Trusted Solaris 8 4/01
Security Target

Issue:	3.1
Date:	12 November 2003
Reference:	TS8_101
Author:	Deniz Kucukreisoglu
Status:	Definitive

Abstract: This document is the Security Target for the EAL4 Common Criteria v2.1 evaluation of Trusted Solaris 8 4/01 developed by Sun Microsystems, Inc.

This document was prepared by:

LogicaCMG CLEF (LFL),
LogicaCMG UK Limited,
Chaucer House,
The Office Park,
Leatherhead,
Surrey.
KT22 7LP

This document was prepared for and on behalf of:

SUN Microsystems, Inc.
17 Network Circle,
Menlo Park, California
94025
USA

Document History

Version	Date	Notes
2.0	14 June 2002	Issued Security Target for TSOL 8 4/01
3.0	4 Sep 2003	Updated to include ALC_FLR.1 for AMS1 - TSOL 8 HW 12/02
3.1	12 Nov 2003	Updated to include ALC_FLR.3 for AMS2 - TSOL 8 HW 7/03

Contents

References

Standards & Criteria

[CC] Common Criteria for Information Technology Security Evaluation, CCIMB-99-031, Version 2.1, August 1999

[CAPP] Controlled Access Protection Profile, Issue 1.d, 8 October 1999

[LSPP] Labelled Security Protection Profile, Issue 1.b, 8 October 1999

[RBAC] Role Based Access Control Protection, Issue 1.0, 30 July1998

[SOL8ST] Solaris 8 Security Target
Ref.: S8.0_101, Version 1.0, 28/07/00.

[NIST1] Letter from R. Chandramouli, re: FIA_UAU.2 in RBAC PP, Computer Security Division, NIST, dated 28 June 2001.

[NIST2] Letter from R. Chandramouli, re: FPT_TST.1.1 in RBAC PP, Computer Security Division, NIST, dated 16 July 2001.

[IAR] Impact Analysis & Rationale for Multiple CPU Variants of SunBlade 1000 and SunFire 280R running, TSOL 8 4/01, Issue 1.0, 22 November 2001

[FLR] Common Methodology for Information Technology Security Evaluation, Supplement: ALC_FLR - Flaw Remediation Version 1.1, February 2002

This Page Intentionally Left Blank

1 Introduction

1.1 ST Identification

Title: Trusted Solaris 8 4/01 Security Target

Keywords: Trusted Solaris 8 4/01, general-purpose operating system, POSIX, UNIX.

This document is the security target for the CC evaluation of the Trusted Solaris 8 4/01 operating system product, and is conformant to the Common Criteria for Information Technology Security Evaluation [CC].

1.2 ST Overview

This security target documents the security characteristics of the Trusted Solaris 8 4/01 operating system.

Trusted Solaris is a highly-configurable UNIX-based operating system which has been developed to meet the requirements for secure computing, including:

- "Multi-Level" Operations are a super-set of the System High operations supported through [LSPP] functionality with the addition of trusted networking and windowing;
- "System High" operation is supported via enhanced [CAPP] functionality, including the use of Access Control Lists (ACL) and privileges.

These broad requirements are described for the Common Criteria scheme in [CAPP], the Controlled Access Protection Profile, [LSPP], the Labeled Security Protection Profile and [RBAC], the Role-Based Access Control Protection Profile.

[LSPP] is a superset of [CAPP] and therefore when reference is made to [LSPP] then [CAPP] is encompassed within that.

Where DAC and MAC policy checks apply to the same operation, both checks must succeed in order for the operation to be permitted. The RBAC policy supports the DAC and MAC policies by providing the basis for security management. Possession of certain privileges allow subjects to bypass or override DAC or MAC checks, but this is an integral part of the DAC and MAC policy rules.

A Trusted Solaris 8 4/01 system consists of a number of workstations and servers linked together to form a single distributed system. Users share the resources of multiple workstations and servers connected together in a single, distributed Trusted Computing Base (TCB).

1.3 CC Conformance

This ST is conformant with the following:

- Controlled Access Protection Profile version 1.d [CAPP];
- Labeled Security Protection Profile, version 1.b [LSPP];
- Role-Based Access Control Protection Profile, version 1.0 [RBACPP].

This ST is CC *Part 2 extended* and *Part 3 conformant*, with a claimed Evaluation Assurance Level of EAL4 Augmented (see section 7.3.3). It is extended because it conforms to the above protection profiles.

1.4 Structure

The structure of this document is as defined by [CC] Part 1 Annex C.

- Section 2 is the TOE Description.
- Section 3 provides the statement of TOE security environment.
- Section 4 provides the statement of security objectives.
- Section 5 provides the statement of IT security requirements.
- Section 6 provides the TOE summary specification, which includes the detailed specification of the IT Security Functions.
- Section 7 provides the rationale for the security objectives, security requirements, TOE summary specification and PP claims against [CAPP], [LSPP] and [RBAC].

1.5 Terminology

This section contains definitions of technical terms that are used with a meaning specific to this document. Terms defined in the [CC] are not reiterated here, unless stated otherwise.

Action: An action is an execution of a command or system call.

Administrative User: This term refers to an administrator of a Trusted Solaris 8 4/01 system. Administrators are granted a rights profile, and may also be granted roles.

Audit Class: This is the name given to the definition of a collective grouping of events representing particular types of activity to be monitored; e.g. file read, network, administrative, application, process, file attribute modify, etc.

Authentication data: This includes a user identifier, password and authorizations for each user of the product.

Authorization: An authorization is a right granted to a user to perform an action that would otherwise by prohibited by the product. Trusted processes check for specific authorizations (for example, to change the sensitivity label on a file) before performing actions that require authorization.

*Common Desktop Environment (*or *CDE)*: An enhanced version of the Common desktop Environment, is provided with Trusted Solaris 8 4/01. CDE supports window and icon labelling, a trusted stripe, a trusted path, user and administrative workspaces, multilevel operations, and restricted execution based on rights profiles.

Object: In Trusted Solaris 8 4/01, objects belong to one of four categories: file system objects, other kernel objects (such as processes, programs and interprocess communication), window system objects and miscellaneous objects.

Process privilege: A process, typically executing on behalf of an authorized user or the TCB, must possess any necessary privileges if it has to perform security-related actions. A privilege is a right granted to a process to perform an action that would otherwise be prohibited by the product.

Product: The term product is used to define all hardware and software components that comprise the distributed Trusted Solaris 8 4/01 system.

Profile: see Rights Profile.

Public object: A type of object for which all subjects have read access, but only the TCB has write access.

Rights Profile: Rights profiles, often known simply as profiles, are a bundling mechanism for defining the capabilities of individual users and roles. Each named rights profile is a building block which consists of a set of UNIX commands, CDE Actions and authorizations. A rights profile also includes security attributes associated with each command and action. One or more rights profiles may be assigned to each user or role. In this way they allow administrators to define commands, and CDE actions that users are allowed to perform, along with the authorizations the user has.

Role: A role represents a set of actions that an authorized user, upon assuming the role, can perform.

Security Attributes: As defined by functional requirement FIA_ATD.1, the term 'security attributes' includes the following as a minimum: user identifier; group memberships; user authentication data; sensitivity label, clearance; and rights profile (including authorizations and roles).

Sensitivity labels: In Trusted Solaris 8 4/01, a sensitivity label is one of the security attributes used to enforce access rights to subjects and objects. It represents the level at which information is protected. Sensitivity labels consist of two parts: a hierarchical *classification* and non hierarchical *compartment* sets. The classification represents the security level (for example, RESTRICTED), while compartments comprise a set that usually represent work groups, projects or topics (for example, CODEWORD).

Subject: There are two classes of subjects in Trusted Solaris 8 4/01:

- untrusted subject - this is a Trusted Solaris 8 4/01 process running on behalf of some user, running outside of the TCB (for example, with no privileges).
- trusted subject - this is a Trusted Solaris 8 4/01 process running as part of the TCB. Examples are service daemons and the processes implementing the windowing system.

System: Includes the hardware, software and firmware components of the Trusted Solaris 8 4/01 product which are connected/networked together and configured to form a usable system.

Target of Evaluation (TOE): The TOE is defined as the Trusted Solaris 8 4/01 operating system, running and tested on the hardware and firmware specified in this Security Target. The Openboot PROM firmware forms part of the IT Environment (see section 5.4).

Trusted Process: A process which is part of the TCB and which, due to its privileges, may perform actions on behalf of a user.

User: Any individual/person who has a unique user identifier and who interacts with the Trusted Solaris 8 4/01 product.

1.6 Document Layout

IT security functions are assigned a unique reference identifier of the form Name.1 to enable ease of reference. For example, DAC.1, Audit.1.

2 TOE Description

2.1 Introduction

The TOE description aims to aid the understanding of the TOE's security requirements and provides a context for the evaluation. It defines the scope and boundaries of the TOE, both physically and logically, and describes the environment into which the TOE will fit.

2.2 Intended Use

Trusted Solaris 8 4/01 is a highly-configurable UNIX-based trusted operating system which has been developed to meet a number of operational requirements for secure computing, including:

- "Multi-Level" Operations are a super-set of the System High operations supported through [LSPP] functionality with the addition of trusted networking and windowing;
- "System High" Operation is supported via enhanced discretionary access control functionality, including the use of Access Control Lists and privileges.

Trusted Solaris 8 4/01 is intended for use in organisations who need to safeguard sensitive information (e.g., organisations concerned with processing commercially sensitive or classified information) and who require security features unavailable in standard commercial operating environments.

A Trusted Solaris 8 4/01 system consists of a number of workstations and servers linked together to form a single distributed system. Users share the resources of multiple workstations and servers connected together in a single, distributed Trusted Computing Base (TCB).

Trusted Solaris 8 4/01 allows both the system and individual users to be configured either as single or multi-level. The appearance that Trusted Solaris 8 4/01 presents to users can also be configured, as it is possible to enable or disable the display of sensitivity labels (on a per user basis). It should be noted however, that even with the display of sensitivity labels disabled, the underlying security mechanisms uphold the multi-level security policy even though the user is unaware of it. Thus, Trusted Solaris 8 4/01 can be configured to appear to end users as, for example, a multi-level system [LSPP], or a system-high secure system. Admin.10 provides the mechanism to configure the system into multi-level or system-high mode.

The Trusted Solaris 8 4/01 product offers users:

- trusted version of the Solaris 8 UNIX-based operating system consisting of security features in excess of [LSPP] requirements;
- trusted client/server network architecture;
- trusted networking to other trusted and commercial (unlabelled) systems, including TCP/IP and TSIX *(not within the scope of evaluation)*;
- a multi-level secure X11 window environment (including remote windows) based on the Common Desktop Environment (CDE);
- compatibility with a large number of commercial applications targeted for Solaris 8 *(not within the scope of evaluation)*; and
- ease of use for users, administrators and security officers, including a graphical user interface based on the Common Desktop Environment (CDE).

2.3 Evaluated Configurations

2.3.1 Target of Evaluation

This section defines the Workstations/Servers, Peripherals and Software that comprise the ToE.

2.3.1.1 Workstations/Servers

The target of evaluation is a (distributed) product based on Sun UltraSPARC II, IIe and III based workstations and servers and Intel Pentium III processors.

Each system is configured with a minimum of 128 MByte of RAM and a colour bitmap monitor. A mass storage disk of at least 2 GB is configured.

Platform1A: PC, Intel Pentium III CPU, with Hard disk, PCI graphics card, Ethernet Network card, standard IDE CD-ROM drive, Standard Floppy disk drive, Standard keyboard, PS/2 mouse, 1 Parallel and 2 Serial External Interfaces;

Platform1B: PC, Intel Pentium III CPU, with Hard disk, graphics card, Ethernet Network card, standard IDE CD-ROM drive, Standard Floppy disk drive, Standard keyboard, PS/2 mouse, 1 Parallel and 2 Serial External Interfaces;

Platform2: SunBlade 100, 500Mhz UltraSPARC IIe CPU, with IDE Hard disk, Ethernet Network card, built-in graphics card, built-in audio card, USB keyboard, and mouse, standard DVD-ROM drive, standard floppy disk drive, built-in Smart-

card Reader (not within the scope of evaluation), 1 Parallel and 2 Serial External Interfaces;

Platform3A: SunBlade 1000 model 2750, dual UltraSPARC III CPU, 2 x Hard disk, 2 x Firewire External Interfaces, Ethernet Network card, graphics card, built-in audio card, USB keyboard and mouse, standard DVD-ROM drive, standard floppy disk drive, built-in Smartcard Reader (not within the scope of evaluation), 1 UltraSCSI (SCSI-3),1 Parallel and 2 Serial External Interfaces;

Platform3B: SunFire 280R, dual UltraSPARC III CPU, 2 x Hard disk, 2 x Firewire External Interfaces, Ethernet Network card, graphics card, built-in audio card, USB keyboard and mouse, standard DVD-ROM drive, 1 UltraSCSI (SCSI-3),1 Parallel and 2 Serial External Interfaces;
(Note that this platform is the rack mountable equivelent of the SunBlade1000 demostrated by the [IAR].

Platform4: Enterprise 420R, dual 450Mhz UltraSPARC II, 2 x SCSI-3 Hard disk, built-in Ethernet Network card, PCI graphics card, standard PS2keyboard 2-button mouse, standard CD-ROM drive, standard floppy disk drive, 1 UltraSCSI (SCSI-3), 1 Parallel and 2 Serial External Interfaces;

2.3.1.2 Software

The Target of Evaluation is based on the following system software:

Trusted Solaris 8 4/01 including SMC.

The TOE documentation is supplied on CD-ROM.

2.3.2 File systems

The following multilevel file systems are supported:

- the native UNIX file system, `ufs` with Trusted Solaris attributes;
- the remote filesystem protocol for UNIX filesystem access with Trusted Solaris attributes, `tnfs` (Trusted Solaris 8 4/01, TSIG);
- the in-memory filesystem, `tmpfs`; and
- the loopback filesystem, `lofs`.

The following single level filesystems types are supported (with fixed attributes):

- the Solaris UNIX filesystem, `ufs`;
- the remote filesystem access protocol, `nfs` (V2 and V3);
- the MS-DOS formatted filesystem `pcfs`; and
- the High Sierra filesystem for CD-ROM drives, `hsfs`.

In addition to the above file systems a number of "internal" filesystems are supported:

- The file descriptor file system, `fd`, allows programs to access their own file descriptors through the file name space, such as `/dev/stdin` corresponding to `/dev/fd0`;
- The names file system, `namefs` (or `namfs`) allows the arbitrary mounting of any file descriptor on top of another file name;
- The doors file system, `doorfs` allows fast control transfer between processes on the same machine;
- the swap filesystem, `swapfs`;
- The process file system, `procfs` (`/proc`), provides access to the process image of each process on the machine as if the process were a "file". Process access decisions are enforced by DAC and MAC attributes inferred from the underlying process' DAC and MAC attributes.

2.3.3 Configurations

The evaluated configurations are defined as follows.

The product comprises one or more of the above listed workstations (and optional peripherals) running the above listed system software (a workstation running the above listed software is referred to as a "TOE workstation" below).

If the product is configured with more than one TOE workstation, they are linked by LANs, which may be joined by bridges/routers or by TOE workstations which act as routers/gateways.

No other processors may be connected over the network, except as noted below.

The product supports the NIS+ protocol.

Interoperability with Trusted Solaris 2.5.1 is supported *(this was not within the scope of evaluation)* with the following limitations:

- Internet services, including **rlogin**, **telnet** and **ftp** *are* supported between Trusted Solaris 8 4/01 and Trusted Solaris 2.5.1.
- Multilevel data *can* be transferred between Trusted Solaris 8 4/01 and Trusted Solaris 2.5.1 using **tar**.
- File transfer via **ufsdump** and **ufsrestore** is not supported.
- A Trusted Solaris 8 4/01 machine cannot be used as an audit server for a Trusted Solaris 2.5.1 machine (and vice versa);
- The ability to cross administrate machines between Trusted Solaris 8 4/01 and Trusted Solaris 2.5.1 is not supported.
- Non privileged multilevel window operations are supported between Trusted Solaris 8 4/01 and Trusted Solaris 2.5.1.

Interoperability with Solaris 8 is supported *(this was not within the scope of evaluation)* with the following limitations:

- Data exchange can be carried out using **tar** or **cpio**, dumping and restoring filesystems using **ufsdump** and **ufsrestore** is not supported;
- Trusted Solaris 8 4/01 can be used as an audit server for Solaris machines, however the reverse is not possible due to the addition of additional security attributes to the audit data;
- Cross administration between Trusted Solaris 8 4/01 and Solaris is not supported.
- Networking is supported at a single sensitivity level, this includes various internet services such as **rsh**, **rcp**, **rlogin**, **telnet** and **ftp**;
- NFS client and server functions are supported at a single level is supported in either direction;
- Windows can be displayed between Solaris 8 and Trusted Solaris 8 4/01 at a single sensitivity level;
- Solaris 8 can be used as an unlabelled print server for Trusted Solaris 8 4/01 (but not vice versa)

The diagram below is a typical evaluated configuration.

