guideline and provide a starting point for the reader to develop a SFUG. The bibliography includes a list of the documents accepted as SFUGs for all products on the Evaluated Product List (EPL) at the time the guideline was published.

2. DEVELOPING THE SECURITY FEATURES USER'S GUIDE

The primary purpose of a SFUG is to explain how the security mechanisms in a specific system work, so that users are able to consistently and effectively protect their information. To properly communicate this information, the SFUG author must identify the audience for the SFUG and the information that audience needs to use the security mechanisms in the system and then select an appropriate way to present the information.

2.1 AUDIENCE AND PACKAGING

The SFUG requirement starts with "A single summary, chapter, or manual in user documentation . . ." "User" in this context refers to a person who uses the system, but has no special privileges to affect the configuration of the system. The user for most general purpose trusted systems is often assumed to be a person with little or no computer experience, but this is not always the case. For example, the users of the UNIX(TM) system have traditionally been considered programmers or computer professionals with fairly extensive knowledge of computer concepts. In any system, the users are the audience for the SFUG and the SFUG author will have to characterize them to determine both the format and the level of discourse for the material presented in the SFUG.

In many cases, the SFUG requirement is satisfied by changing an existing document, which is one of the reasons that the SFUG requirement is so general. As stated in the requirement, the SFUG could be:

- A summary of the security features and user responsibilities,
- A chapter devoted to these issues, or
- A whole manual devoted to security.

Some presentation schemes that previous participants in the Trusted Product Evaluation Program have used include:

- A separate manual devoted to the general user of the system that covers the security features and responsibilities pertaining to users. This is usually the best choice when a document of this sort is already in place and the security functions have always been present in the system in some form anyway. For a system in which user services are provided by individual subsystems, one of which provides all the security functionality, and the user guide is the collection of user guides `for the individual subsystems, the SFUG would most likely be a stand-alone manual addressing only the security issues.

- A subsection of the manual produced to satisfy the Trusted Facility Manual (TFM) requirement of the TCSEC. From a security standpoint, this is considered unwise, since it tends to make the system configuration and vulnerability information available to anyone looking for information on how to use the security features of the system. From a documentation standpoint, it seems the easiest, since it places all of the security discussion in one place and allows a certain amount of synergy in the writing process, i.e., privileged users do many of the same activities as general users. This approach eliminates the need to document those facilities in two places.

- A chapter or an appendix of a user manual that discusses the user's security responsibility and then provides an index to the detailed discussions of individual functions that are already part of the general user manual. An extension of this could be a small pamphlet that does the same thing but can be reproduced separately and given out as needed - something like a pocket guide to system security.

Trusted product evaluators tend to favor centralization of information, because that makes it easier to determine whether the system satisfies the TCSEC (Orange Book) requirements. Given that bias, bullet one would usually be the most preferred option, since it satisfies the requirement in one unique place. Bullet two is a less desirable option, because, in addition to the procedural security considerations, it requires some discrimination to identify which parts of the document satisfy the SFUG requirement and which parts satisfy the TFM requirement. Bullet three is least desirable for two reasons. First, it involves pointers to other information, making it more cumbersome for both evaluators and users to get to some aspects of the information. Second, there might be a tendency to make the document so terse that it excludes some information that is relevant to system security.

2.2 PRESENTATION

The SFUG provides the users of the system with the necessary background and specific information to use the protection features of the system correctly. Its purpose is twofold. First, it provides the information that a user needs to enter the system and start working-within the system security constraints. Second, it explains the user's role in maintaining the security of the system. Its scope should be limited to documenting only the features available to all users and only the responsibilities that all users have for system security. To accomplish this purpose, within the scope, the SFUG should explain what security means in the system, what security features are present and why, how the features work, and how to use the features properly. The SFUG should be clear, concise, and complete to increase its readability.

This information can be organized either by the security features present in the system or by the tasks performed by a user that require the use of these features. A feature-oriented presentation is more natural to a user who is already familiar with the system. In the SFUG, this organization would usually look like the TCSEC itself, with descriptions of each feature required by the TCSEC and explanations of the commands that make those features available to users. A task- oriented presentation is the more common approach taken in most user manuals, since it is oriented towards the specific actions that are necessary to enter a system and start working. Such a presentation will often take the form of a tutorial that describes the interactions that a user will usually have with the system, e.g., logging on, setting file access, changing the password, etc.

2.3 CONTENT

Because this guideline is devoted to explaining a TCSEC requirement, it will consider the content of a SFUG only from the perspective of the features required by the TCSEC that should be documented in the SFUG. Other security-relevant features not addressed by the TCSEC (e.g., object downgrading or network commands) might also be included in the SFUG, but will not be discussed in this guideline.