.

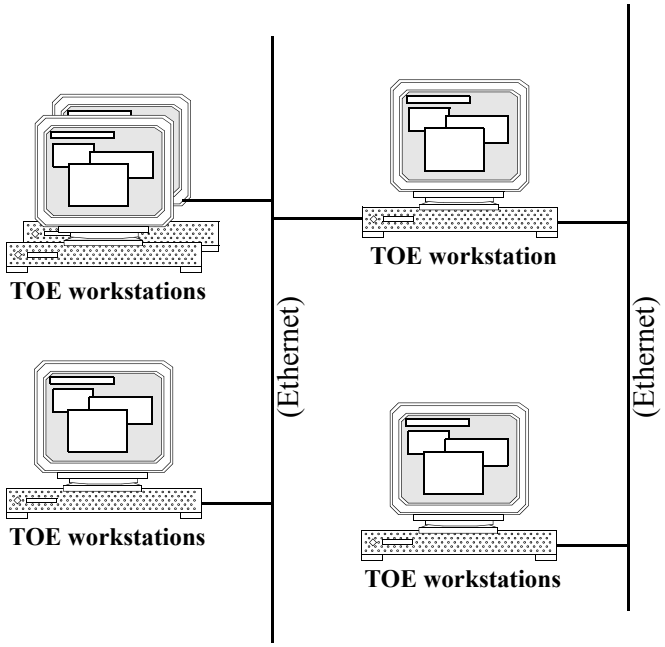

Table 1: Typical Evaluation Configuration

2.4 Summary of Security Features

The primary security features of the product are:

- Mandatory Access Control (MAC);
- Discretionary Access Control (DAC);
- Object Reuse functionality;
- Identification and Authentication;
- Privileges and Authorisations;
- Trusted Path;
- Roles and Profiles; and
- Auditing.

2.4.1 MAC

Sensitivity labels are used to represent the security level of users, files and other system objects. Trusted Solaris 8 4/01 assigns Sensitivity Labels to objects such as users' processes and files and these labels are used by Trusted Solaris 8 4/01 as the basis for Mandatory Access Control.

2.4.2 DAC

Discretionary Access Control (DAC) restricts access to objects, such as files and is based on Access Control Lists (ACLs) and the standard UNIX permissions for user, group and other users.

2.4.3 Object Reuse

Object Reuse functionality ensures that memory and other storage objects do not contain data when they are re-allocated.

2.4.4 Identification and Authentication

Trusted Solaris 8 4/01 provides identification and authentication based upon user passwords.

2.4.5 Privileges and Authorizations

Privileges and Authorizations are two separate mechanisms that confer security rights to processes and users respectively. Authorizations apply to users. In order for a user to perform an action that would otherwise be prohibited by the Trusted Solaris 8 4/01 security policy, the user must have an authorization.

2.4.6 Trusted Path

The Trusted Path is a visible feature that acts as a non-bypassable communications path between the user and the security-related software.

2.4.7 Roles and Profiles

Trusted Solaris 8 4/01 supports the concept of Roles, allowing administrative powers to be broken into many discrete Roles. This removes the requirement of one *superuser (root or only one system-administrator)* to administer the TOE. A Role consists of a set of profiles. Profiles can be populated with the required authorisations appropriate to the defined Role, thus allowing the administrative functionality to be distributed and hence diluted amongst the Roles, to reduce the impact of any misuse of a Role.

2.4.8 Auditing

Trusted Solaris 8 4/01 can collect extensive auditing information about security related actions taken or attempted by users, ensuring that users are accountable for their actions. For each such action or event an audit record is generated containing: date & time of the event, user, security attributes and success or failure. This audit trail can be analysed to identify attempts to compromize security and determine the extent of the compromize.

3 TOE Security Environment

3.1 Introduction

The statement of TOE security environment describes the security aspects of the environment in which the TOE is intended to be used and the manner in which it is expected to be employed.

To this end, the statement of TOE security environment identifies the assumptions made on the operational environment (including physical and procedural measures) and the intended method of use of the for the product, defines the threats that the product is designed to counter, and the organisational security policies with which the product is designed to comply.

3.2 Threats

The assumed security threats are listed below.

The **IT assets** to be protected comprise the information stored, processed or transmitted by the TOE. The term “information” is used here to refer to all data held within a workstation, including data in transit between workstations.

The TOE counters the general threat of unauthorised access to information, where “access” includes disclosure, modification and destruction.

The **threat agents** can be categorised as either:

- unauthorised users of the TOE, i.e., individuals who have not been granted the right to access the system; or
- authorised users of the TOE, i.e., individuals who have been granted the right to access the system.

The threat agents are assumed to originate from a well managed user community in a non-hostile working environment, and hence the product protects against threats of inadvertent or casual attempts to breach the system security. The TOE is not intended to be applicable to circumstances in which protection is required against determined attempts by hostile and well funded attackers to breach system security.

[T.ACCESS_INFO] An authorised user of the TOE accesses information without having permission from the person who owns, or is responsible for, the information.

In this context ‘access’ is to be interpreted as observing information for which the user has no ‘need to know’, even though that user may have sufficient clearance to see the information.

[T.ACCESS_TOE] An unauthorised user of the TOE gains access to the system, thereby gaining unauthorised access to information.

An unauthorised user of the TOE could gain access to the system by impersonating an authorised user, or by gaining access to an unattended workstation at which an authorised user is logged on. Failure to detect the fact that an attack is taking place, or that many attempts have taken place over a period of time, may result in the attack eventually succeeding, resulting in the attacker gaining unauthorised access to information.

[T.MODIFY] Unauthorised modification or destruction of information by an authorised user of the TOE.

In this context ‘unauthorised’ means not having the explicit or implicit permission of the designated owner of the information.

[T.ADMIN_RIGHTS] Unauthorised use of facilities which require administration rights by an authorised user of the TOE.

Unauthorised use of such facilities by a user who cannot be trusted not to misuse them (whether intentionally or accidentally) could be exploited to gain unauthorised access to information.

[T.CLEARANCE] Unauthorised access to information for which the user is not cleared.

In this context ‘access’ is interpreted as observing information which the user is not cleared to see, even though that user may not be explicitly denied access by the person who owns, or is responsible, for that information.

[T.TRANSIT] Data transferred between workstations is disclosed to or modified by unauthorised users or processes either directly or indirectly (e.g., through spoofing of workstation identity).

3.3 Organisational Security Policies

The TOE complies with the following organisational security policies:

[P.AUTH] Only those users who have been authorised to access the information within the system may access the system.

[P.DAC] The right to access specific data objects is determined on the basis of:

a) the owner of the object; and

b) the identity of the subject attempting the access; and

c) the privilege of the subject attempting the access; and

d) the implicit and explicit access rights to the object granted to the subject by the object owner.

[P.ACCOUNTABLE] The users of the system shall be held accountable for their actions within the system.

[P.CLASSIFICATION] Subjects shall only be able to:

- read information if the sensitivity label of the object is less than or equal to the sensitivity label of the subject; and
- write to an object if the sensitivity label of the subject is less than or equal to the sensitivity label of the object, and the sensitivity label of the object is less than or equal to the clearance of the subject; and
- read or write information if the subject has privileges to override the rules above.

Information is therefore to be assigned a label designating the sensitivity of the information, controlling the set of individuals who are allowed by the organisation to see that information, in accordance with the designated clearance. Subjects are not permitted to 'write-up' beyond their clearance. Downgrade of the sensitivity of the information is only to be performed by authorised individuals.

3.4 Assumptions

This section describes the assumptions about the environment in which the TOE is to be used and its intended method of use. It is not a complete list, as specific measures may be required for different configurations and sites.

3.4.1 Physical Aspects

[A.PROTECT] It is assumed that all software and hardware, including network and peripheral cabling is approved for the transmittal of the most sensitive data held by the system. Such items are assumed to be physically protected against threats to the confidentiality and integrity of the data transmitted.

3.4.2 Personnel Aspects

[A.ADMIN] It is assumed that there are one or more competent individuals who are assigned to manage the TOE and the security of the information it contains. Such personnel are assumed not to be careless, wilfully negligent or hostile.

3.4.3 Procedural Aspects

[A.USER] Each individual user is assumed to have a unique user ID.

[A.PASSWORD] Those responsible for the TOE must configure minimum password length for normal users to be at least 8 characters.

3.4.4 Connectivity Aspects

[A.NIS_DOMAINS] It is assumed that, if the product comprises more than one workstation, all workstations are administered from a central point within each NIS+ domain.

NIS+ allows the creation of multiple administrative domains, thus allowing administrators to control local resources and user accounts, yet making it possible for users and resources to operate seamlessly over the entire organisation.

Administrators can control *nsswitch.conf* file on each workstation to specify the sources of information, and give a look up order, that each workstation uses to retrieve critical data (e.g., hosts, users, groups).

[A.BRIDGES&ROUTERS] All bridges and routers are assumed to correctly pass data without modification.

4 Security Objectives

4.1 Security Objectives for the TOE

[O.AUTHORISATION] The TOE must ensure that only authorized users gain access to the TOE and its resources.

[O.DAC] The TOE must provide its users with the means of controlling and limiting access to the objects and resources they own or are responsible for, on the basis of individual users or identified groups of users, and in accordance with the set of rules defined by the P.DAC security policy.

[O.MAC] The TOE must provide its users with the means of controlling and limiting access to objects and resources, on the basis of sensitivity labels and categories of the information being accessed and the clearance of the subject attempting to access that information in accordance with the set of rules defined by the P.CLASSIFICATION security policy.

[O.AUDIT] The TOE must provide the means of recording any security relevant events, so as to:

a) assist an administrator in the detection of potential attacks or misconfiguration of the TOE security features that would leave the TOE susceptible to attack; and

b) hold users accountable for any actions they perform that are relevant to security.

[O.RESIDUAL_INFO] The TOE must ensure that any information contained in a protected resource is not accessible when the resource is recycled.

[O.MANAGE] The TOE must allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.

[O.ENFORCEMENT] The TOE security policy is enforced in a manner which ensures that the organisational policies are enforced in the target environment i.e., the integrity of the TSF is protected.

[O.DUTY] The TOE must provide the capability of enforcing separation of duties, so that no single user is required to perform all administrative functions.

[O.HIERARCHICAL] The TOE must allow hierarchical definitions of profile rights. The hierarchical definition of rights gives the ability to define profile rights in terms of other profile rights.

[O.ROLE] The TOE must prevent users from gaining access to and performing operations on its resources and objects unless they have been granted access by the resource or objects owner or have been assigned a rights profile or role which permits those operations.

4.2 Security Objectives for the TOE Environment

[O.ADMIN] Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.

[O.ACCOUNTABLE] Those responsible for the TOE must ensure that:

a) The product is configured such that only the approved group of users for which the system was accredited may access the system.

b) Each individual user is assigned a unique user ID.

[O.AUDITDATA] Those responsible for the TOE must ensure that the audit functionality is used and managed effectively. In particular:

a) Procedures must exist to ensure that the audit trail for the product (i.e., all networked components containing an audit trail) is regularly analysed and archived, to allow retrospective inspection.

b) The auditing system must be configured such that the loss of audit data is minimized upon:

- planned or unplanned shutdown; or
- lack of available audit storage (in particular administrators should ensure that the AUDIT_CNT flag is correctly set as identified in the Administration documentation supplied with the TOE, and that remote partitions are mounted with the appropriate option so that audit information is not lost when the partition fills).

c) The auditing system must be configured such that bad authentication data will not be stored in the audit trail (in particular, administrators should ensure that the PASSWD flag is correctly set as identified in the Administration documentation supplied with the TOE).

d) The media on which audit data is stored must not be physically removable from the workstation by unauthorized users.

[O.AUTHDATA] Those responsible for the TOE must ensure that user authentication data is stored securely and not disclosed to unauthorized individuals. In particular:

a) Procedures must be established to ensure that user passwords generated by an administrator during user account creation or modification are distributed in a secure manner, as appropriate for the clearance of the system.

b) The media on which authentication data is stored must not be physically removable from the workstation by unauthorized users.

c) Users must not disclose their passwords to other individuals.

[O.BOOT] Hardware and firmware within the IT environment shall ensure that the correct copy of the Trusted Solaris 8 4/01 operating system is “booted” during system start-up.

Note: The above is enforceable in Sparc workstations and servers. For Intel platforms, the above may be achieved through the PC BIOS (i.e., firmware), but administrators should also take precautions to prevent booting from the floppy drive, CD device or over the network where this is considered a threat.

[O.CLEARANCE] Procedures exist for granting users authorisation for access to specific security levels.

[O.CONNECT] Those responsible for the TOE must ensure that no connections to outside systems or users undermine the security of IT assets.

[O.CONSISTENCY] Administrators of the TOE must establish and implement procedures to ensure the consistency of the security-related data across all distributed components that are networked to form a single system (e.g., authentication data). In particular, if the product comprises more than one workstation, all such workstations are administered from a central point within each NIS+ domain.

[O.INSTALL] Those responsible for the TOE must establish and implement procedures to ensure that the hardware, software and firmware components that comprise the networked product are distributed, installed and configured in a secure manner.

[O.INFO_PROTECT]Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular:

a) DAC and MAC protections on security critical files (such as audit trails and authentication databases) shall always be set up correctly.

b) All network and peripheral cabling must be approved for the transmittal of the most sensitive data held by the system. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted.

[O.LABELS] Removable information storage shall bear visible labels indicating the security classification of the information and associated security markings, such as handling caveats and dissemination limitations.

[O.MAINTENANCE] Administrators of the TOE must ensure that the comprehensive diagnostics facilities provided by the product are invoked at every scheduled preventative maintenance period.

[O.RECOVER] Those responsible for the TOE must ensure that procedures and/or mechanisms are provided to assure that, after system failure or other discontinuity, recovery without a protection (i.e., security) compromise is obtained.

[O.SOFTWARE_IN] Those responsible for the TOE shall ensure that the system shall be configured so that only an administrator can introduce new software into the system.

[O.SENSITIVITY] Procedures exist for establishing the security level of all information imported into the system, for establishing the security level for all peripheral devices (e.g., printers, disk drives) attached to the TOE, and marking a sensitivity level on all output generated.

The following security objective applies in environments where specific threats to distributed systems need to be countered, as described in section 3. Typically this objective is met by cryptographic protection of network connections.

[O.PROTECT] Those responsible for the TOE must ensure that procedures and/or mechanisms exist to ensure that data transferred between workstations is secured from disclosure, interruption or tampering.

5 Security Requirements

5.1 TOE Security Functional Requirements

The security functional requirements for the TOE are listed in the following table (classes, families, components and elements), with cross-references to [LSPP] and [RBAC] where these are derived from either PP. An asterisk (*) after the element's name indicates that one or more operations on that element are completed in this ST. Iteration of a component is indicated by ";N" after the element name.

CLASS	FAMILY	COMPONENT	ELEMENT	[LSPP] paragraph	[RBAC] paragraph
FAU	FAU_GEN	FAU_GEN.1	FAU_GEN.1.1 FAU_GEN.1.2	5.1.1.1 5.1.1.2	5.1.1 5.1.1
		FAU_GEN.2	FAU_GEN.2.1	5.1.2.1	5.1.1
	FAU_SAR	FAU_SAR.1	FAU_SAR.1.1 FAU_SAR.1.2	5.1.3.1 5.1.3.2	5.1.1 5.1.1
		FAU_SAR.2	FAU_SAR.2.1	5.1.4.1	5.1.1
		FAU_SAR.3	FAU_SAR.3.1*	5.1.5.1	5.1.1
	FAU_SEL	FAU_SEL.1	FAU_SEL.1.1*	5.1.6.1	5.1.1
	FAU_STG	FAU_STG.1	FAU_STG.1.1 FAU_STG.1.2	5.1.7.1 5.1.7.2	5.1.1 5.1.1
		FAU_STG.3	FAU_STG.3.1*	5.1.8.1	
		FAU_STG.4	FAU_STG.4.1*	5.1.9.1	
FDP	FDP_ACC	FDP_ACC.1	FDP_ACC.1.1;1* FDP_ACC.1.1;2	5.2.1.1	 5.1.2
	FDP_ACF	FDP_ACF.1	FDP_ACF.1.1;1* FDP_ACF.1.2;1* FDP_ACF.1.3;1* FDP_ACF.1.4;1* FDP_ACF.1.1;2 FDP_ACF.1.2;2 FDP_ACF.1.3;2 FDP_ACF.1.4;2	5.2.2.1 5.2.2.2 5.2.2.3 5.2.2.4	 5.1.2 5.1.2 5.1.2 5.1.2
	FDP_ETC	FDP_ETC.1	FDP_ETC.1.1 FDP_ETC.1.2 LSPP Note 6*	5.2.3.1 5.2.3.2 5.2.3.3	

Table 2: Security Functional Requirements

CLASS	FAMILY	COMPONENT	ELEMENT	[LSPP] paragraph	[RBAC] paragraph
		FDP_ETC.2	FDP_ETC.2.1 FDP_ETC.2.2 FDP_ETC.2.3 FDP_ETC.2.4*	5.2.4.1 5.2.4.2 5.2.4.3 5.2.4.4	
	FDP_IFC	FDP_IFC.1	FDP_IFC.1.1*	5.2.5.1	
	FDP_IFF	FDP_IFF.2	FDP_IFF.2.1 FDP_IFF.2.2* FDP_IFF.2.3* FDP_IFF.2.4* FDP_IFF.2.5* FDP_IFF.2.6* FDP_IFF.2.7	5.2.6.1 5.2.6.2 5.2.6.3 5.2.6.4 5.2.6.5 5.2.6.6 5.2.6.7	
	FDP_ITC	FDP_ITC.1	FDP_ITC.1.1 FDP_ITC.1.2 FDP_ITC.1.3*	5.2.7.1 5.2.7.2 5.2.7.3	
		FDP_ITC.2	FDP_ITC.2.1 FDP_ITC.2.2 FDP_ITC.2.3 FDP_ITC.2.4 FDP_ITC.2.5*	5.2.8.1 5.2.8.2 5.2.8.3 5.2.8.4 5.2.8.5	
	FDP_RIP	FDP_RIP.2	FDP_RIP.2.1	5.2.9.1	
			LSPP Note 1	5.2.10.1	
FIA	FIA_ATD	FIA_ATD.1	FIA_ATD.1.1*	5.3.1.1	5.1.3
	FIA_SOS	FIA_SOS.1	FIA_SOS.1.1	5.3.2.1	
	FIA_UAU	FIA_UAU.2	FIA_UAU.2.1	5.3.3	5.1.3
		FIA_UAU.7	FIA_UAU.7.1	5.3.4.1	
	FIA_UID	FIA_UID.2	FIA_UID.2.1	5.3.5	5.1.3
	FIA_USB	FIA_USB.1	FIA_USB.1.1;1* FIA_USB.1.1;2* FIA_USB.1.1;3*	5.3.6.1 5.3.6.2 5.3.6.3	5.1.3
FMT	FMT_MSA	FMT_MSA.1	FMT_MSA.1.1;1* FMT_MSA.1.1;2* FMT_MSA.1.1;3 FMT_MSA.1.1;4	5.4.1.1 5.4.1.2	 5.1.4(3) 5.1.4(4)
		FMT_MSA.2	FMT_MSA.2.1		5.1.4
		FMT_MSA.3	FMT_MSA.3.1;1 FMT_MSA.3.1;2 FMT_MSA.3.1;3* FMT_MSA.3.2*	5.4.2.1 5.4.2.2 5.4.2.3	 5.1.4 5.1.4

Table 2: Security Functional Requirements

CLASS	FAMILY	COMPONENT	ELEMENT	[LSPP] paragraph	[RBAC] paragraph
	FMT_MTD	FMT_MTD.1	FMT_MTD.1.1;1 FMT_MTD.1.1;2 FMT_MTD.1.1;3 FMT_MTD.1.1;4 FMT_MTD.1.1;5	5.4.3.1 5.4.4.1 5.4.5.1 5.4.6.1 5.4.6.2	5.1.4
		FMT_MTD.3	FMT_MTD.3.1		5.1.4
	FMT_REV	FMT_REV.1	FMT_REV.1.1;1 FMT_REV.1.2;1* FMT_REV.1.1;2 FMT_REV.1.2;2*	5.4.7.1 5.4.7.2 5.4.8.1 5.4.8.2	5.1.4 5.1.4
	FMT_SMR	FMT_SMR.1	FMT_SMR.1.1* FMT_SMR.1.2	5.4.9.1 5.4.9.2	
		FMT_SMR.2	FMT_SMR.2.1* FMT_SMR.2.2 FMT_SMR.2.3		5.1.4 5.1.4 5.1.4
FPT	FPT_AMT	FPT_AMT.1	FPT_AMT.1.1*	5.5.1.1	5.1.5
	FPT_FLS	FPT_FLS.1	FPT_FLS.1.1		5.1.5
	FPT_RCV	FPT_RCV.1	FPT_RCV.1.1		5.1.5
		FPT_RCV.4	FPT_RCV.4.1*		5.1.5
	FPT_RVM	FPT_RVM.1	FPT_RVM.1.1	5.5.2.1	5.1.5
	FPT_SEP	FPT_SEP.1	FPT_SEP.1.1 FPT_SEP.1.2	5.5.3.1 5.5.3.2	5.1.5 5.1.5
	FPT_STM	FPT_STM.1	FPT_STM.1.1	5.5.4.1	5.1.5
	FPT_TST	FPT_TST.1	FPT_TST.1.1 FPT_TST.1.2 FPT_TST.1.3		5.1.5
FTA	FTA_LSA	FTA_LSA.1	FTA_LSA.1.1		5.1.6
	FTA_SSL	FTA_SSL.1	FTA_SSL.1.1* FTA_SSL.1.2*		
		FTA_SSL.2	FTA_SSL.2.1 FTA_SSL.2.2*		
	FTA_TSE	FTA_TSE.1	FTA_TSE.1.1		5.1.6
FTP	FTP_TRP	FTP_TRP.1	FTP_TRP.1.1* FTP_TRP.1.2* FTP_TRP.1.3*		

Table 2: Security Functional Requirements

The following should be noted:

- The set of auditable events for FAU_GEN.1.1 is formed from the union of the sets of auditable events mandated in [LSPP] and [RBAC].
- "LSPP Note 1" and "LSPP Note 6" refer to extensions of CC Part 2 components as specified in [LSPP].
- The first and second iterations of FMT_MSA.1.1 in [RBAC] are addressed by FMT_MTD.1.1;3.

The following subsections specify SFRs from [LSPP] and [RBAC] that are tailored in this security target, together with FTA_SSL.1&2 and FTP_TRP.1 which are additional to those stated in the protection profiles. (Note in some cases an untailored element has been included where it is key to understanding the tailored elements within the same component.)

Completion of assignment or selection operations within this security target is indicated by underlined text. Refinement of CC Part 2 functional components is indicated by *italicised* text.

5.1.1 Security Audit (FAU)

5.1.1.1 Security Audit Review

The TSF shall provide the ability to perform searches, sorting and ordering of audit data based on the following attributes: FAU_SAR.3.1

a) User identity;

b) Subject label;

c) Object label;

d) Date and time of audit event;

e) Object name & type of access;

f) Role that enabled the access (through what role was assumed);

g) Any combination of items (a), (d), (e) or (f);

h) Sensitivity Label;

i) type of audit event and audit class.

5.1.1.2 Security Audit Event Selection

The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes: FAU_SEL.1.1

a) User identity;

b) Subject label;

c) Object label;

d) Object identity;

e) Subject identity;

f) Host identity;

g) Users belonging to a specified Role and Access types (e.g. delete, insert) on a particular object;

h) Sensitivity Label;

i) audit class.

5.1.1.3 Security Audit Event Storage

The TSF shall generate an alarm to the authorized administrator if the audit trail reaches 100% full. FAU_STG.3.1

The TSF shall *be able to* prevent auditable events, except those taken by the authorized administrator, if the audit trail is full. FAU_STG.4.1

5.1.2 User Data Protection (FDP)

5.1.2.1 Discretionary Access Control

The TSF shall enforce the Discretionary Access Control Policy on subjects acting on the behalf of users, filesystem objects and all operations among subjects and objects covered by the DAC policy. FDP_ACC.1.1;1

The TSF shall enforce the Discretionary Access Control Policy to objects based on the following: FDP_ACF.1.1;1

a) The user identity and group membership(s) associated with a subject; and

b) The access control attributes associated with an object: ACL, permission bits

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: FDP_ACF.1.2;1

IF the object has an explicit ACL, THEN:

- access granted to the object's owner is based on the user::rwx permissions
- access granted to individuals specified in the ACL is based on the bitwise AND operation of the user:[specified]:rwx and mask:rwx permissions
- access granted to subjects who belong to the object's group is based on the bitwise AND operation of the group::rwx and the mask:rwx entries
- access granted to subjects who belong to groups specified in the ACL is based on the bitwise AND operation of the group:[specified]:rwx and mask:rwx permissions
- access granted to all other subjects is based on the object's *other* permissions

ELSE

- access granted to the object's owner is based on the object *user* rwx permissions
- access granted to subjects who belong to the object's group is based on the object *group* rwx permissions
- access granted to all other subjects is based on the object *other* rwx permissions

The TSF shall explicitly authorize access of subjects to objects based on the following additional rule: FDP_ACF.1.3;1

a) If a subject has an appropriate override privilege the TSF shall authorize access of the subject to any filesystem object, even if such access is disallowed by FDP_ACF.1.2.

The TSF shall explicitly deny access of subjects to objects based on no additional rules. FDP_ACF.1.4;1

5.1.2.2 Import From Outside TSF Control

The TSF shall enforce the following rules when *unlabelled* user data is exported from the TSC:LSPP NOTE 6

a) Devices used to export data without security attributes cannot be used to export data with security attributes unless the change in device state is performed manually and is auditable.

The TSF shall enforce the following rules when *labelled* user data is exported from the TSC:FDP_ETC.2.4

a) When data is exported in a human-readable or printable form:

- The authorised administrator shall be able to specify the printable label which is assigned to the sensitivity label associated with the data.
- Each print job shall be marked at the beginning and end with the printable label assigned to the "least upper bound" sensitivity label of all the data exported in the print job.
- Each page of printed output shall be marked with the printable label assigned to the "least upper bound" sensitivity label of all the data exported to the page. By default this marking shall appear on both the top and bottom of each printed page.

b) Devices used to export data with security attributes cannot be used to export data without security attributes unless the change in device state is performed manually and is auditable.

c) Devices used to export data with security attributes shall completely and unambiguously associate the security attributes with the corresponding data.

5.1.2.3 Mandatory Access Control

The TSF shall enforce the Mandatory Access Control Policy on subjects, objects and all operations amongst subjects and objects covered by the MAC policy.[FDP_IFC.1.1]

The TSF shall enforce the Mandatory Access Control Policy based on the following types of subject and information security attributes:[FDP_IFF.2.1]

- the sensitivity label of the subject; and
- the sensitivity label of the object containing the information.

Sensitivity label of subjects and objects shall consist of the following:

- a hierachical level; and
- a set of non-hierachical categories.

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules based on the ordering relationships between security attributes hold:[FDP_IFF.2.2]

- if the sensitivity label of the subject is greater than or equal to the sensitivity label of the object, then the flow of information from the object to the subject is permitted (a read operation);

- if the sensitivity label of the object is greater than or equal to the sensitivity label of the subject, *and the sensitivity label of the object is less than or equal to the clearance of the subject,* then the flow of information from the subject to the object is permitted (a write operation);

- if the sensitivity label of subject **A** is greater than or equal to the sensitivity label of subject **B**, then the flow of information from subject **B** to subject **A** is permitted.

The TSF shall enforce no additional information flow control SFP rules.[FDP_IFF.2.3]

The TSF shall enforce no additional information flow control SFP capabilities.[FDP_IFF.2.4]

The TSF shall explicitly authorize an information flow based on the following additional rule: [FDP_IFF.2.5]

a) If a subject has an appropriate override privilege the TSF shall authorize the information flow, even if such access is disallowed by FDP_IFF.2.2.

The TSF shall explicitly deny an information flow based on no additional rules. [FDP_IFF.2.6]

5.1.2.4 Import From Outside TSF Control

The TSF shall enforce the following rules when importing *unlabelled* user data controlled under the *MAC policy* from outside the TSC:[FDP_ITC.1.3]

a) Devices used to import data without security attributes cannot be used to import data with security attributes unless the change in device state is performed manually and is auditable.

The TSF shall enforce the following rules when importing *labelled* user data controlled under the *MAC policy* from outside the TSC:[FDP_ITC.2.5]

a) Devices used to import data with security attributes cannot be used to import data without security attributes unless the change in device state is performed manually and is auditable.

5.1.3 Identification and Authentication (FIA)

5.1.3.1 User Attribute Definition

The TSF shall maintain the following list of security attributes belonging to individual users: FIA_ATD.1.1

a) User Identifier;

b) User Clearance;

c) Group Memberships;

d) Authentication Data;

e) Rights Profile (including authorizations and roles);

f) Login shell; and

g) Minimum user sensitivity label.

5.1.3.2 User Authentication

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. FIA_UAU.2.1

5.1.3.3 User Identification

The TSF shall require each user to identify itself before allowing any other TSF-mediated action on behalf of that user. FIA_UID.2.1

<Application Note: The following non-TSF mediated functions are permitted to a user by the TOE prior to identification and authentication: select language; select remote host for login; and use of help for the login function. [NIST1] provides confirmation from the RBAC author that this does not contradict the intent of FIA_UID.2.1 or FIA_UAU.2.1 above.>

5.1.3.4 User-Subject Binding

The TSF shall associate the *following* user security attributes with subjects acting on the behalf of that user: FIA_USB.1.1;1

a) The audit user identity;

b) The effective user identity;

c) The effective group identities;

d) The real user identity and real group identities;

e) The user clearance which consists of the following:

- hierarchical level; and
- a set of non-hierarchical categories.;

f) The privileges of the program executing within the subject;

g) The set of rights profiles.

<Application note: for the purposes of comparison with [LSPP], real and effective user and group identities are both used to enforce the DAC policy and hence both are included above. An 'effective' user or group identity is one assumed by a user or a group for in a particular security context.>

The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of a user: FIA_USB.1.1;2

a) The sensitivity label associated with a subject shall be within the clearance range of the user;

b) Upon successful identification and authentication, the real and effective and audit user identities shall be those specified via the User Identifier attribute held by the TSF for the user.

c) Upon successful identification and authentication, the real and effective group identities shall be those specified via the Group Memberships attributes held by the TSF for the user.

The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of a user: FIA_USB.1.1;3

a) The effective user identity associated with a subject can be changed to another user's identity via a command, provided that
the user has appropriate override privilege, or
successful authentication as the new user identity has been achieved;

b) When executing a file which has the UID permission bit set, the effective user identity associated with the subject shall be changed to that of the owner of the file;

c) When executing a file which has the set GID permission bit set, the effective group identity associated with the subject shall be changed to that of the group attribute of the file.

5.1.4 Security Management (FMT)

5.1.4.1 Management Of Security Attributes

The TSF shall enforce the Discretionary Access Control Policy to restrict the ability to modify the access control attributes associated with a named object to the subject that owns the object and a subject with an appropriate override privilege.FMT_MSA.1.1;1

The TSF shall enforce the Mandatory Access Control Policy to restrict the ability to modify the sensitivity label associated with an object to a subject that has mandatory and discretionary write access and possesses an appropriate privilege.FMT_MSA.1.1;2

The TSF shall ensure that only secure values are accepted for security attributes.FMT_MSA.2.1

<Application Note: Since this SFR is included purely for conformance with the RBAC PP, it would be reasonable to interpret this requirement as applying only to those security attributes that are explicitly covered by the RBAC PP [RBAC B.3.4]. However, in practice, the application of this SFR is restricted even further; this is reflected both in the SF specifications (ENF.4) and in the rationale (section 7.4.2).>

The TSF shall enforce the RBAC SFP to provide restrictive default values for object security attributes that are used to enforce the SFP.FMT_MSA.3.1;3

The TSF shall allow the authorized administrators and users authorized by the Discretionary Access Control, Mandatory Access Control and RBAC Policies to modify object security attributes to specify alternative initial values to override the default values when an object or information is created.FMT_MSA.3.2;1

5.1.4.2 Management Of TSF Data

The TSF shall ensure that only secure values are accepted for TSF data.FMT_MTD.3.1

<Application Note: Since this SFR is included purely for conformance with the RBAC PP, it would be reasonable to interpret this requirement as applying only to those items of TSF data that are explicitly covered by the RBAC PP [RBAC B.3.4]. However, in practice, the application of this SFR is restricted even further; this is reflected both in the SF specifications (ENF.4) and in the rationale (section 7.4.2).>

5.1.4.3 Revocation

The TSF shall enforce the rules: FMT_REV.1.2;1

a) The immediate revocation of security-relevant authorizations; and

b) Administrative users shall be able to revoke security-relevant authorisations by completely deleting user security attributes, or by modifying the user identity, user name, primary group, secondary group and login shell, or by setting a new password. Such revocation is to take effect when the user next authenticates to the system.