The remainder of this section will list the features required by the TCSEC, identify the specific requirements that define them, and discuss how they apply to the SFUG. Many of the requirements cited use the acronym TCB, which expands to Trusted Computing Base. As defined in the TCSEC, the TCB is:

> "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 correctly enforce a security policy 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." [TCSEC, p. 116]

2.3.1 TECHNICAL SECURITY POLICY

The technical security policy is the description of the access control model that the system enforces. This description can be either informal or formal for classes C1 through B1, but classes B2 to A1 must have a formal description. The TCSEC design documentation requirement mandates that the informal description exist for all criteria classes where it states:

> "Documentation shall be available that provides a description of the manufacturer's philosophy of protection . . .,` [x.x.4.4]

Starting at B1, the design specification and verification requirement strengthens this notion of a technical security policy with the explicit requirement that:

> "An informal or formal model of the security policy supported by the TCB shall be maintained over the life cycle of the ADP system and demonstrated to be consistent with its axioms." [x.x.3.2.2]

At class B2, the design specification and verification requirement is changed to mandate a formal technical security policy model. Classes B3 and A1 incorporate new requirements for additional supporting documentation that makes it possible to trace the basis for each feature in the system from the technical security policy to the implementation.

In the context of the TCSEC, neither the philosophy of protection nor the formal model have to be available to the user; however, the fact that the features of the system flow from these fundamental statements makes either one an appropriate starting point for describing how the system works. The philosophy of protection is probably the better choice for the SFUG, since it is usually written in a more intuitive style than a precisely stated security policy statement. In either case, the technical policy would be presented early in the SFUG to provide the overall context for the rest of the discussion, effectively becoming the thesis for the SFUG.

2.3.2 IDENTIFICATION AND AUTHENTICATION

The single largest and most crucial section of the SFUG, both from the perspective of the TCSEC and of overall system documentation, is the section that discusses how users identify and authenticate themselves (i.e., logon) to the system. The process of identification and authentication (I&A) defines the identity of the subject that the TCB creates to act on the user's behalf. For division B and A multilevel systems, the I&A process defines the upper and lower bounds on the security level of the subject as well. All subsequent access control decisions depend on this information being correct. The SFUG should therefore be very specific in describing both the I&A procedures and the user's responsibilities for protecting any information that is expected to be kept secret (e.g., passwords or personal identification numbers).

The TCSEC requirement for division C computer systems is shown below, with bold type showing the C2 requirements that go beyond those at C1.

> "The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user. The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual ADP system user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual." [2.2.2.1]

Based on this requirement, the SFUG for a division C system should describe the identification process, including the use of a protected authentication mechanism. To complement the protection that the TCB must give the authentication data, the SFUG should make it clear that the user must protect the data too, for example, by not sharing a password with other users or writing it down on a sheet of paper next to the terminal.

For divisions B and A, the addition of multiple security levels changes the requirement, primarily by requiring the use of a user's clearance as a bound on the security label of any subject that the TCB creates for that user. The B1 requirement, which does not change for the higher classes, is shown below, with bold type showing additional wording and struck-out type showing wording that was deleted.

> "The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall maintain authentication data

that includes information for verifying the identity of individual users (e.g., passwords) as well as information for determining the clearance and authorizations of individual users. This data shall be used by the TCB to authenticate the user's identity and to ensure that the security level and authorization of subjects external to the TCB that may be created to act on behalf of the individual user are dominated by the clearance and authorization of that user. The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user. The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual ADP system user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual." [3.1.2.1]

For all division B and A systems, the SFUG should incorporate a discussion of the relationship between a user's clearance (i.e., his or her general authorization to see information of a particular sensitivity-whether or not it is electronic) and the security level that the TCB associates with a particular subject (e.g., computer process or interactive session) that is acting on that user's behalf. Additionally, the practical consideration of how to establish the security level of that subject, for example, by using a logon option or a specific terminal, should be explained in the SFUG.

Starting at B2, there is an additional requirement for a trusted path to strengthen the confidence of both the user and the TCB that, the I&A process is happening correctly. This requirement is shown below in both the B2 and B3/A1 forms.

"The TCB shall support a trusted communication path between itself and user for initial login and authentication. Communications via this path shall be initiated exclusively by a user." [3.2.2.1.1(B2)]

"The TCB shall support a trusted communication path between itself and users for use when a positive TCB-to-user connection is required (e.g., login, change subject security level). Communications via this trusted path shall be activated exclusively by a user or the TCB and shall be logically isolated and unmistakably distinguishable from other paths." [3.3.2.1.1 (B3/A1)]

Trusted path is useless if it is not used; therefore, the SFUG should be written so that the user understands how to initiate the trusted path, especially at logon, and why it is important to do so. For systems that satisfy the B3 trusted path requirement, the SFUG should also explain how the initiation of a trusted path during a session, whether by the user or the TCB, affects the currently running subject, as well as how to recognize the trusted path.

2.3.3 DISCRETIONARY ACCESS CONTROL FACILITY

The discretionary access control (DAC) facility provides the mechanism by which the individual user can control access to his or her data. Some form of DAC is required for every class of the TCSEC. After the procedures for identifying and authenticating themselves to the system, the DAC facilities will be the aspects of the system security of most interest to most users.

The DAC facility is first defined by the C1 DAC requirement that:

> "The TCB shall define and control access between named users and named objects (e.g., files and programs) in the ADP system. The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects by named individuals or defined groups or both." [2.1.1.1]

At C2 this requirement is enhanced to read (bold type shows added words):

> "The TCB shall define and control access between named users and named objects (e.g., files and programs) in'the ADP system. The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects by named individuals, or defined groups of individuals, or by both, and shall provide controls to limit propagation of access rights. The discretionary access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users." [2.2.1.1]

After this it remains the same until B3, when it is changed to read (bold type shows added words, struck-out type shows deleted words):

> "The TCB shall define and control access between named users and named objects (e.g.,files and programs) in the ADP system. The enforcement mechanism (e.g., access control lists) shall allow users to specify and control sharing of those objects, and shall provide controls to limit propagation of access rights. The discretionary access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of specifying, for each named object, a list of named individuals and a list of groups of named individuals with their respective modes of access to that object. Furthermore, for each such named object, it shall be possible to specify a list of named individuals and a list of groups of named individuals for which no access to the object is to be given. Access permission to an object by users not already possessing,,access permission shall only be assigned by authorized users. [3.3.1.1]

For any version of this requirement, the goal for the SFUG author is the same - to describe to users how to use the DAC enforcement mechanism to control access to the objects that they own. The SFUG should provide enough information for the user to understand what a named object, a named user, and a group are, as well as what types of objects can be controlled with DAC. It should also explain how a new user or group is defined to the system. The SFUG should also describe the process by which access rights are initially determined and then propagated. Finally, the SFUG should describe the system commands and procedures for using the DAC facility.

2.3.4 ELECTRONIC LABELS

The distinguishing feature of all division B and A computer classes is the electronic label. An electronic label is an attribute of each subject and object under TCB control that indicates the sensitivity of the information that a subject is authorized to see or that is contained in an object. The real world equivalents of these concepts are security clearances and classification markings. Many users who are familiar with these real world examples have trouble adapting to electronic labels; therefore, the SFUG written for a multilevel system should discuss labels and their effect on a user's actions.

The basic label requirement is defined by the following words at B1:

> "Sensitivity labels associated with each subject and storage object under its control (e.g., process, file, segment, device) shall be maintained by the TCB. These labels shall be used as the basis for mandatory access control decisions. In order to import non-labeled data, the TCB shall request and receive from an authorized user the security level of the data, and all such actions shall be auditable by the TCB." [3.1.1.3]

At B2, the first sentence is changed to read:

> "Sensitivity labels associated with each ADP system resource (e.g., subject, storage object, ROM) that is directly or indirectly accessible by subjects external to the TCB shall be maintained by the TCB." [3.2.1.3]

This reflects the general B2 through A1 requirement that all computer resources be under the control of the TCB.

Another label-related requirement that affects the users of a system is the one for labeling human-readable output, which states that:

> "The ADP system administrator shall be able to specify the printable label names associated with exported sensitivity labels. The TCB shall mark the beginning and end of all human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly represent the sensitivity of the output. The TCB shall, by default, mark the top and bottom of each page of human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly represent the

overall sensitivity of the output or that properly represent the sensitivity of the information on the page. The TCB shall, by default and in an appropriate manner, mark other (forms of human-readable output (e.g., maps, graphics) with human-readable sensitivity labels that properly represent the sensitivity of the output. Any override of these marking defaults shall be auditable by the TCB." [3.1.1.3.2.3]

The above requirement is the same for classes B1 through A1.

These two requirements, for subject sensitivity labels and labeled human-readable output, apply to any multilevel system; therefore, the SFUG for all B and A level systems should, at the least, explain:

. How labels are attached to subjects and objects,
. The relationship between the "clearance" that a user has and the label that is associated with a particular computer session, and
. The reason for job and page labels on printed output and terminal or window labels on computer displays (as well as cautions about disabling the display of such labels).

The last requirement that affects users is one for subject sensitivity labels that requires that:

"The TCB shall immediately notify a terminal user of each change in the security level associated with that user during an interactive session. A terminal user shall be able to query the TCB as desired for a display of the subject's complete sensitivity label." [3.2.1.3.3]

The above requirement applies to classes B2 through A1; therefore, the SFUG for these systems should explain the mechanism used to notify a user of a security level change.

2.3.5 MANDATORY ACCESS CONTROL FACILITY

Closely associated with, but separate from, the requirement for labels is the requirement for mandatory access control (MAC). MAC refers to the set of rules that control a subject's access to an object based on the label attached to each.

The MAC facility is first defined by the B1 MAC requirement that:

"The TCB shall enforce a mandatory access control policy over all subjects and storage objects under its control (e.g., processes, files, segments, devices). These subjects and objects shall be assigned sensitivity labels that are a combination of hierarchical classification levels and non-hierarchical categories, and the labels shall be used as the basis for mandatory access control decisions. The TCB shall be able to support two or more such security levels. The following requirements shall hold for all accesses between subjects and objects controlled by the TCB: A subject can read an object only if the hierarchical classification in the subject's security level is greater than or equal to the hierarchical classification in the object's security level and the non-hierarchical categories in the subject's security level include all the non-hierarchical categories in the object's security level. A subject can write an object only if the hierarchical classification in the subject's security level is less than or equal to the hierarchical classification in the object's security level and all the non-hierarchical categories in the subject's security level are included in the non-hierarchical categories in the object's security level. Identification and authentication data shall be used by the TCB to authenticate the user's identity and to ensure that the security level and authorization of subjects external to the TC8 that may be created to act on behalf of the individual user are dominated by the clearance and authorization of that user." [3.1.1.4]

For classes B2 through A1, the requirement is enhanced to reflect the pervasive TCB control required by these higher classes. (The bold type in the following quote shows the additional wording, while the struck-out type shows the phases deleted.)