The TSF shall enforce the rules: FMT_REV.1.2;2

a) The access rights associated with an object shall be enforced when an access check is made.

b) The rules of the Mandatory Access Control policy (FDP_IFF.2) are enforced on all future operations.

5.1.4.4 Security Management Roles

The TSF shall maintain the roles:

a) Set of RBAC administrative roles;

b) users authorized by the Discretionary Access Control Policy to modify object security attributes;

c) users authorized by the Mandatory Access Control Policy to modify object security attributes;

d) users authorized to modify their own authentication data;

e) Roles for the Object Owners.FMT_SMR.1.1 and FMT_SMR.2.1

The TSF shall be able to associate users with roles. FMT_SMR.2.2

The TSF shall ensure that the following conditions are satisfied:

a) Object owners can modify security attributes for only the objects that they own;

b) the set of RBAC administrative roles can modify security attributes for all objects under the control of the TOE.FMT_SMR.2.3

5.1.5 Protection of the TOE Security Functions (FPT)

5.1.5.1 Underlying Abstract Machine Test

The TSF shall run a suite of tests periodically during normal operation and at the request of an authorized administrator to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF. FPT_AMT.1.1

5.1.5.2 Trusted Recovery

After a failure or service discontinuity, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided. FPT_RCV.1.1

The TSF shall ensure that the following SFs and failure scenarios have the property that the SF either completes successfully, or the indicated failure scenarios, recovers to a consistent and secure state:

a) The SF that checks whether a specified privilege is assigned to any role but the database containing the privilege data is not on-line or the particular data table is inaccessible;

b) the SF checks whether a specified role has been assigned to a particular user but the database containing the role membership information is not on-line or the particular data table is inaccessible. FPT_RCV.4.1

5.1.5.3 TSF Self Test

The TSF shall run a suite of self tests periodically during normal operation, at the request of the authorized user, and when invocation of access rights on selected objects occurs to demonstrate the correct operation of the TOE. FPT_TST.1.1

<Application Note: The requirement of FPT_TST.1 for self tests when access rights are invoked on selected objects is currently not met by Trusted Solaris8. However, [NIST2] from the RBAC author clarifies that "In my best judgement, I feel this functionality is not implemented as a state of practice and hence conformance to the PP can be claimed without implementing this particular aspect of FPT_TST.1.1 requirement. Hence, although Trusted Solaris8 does not implement this SFR, conformance claims with [RBAC] are not affected.>

The TSF shall provide authorized users with the capability to verify the integrity of TSF data. FPT_TST.1.2

The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code. FPT_TST.1.3

5.1.6 TOE Access

5.1.6.1 Session Locking

The TSF shall lock an interactive session after an administrator-defined time interval of user inactivity by:

- clearing or overwriting display devices, making the current contents unreadable;
- disabling any activity of the user's data access/display devices other than unlocking the session.[FTA_SSL.1.1]

The TSF shall require the following events to occur prior to unlocking the session: the user must be successfully re-authenticated. [FTA_SSL.1.2]

The TSF shall allow user-initiated locking of the user's own interactive session by:

- clearing or overwriting display devices, making the current contents unreadable;
- disabling any activity of the user's data access/display devices other than unlocking the session.[FTA_SSL.2.1]

The TSF shall require the following events to occur prior to unlocking the session: the user must be successfully re-authenticated. [FTA_SSL.2.2]

5.1.7 Trusted Path

The TSF shall provide a communication path between itself, remote and local users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure. [FTP_TRP.1.1]

The TSF shall permit the TSF, local users and remote users to initiate communication via the trusted path.[FTP_TRP.1.2]

The TSF shall require the use of the trusted path for initial user authentication.[FTP_TRP.1.3]

5.2 Strength of Function

The claimed minimum strength of function is *SOF-medium*.

5.3 TOE Security Assurance Requirements

The target evaluation assurance level for the product is EAL4 Augmented with ALC_FLR.3 *Systematic Flaw Remediation* [CC], [FLR].

5.4 Security Requirements for the IT Environment

The IT environment is required to meet the objectives described in Section 4.2. All but one of these objectives is met by procedural measures, however O.BOOT is met by the OpenBoot PROM for Sparcstations. For Intel platforms, this may be achieved through the PC BIOS (i.e., firmware), but administrators should also take precautions to prevent booting from the floppy drive, CD ROM device or over the network where this is considered a threat. The functionality provided by the Sparc-station firmware is specified as follows:

The OpenBoot PROM on Sparc workstations shall restrict the ability to modify the behaviour of the boot strapping process to users who know the valid PROM password.FMT_MOF.1

Refinement:

a) In fully secure mode, the valid password is required in order to boot the workstation;

b) In command-secure mode, the valid password is required in order to boot a non-default operating system;

c) In fully secure mode the valid password or the appropriate eeprom access privilege is required in order to configure PROM operating modes, PROM passwords or boot parameters.

This Page Intentionally Left Blank

6 TOE Summary Specification

6.1 IT Security Functions

The ITSFs to which the claimed Strength of Function (SoF) rating applies are as follows:

- IA.1
- IA.6
- IA.7
- IA.9

6.1.1 Discretionary Access Control (DAC)

Policy

The security-related software shall define and control access between named users and named objects (e.g., files and programs) in the data processing system. All named users and named objects shall be uniquely identifiable over all the workstations in the system.

Within Trusted Solaris, DAC is applied in two different ways depending on the type of object. This security target therefore defines two object types:

- Objects that have permissions that can be assigned or changed by the owner;
- Objects that have permissions that are fixed or implicit given a process context.

The enforcement mechanisms for the former type of object shall allow users to specify and control sharing of those objects, initially generated by the user, by named users (group control is optional) using the specific designations of read, write, execute/search.

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 down to the level of a single user.

Access permission to these objects by users not already possessing access permission shall only be assigned by an authority responsible and authorized to grant access.

Subjects have a number of IDs associated with them:-

- effective user ID;
- effective group ID, and supplemental groups.

Self/Group/Public/ACL Permissions

The product shall implement a discretionary access control mechanism that controls the access of subjects to named owner controlled objects. The discretionary access control mechanism shall associate with each object an owner identification, a group identification, a set of access permissions and/or an access control list (ACL).

DAC.1 The access permissions on a filesystem object can be modified only by a subject that owns the object.

DAC.2 No subject may change the owner or group of a filesystem object unless it has the *file_setdac* privilege, or optionally is the owner of the object or has the following privilege effective:

- *file_chown* - allows a process to change a file's owner user ID. Also allows a process to change a file's group ID to one other than the process' effective group ID or one of the process' supplemental group IDs.

DAC.3 Subject to DAC.1, a subject may assign any combination of the following access modes to an object:-

- read, write, execute/search

to:-

- the owner of the object (self);
- any member of the owning group (group); and
- any user other than the owner or a member of the owning group (other).

DAC.4 Subject to DAC.1, an Access Control List (ACL) can be created for a *ufs*, *nfs, tmpfs, specfs, or namefs* filesystem object to specify a set of allowable access modes (as per DAC.3) for individually named users or groups. If an ACL entry for a user or group contains no access modes, the specified user or group is specifically excluded from accessing the object. Users not listed anywhere in an ACL (either through explicit user ACL entries or through any applicable group ACL entries) shall have their access to the object determined by the "Other" ACL entry.

Note that the scope of the above Security Function includes every object on a file system. It does not include System V Inter-process Communication (IPC) objects which have their own namespace and Owner, Creator Group, etc attributes. This is because although these objects are owner modifiable they do not have ACLs.

DAC.5 Whenever a subject requests access to a filesystem object, the access permissions for that object shall be checked to determine whether the user who owns the subject can access the object in the requested mode. Where an ACL is defined for an object, it shall be used instead of the object's permission bits.

DAC.6 When a subject creates a filesystem object, the user ID of the subject is assigned to the object, and the user's umask restricts the initial access permissions of the object. The TOE default is that a user's umask is set to prevent any user other than the owner having write access to the object.

DAC.7 Subjects may only override discretionary access control if they have one or more of the following privileges effective:

- *file_dac_execute*
- *file_dac_read*
- *file_dac_search*
- *file_dac_write*
- *ipc_dac_read*
- *ipc_dac_write*
- *file_setdac*
- *ipc_owner*
- *file_owner*
- *file_setid*

DAC.8 Access to an object with fixed access permissions is restricted to the owner of the object only.

6.1.2 Mandatory Access Control (MAC)

MAC.1 The product shall assign a sensitivity label with all subjects and objects that can contain classified data, including files, devices, network endpoints and windows. These labels shall consist of:

- a hierarchical security level that represents the classification of the subject or object;

- compartments that can separate subjects or objects at the same classification.

MAC.2 The security attributes of information imported from, or exported to a multi-level device shall be preserved by the import/export mechanism, and on export shall be stored on the same physical medium as the information itself.

MAC.3 The ToE shall print output surrounded by banner pages that contain the sensitivity label of the subject producing the output. Only users with the *Print Without Banners* authorization can print pages without banners.

MAC.4 The banner pages shall include a statement warning that this output should be handled at the sensitivity level until it is manually reviewed and downgraded.

MAC.5 Only users with the *Print Without Labels* authorisation can print unlabelled pages to a multi-level printer.

MAC.6 Only users with the *Print a PostScript File* authorisation can print PostScript documents to a multi-level printer.

It is possible to define multiple print queues and assign a single security level to each. This allows unlabeled printing (i.e., for PostScript documents) in a secure manner.

MAC.7 Except when entering passwords (including login, re-authentication and password change), all local users can access the TOE via labelled windows only.

MAC.8 Users shall be able to view the sensitivity label of each window at any time, if configured for that user, except when entering passwords.

MAC.9 Unlabelled communications over the local area network are restricted to:

- communications between an unlabelled host and either a labelled or unlabelled host; and
- subjects on a labelled host that have the *net_rawaccess* or *net_broadcast* privileges effective.

MAC.10 Subject to MAC.12, a subject can read (or execute or search) an object only if the subject's sensitivity label dominates the object's sensitivity label.

MAC.11 Subject to MAC.12, a subject can write to an object only if the object's sensitivity label dominates the subject's sensitivity label, and if the subject is associated with a user, only if that user's clearance dominates the object's sensitivity label. If the object is being created, the sensitivity label of the object shall equal the sensitivity label of the creating subject.

MAC.12 A subject may override MAC checks, if and only if it has one or more of the following privileges effective:-

- *file_mac_read*
- *file_mac_search*
- *file_mac_write*
- *ipc_mac_read*
- *ipc_mac_write*
- *net_mac_read*
- *net_reply_equal*
- *proc_mac_read*
- *proc_mac_write*
- *win_mac_read*
- *win_mac_write*

MAC.13 The sensitivity level and clearance of each subject shall be dominated by the user's clearance if the subject is associated with a user, or the admin high sensitivity level of the system if the subject is a system subject associated with no user.

MAC.14 Upon subject creation, the sensitivity level and clearance of the subject shall be initialized to the sensitivity level and clearance of the creating subject, and shall thereafter be fixed, unless changed in accordance with the following requirements in MAC.15 and MAC.16.

MAC.15 In order for a subject to be able to change its sensitivity level, it must have the *proc_setsl* privilege effective. A subject with this privilege may set the sensitivity level to only those that are dominated by the subject's clearance.

MAC.16 Only subjects with the *proc_setclr* privilege effective can change their clearance.

Objects

MAC.17 A subject can set the sensitivity label of objects to which it has mandatory and discretionary write access, only if it has one or more of the following privileges effective:-

- *file_upgrade_sl*
- *file_downgrade_sl*
- *net_upgrade_sl*
- *net_downgrade_sl*
- *win_upgrade_sl*
- *win_downgrade_sl*

MAC.18 For permanent objects (i.e., file system objects), if the changed sensitivity level does not dominate the original one then the subject must additionally be the owner of the object.

Devices

Devices in Unix are accessed as if they are file objects, and hence the MAC mediation rules given in section 5.1.2 define the policy that is assumed when subjects attempt to read or write information to/from devices.

Administrative users can create both single and multi-level devices. Trusted Solaris 8 4/01 implements an allocation mechanism that allows normal users to use a device in single-level mode. If a device is not specified by an administrative user as an allocatable device, it will only act in multi-level mode.

For both single and multi-level devices:-

MAC.19 Only administrative users can specify a device as allocatable, set or change the clearance range of a device, and specify which of the following categories of users may allocate the device:-

- users with the authorisations specified;
- all users; and
- no users.

Users with the *Allocate Device* authorisation will have access to single level allocatable devices. For these devices the following SF applies:-

MAC.20 A user may only import or export data to a single-level device if the device is allocated to that user, and the user's subject has a sensitivity label that is within the clearance range of the device. The data shall be imported or exported at the sensitivity level of the user's subject.

When exporting data to a single-level device, data can only be written to the device by subjects which are dominated by the sensitivity label of the device. As these subjects can only read data that they dominate, only data dominated by the sensitivity label of the device can be written to it.

Windows

MAC.21 The sensitivity level of a window must always be dominated by the clearance of the user logged in at the device on which the window is displayed and must always be contained within the device sensitivity label range of the device on which the window is displayed.

In addition to the standard MAC policing of objects, the following SFs define the additional mediation that applies to windows:

MAC.22 When a process that does not have the *win_selection* privilege requests an inter-window data move from one window to another that does not have the same sensitivity label, the product shall ensure that the user is notified that the windows have different sensitivity labels before allowing the move.

MAC.23 In order to perform an interwindow move when the sensitivity label of the data being moved is not dominated by ("is higher than") the sensitivity label of the destination to which the data is being moved, the user must possess the *Paste to a Downgraded Window* authorisation.

MAC.24 In order to perform an interwindow move when the sensitivity label of the data being moved is dominated by ("is lower than") the sensitivity label of the destination to which the data is being moved, the user must possess the *Paste to a Upgraded Window* authorisation.

Networks

The following additional SFs apply to networks:

MAC.25 The sensitivity label of data transmitted over the network between hosts shall be within the clearance range, as configured by Admin.8, of:

- the local host sending the data;
- the local network interface used to send the data;
- the remote host receiving the data; *and*
- the remote network interface used to receive the data.

The clearance range of a network interface can be set to be a single label by setting the minimum and maximum sensitivity labels to the same level. This constrains all data sent and received over the interface to be at this single label, creating a single-level network, as described in chapter 2.

Unlabeled hosts are configured by placing them on a single-level network of the appropriate sensitivity label, and configuring the Trusted Solaris hosts to communicate with them using unlabeled packets.

MAC.26 Data being transmitted over the local area network between workstations of the distributed product shall be labelled with the sensitivity label of the subject transmitting the data.

6.1.3 Object Reuse

OR.1 When an object is initially assigned, allocated or reallocated to a subject from the system's pool of unused objects, the security-related software shall assure that the object contains no data for which the subject is not authorized.

OR.2 When memory objects are allocated for use by a subject at run-time, the memory shall contain no data from a previous subject.

Any portion of a file object that has not been previously written to shall either:

- not be readable by any subject; or
- shall be cleared before it can be read.

OR.3 The TOE shall revoke all access rights held by a subject to the information contained within a storage object, before reuse by other subjects.

6.1.4 Identification and Authentication

Password Authentication

IA.1 The product shall require users to identify and successfully authenticate themselves, using a user name and a password, before performing any other actions.

IA.2 Upon successful identification and authentication, the real and audit user IDs and the real group IDs, clearances and authorisations of the user's subjects shall be those specified by the authentication data.

IA.3 Subject to IA.16, user accounts shall be locked or unlocked by an administrative user only.

IA.4 Only users with *Remote Login* authorisation may remotely login.

IA.4 is included to ensure that only authorized users login remotely as login will not occur via the trusted path. In addition, the system also allows only users with the *Terminal Login* authorisation to login via a serial port. This however is not claimed as a SF as no serial terminals are included in the evaluated configuration.

Password Protection

The authentication data shall not contain a clear text version of each user's password, but rather a one-way encrypted value based on the user's password. When a user enters his password, it is used to construct an encrypted value and is compared against the encrypted value in the authentication data.

IA.5 On entry, passwords shall not be displayed in cleartext.

Re-authentication

IA.6 The product shall, for all login sessions other than remote login, provide the capability for a user to "lockscreen" their login session such that the product requires users to re-authenticate themself using a password before access to the session is resumed.