> "The TCB shall enforce a mandatory access control policy over all resources (i.e., subjects, storage objects, and 1/0 devices) that are directly or indirectly accessible by subjects external to the TCB. These subjects and objects shall be assigned sensitivity labels that are a combination of hierarchical classification levels and non-hierarchical categories, and the labels shall be used as the basis for mandatory access control decisions. The TCB shall be able to support two or more such security levels. The following requirements shall hold for all accesses between all subjects external to the TCB and all objects directly or indirectly accessible by these subjects: A subject can read an object only if the hierarchical classification in the subject's security level is greater than or equal to the hierarchical classification in the object's security level and the non-hierarchical categories in the subject's security level include all the non-hierarchical categories in the object's security level. A subject can write an object only if the hierarchical classification in the subject's security level is less than or equal to the hierarchical classification in the object's security level and all -the non-hierarchical categories in the subject's security level are included in the non-hierarchical categories in the object's security level. Identification and authentication data shall be used by the TCB to authenticate the user's identity and to ensure that the security level and authorization of subjects external to the TCB that may be created to act on behalf of the individual user are dominated by the clearance and authorization of that user." [3.2.1.4]

Because the TCB, rather than the user, controls the actual interaction between the labels of subjects and objects, the SFUG only needs to explain to users how MAC constrains their actions. This discussion is probably most natural under the section that addresses the technical security policy. In most cases, a user can have only one effect on the MAC policy-to change the label for a session, which is already described under either the discussion of identification and authentication or labels.

2.3.6 TRUSTED FACILITY MANAGEMENT

Beginning at B2, there is a TCSEC requirement that:

> "The TCB shall support separate operator and administrator functions." [3.2.3.1.4]

This mandates a separation of duties in the administration of computer systems that are supposed to be protecting information. This corresponds to the natural separation of duties found in most human activity. Although this is not a requirement until B2, many sites that are concerned about security are instituting programs `rvhere the responsibility for security administration of the computer system is centralized in a person with the title of computer, or information system, security officer (CSO or ISS0, respectively). Whether the computer system being described in the SFUG satisfies the trusted facility management requirement or not, the author of the SFUG for that system may want to postulate the existence of such a position to represent the entity that is responsible for security issues that are outside the control of the users. This both allows the SFUG to be written in a more active voice and simplifies the job of conveying distinctions between user security responsibilities and site management security responsibilities.

3. EXAMPLES OF SFUG PRESENTATION STYLES

This chapter presents two sample stand-alone SFUGs to show what could go into a SFUG and possibly give the reader some ideas for organizing a system specific SFUG. The actual contents and organization of a real SFUG will be different to reflect the specific mechanisms of the individual system and the organization of the rest of the system documentation. The first example uses a feature-oriented style presentation, while the second shows a task-oriented style.

In addition to these generic examples, the reader may find it helpful to review the SFUGs of previously evaluated systems to see what worked for them. Entries 2 through 16 in the bibliography list the Final Evaluation Reports (FERs) for products on the Evaluated Products List that had published FERs at the time this guideline was printed. Each entry is annotated with the document(s) identified in the FER as satisfying the SFUG requirement for that product.

THE FEATURE-ORIENTED SFUG

At a high level, the feature-oriented example SFUG is arranged in the following fashion:

1. INTRODUCTION TO THE SFUG

2. SYSTEM SECURITY OVERVIEW
   2.1 SYSTEM PHILOSOPHY OF PROTECTION
   2.2 DEFINITION OF TERMS AND SERVICES
   2.3 THE INFORMATION SYSTEM SECURITY OFFICER
   2.4 USER SECURITY RESPONSIBILITIES
3. SECURITY-RELATED COMMANDS FOR USERS
   3.1 USER IDENTIFICATION AND AUTHENTICATION
      3.1.1 Trusted Path
      3.1.2 Logging On to the System
      3.1.3 Password Considerations
      3.1.4 Changing Group Membership
      3.1.5 Changing Current MAC Authorizations
      3.1.6 Logging Off of the System
      3.1.7 I&A Errors and Their Causes
   3.2 DISCRETIONARY ACCESS CONTROL FACILITIES
      3.2.1 Setting DAC on Named Objects
      3.2.2 Default DAC Protection
      3.2.3 DAC Groups
      3.2.4 DAC Errors and Their Causes
   3.3 MANDATORY ACCESS CONTROL FACILITIES
      3.3.1 Printing Labeled Objects
      3.3.2 Accessing Single-Level Devices
      3.3.3 Accessing Multilevel Devices
      3.3.4 Downgrading Labeled Objects
      3.3.5 MAC Errors and Their Causes
   3.4 OBJECT MANIPULATION FACILITIES
      3.4.1 Object Creation, Reuse, and Deletion
      3.4.2 Importing Machine-Readable Objects
      3.4.3 Exporting Machine-Readable Objects
      3.4.4 Determining the Properties of Objects
      3.4.5 Object Manipulation Errors and Their Causes

The annotated outline follows.