IA.7 The product shall provide the capability for the "lockscreen" specified in IA.6 to be invoked automatically after a defined time interval, as defined by an administrative user, if there is no user activity in the session

IA.8 User passwords are always stored in encrypted form.

Note: this ITSF does not apply to Openboot PROM passwords (which are not user passwords, and are beyond the scope of this security target).

IA.9 The authentication data shall be protected so that it cannot be written other than as follows:

- by administrative users who may
  - create, delete user identities,
  - modify the name, primary group, secondary group, login shell;
  - set passwords if required
  - modify the minimum login label, user clearance, user label view, user label visibility; and
- by a user supplying a new password, or a password being generated by the TOE, depending on the configuration of the TOE.

IA.10 Subject to DAC.7 and MAC.12, stored passwords shall be protected so that they can only be read (in encrypted form) by the owning user.

Password Generation and Selection

IA.11 Users shall be required to change their passwords within a specific frequency determined by an administrative user.

It should be noted that this SF does not preclude users from changing their passwords more frequently than required.

IA.12 If enabled by an administrative user, the product shall automatically notify users that their password must be changed.

IA.13 If enabled by an administrative user, the product shall perform all password changes by generating a random, pronounceable password and assigning it to the user.

Otherwise, passwords shall be assigned by an administrative user or chosen by the users themselves.

IA.14 The product enforces a minimum user password length (except for PROM passwords), as specified in the /etc/default/passwd file.

Identification of Workstations

IA.15 A workstation shall have the capability to identify positively other workstations of the distributed product before allowing them to be used for accessing system resources at that workstation.

Configurable failed login attempts

IA.16 The maximum number of failed login attempts shall be configured by an administrator user only. If this limit is reached, the user account shall be locked.

6.1.5 Trusted Path

The security-related software shall support a direct trusted communication path, known as the trusted path, between itself and users for use when a positive connection between a user and the security-related software (TOE) is required (e.g., identification and authentication, change subject security label).

TPath.1 Communications via the trusted path shall be initiated exclusively by a user or the security-related software and shall be logically isolated and unmistakably distinguishable from other communications paths.

TPath.2 The product shall achieve a trusted path between itself and the user for initial identification and authentication.

TPath.3 No user subject shall be able to read or write to the screen during initial identification and authentication.

TPath.4 No non-trusted path windows shall be displayed on the screen before trusted path communication.

TPath.5 When the workstation is first started, the trusted path shall be activated.

TPath.6 After a successful login, the trusted path shall be controlled by the product, which shall:

1) provide for reserved portions of the screen to which user subjects cannot write;

2) read all user input to determine whether the user is attempting to communicate via the trusted path;

3) use a reserved portion of the screen to provide the user with visual confirmation that the current user input is via the trusted path.

TPath.7 The product shall use the trusted path mechanisms to allow the user to perform security-critical functions via the trusted path including, as a minimum:

- user identification;
- all operations that require users to enter passwords (e.g., authentication, change password);
- all operations that set security labels;
- allocation/deallocation of devices;
- all use of the actions or commands for the administration roles.

6.2 Privileges and Authorisations

Trusted Solaris 8 4/01 has two mechanisms that confer security rights to the subjects of trusted users, privileges and authorisations. For the purposes of this security target it is important that the reader understands the difference between the two.

Privileges are associated with subjects and are used by the TCB to determine if a subject may execute a trusted system call, or a general system call in a trusted manner (i.e., file write with MAC override).

Authorisations are associated with users and are used by TCB applications to verify that particular users are entitled to use that TCB application or application subfunction. Typically a TCB application will execute with privileges gained from the *forced* privilege set (see the following section on file privileges), thereby overriding aspects of the TCB's security policy. The authorisation mechanism ensures that where this occurs, the TCB applications can uphold the system's security policy.

The following sections present the SFs required to ensure the integrity of the privilege mechanism.

Subject Privileges

There are four privilege sets associated with each subject: permitted, effective, inheritable and saved. Permitted privileges are those privileges that a subject is allowed to use. Effective privileges are those that a subject is currently using (has active). Inheritable privileges are passed across to a child subject, and saved privileges are the set that were actually inherited from a subject's parent. A subject may also change its permitted and effective privileges as long as the following invariant condition holds.

Priv.1 The following subject privilege invariants are maintained by the ToE at all times:-

- $Effective \subseteq Permitted$
- $Saved \subseteq Permitted$
- and where a subject modifies its own privileges:
  - $Permitted' \subseteq Permitted$
  - $Inheritable' \subseteq Inheritable \cup Permitted$

where *set'* is a new privilege set, and *set* is the old.

Priv.2 When a subject creates a child subject, the privilege sets of the child subject shall be identical to those of the parent at that time.

File Privileges

Files have two privilege sets: *forced* and *allowed*. These, along with the subject's inheritable set, determine the set of privileges that a subject will have during the execution of a program. *Forced* privileges are automatically added to a subject's *permitted*, *effective* privilege sets (see next section). The *allowed* privilege set constrains the privileges that a process may have in it's permitted, effective or saved sets.

Priv.3 The following privilege transitions are performed by the ToE upon execution of a file:-

- $Permitted_p = Effective_p = (Inheritable_{p*} \cup Forced_f) \cap Allowed_f$
- $Inheritable_p = Inheritable_{p*}$
- $Saved_p = Inheritable_{p*} \cap Allowed_f$
- *where* $_P$ *is the subject,* $_{P*}$ *is the old subject and* $_f$ *is the file exec'ed*

Priv.4 A subject may set the privileges on a file object that it owns only if the subject has the *file_setpriv* privilege effective.

Priv.5 A subject may set the privileges on an outgoing network packet only if the subject has the *net_setpriv* privilege effective.

Authorisations

Authorisations are used by the trusted system tools to determine if a user can them to perform trusted actions. Annex A describes the default authorisations that are delivered with Trusted Solaris 8 4/01. Additional authorisations can be introduced into the system if required.

The use of authorisation is described locally with each applicable SF.

6.3 Administration

Profiles

Trusted Solaris 8 4/01 provides the ability for an administrator to define profiles and assign profiles to users. Profiles are a powerful mechanism that allow administrators to define the commands, and CDE actions that users are allowed to perform, together with the authorisations that the user has. This mechanism provides fine-grain control over user-capabilities and allows the system to rigorously implement the principle of least privilege.

Admin.1 Only administrators may assign a user profile to a user. The profile shall include:

- a list of CDE actions that the user is allowed to perform, and for each action:
    - the privileges that the action shall be performed with;
    - the sensitivity level and clearance at which the command is executed; and
    - the real and effective user ID and real and effective group ID that the action shall be performed with.
- a list of commands that the user is allowed to perform, and for each command:
    - the privileges that the command shall be executed with;
    - the sensitivity level and clearance at which the command is executed; and
    - the real and effective user ID and real and effective group ID that the command shall be executed with.
- a list of authorisations that shall be granted to the users assigned this profile.

Admin.2 Users may perform only those CDE actions as specified in their profiles, and when executed they are executed with the security attributes as specified by Admin.1.

Admin.3 Users, who are configured to use the profile shell, may execute only those commands as specified in their profiles, and when executed they are executed with the security attributes as specified by Admin.1.

Note: commands executed by other commands are outside the scope of Admin.3.

Roles

Roles are configurable with Trusted Solaris 8 4/01, allowing system to be configured so that the principle of least privilege can be optimally implemented for each installation and application.

The following rules apply to the configuration of roles:-

Admin.4 Only an authorized user can define and assign roles to users.

Admin.5 The TSF shall restrict the scope of a session based on the role assigned to the user.

Object Management

Admin.6 Users may perform the following operations if and only if they have the corresponding authorization:

Authorization	Operation
label.file .downgrade	Allows a user to specify the Sensitivity Label on a file that does not dominate the file's existing Sensitivity Label.
label.file .upgrade	Allows a user to specify the Sensitivity Label on a file that dominates the file's existing Sensitivity Label.
file.owner	Allows a user to act as a file's owner. This includes the ability to change the permission bits and ACL, to downgrade the Sensitivity Label of files not owned.
file.chown	Allows a user to change the ownership of a file.
file.privs	Allows a user to specify the allowed and forced privileges to be associated with the execution of a program file.

Table 3: Filesystem Authorizations

User Management

Admin.7 Users may perform the following operations if and only if they have the corresponding authorization:

Authorization	Operation
admin.usermgr.write	Allows an administrator to set the security information related to the user's identity. The user name, primary group, secondary group, comment, and login shell may all be set via the User Manager. This authorization is needed to add, copy or delete a user.
admin.usermgr.pswd	Allows an administrator to set the password information pertaining to a user. A user's password, type of password, life time, expiration date, warning days and the permission to set up the credentials table may all be set.
admin.usermgr.label	Allows an administrator to set various label-related pieces of information associated with a particular user. A user's minimum login label, clearance, and label view may all be set.
admin.usermgr.audit	Allows the setting of per-user audit flags, see Audit.18

Table 4: User Authorizations

Authorization	Operation
profmgr.assign	Allows the assignment of all profiles to a user. *(Note that the word 'all' should be taken to mean any from a set of.)*
profmgr.delegate	Allows the assignment of owned profiles to a user.
profmgr.execattr.write	Allows the management of commands for a user.
profmgr.read	Allows the viewing of profiles for a user.
profmgr.write	Allows the management of profiles for a user.
role.assign	Allows the selection of which roles a user may assume. When a user assumes a role he or she may use all commands and actions granted to that role.

Table 4: User Authorizations

Database Management

Admin.8 Users may perform the following operations if and only if they have the corresponding authorization:

Authorization	Operation
solaris.network.security.write	Allows a user to edit the tnidb, tnrhdb and tnrhtp databases.

Table 5: Database Authorizations

Label Management

Admin.9 Only administrative users may define the label set or the printable representations of that set.

Admin.10 Only administrative users can configure sensitivity labels to be displayed on a per-user basis.

Note: Sensitivity labels are always enforced. The TOE merely determines if sensitivity labels are displayed to the user.

6.3.1 Audit

Audit Events

Audit.1 The use of the identification and authentication mechanisms is auditable. The following information is recorded for each event audited:-

- date;
- time;
- user identity - audit ID and effective user ID (if successful);
- security attributes of the user (if successful);
- type of event;
- identification of the workstation or terminal used; and
- success or failure of the event.

Audit.2 Attempts to access to objects are auditable. The following information is recorded for each event audited:-

- date;
- time;
- user identity - audit ID and effective user ID;
- sensitivity label of the user identity;
- name of the object;
- sensitivity label of the object;
- type of access attempted; and
- success or failure of the attempt.

Audit.3 The creation of an object is auditable. The following information is recorded for each event audited:

- date;
- time;
- user identity - audit ID and effective user ID;
- name of the object;
- sensitivity label of the object;
- sensitivity label of creating subject.

Audit.4 The creation of a subject to run on behalf of a user is auditable. The following information is recorded for each event audited:

- date;
- time;
- user identity - audit ID and effective user ID;
- sensitivity label of the user;
- success or failure of the attempt.

Audit.5 The creation, deletion, disabling or enabling of user accounts is auditable. The following information is recorded for each event audited:

- date;
- time;
- identity of the user implementing the change - audit ID and effective user ID;
- sensitivity label of user implementing the change;
- name of the user account being modified;
- type of action.

Audit.6 Attempts to assign or modify security attributes are auditable. The following information is recorded for each event audited:

- date;
- time;
- identity of the user implementing the change - audit ID and effective user ID;
- sensitivity label of user implementing the change;
- name of the user account or object being modified;
- type of attribute; and
- success or failure of the attempt.

Audit.7 The use of DAC override privileges are auditable. The following information is recorded for each event audited:

- date;
- time;
- user identity - audit ID and effective user ID;
- sensitivity label of user identity;
- name of the object involved (if any);
- sensitivity label of the object involved (if any); and
- the privilege or role granted.

Audit.8 Security relevant events affecting the operation of the auditing functions are auditable. The following information is recorded for each event audited:

- date;
- time;
- user identity (if relevant) - audit ID and effective user ID; and
- type of event.

Audit.9 Import or export of data to a device is auditable. The following information is recorded for each event audited:

- date;
- time;
- user identity - audit ID;
- sensitivity label of data to be imported or exported;
- sensitivity label of user identity;
- name of the device.

Audit.10 The creation or deletion of a logical device for storage media is auditable. The following information is recorded for each event audited:

- date;
- time;
- user identity (if relevant) - audit ID and effective user ID;
- sensitivity label of user identity;
- name of the object and device; and
- sensitivity label of the object and device;
- type of action.

Audit.11 Start-up and shutdown of the system is auditable. The following information is recorded for each event audited:

- date;
- time;
- user identity (mandatory for shutdown only) - audit ID and effective user ID; and
- type of event.

Audit.12 The date and time information recorded in audit records shall be reliable.

Audit.13 Applications can enter their own audit records into the system audit trail, if and only if the subject has either *proc_audit_appl* or *proc_audit_tcb* privileges effective.

Protection of Audit Information

Audit.14 Audit data shall be protected so that access to it is limited to administrative users.

Audit.15 Password data (in clear or encrypted form) is never recorded in the audit log.

Selective Audit Data Collection/Reduction

Audit.16 Only administrative users may define classes of audit event.

Audit.17 Only administrative users shall be able to define the default system audit-mask that defines which audit classes are recorded by default.

Audit.18 Only administrative users shall be able to define a per-user audit-mask that defines which audit classes are recorded for that user. For a given user, the system shall audit those classes that are in the default system audit mask or the per-user audit mask.

Audit.19 Audit reduction software shall be available to allow administrative users to selectively retrieve audit data based on, at a minimum, the identity of users, the type of audit event, and the audit class, the identity of files accessed, and/or the security level of objects accessed.

Audit Data Storage

Audit.20 Each workstation of the (distributed) product may store audit data locally or on another workstation of the product that can act as an audit server.

Audit.21 If another workstation of the product is being used as an audit server, and this audit server becomes unavailable, the (local) workstation shall either:

- automatically switch over to storing audit data locally,

or

- suspend operation until the audit server is again available,

or

- suspend operation until an alternative workstation of the product takes over as an audit server;

or

- if no workstation is able to store audit data then no further auditable events shall occur (i.e., all auditable actions will be suspended).

Audit.22 Facilities are available to allow administrative users to archive and maintain the audit logs. Only such users may use these facilities to archive and maintain the audit logs.

Audit.23 The system shall notify an administrator of audit trail saturation.

6.3.2 System Integrity

Integrity.1 After the Trusted Solaris 8 4/01 is loaded from disk and until logins are enabled by a user with the *Enable Login* authorisation, only users that have the *Enable Login* authorisation can login.

Note that enabling logins requires the enabling user to authenticate, but the authentication of this user does not imply that the user is logged in.

6.3.3 Enforcement Functions

ENF.1 The TOE shall validate all actions between subjects and objects that require policy enforcement, before allowing the action to succeed.

ENF.2 The TOE shall maintain a domain 'kernel space' for its own trusted execution. This shall be kept separate from untrusted subjects which operate in a separate domain 'user space'.

ENF.3 The TOE shall allow an administrator to perform a self test to ensure that the underlying TSF is enforcing process separation.

ENF.4 The TSF shall ensure that only secure values are accepted for user passwords.

6.3.4 Failure

FAIL.1 After a failure or system discontinuity, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

FAIL.2 The TSF shall preserve a secure state when failures occur in the databases containing user privileges information or the functions related to user roles and privileges.

6.4 Required Security Mechanisms

6.4.1 Identification and Authentication

The TOE uses a username and password mechanism to provide authentication of users. The construction of passwords is sufficient to meet the requirements of a strength of function of *SOF-medium*. This mechanism supports the IT SFs IA.1, IA.6, IA.7 and IA.9.

Passwords are encrypted using a one way hashing algorithm, however the assessment of algorithmic strength does not form part of the evaluation.

6.5 Assurance Measures

Assurance measures will be adopted to address each of the EAL4 assurance requirements, as summarized in Table B.1 in [CC, Part 3] and as summarized below.

Assurance components	Description of how requirement will be met
ACM_AUT.1 Partial CM automation	Information on the automated tools will be provided to the evaluators in the Software Development Framework [SDF] document
ACM_CAP.4 Generation support and acceptance procedures	The same assurance measures to those of the CC EAL4 Solaris 8 evaluation are claimed for this assurance requirement.
ACM_SCP.2 Problem tracking CM coverage	Information on the tracking of configuration items will be provided.
ADO_DEL.2 Detection of modification	The same assurance measures to those of the CC EAL4 Solaris 8 evaluation are claimed for this assurance requirement.
ADO_IGS.1 Installation, generation, and start-up procedures	Installation, generation and start-up procedures will be provided.
ADV_FSP.2 Fully defined external interfaces	The Solaris 8 MAN pages, which are relevant to the implementation of the security functions, will be provided to the evaluation and assessed against this assurance requirement.
ADV_HLD.2 Security enforcing high-level design	The Architectural Design document, previously evaluated against ITSEC E3 for the Trusted Solaris 2.5.1 product, will be amended for Trusted Solaris 8 4/01 and submitted to the evaluation for assessment against this requirement.
ADV_IMP.1 Subset of the implementation of the TSF	The source code for Trusted Solaris 8 4/01 will be provided to the evaluation.