1. INTRODUCTION TO THE SFUG

This part of the SFUG should identify what the SFUG is, who it is written for, what it will cover, and where to go for more information, if needed.

2. SYSTEM SECURITY OVERVIEW

This section provides the background on the overall operation of the security controls in the system so that users can then understand the options and actions of individual security-relevant commands.

2.1 SYSTEM PHILOSOPHY OF PROTECTION

This section should describe the general environment for which the system is designed and briefly explain how this environment motivates the approach to protecting information stored in the system. The purpose of this section is to lay the foundation for the user's understanding of the system's security features, with later sections detailing what specific security services are available and when and how to use them.

2.2 DEFINITION OF TERMS AND SERVICES

This section should first introduce the terms that will be used to describe the security services available in the system and then proceed to introduce those services, without detailing exactly how they are used. Recommended topics for this section are:

- An explanation of the general concepts of subjects and objects, followed by the identification of the subjects and objects in the system.
- An explanation of object reuse and its role in protecting information in the system.
- An explanation of the components of the l&A (identification and authentication) process (e.g., user-id, password, or smartcard) in the system and the importance of l&A to system security.
- An explanation of DAC, groups, privileges, protection bits/ACLs, and any other terms and concepts related to the system's DAC policy, followed by a description of how the DAC policy applies to the systern subjects and objects.
- An explanation of MAC, security labels, sensitivity levels, categories, authorizations, and any other terms and concepts related to the system's MAC policy, followed by a description of how the MAC policy applies to the system subjects and objects.

2.3 THE INFORMATION SYSTEM SECURITY OFFICER

This section discusses the role of the Information System Security Officer (ISSO) in maintaining the security of the system. It can also explain which problems should be reported to the ISSO and which should be reported to the system administrator (if the roles are separate). If the format of the SFUG allows it, this section could have space for site-specific notes on the ISSO/user relationship.

2.4 USER SECURITY RESPONSIBILITIES

This section discusses the user's responsibilities with respect to properly using the system security features. This would optimally be a tutorial that teaches effective use of the system security services, but any presentation that relates the security services to the user's day-to-day use of the system is appropriate. Some issues that might be addressed are:

- Authentication token (e.g., password or smartcard) protection.
- Warnings about leaving a terminal unattended.
- Procedures for "locking" a process when the terminal must be left unattended, but logged in.

- Default DAC access for named objects (e.g., files andkdirectories).

- Cautions about using programs that are not part of the standard system configuration (e.g., utilities or applications that have not been reviewed and tested by the system administrator(s)).

- Cautions about the effect of network access on system and data security.

3. SECURITY-RELATED COMMANDS FOR USERS

This section comprises the majority of the SFUG since it describes in detail the commands and procedures for actually using the system.

3.1 USER IDENTIFICATION AND AUTHENTICATION

This section should step through the procedures for logging on to and off of the system and for manipulating privileges and participation in the system. Additionally, any of the errors that might occur during the use of these commands and the corrective actions should be described here.

3.1.1 Trusted Path

In B2 and above systems, the first thing that a user will have to do to logon is establish a trusted path between his terminal and the system TCB. This section should describe that process. For B3 and A1 systems, this trusted path is available for any direct interaction between the TCB and the user; therefore, in-session invocation of the trusted path and its effects on currently executing processes should be described here.

3.1.2 Logging On to the System

The procedure for logging on to the system should be described. If the system has MAC, the procedures for logging on with specific, non-default authorizations should be described.

3.1.3 Password Considerations

The procedures and commands for setting, changing, and protecting passwords should be described.

3.1.4 Changing Group Membership

In systems with the concept of DAC groups, the mechanisms for users to specify the group membership(s) that should be used in making DAC access decisions (if such capability is present) should be described.

3.1.5 Changing Current MAC Authorizations

In systems with MAC, if the user can change their current authorization level and category set without logging off, the mechanism and procedure should be described.

3.1.6 Logging Off of the System

The command or procedure for logging off the system should be described.

3.1.7 I&A Errors and Their Causes

The possible error messages that can occur when I&A commands are improperly invoked should be noted and the correct or expected inputs should be explained.

3.2 DISCRETIONARY ACCESS CONTROL FACILITIES

This section should describe the DAC-related commands and procedures for the system. This section will be present in some form at all levels of the criteria.

3.2.1 Setting DAC on Named Objects

This section should describe how users can set the discretionary access permissions, and what the permissions mean, for the different types of named objects in the system.

3.2.2 Default DAC Protection

The means for determining and setting the default discretionary access controls on user controlled or owned named objects should be described.

3.2.3 DAC Groups

When the capability exists for users to define groups of users for the purpose of DAC, the mechanisms for defining these groups should be described.

3.2.4 DAC Errors and Their Causes

The possible error messages that can occur when DAC commands are improperly invoked should be noted and the correct or expected inputs should be explained.

3.3 MANDATORY ACCESS CONTROL FACILITIES

This section is for systems in the B and A classes. It describes the commands that a general user will need for dealing with labeled objects.

3.3.1 Printing Labeled Objects

This section describes the mechanism for printing or otherwise producing non-electronic versions of labeled objects. Of specific interest is the mechanism that would be used for overriding the default printing of the object's label in human- readable form. The description of this capability could be accompanied by a discussion of the security considerations that go with its use.

3.3.2 Accessing Single-Level Devices

This section should discuss the constraints on the use of single-level devices in the presence of multiple authorization levels. For example, this section could discuss how the TCB determines a user's access to a single-level device based on the user's authorization level.

3.3.3 Accessing Multilevel Devices

This section should discuss the rules for the interaction between users at multiple authorization levels and multilevel devices.

3.3.4 Downgrading Labeled Objects

Although it is not a part of TCSEC evaluations, if the system offers an object downgrade facility that is available to the target audience of the SFUG, this facility and cautions on its proper use should be described.

3.3.5 MAC Errors and Their Causes

The possible error messages that can occur when MAC commands are improperly invoked should be noted and the correct or expected inputs should be explained.

3.4. OBJECT MANIPULATION FACILITIES

This section should discuss the commands and mechanisms available for dealing with objects.

3.4.1 Object Creation, Reuse, and Deletion

This section should discuss how the system creates, reuses, and deletes user visible objects. Any commands which allow the creation of user owned objects (e.g., mailboxes or blank files) should be described. The information on object reuse should be for informational purposes only, since all C2 and above systems are required to do object reuse without user intervention. For systems with MAC, this section should describe how sensitivity labels and discretionary access lists are assigned to an object.

3.4.2 Importing Machine-Readable Objects

The mechanisms for a user to introduce a machine-readable object into the system from an external source (e.g., tape, removable diskette, or network) and assign discretionary and mandatory access control properties to it should be described if such a facility exists.

3.4.3 Exporting Machine-Readable Objects

The mechanisms for a user to export a machine readable object from the system to an external source (e.g., tape, removable diskette, or, network), along with its discretionary and mandatory access control properties, should be described if such a facility exists.

3.4.4 Determining the Properties of Objects

The commands or mechanisms for determining the discretionary and mandatory access control properties of an object should be described.

3.4.5 Object Manipulation Errors and Their Causes

The possible error messages that can occur when object manipulation commands are improperly invoked should be noted and the correct or expected inputs should be explained.

THE TASK-ORIENTED SFUG

At a high level, the task-oriented example SFUG is arranged in the following fashion:

1. INTRODUCTION TO THE SFUG
2. SYSTEM SECURITY OVERVIEW
   - 2.1 SYSTEM PHILOSOPHY OF PROTECTION
   - 2.2 DEFINITION OF TERMS AND SERVICES
   - 2.3 THE SYSTEM SECURITY OFFICER
   - 2.4 USER SECURITY RESPONSIBILITIES
3. SECURITY-RELATED COMMANDS FOR USERS
   - 3.1 SYSTEM ACCESS
     - 3.1.1 Session Initiation
     - 3.1.2 Changing the Session Profile
     - 3.1.3 Changing the User Profile
     - 3.1.4 Potential Access Problems and Solutions
   - 3.2 ACCESS CONTROL FACILITIES
   - 3.3 PROTECTING REMOVABLE OBJECTS
   - 3.4 LOGGING SECURITY-RELEVANT EVENTS

The annotated outline follows.

1. INTRODUCTION TO THE SFUG

This part of the SFUG should identify what the SFUG is, who it is written for, and what it will cover. It might also explain where the SFUG fits in with the rest of the user documentation. If appropriate, it can also describe the relationship between the SFUG and the TFM.

2. SYSTEM SECURITY OVERVIEW

This section provides the background on the overall operation of the security controls in the system so that users can then understand the options and actions of individual security-relevant commands.

2.1 SYSTEM PHILOSOPHY OF PROTECTION

This section should describe the general environment for which the system is designed and briefly explain how this environment motivates the approach to protecting information stored in the system. The purpose of this section is to lay the foundation for the user's understanding of the system's security features, with later sections detailing what specific security services are available and when and how to use them.

2.2 DEFINITION OF TERMS AND SERVICES

This section should first introduce the terms that will be used to describe the security services available in the system and then proceed to introduce those services, without detailing exactly how they are used. Recommended topics (and the criteria classes for.which they are relevant) for this section are:

- An explanation of the general concepts of subjects and objects, followed by the identification of the subjects and objects in the system.

- An explanation of object reuse and its role in protecting information in the system.

- An explanation of the components of the I&A (identification and authentication) process (e.g., user-id, password, or smartcard) in the system and the importance of I&A to system security.

- An explanation of DAC, groups, privileges, protection bits/ACLs (access control lists), and any other terms and concepts related to the system's DAC policy, followed by a description of how the DAC policy applies to the system subjects and objects.

- An explanation of MAC, security labels, sensitivity levels, categories, authorizations, and any other terms and concepts related to the system's MAC policy, followed by a description of how the MAC policy applies to the system subjects and objects.