Table 6: How Assurance Requirements Will Be Met

Assurance components	Description of how requirement will be met
ADV_LLD.1 Descriptive low-level design	The Detailed Design document, previously evaluated against ITSEC E3 for the Trusted Solaris 2.5.1 product, will be amended for Trusted Solaris 8 4/01 and submitted to the evaluation for assessment against this requirement.
ADV_RCR.1 Informal correspondence demonstration	This correspondence information will be contained in the functional specification and design documents. The functional specification will map ITSFs to MAN pages. The HLD will map ITSFs to the HLD, and the LLD will map ITSFs and source code modules to the LLD basic components
ADV_SPM.1 Informal TOE security policy model	A separate Informal Security Policy Model (ISPM) will be produced in accordance with CCIMB Interpretation 069.
AGD_ADM.1 Administrator guidance	The Trusted Solaris 8 4/01 operational documentation relevant to an administrator will be submitted to the evaluation and assessed against this requirement.
AGD_USR.1 User guidance	The Trusted Solaris 8 4/01 operational documentation relevant to an end user will be submitted to the evaluation and assessed against this requirement.
ALC_DVS.1 Identification of security measures	The same assurance measures to those of the CC EAL4 Solaris 8 evaluation are claimed for this assurance requirement.
ALC_FLR.3 Systematic Flaw Remediation	Flaw remediation procedures will be provided.
ALC_LCD.1 Developer defined life-cycle model	The Life Cycle definition is documented in the [SDF]. This will be submitted to the evaluation against this requirement.
ALC_TAT.1 Well-defined development tools	The tools used in the development of Trusted Solaris 8 4/01 are the same as for Solaris 8. Full reuse of results will therefore be claimed.

Table 6: How Assurance Requirements Will Be Met

Assurance components	Description of how requirement will be met
ATE_COV.2 Analysis of coverage	The analysis of test coverage will be presented to the evaluation in a form similar to that provided to the Trusted Solaris 2.5.1 evaluation. The existing coverage is against both High and Low level designs and should therefore be to a sufficient depth.
ATE_DPT.1 Testing: high-level design	As for ATE_COV.2
ATE_FUN.1 Functional testing	The test documentation provided to the evaluation will be in a format similar to that provided to the Trusted Solaris 2.5.1 evaluation. The tests will be run on a range of platforms including: - small, medium and large Ultra II workstations as representative examples of the UltraSparc II processor range of workstations. - an Intel platform.
ATE_IND.2 Independent testing - sample	The resources provided to the CLEF for functional testing will be made available for them to perform additional, independent testing.
AVA_MSU.2 Validation of analysis	The Misuse analysis, previously submitted for the CC EAL4 evaluation of Solaris 8, will be updated for Trusted Solaris 8 4/01 and submitted to the evaluation against this requirement.
AVA_SOF.1 Strength of TOE security function evaluation	The Strength of Function analysis, previously submitted for the CC evaluation of Solaris 8, will be updated for Trusted Solaris 8 4/01 and submitted to the evaluation against this requirement.
AVA_VLA.2 Independent vulnerability analysis	The construction and operational vulnerability analyses, previously submitted for the CC evaluation of Solaris 8, will be updated for Trusted Solaris 8 4/01 and submitted to the evaluation against this requirement. In addition, evidence of Sun's continuing search for vulnerabilities and the resolution of them in the Solaris product, will be provided.

Table 6: How Assurance Requirements Will Be Met

This Page Intentionally Left Blank

7 Rationale

This chapter presents the evidence used in the Security Target evaluation. This evidence supports the claims that the ST is a complete and cohesive set of requirements, that a conformant TOE would provide an effective set if IT security countermeasures within the security environment, and that the TOE summary specification addresses the requirements. The rationale also demonstrates that any PP conformance claims are valid.

7.1 Correlation of Threats, Policies, Assumptions and Objectives.

The correlation between threats, organisational policies, assumptions and objectives is detailed in the following sections, and is summarized below.

Objectives:	O.AUTHORISATION	O.DAC	O.MAC	O.AUDIT	O.RESIDUAL_INFO	O.MANAGE	O.ENFORCEMENT	O.DUTY	O.HIERACHICAL	O.ROLE
T.ACCESS_INFO	✓	✓		✓	✓	✓	✓			✓
T.ACCESS_TOE	✓			✓		✓	✓			
T.MODIFY	✓	✓		✓		✓	✓	✓		✓
T.ADMIN_RIGHTS	✓			✓		✓	✓	✓	✓	✓
T.CLEARANCE	✓		✓	✓	✓	✓	✓			
T.TRANSIT	✓						✓			
P.AUTH	✓					✓	✓			
P.DAC		✓			✓	✓	✓			
P.ACCOUNTABLE	✓			✓		✓	✓			
P.CLASSIFICATION	✓		✓		✓	✓	✓			

Table 7: Threats and Policies against Security Objectives for the TOE

	O.ADMIN	O.ACCOUNTABLE	O.AUDITDATA	O.AUTHDATA	O.BOOT	O.CLEARANCE	O.CONSISSTENCY	O.CONNECT	O.INSTALL	O.INFO_PROTECT	O.LABELS	O.MAINTENANCE	O.RECOVER	O.SENSITIVITY	O.SOFTWARE_INSTALL	O.PROTECT
T.ACCESS_INFO	✓			✓	✓		✓	✓	✓	✓			✓			✓
T.ACCESS_TOE	✓	✓	✓	✓	✓		✓	✓	✓							
T.MODIFY	✓				✓		✓	✓	✓	✓						✓
T.ADMIN_RIGHTS	✓	✓		✓	✓		✓	✓	✓						✓	
T.CLEARANCE	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓			✓		✓
T.TRANSIT								✓	✓	✓						✓
P.AUTH				✓												
P.DAC																
P.ACCOUNTABLE	✓	✓	✓													
P.CLASSIFICATION				✓		✓				✓	✓			✓		
A.PROTECT										✓						✓
A.ADMIN	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
A.USER	✓	✓		✓												
A.PASSWORD	✓								✓							
A.NIS_DOMAINS									✓							
A.BRIDGE&ROUTERS										✓						✓

Table 8: Threats and Policies against Security Objectives for the TOE Environment

The threats, objectives and correlation between them provides the primary focus for the reader in portraying the intended purpose and use of Trusted Solaris.

The OSPs are derived from [CAPP], [LSPP] and [RBAC] and are included to indicate how the OSPs relate to the TOE security objectives and the primary non-IT security objectives. The OSPs are generally more abstract than the threats and so the correlation between similar threats and OSPs to objectives is not necessarily

the same.

The environmental objectives O.ADMIN, O.BOOT, O.INSTALL, O.CONNECT and O.CONSISTENCY are general objectives which are help counter all the threats (with the exception of T.TRANSIT in some cases) as follows:

- O.ADMIN: Those responsible for administering the TOE must be competent and trustworthy in order to manage the security functions effectively. Effective management is necessary in order that the threats are not inadvertently or deliberately realized;
- O.BOOT and O.INSTALL ensure that the correct copy of the operating system is installed and subsequently booted in a secure manner, and is hence relevant to help counter all the threats;
- O.CONNECT ensure that connections to other systems or users do not undermine the IT assets.
- O.CONSISTENCY is required to ensure that data is set up and maintained in a consistent manner across all workstations in the distributed system. Erroneous or duplicate entries in the authentication information may allow any of the threats to be realized.

7.2 Security Objectives Rationale

This section demonstrates that the security objectives stated in Section 4 above are traceable to all of the aspects identified in the TOE security environment and are suitable to cover them.

7.2.1 Complete Coverage - Threats

This section provides evidence demonstrating coverage of the threats by both the IT and Non-IT security objectives. The table is followed by a discussion of the coverage for each threat.

[T.ACCESS_INFO] *An authorized user of the TOE accesses information without having permission from the person who owns, or is responsible for, the information.*

Security objectives O.DAC and O.ROLE counter this threat directly by ensuring the means are provided by which users can securely implement compartmentalisation of information in order to counter this threat. O.RESIDUAL_INFO helps counter the threat by ensuring that once an object has passed outside the control of the above security objectives, that residual information contained in it is not passed to other users.

Security objective O.AUTHORISATION supports O.DAC and O.ROLE in countering this threat by ensuring that an authorized user cannot impersonate another authorized user, thereby undermining the intent of these objectives.

O.AUDIT helps counter this threat by ensuring that repeated [unsuccessful] attempts to access information to which the user is not granted permission, can be detected, thereby allowing the administrator to take action before the attack is successful.

O.MANAGE and O.ENFORCEMENT counter this threat by ensuring:
- privileged actions are controlled; and
- the access controls cannot be bypassed.

Support is also provided by the following security objectives for the environment:

a) O.ADMIN - to administer the controls over access to information;
b) O.BOOT - to ensure that information cannot be accessed by booting an alternative operating system;
c) O.AUTHDATA is require to protect the information which would otherwise enable attackers to gain access to the TOE;
d) O.INFO_PROTECT - ensures that procedures are implemented to ensure that the information is protected in an appropriate manner;
e) O.PROTECT - to ensure that data transmitted over network cabling is appropriately protected;
f) O.RECOVER - to ensure that information cannot be accessed by terminating the operation of a workstation (whether intentional or not);

[T.ACCESS_TOE] *An unauthorized user of the TOE gains access to the system, thereby gaining unauthorized access to information.*

O.AUTHORISATION ensures that all users identify themselves to the system, and that their claimed identity is authenticated before being granted access to the system. This therefore prevents unauthorized users gaining access to the system.

O.AUDIT provides support in the form of auditing attempts to access the TOE. The auditing of unsuccessful attempts to login help to detect and hence counter the threat of repeated attacks on the login functions.

O.MANAGE and O.ENFORCEMENT help counter this threat by ensuring:
- the database of authorized users is properly managed and maintained;
- the authorisation functions are always invoked and cannot be bypassed;
- the auditing functions are set up appropriately to detect repeated attempts to login.

Support is also provided by the following security objectives for the environment:

a) O.ADMIN - to ensure that the introduction of new user identities is a restricted operation and performed only by the users responsible.
b) O.ACCOUNTABLE - to ensure that unauthorized users are not provided with accounts enabling them to access the TOE;
c) O.AUDITDATA - which ensures that bad passwords, which might be used to determine valid passwords, are not stored in the audit trail, and hence not known to any users.
d) O.AUTHDATA - which ensures that valid authentication data is not disclosed to unauthorized individuals;
e) O.CONSISTENCY - which ensures that access is granted to individuals on a basis consistent across all workstation. This avoids possible duplication of authentication data.

[T.MODIFY] *Unauthorized modification or destruction of information by an authorized user of the TOE.*

The security objective O.DAC provides the means to ensure that users can protect the integrity of the information they own or are responsible for.

Security objective O.AUTHORISATION supports O.DAC in countering this threat by ensuring that an authorized user cannot impersonate another authorized user, thereby undermining the intent of these objectives. O.MANAGE ensures that the administrative users can control access to information.

O.AUDIT helps counter this threat by ensuring that repeated [unsuccessful] attempts to modify information to which the user is not granted permission, can be detected, thereby allowing the administrator to take action before the attack is successful.

O.ENFORCEMENT helps counter this threat by ensuring the access control functions are always invoked and cannot be bypassed.

Role based access to the information is countered by the objectives O.DUTY and O.ROLE which ensure that only those users are assigned roles and only those users that have been assigned the correct role can access the information.

Support is also provided by the following security objectives for the environment:

a) O.INFO_PROTECT and O.PROTECT - ensures that information transmitted over the network is not accessible to other authorized users of the TOE and hence the data cannot be modified or destroyed;
b) O.ADMIN ensures that the default access permissions are set appropriately so that access is granted, by default, to a restricted set of users;

c) O.CLEARANCE ensures that users cannot access information that they are not authorized to access;
d) O.SENSITIVITY ensure that all information imported and exported to and form the TOE is appropriately marked such that an unauthorized user cannot modify the system.

[T.ADMIN_RIGHTS] *Unauthorized use of facilities which require administration rights by an authorized user of the TOE.*

O.MANAGE and O.ENFORCEMENT counters this by ensuring:
- the database of authorized administrators is properly managed and maintained;
- the administration functions are always checked when invoked and cannot be bypassed;
- the auditing functions are set up appropriately to detect repeated attempts to use the administration functions by non-administrative users.

O.DUTY provides the capability of enforcing separation of roles and O.HIERARCHICAL allows for hierarchical definition of these roles. O.ROLE ensures that a user cannot access or perform operations on its resources or objects unless they have been assigned the appropriate role.

O.AUTHORISATION ensures that only authorized users can access the TOE, and provides for identification of users to determine the administration right assigned to the user.

O.AUDIT discourages the unauthorized use of administrator facilities by ensuring that any such breach of security policy can be detected.

O.AUTHDATA ensures user's authentication data is kept secure. This prevents an authorized user impersonating an administrator to gain unauthorized access to administrator facilities. O.CONSISTENCY ensures that a single set of administration rights exist across the TOE, thereby avoiding errors caused by duplication or erroneous entries in the authorisation data. O.ACCOUNTABLE ensure that users are uniquely identified and the use of privileged facilities can be controlled amongst the user community.

O.SOFTWARE_INSTALL ensures that only administrators can introduce software into the TOE and hence counters the threat of malicious software being introduced. The introduction of some software e.g., compilers, may provide enhanced facilities to an attacker which could be used to mount a successful attack on the TOE and hence make unauthorized use of administration facilities.

Administration of the TOE has been divided into user roles. The objective for this functionality is divided between O.DUTY, O.HIERACHICAL and O.ROLE, which ensure that the roles are appropriately defined.

[T.CLEARANCE] *Unauthorized access to information for which the user is not cleared.*

O.MAC provides a means of controlling access to information, based on sensitivity label of the information and the clearance of the subject, which satisfies the above threat. O.AUDIT discourages unauthorized access to information by ensuring that any such breach of security policy can be detected.

O.AUTHORISATION (with O.AUTHDATA) and O.RESIDUAL_INFO and ensures that only authorized users of the TOE can access information on the TOE and that no information is contained on a resource when it is re-used.

O.MANAGE and O.ENFORCEMENT ensures that the administrative users can manage the TOE effectively and that the TOE security policy is enforced.

O.ADMIN supports the above objectives by ensuring that the TOE is correctly administered. O.AUDITDATA and O.INFO_PROTECT support O.AUDIT to ensure that the audit data is not compromised. O.CLEARANCE, O.LABELS and O.SENSITIVITY ensures that information cannot be accessed unless the user is authorized to access the information.

O.BOOT, O.INSTALL, and O.PROTECT ensure that a user cannot access information for which they are not cleared through incorrect installation, booting, serial logins, or accessing data transmitted over network cabling.

[T.TRANSIT] *Data transferred between workstations is disclosed or modified to unauthorized users or processes either directly or indirectly (e.g., through spoofing of workstation identity).*

Administrators must ensure that data transferred between workstations i.e., along network cabling, is suitably protected against physical or other (e.g., tempest) attacks which may result in the disclose, modification or delay of information transmitted between workstations. Objective O.PROTECT ensures this is achieved. Because such issues need to be considered at installation time, objectives O.INSTALL and O.INFO_PROTECT are also applicable.

O.AUTHORISATION counters this threat by ensuring that only authorized users gain can gain access to the TOE or its resources. O.ENFORCEMENT counters this threat by ensuring that the Security Policy is not compromised.

7.2.2 Complete Coverage - Policy

This section provides evidence demonstrating coverage of the Organisational Security Policy by both the IT security objectives. The table is followed by a discussion of the coverage for each Security Policy.

[P.AUTH] Only those users who have been authorized to access the information within the system may access the system.

This policy is implemented through the objective O.AUTHORISATION which ensures that only authorized users are allowed access to the system. O.MANAGE and O.ENFORCEMENT support this policy by ensuring that the set of authorized users is effectively managed and that the authorisation functions are always invoked and cannot be bypassed.

O.AUTHDATA supports this policy by ensuring that authorisation data is constructed in a manner commensurate with the protection required for the information on the TOE and that passwords are not disclosed since doing so would compromise the policy.

[P.DAC] The right to access specific data objects is determined on the basis of:

a) the owner of the object; and
b) the identity of the subject attempting the access; and
c) the implicit and explicit access rights to the object granted to the subject by the object owner.