2.3 THE INFORMATION SYSTEM SECURITY OFFICER

This section discusses the role of the information system security officer (ISSO) in maintaining the security of the system. It can also explain which problems should be reported to the ISSO and which should be reported to the system administrator (if the roles are separate). If the format of the SFUG allows it, this section could have space for site-specific notes on the ISSO/user relationship.

2.4 USER SECURITY RESPONSIBILITIES

This section discusses the user's responsibilities with respect to properly using the system security features. This would optimally be a tutorial that teaches effective use of the system security services, but any presentation that relates the security services to the user's day-to-day use of the system is appropriate. Some issues that might be addressed are:

- Authentication token (e.g., password or smartcard) protection.

- Warnings about leaving a terminal unattended.

- Procedures for "locking" a process when the terminal must be left unattended, but logged in.

- Default DAC access for named objects (e.g., files and directories).

- Cautions about using programs that are not part of the standard system configuration (e.g., utilities or applications that have not been reviewed and tested by the system administrator(s)).

- Cautions about the effect of network access on system and data security.

3. SECURITY-RELATED COMMANDS FOR USERS

This section comprises the majority of the SFUG since it describes in detail the commands and procedures for actually using the system. It should describe both the usage of the commands and reemphasize their role as tools to protect information stored on the system. For example, this part might consist of command reference pages (e.g., UNIX "man" pages) grouped by subject, possibly with a brief introduction at the beginning of each subject area. Alternatively, this section could contain general descriptions of the operation and options of individual commands or groups of commands, along with pointers to the detailed documentation of the invocation sequence(s) for the commands.

3.1 SYSTEM ACCESS

This section should explain the procedures for logging on and off the system. It should also discuss how the TCB assigns privileges and authorizations during the login process and how the user can change them during the session (if the system allows in-session changes). This section might also discuss how users can prevent and detect compromise of their accounts. For systems that provide trusted path during a session, this section of the SFUG should describe the mechanism for invoking the trusted path and the effect of the invocation on the currently running process. Finally, the errors that might occur during the use of these commands and corrective actions should be described here.

3.1.1 Session Initiation

This section should describe the procedures that a user goes through to establish a session with the system. In B2 and above systems, this discussion will start by describing how a user establishes a trusted path between the terminal and the TCB. For any system, it will discuss the procedure for presenting the identification and authentication tokens (typically a user-id and password) to the system so that the system can establish a subject to act on behalf of the user. When the Iogin process provides the means for overriding the default group/project and subject sensitivity level, the use of these options should be described.

3.1.2 Changing the Session Profile

When the system provides the facilities for the user to dynamically modify his or her group/project participation and/or subject sensitivity level, this section should describe them.

3.1.3 Changing the User Profile

Many systems have the concept of a user profile, which contains the default settings for the creation of a user subject. Although it may actually be maintained separately, the user password is logically part of this profile. This section should provide information on how to modify the parts of the user profile over which the user has control. At a minimum, this section should show how the user can change his or her password (for systems where the password is the authentication token).

3.1.4 Potential Access Problems and Solutions

This section should discuss the possible problems that a user could encounter when logging into the system or modifying session and user profiles. This section could be organized as a troubleshooting guide, where each problem and its potential solution(s) is presented in a table format.

3.2 ACCESS CONTROL FACILITIES

This section describes the commands available to a user for managing the objects under his or her control. The major issue confronting the SFUG author in this section is how to organize the commands. Two possible options are:

- By security' policy functionality, i.e., all commands that manipulate MAC attributes, DAC attributes, exportation to devices, labeled human-readable output etc.

- By target object class, i.e., all security-relevant commands that manipulate files, directories, printers, tape drives, interprocess communication, floppy disks, etc.

Experience during previous evaluations indicates that the second option more closely matches the needs of the user, since it is closer to the organization expected when trying to search for a specific command to do a specific job.

3.3 PROTECTING REMOVABLE OBJECTS

This section should discuss some of the basic actions that a user should take to ensure that the data contained in hardcopy or external storage form is protected as fully as when it is on the computer system. In a site-specific SFUG, this section could be an even stronger statement regarding the site's procedures for protecting information once it leaves the system.

3.4 LOGGING SECURITY-RELEVANT EVENTS

In some systems, it may be possible for users to do limited auditing on the objects over which they have control. In these cases, the commands available to the user for this purpose should be described.

BIBLIOGRAPHY

1. DoD Trusted Computer System Evaluation criteria, Natonal Computer Security Center, DoD 5200.28-STD, 1985.

2. American Telephone and Telegraph System V/MLS Release 1.1.2 Running on UNIX System V Release 3.1.1 (Final Evaluation Report), National Computer Security Center, CSC-EPL-89/003, October 1989.
   This FER identified the following four documents as the SFUG for this product:
   - System V/MLS User's Guide and Reference Manual, August 1989,
   - 630/MLS User's Guide, August 1989,
   - 302 UNIX System V Programmer's Reference Manual, August 1989,
   - UNIX System V User's Guide, August 1989.