P.DAC is implemented through the objective O.DAC which provides the means of controlling access between objects and subjects on the attributes defined by the policy, and is supported by O.RESIDUAL_INFO objective which ensures that information will not given to users which do not have a need to know, when resources are reused. O.ENFORCEMENT supports this policy by ensuring that the access control functions are always invoked and cannot be bypassed. O.MANAGE supports this policy by requiring authorized administrator be able to manage the functions.

[P.ACCOUNTABLE] The users of the system shall be held accountable for their actions within the system.

Accountability is implemented primarily through the objective O.AUDIT which ensures uses' security relevant events can be recorded so as to be able to hold users accountable for their actions. An unauthorized user can not be held accountable for their actions and O.AUTHORISATION therefore supports this policy by ensuring that only authorized users are allowed access. O.MANAGE and O.ENFORCEMENT support this policy by ensuring that an effective set of actions are audited in order to detect attempted breaches of the security policy and that the auditing functions are always invoked and cannot be bypassed.

O.ADMIN, O.ACCOUNTABLE and O.AUDITDATA ensure that the administrator manages the auditing security functions effectively.

[P.CLASSIFICATION] *Subjects shall only be able to:*

- *read information if the sensitivity label of the object is less than or equal to the clearance of the user; and*
- *write to an object if the sensitivity label of the subject is less than or equal to the sensitivity label of the object, and the sensitivity label of the object is less than or equal to the clearance of the subject; and*
- *read or write information if the subject has privileges to override the rules above.*

This policy is primarily supported by O.MAC, which states that the TOE must provide its users with means of controlling access to objects and resources, on the basis of sensitivity labels and clearances.

O.INFO_PROTECT ensures that the information is protected such that the information is protected in an appropriate manner and therefore that subjects can only access information that is of a lower sensitivity label than the subjects clearance. O.AUTHDATA protects the user clearance data.

O.AUTHORISATION and O.RESIDUAL_INFO ensures that a user can only read/write to an object if they are authorized.

O.MANAGE and O.ENFORCEMENT support this policy by ensuring:
- the database of authorized administrators is properly managed and maintained;
- the administration functions are always checked when invoked and cannot be bypassed;
- the auditing functions are set up appropriately to detect repeated attempts to use the administration functions by non-administrative users.

O.CLEARANCE, O.LABELS, and O.SENSITIVITY support the above policy by ensuring that only users with the appropriate clearance can access protectively marked information.

7.2.3 Complete Coverage - Environmental Assumptions

This section provides evidence demonstrating coverage of the environmental assumptions by security objectives. The table is followed by a discussion of the coverage for each environmental assumption.

[A.PROTECT] *It is assumed that all network and peripheral cabling is approved for the transmittal of the most sensitive data held by the system. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted.*

The environmental objective O.PROTECT ensures that network cabling is suitably protected against threats of modification, tampering or interruption of the data transmitted via this medium. O.INFO_PROTECT ensures that, where the cabling is carrying classified information, that the infrastructure has been approved.

[A.ADMIN] *It is assumed that there are one or more competent individuals who are assigned to manage the TOE and the security of the information it contains. Such personnel are assumed not to be careless, wilfully negligent or hostile.*

This assumption is met primarily by O.ADMIN, and supported by all the other environmental objectives which ensure that the administrative functions are performed in an manner effective in maintaining the security functions of the TOE.

[A.USER] *Each individual user must have a unique user ID.*

This is primarily met by O.ACCOUNTABLE which states that *Each individual user is assigned a unique user ID*. This is supported by O.ADMIN and O.AUTH-DATA which ensure that those responsible for the TOE are competent and that the user IDs are not disclosed to unauthorized individuals.

[A.PASSWORD] *It is assumed that the length of password for normal users will be at least 8 characters.*

This is primarily met by O.INSTALL which states that *Those responsible for the TOE must establish and implement procedures to ensure that the ... software ... components .. are configured in a secure manner*. It is also supported by O.ADMIN which ensures that the administrator is competent enough to ensure this setting within the TOE remains set.

[A.NIS_DOMAINS] *It is assumed that, if the product comprises more than one workstation, all workstations are administered from a central point within each NIS+ domain.*

Note: NIS+ allows the creation of multiple administrative domains, thus allowing administrators to control local resources and user accounts, yet making it possible for users and resources to operate seamlessly over the entire organisation.

NIS+ is installed and configured at installation time, and therefore objective O.INSTALL ensures this assumption is upheld.

[A.BRIDGES&ROUTERS] *All bridges and routers are assumed to correctly pass data without modification.*

As for A.Protect, this assumptions is met by O.PROTECT and O.INFO_PROTECT; bridges and routers are part of the cabling infrastructure.

7.3 Security Requirements Rationale

This section demonstrates that the set of security requirements is suitable to meet and is traceable to the set of security objectives.

7.3.1 Complete Coverage - Objectives

This section demonstrates that the functional components selected for the TOE provide complete coverage of the defined security objectives. The mapping of components to security objectives is depicted in the following table.

Security Objective	Functional Component
O.AUTHORISATION	User Attribute Definition (FIA_ATD.1)
	Strength of Authentication Data (FIA_SOS.1)
	User Authentication Before Any Action (FIA_UAU.2)
	Protected Authentication Feedback (FIA_UAU.7)
	User Identification Before Any Action (FIA_UID.2)
	Management of Authentication Data (FMT_MTD.1;4)
	TSF initiated screen locking (FTA_SSL.1)
	User initiated locking (FTA_SSL.2)
	Trusted Path (FTP_TRP.1)
O.DAC	Discretionary Access Control Policy (FDP_ACC.1;1)
	Discretionary Access Control Functions (FDP_ACF.1;1)
	User Attribute Definition (FIA_ATD.1)
	User-subject Binding (FIA_USB.1;1-3)
	Management of Object Security Attributes (FMT_MSA.1;1)
	Static Attribute Initialisation (FMT_MSA.3;1)
	Revocation of Object Attributes (FMT_REV.1;2)
O.MAC	User Attribute Definition (FIA_ATD.1)
	User-subject Binding (FIA_USB.1;1-3)
	Management of Object Security Attributes (FMT_MSA.1;2)
	Static Attribute Initialisation (FMT_MSA.3;2)
	Revocation of Object Attributes (FMT_REV.1;2)
	Export of Unlabelled User Data (FDP_ETC.1)[a]
	Export of Labelled User Data (FDP_ETC.2)
	Mandatory Access Control Policy (FDP_IFC.1)

Security Objective	Functional Component
	Mandatory Access Control Function (FDP_IFF.2)
	Import of Unlabelled User Data (FDP_ITC.1)
	Import of Labelled User Data (FDP_ITC.2)
O.AUDIT	Audit Data Generation (FAU_GEN.1)
	User Identity Generation (FAU_GEN.2)
	Audit Review (FAU_SAR.1)
	Restricted Audit Review (FAU_SAR.2)
	Selectable Audit Review (FAU_SAR.3)
	Selective Audit (FAU_SEL.1)
	Guarantees of Audit Data Availability (FAU_STG.1)
	Action in case of Possible Audit Loss (FAU_STG.3)
	Prevention of Audit Data Loss (FAU_STG.4)
	User Subject Binding (FIA_USB.1;1-3)
	Management of the Audit Trail (FMT_MTD.1;1)
	Management of the Audited Events (FMT_MTD.1;2)
	Reliable Time Stamps (FPT_STM.1)
O.RESIDUAL_INFO	Object Residual Information Protection (FDP_RIP.2)
	Subject Residual Information Protection (LSPP Note 1)
O.MANAGE	Audit Review (FAU_SAR.1)
	Selectable Audit review (FAU_SAR.3)
	Selectable Audit (FAU_SEL.1)
	Action in case of Possible Audit Data Loss (FAU_STG.3)
	Prevention of Audit Data loss (FAU_STG.4)
	Management of Audit Trail (FMT_MTD.1;1)
	Management of Audit Events (FMT_MTD.1;2)
	Management of User Attributes (FMT_MTD.1;3)
	Management of Authentication Data (FMT_MTD.1;4-5)
	Revocation of User Attributes (FMT_REV.1;1)
	Security Management Roles (FMT_SMR.1)
	Secure Security Attributes (FMT_MSA.2)
	Secure TSF Data (FMT_MTD.3)

Security Objective	Functional Component
	Failure with Preservation of State (FPT_FLS.1)
	Manual Recovery (FPT_RCV.1)
	Function Recovery (FPT_RCV.4)
O.ENFORCEMENT	Abstract Machine Testing (FPT_AMT.1)
	Reference Mediation (FPT_RVM.1)
	Domain Separation (FPT_SEP.1)
	TSF Self test (FPT_TST.1)
	Trusted Path (FTP_TRP.1)
O.DUTY	Security Roles (FMT_SMR.2)
O.HIERACHICAL	Security Roles (FMT_SMR.2)
O.ROLE	RBAC Policy (FDP_ACC.1;2)
	RBAC Functions (FDP_ACF.1;2)
	Management of Object Security Attributes (FMT_MSA.1;3-4)
	Static Attribute Initialisation (FMT_MSA.3;3)
	Management of User Attributes (FMT_MTD.1;3)
	Security Roles (FMT_SMR.2)
	Limitation on the Scope of Selectable Attributes (FTA_LSA.1)
	TOE Session Establishment (FTA_TSE.1)

a. Including LSPP Note 6

O.AUTHORISATION

The TSF must ensure that only authorized users gain access to the TOE and its resources.

Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.2 and FIA_UAU.2]. To ensure authorized access to the TOE, authentication data is protected [FIA_ATD.1, FIA_UAU.7, FMT_MTD.1;4 and FTP_TRP.1]. The strength of the authentication mechanism must be sufficient to ensure unauthorized users cannot pose as authorized users with reasonable time, effort and other constraints [FIA_SOS.1]. Lock screen can be initiated to ensure that only authorized users can gain access [FTA_SSL.1 and FTA_SSL.2].

O.DAC

The TSF must provide its users with the means of controlling and limiting access to the objects and resources they own or are responsible for, on the basis of individual users or identified groups of users, and in accordance with the set of rules defined by the P.DAC security policy.

Discretionary access control must have a defined scope of control [FDP_ACC.1;1]. The rules of the DAC policy must be defined [FDP_ACF.1;1]. The security attributes of objects used to enforce the DAC policy must be defined [FDP_ACF.1;1]. The security attributes of subjects used to enforce the DAC policy must be defined [FIA_ATD.1 and FIA_USB.1;1-3]. Authorized users must be able to control who has access to objects [FMT_MSA.1;1] and be able to revoke that access [FMT_REV.1;2]. Protection of named objects must be continuous, starting from object creation [FMT_MSA.3;1].

O.MAC

The TOE must provide its users with the means of controlling and limiting access to objects and resources, on the basis of sensitivity labels and categories of the information being accessed and the clearance of the subject attempting to access that information.

The TSF must enforce Mandatory Access Control when exporting labelled and unlabelled user data [FDP_ETC.1 and FDP_ETC.2] and shall enforce Mandatory Access Control when importing labelled and unlabelled user data [FDP_ITC.1 and FDP_ITC.2]. User attributes necessary to enforce the MAC policy must be defined and applied [FIA_ATD.1 and FIA_USB.1;1-3]. Object attributes necessary to enforce the MAC policy must be securely initialised and managed [FMT_MSA.1;2, FMT_MSA.3;2 and FMT_REV.1;2]. The TSF shall enforce MAC Policy on subjects, objects and all operations among subjects and objects covered by the MAC policy (FDP_IFC.1). The TSF shall enforce the Mandatory Access Control Policy on the following types of subject and information security attributes:(FDP_IFF.2)

- the sensitivity label of the subject; and
- the sensitivity of the object containing the information.

O.AUDIT

The TOE must provide the means of recording any security relevant events, so as to (a) assist an administrator in the detection of potential attacks or misconfiguration of the TOE security features that would leave the TOE susceptible to attack; and (b) hold users accountable for any actions they perform that are relevant to security.

Security-relevant actions must be defined, auditable [FAU_GEN.1], and capable of being associated with individual users [FAU_GEN.2 and FIA_USB.1;1-3]. The audit trail must be protected so that only authorized users may access it [FAU_SAR.2 and FAU_STG.1]. The TSF must provide the capability to audit the actions of an individual user [FAU_SAR.3, FAU_SEL.1 and FIA_USB.1;1-3]. The audit trail must be complete [FAU_STG.1 and FAU_STG.4]. The time stamp associated must be reliable [FPT_STM.1]. An authorized administrator must be able to review [FAU_SAR.1] and manage [FAU_STG.3 and FMT_MTD.1;1-2] the audit trail.

O.RESIDUAL_INFO

The TSF must ensure that any information contained in a protected resource is not released when the resource is recycled.

Residual information associated with defined objects in the TOE must be purged prior to the reuse of the object containing the residual information [FDP_RIP.2, LSPP Note 1].

O.MANAGE

The TSF must allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.

The TSF must provide for an authorized administrator to manage the TOE [FMT_SMR.1]. The administrator must be able to administer user accounts [FMT_MTD.1;3-5 and FMT_REV.1;1]. The administrator must be able to review and manage the audit trail [FAU_SAR.1, FAU_SAR.3, FAU_SEL.1, FAU_STG.3, FAU_STG.4, FMT_MTD.1;1-2]. Only secure values must be accepted for RBAC-related attributes and TSF data [FMT_MSA.2, FMT_MTD.3].

The TSF shall provide a secure state following failure and allow manual and Function recovery [FPT_FLS.1, FPT_RCV.1, FPT_RCV.4].

O.ENFORCEMENT

The TOE security policy is enforced in a manner which ensures that the organisational policies are enforced in the target environment i.e., the integrity of the TSF is protected.

The TSF must make and enforce the decisions of the TSP [FPT_RVM.1]. It must be protected from interference that would prevent it from performing its functions [FPT_SEP.1]. Additionally, the TOE must provide the capability to demonstrate correct operation of the TSF's underlying abstract machine [FPT_AMT.1]. The correctness of this objective is further met through the assurance requirements defined in this PP.

The TSF shall run a suite of self tests to demonstrate the correct operation of the TOE [FPT_TST.1]. The integrity of the TOE is enforced via the trusted path [FTP_TRP.1]

O.DUTY

The TOE must provide the capability of enforcing separation of duties, so that no single user is required to perform all administrative functions.

The TSF shall be able to associate users with roles [FMT_SMR.2].

O.HIERACHICAL

The TOE must allow hierarchical definitions of roles. Hierarchical definition of roles means that they are constructed hierarchically using rights profiles.

The TSF shall ensure that the set of administrative roles can modify security attributes for all objects under the control of the TOE [FMT_SMR.2].

O.ROLE

The TOE must prevent users from gaining access to and performing operations on its resources and objects unless they have been granted access by the resource or objects owner or have been assigned a role which permits those operations.

The TSF shall enforce an RBAC policy [FDP_ACC.1;2 and FDP_ACF.1;2]. User and object security attributes required to enforce the RBAC policy must be securely managed [FMT_MTD.1;3, FMT_MSA.1;3-4 and FMT_MSA.3;3]. The TSF shall be able to associate users with roles [FMT_SMR.2]. The TSF shall deny and restrict the scope of a session [FTA_LSA.1 and FTA_TSE.1].