3. Computer Associates International CA-ACF2/VM, Release 3.1 (Final Evaluation Report), National Computer Security Center, CSC-EPL-87/007, September 1987.
   This FER identified the following four documents as the SFUG for this product:
   - Overview for CA-ACF2/""M Release 3.1, Publication Number AAG0042, Sept 1987,
   - General Information Manual for CA-ACF2/""M Release 3.1, PN AAG0033, 5ept1987,
   - New Features and Enhancements Manual for CA-ACF2NM Release 3.1, PN AAP0073, Sept 1987,
   - User's Guide for CA-ACF2NM Release 3.1, PN AAP0037, Sept 1987.

4. Computer Associates International Top Secret, Version 3.0 (Final Evaluation Report), DoD Computer Security Center, CSC-EPL-85/002,,- April 1985.
   This FER identified the following two documents as the SFUG for this product:
   - TOP SECRET User's Guide, Document US-03, 1985,
   - TOP SECRET TSS Reference Manual, Document TS-03, 1985.

5. Control Data Corporation Network Operating System Security Evaluation Package (Final Evaluation Report), National Computer Security Center, CSC-EPL-86/003, May 1986.
   This FER identified the following document as the SFUG for this product:
   - NOS Version 2 Reference Set, Volume 2: Guide to System Usage, Section14, Publication Number 60459670, Revision D, 1986.

6. Digital Equipment Corporation VAX/VMS, Version 4.3 (Final Evaluation Report), National Computer Security Center, CSC-EPL-86/004, July 1986.
   This FER identified the following document as the SFUG for this product:
   - Guide to VAX/VMS System Security, Chapters 1-4, AA-Y51 0A-TE, AA-Y51 0A-Tl, VAX/VMS Version 4.2, July 1985.

7. Data General Corporation Advanced Operating System/Virtual Storage

(A 05/VS) (Final Evaluation Report), National Computer Security Center, CSC-EPL-89/001, February 1989.

This FER identified the following two documents as the SFUG for this product:

- Learning to Use Your AOS/VS System, Product Number 069-000031-02, November 1088,
- AOS/VS System Calls Dictionary, Product Number 093-000241-03, September 1986.

8. Gould, Inc Computer Systems Division UTX/32S, Release 1.0 (Final Evaluation Report), National Computer Security Center, CSC-EPL-86/007, December 1986.

This FER identified the following document as the SFUG for this product:

- Using Gould UTX/325, Release 1.0, which is Volume 1 of Gould UTX/ 32S Document Set, Volume Order Number 323-005231-000, November 1986.

9. Hewlett Packard Commercial Systems Division MPE v/E (Final Evaluation Report), National Computer Security Center, CSC-EPL-88/01 0, October 1988.

This FER identified the following document as the SFUG for this product:

- MPE V/E Security and Account Structure User's Guide, Product Number 32033-90136, October 1988.

10. Honeywell MULTICS, MR1 1.0 (Final Evaluation Report), National Computer Security Center, CSC-EPL-85/003, June 1986.

This FER identified the following document as the SFUG for this product:

- Multics Programmers Reference Manual, Chapter 6, Order Number AG91-04,1986.

11. Honeywell SCOMP (Secure Communications Processor) STOP Release 2.1 (Final Evaluation Report), DoD Computer Security Center, CSC-EPL-85/001, September 1985.

This FER identified the following document as the SFUG for this product:

- SCOMP User's Reference Manual, STOP Release 2.1, November 1984.

12. International Business Machines Resource Access Control Facility (RACF), Version 1, Release 5 (Final Evaluation Report), DoD Computer Security Center, CSC-EPL-84/001, July 1984.

This FER identified the following document as the SFUG for this product:

- OS/VS2 MVS Resource Access Control Facility (RACF): General Information Manual, 5C28-0722-6, 1984.

13. International Business Machines Corporation VM/SP with RACF (Final Evaluation Report), National Computer Security Center, CSC-EPL-89/005, September 1989.

This FER identified the following six documents as the SFUG for this product:

- "Part Three: For General Users" in Virtual Machine/System

Product C2 Security Guide VMISP Release 5 and VM/SP HPO Release 5, Library Number 5C24-5384-0,' no date,
- RACF General User's Guide, Library Number 5C28-1341, December 1987,
- VM/SP CMS Command Reference, Library Number SCl 9-6209, no date,
- VM/Directory Maintenance Operation and Use, Library~Number 5C23-0437, March 1989,
- VMTAPE-MS User's Guide, Library Number 5H20-6245, September 1988,
- The VM HELP Facility, online function.

14. Prime Computer, Inc PRlMOS Rev 21.0.1. DODC2A (Final Evaluation Report), National Computer Security Center, CSC-EPL88/009, July 1988.
This FER identified the following document as the SFUG for this product:
- Security Features User's Guide, 1st Edition for Revision 21.0, 1987.

15. UNISYS Corporation A Series MCP/AS Release 3.7 (Final Evaluation Report), National Computer Security Center, CSC-EPL-87/003, August 1987.
This FER identified the following document as the SFUG for this product:
- A Series Security Features Operations and Programming Guide, Document Number 1195203, July 1987.

16. UNISYS Corporation OS 1100 (Final Evaluation Report), National Computer Security Center, CSC-EPL-89/004, September 1989.
This FER identified the following document as the SFUG for this product:
- OS 1100 Security System Operations Guide, UP-I 3011.1, August 1989.