7.3.2 Requirements are Mutually Supportive and Internally Consistent

	FAU_GEN.1	FAU_SAR.1	FAU_STG.1	FDP_ACC.1	FDP_ACF.1	FDP_IFF.1	FDP_IFC.1	FIA_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MSA.1	FMT_MSA.3	FMT_MTD.1	FMT_SMR.1	FPT_AMT.1	FPT_STM.1	FPT_TST.1	FTP_TRP.1
FAU_GEN.1																✓		
FAU_GEN.2	✓																	
FAU_SAR.1	✓																	
FAU_SAR.2		✓																
FAU_SAR.3		✓																
FAU_SEL.1	✓												2					
FAU_STG.1	✓																	
FAU_STG.3			✓															
FAU_STG.4			✓															
FDP_ACC.1;1					1													
FDP_ACF.1;1				1								1						
FDP_ACC.1;2					2							3						
FDP_ACF.1;2				2								3						
FDP_ETC.1							✓											
FDP_ETC.2							✓											
FDP_IFC.1						✓												
FDP_IFF.2							✓					2						
FDP_ITC.1							✓					2						
FDP_ITC.2							✓											✓
FDP_RIP.2																		
LSPP Note 1																		
FIA_ATD.1																		
FIA_SOS.1																		

Table 9: Dependencies between Functional Components

	FAU_GEN.1	FAU_SAR.1	FAU_STG.1	FDP_ACC.1	FDP_ACF.1	FDP_IFF.1	FDP_IFC.1	FIA_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MSA.1	FMT_MSA.3	FMT_MTD.1	FMT_SMR.1	FPT_AMT.1	FPT_STM.1	FPT_TST.1	FTP_TRP.1
FIA_UAU.2										✓								
FIA_UAU.7									✓									
FIA_UID.2																		
FIA_USB.1;*								✓										
FMT_MSA.1;1				1										✓				
FMT_MSA.1;2							✓							✓				
FMT_MSA.1;3-4				2										✓				
FMT_MSA.2				2							1			✓				
FMT_MSA.3;1											1			✓				
FMT_MSA.3;2											2			✓				
FMT_MSA.3;3											4			✓				
FMT_MTD.1;*														✓				
FMT_MTD.3													2-5					
FMT_REV.1;*														✓				
FMT_SMR.1										✓								
FMT_SMR.2										✓								
FPT_AMT.1																		
FPT_FLS.1																		
FPT_RCV.1																	✓	
FPT_RCV.4																		
FPT_RVM.1																		
FPT_SEP.1																		
FPT_STM.1																		

Table 9: Dependencies between Functional Components

	FAU_GEN.1	FAU_SAR.1	FAU_STG.1	FDP_ACC.1	FDP_ACF.1	FDP_IFF.1	FDP_IFC.1	FIA_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MSA.1	FMT_MSA.3	FMT_MTD.1	FMT_SMR.1	FPT_AMT.1	FPT_STM.1	FPT_TST.1	FTP_TRP.1
FPT_TST.1															✓			
FTA_LSA.1																		
FTA_SSL.1									✓									
FTA_SSL.2									✓									
FTA_TSE.1																		
FTP_TRP.1																		

Table 9: Dependencies between Functional Components

The above table identifies the dependencies of all functional components included in the ST. The key to the symbols used are:

✓ required dependency

N dependency satisfied by iteration N of the component

All dependencies between functional components are satisfied within this ST, with the following exceptions.

- The dependency of FDP_ITC.2 on FPT_TDC.1 is not satisfied as it is not relevant to this ST. Note that FDP_ITC.2 is mandated by [LSPP] which does not include FPT_TDC.1.

- Dependencies on FIA_UAU.1 and FIA_UID.1 are satisfied, respectively, by the inclusion of FIA_UAU.2 and FIA_UID.2 which are hierarchic to these components.

Additional support between functional components is provided to address potential bypass and tampering threats to some of the above security requirements; these are provided by the following:

- The SFRs which achieve O.ENFORCEMENT help to defend other SFRs against bypass and tampering attacks;

- The SFRs which achieve O.AUTHORISATION help defend DAC, MAC security management and Audit SFRs against bypass through defeat of the Identification and Authentication mechanism;

- The SFRs which achieve O.RESIDUAL_INFO help to defend DAC and MAC SFRs against bypass;
- The SFRs which achieve O.MANAGE, O.DUTY, O.HIERARCHICAL and O.ROLE help defend DAC, MAC, Audit and Identification and Authentication SFRs against bypass and tampering attacks;
- The SFRs which achieve O.AUDIT help defend DAC, MAC, security management and Identification and authentication SFRs by helping to detect security relevant events which may indicate a potential or imminent compromise of those functions.

There is no conflict between the three access control policies enforced by the TOE, namely DAC, MAC and RBAC. Where DAC and MAC checks apply to the same operation, both checks must succeed in order for the operation to be permitted. The RBAC SFRs support the DAC and MAC SFRs by providing the basis for security management. Possession of certain privileges allow subjects to bypass or override DAC or MAC checks, but this is an integral part of the DAC and MAC policy rules.

EAL4 is a self-contained assurance package. ALC_FLR.3 introduces no additional dependencies.

7.3.3 Justification for Choice of Assurance Requirements

This security target has been based largely on [LSPP]. It specifies security requirements for a product which is to be used in an environment with a moderate level of risk to the assets. In such environments, an assurance level of at least EAL3 is recommended as stated in [LSPP]. This security target claims an assurance level of EAL4 Augmented, which also meets these requirements.

[RBAC] requires EAL2 assurance augmented with ADV_SPM.1. EAL4 Augmented is a superset of these requirements.

7.3.4 Strength of Function Claim is Consistent with Security Objectives

The claimed strength of function rating is SOF-medium. This is consistent with [LSPP] which states that a ‘one off’ probability of guessing the password shall be 1,000,000. This is specified in SFR FIA_SOS.1 which is in turn consistent with the security objectives described in section 7.3.

7.4 TOE Summary Specification Rationale

This section demonstrates that the TOE security functions and assurance measures are suitable to meet the TOE security requirements.

7.4.1 IT Security Functions Satisfy Functional Requirements

This section demonstrates that the combination of the specified TOE IT security functions work together to satisfy the TOE security functional requirements. The following table shows the TOE security functions which together satisfy each security functional requirement. They are grouped under the relevant TOE security objective.

Security Functional Requirement	TOE Security Function(s)
Audit Data Generation (FAU_GEN.1.1)	Audit.1 to Audit.11, Audit.15[a]
Audit Data Generation (FAU_GEN.1.2)	Audit.1,2,3,4,5,6,8,11,21
User Identity Generation (FAU_GEN.2.1)	Audit.1 to Audit.11
Audit Review (FAU_SAR.1.1)	Audit.19
Audit Review (FAU_SAR.1.2)	Audit.19
Restricted Audit Review (FAU_SAR.2.1)	Audit.14
Selectable Audit Review (FAU_SAR.3.1)	Audit.19
Selective Audit (FAU_SEL.1.1)	Audit.17, Audit.18
Protected Audit Trail Storage (FAU_STG.1.1)	Audit.14, Audit.22
Protected Audit Trail Storage (FAU_STG.1.2)	Audit.13, Audit.14
Action in Case of Possible Audit Data Loss (FAU_STG.3.1)	Audit.22, Audit.23
Prevention of Audit Data Loss (FAU_STG.4.1)	Audit.20, Audit.21
Discretionary Access Control Policy (FDP_ACC.1.1;1)	DAC.6
Discretionary Access Control Functions (FDP_ACF.1.1;1)	DAC.3, DAC.4
Discretionary Access Control Functions (FDP_ACF.1.2;1)	DAC.5, DAC.8
Discretionary Access Control Functions (FDP_ACF.1.3;1)	DAC.7
Discretionary Access Control Functions (FDP_ACF.1.4;1)	DAC.3, DAC.4, DAC.6
RBAC Policy (FDP_ACC.1;2)	DAC.2, DAC.7 MAC.5,6,9,12,15,16,17,19,22,23,24 IA.3, IA.4, IA.16, Priv.1, Priv.4, Priv.5 Admin.2,3,6,7,8,9,10 Audit.13,16,17,18 Integrity.1

Table 10: SFR - IT SF Mapping

Security Functional Requirement	TOE Security Function(s)
RBAC Functions (FDP_ACF.1;2)	DAC.2, DAC.7 MAC.5,6,9,12,15,16,17,19,22,23,24 IA.3, IA.4, IA.16, Priv.1, Priv.4, Priv.5 Admin.2,3,6,7,8,9,10 Audit.13,16,17,18 Integrity.1
Export of Unlabelled User Data (FDP_ETC.1)[b]	MAC.19, MAC.20
Export of Labelled User Data (FDP_ETC.2)	MAC.2,3,4,19,20
Mandatory Access Control Policy (FDP_IFC.1)	MAC.1 to MAC.26
Mandatory Access Control Functions (FDP_IFF.2.1)	MAC.1
Mandatory Access Control Functions (FDP_IFF.2.2)	MAC.10, MAC.11, MAC.22
Mandatory Access Control Functions (FDP_IFF.2.3)	Null requirement
Mandatory Access Control Functions (FDP_IFF.2.4)	Null requirement
Mandatory Access Control Functions (FDP_IFF.2.5)	MAC.12, MAC.23, MAC.24
Mandatory Access Control Functions (FDP_IFF.2.6)	Null requirement
Mandatory Access Control Functions (FDP_IFF.2.7)	MAC.1,10,11,13,15,18,20,21,23,24,25
Import of Unlabelled User Data (FDP_ITC.1)	MAC.19, MAC.20
Import of Labelled User Data (FDP_ITC.2)	MAC.2, MAC.19, MAC.20
Object Residual Information Protection (FDP_RIP.2.1)	OR.1, OR.2, OR.3
Subject Residual Information Protection (LSPP Note 1)	OR.1, OR.2, OR.3
User Attribute Definition (FIA_ATD.1.1)	IA.9
Strength of Authentication Data (FIA_SOS.1.1)	IA.1, IA.6, IA.7, IA.9[c], IA.13, IA.14
User Authentication Before Any Action (FIA_UAU.2)	IA.1
Protected Authentication Feedback (FIA_UAU.7.1)	IA.5
User Identification Before Any Action (FIA_UID.2)	IA.1, IA.15
User-Subject Binding (FIA_USB.1.1;1-3)	IA.2, MAC.9, MAC.10, Priv.2, Priv.3
Management of Object Security Attributes (FMT_MSA.1.1;1)	DAC.1-4
Management of Object Security Attributes (FMT_MSA.1.1;2)	MAC.17, MAC.18
Management of Object Security Attributes (FMT_MSA.1.1;3)	Admin.7[d]
Management of Object Security Attributes (FMT_MSA.1.1;4)	Priv.4, Priv.5

Table 10: SFR - IT SF Mapping

Security Functional Requirement	TOE Security Function(s)
Secure Security Attributes (FMT_MSA.2)	ENF.4
Static Attribute Initialization (FMT_MSA.3.1;1)	DAC.6
Static Attribute Initialization (FMT_MSA.3.1;2)	MAC.11
Static Attribute Initialization (FMT_MSA.3.1;3)	Priv.4, Priv.5
Static Attribute Initialization (FMT_MSA.3.2)	DAC.6, Priv.4, Priv.5
Management of the Audit Trail (FMT_MTD.1.1;1)	Audit.14
Management of Audited Events (FMT_MTD.1.1;2)	Audit.16, 17, 18
Management of User Attributes (FMT_MTD.1.1;3)	IA.10, Admin.1, Admin.6
Management of Authentication Data (FMT_MTD.1.1;4)	IA.9
Management of Authentication Data (FMT_MTD.1.1;5)	IA.8-14
Secure TSF Data (FMT_MTD.3)	ENF.4
Revocation of User Attributes (FMT_REV.1.1;1)	IA.3, IA.9, IA.16, Admin.1
Revocation of User Attributes (FMT_REV.1.1;2)	IA.9, Admin.1, Admin.6
Revocation of Object Attributes (FMT_REV.1.2;1)	DAC.6, MAC.17, MAC.18
Revocation of Object Attributes (FMT_REV.1.2;2)	DAC.5, DAC.6 MAC.10, MAC.11, MAC.17, MAC.18
Security Management Roles (FMT_SMR.1.1)	DAC.1, DAC.2, IA.9, Admin.1, Admin.4, Admin.5, Admin.8
Security Management Roles (FMT_SMR.1.2)	Admin.1, Admin.4
Security Management Roles (FMT_SMR.2.1)	DAC.1, DAC.2, IA.9, Admin.1, Admin.4, Admin.5, Admin.8
Security Management Roles (FMT_SMR.2.2)	Admin.1, Admin.4
Security Roles (FMT_SMR.2.3)	DAC.1, DAC.2, MAC.18
Abstract Machine Testing (FPT_AMT.1.1)	ENF.3
Failure With Preservation Of Secure State (FPT_FLS.1)	Fail.2
Manual Recovery (FPT_RCV.1)	Fail.1
Function Recovery (FPT_RCV.4)	Fail.2
Reference Mediation (FPT_RVM.1.1)	ENF.1
Domain Separation (FPT_SEP.1.1)	ENF.2
Domain Separation (FPT_SEP.1.2)	ENF.2

Table 10: SFR - IT SF Mapping

Security Functional Requirement	TOE Security Function(s)
Reliable Time Stamps (FPT_STM.1.1)	Audit.12
TSF Self Test (FPT_TST.1)	ENF.3
Limitation on Scope of Selectable Attributes (FTA_LSA.1)	Admin.5
TSF initiated session locking (FTA_SSL.1)	IA.7
User initiated locking (FTA_SSL.2)	IA.6
TOE Session Establishment (FTA_TSE.1)	Admin.5
Trusted Path (FTR_TRP.1)	TPath.1-7

Table 10: SFR - IT SF Mapping

a. FAU_GEN.1.1 implicitly includes the requirement not to store password information in the audit trail as required by IT SF Audit.15.
b. Including LSPP Note 6
c. Supplying a new password is stated in ITSF IA.9, and it is the process through which a user enters a new password that enforces the construction of the password and hence the probability of guessing the correct password.
d. Specifically, the *role.assign* authorisation.

7.4.2 Justification for Mapping of ENF.4 to FMT_MSA.2 and FMT_MTD.3

The SFRs from which ENF.4 are derived require that the TSF ensure that only secure values are accepted for security attributes and TSF data. These requirements assume that the TOE implements an apriori definition of security for which the value for a specified subset of security attributes and items of TSF data can be said to be secure or insecure. In such a case, a TOE could ensure such security attributes and TSF data have secure values.

For most TSF data items within Trusted Solaris 8 4/01, the TOE itself cannot make a determination as to whether a particular value for an attribute or TSF data item is "secure". In this context, "secure" is a relative term that depends entirely on the environment in which the TOE is being used. Such attributes/data include:

- user attributes such as clearances, privileges and authorizations - "secure" depends on the identity of the user in question;
- object attributes such as permissions, ACLs, labels - "secure" depends on the object, its content, and in (some cases) the identity of users, owners or user groups;
- system wide configuration parameters such as the list of events to be audited - "secure" depends on what is appropriate for the system.

For each of the above, the notion of "secure" may vary from day to day, and even from hour to hour. Human intervention is required to assess what is secure, and to take the appropriate actions as offered in the features of the TOE.

However, Trusted Solaris does require that each normal user password be set to a secure value in terms that can be enforced internal to the TOE. This is required in order to uphold the security target strength of function claim. Passwords are required to be of at least 8 characters in length, and the TOE ensures the content of the password is secure by either generating a value for the password, or applying rules to the content of the password selected by the user.

Therefore, in the context of Trusted Solaris 8 4/01, the derivation of ENF.4 from FMT_MSA.2 and FMT_MTD.3 is "The TSF shall ensure that only secure values are accepted for user passwords." "Secure values" as required under the broader definition of FMT_MSA.2 and FMT_MTD.3 do not apply in the context of Trusted Solaris 8 4/01 to any other type of security attribute or TSF data.

7.4.3 Justification for Compliance of Assurance Measures

Section 6.5 shows that all assurance requirements are met by an appropriate assurance measure.

7.5 PP Claims and Rationale

7.5.1 PP Reference

The TOE meets all of the requirements of the Controlled Access Protection Profile, the Labeled Security Protection Profile and the Role Based Access Control Protection Profiles which are defined in [CAPP], [LSPP], [RBAC] respectively.

7.5.2 PP Tailoring

The security functional requirements for the TOE are as defined in [CAPP], [LSPP] and [RBAC] with refinements as necessary and appropriate for a Security Target. These refinements are detailed in section 5.1.

7.5.3 PP Additions

There are three additional security functional requirements for the TOE beyond that defined in [LSPP] and [RBAC], FTA_SSL.1, FTA_SSL.2 and FTP_TRP.1. It should be noted that [CAPP] is a subset of [LSPP]. Table 2 in Chapter 5 illustrates the [LSPP] SFRs that are not included in [RBAC] and vice versa.

There are no additional TOE security objectives to those contained in [LSPP] and [RBAC]. The security objectives for the TOE environment in this security target

may be regarded as additional to those contained in [LSPP] and [RBAC], although they are deemed to be broadly equivalent, and refined due to the specific environment assumed for the Trusted Solaris 8 4/01 product.

O.HIERARCHICAL, O.DUTY and O.ROLE are the objectives that specifically satisfy [RBAC]. O.DAC, O.MAC and O.RESIDUAL_INFO are the objectives that specifically satisfy [LSPP].

7.5.4 PP Rationale

The objectives used in this Security Target are derived from [LSPP] and [RBAC]. The differences are minor and result from refinements appropriate to a Security Target where a specific product and the assumed environment are being described.

The SFRs used in this Security Target are derived from [LSPP] and [RBAC], and have been refined as required for inclusion in a Security Target.

The rationale presented in this document describing why the SFRs are appropriate to meet the security objectives has been taken from [LSPP] and [RBAC] also. Because of the similarities between the objectives and SFRs contained in this Security Target and in [LSPP], the justification provided in [LSPP] is also appropriate for this Security Target.