Solaris 9

Security Target

Document Number:	S9_101
Date:	24 January, 2005
Version:	1.0 DEFINITIVE

Abstract

This document is the Security Target for the EAL4+ Common Criteria v2.1 evaluation of Solaris 9 developed by Sun Microsystems, Inc.

4150 Network Circle, Santa Clara, California, 94054

THIS PUBLICATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THIS PUBLICATION COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN, THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THE PUBLICATION. SUN MICROSYSTEMS, INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAMS(S) DESCRIBED IN THIS PUBLICATION AT ANY TIME.

SUN MICROSYSTEMS, INC.

References

Standards & Criteria

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

[CEM-2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements CCIMB-99-032, Version 2.1, Annotate with interpretations as of 2003-12-31

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

[RBAC] Role Based Access Control Protection Profile, Version 1.0, 30 July 1998

[ALC_FLR] Part 2: Evaluation Methodology Supplement: Flaw Remediation, Version 1.1, February 2002

[Sol8_ST_FCS] Solaris 8 02/02 Security Target Version 2.0, 7 March 2003.

[NIST1] Letter from R. Chandramouli, re: FIA_UAU.2 in RBAC PP, Computer Security Division, NIST, dated 16 July 2001

[NIST2] Letter from R. Chandramouli, re: FPT_TST.1 in RBAC PP, Computer Security Division, NIST, dated 16 July 2001

Public Revision History

Version	Date	Author	Comments
1.0	January 2005	Jane Medefesser	Unclassified

Contents

This Page Intentionally Left Blank

Introduction 1

1.1 ST Identification

Title: Solaris 9 08/03 Security Target

Keywords: Solaris 9, general-purpose operating system, POSIX, UNIX.

This document is the security target for the CC evaluation of the Solaris 9 08/03 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 Solaris 9 operating system.

Solaris is a highly-configurable UNIX-based operating system. Originally developed to meet the requirements of the C2 class of the U.S. Department of Defence (DoD) Trusted Computer System Evaluation Criteria (TCSEC), it now meets specific equivalent Protection Profiles developed within the Common Criteria Project. These broad requirements are described for the Common Criteria scheme in [CAPP], the Controlled Access Protection Profile and in [RBAC], the Role Based Access Control Protection Profile.

A Solaris 9 system consists of a number of workstations and/or servers linked together to form a single distributed system. Users share the resources of multiple workstations and/or servers connected together in a single, distributed Trusted Computing Base (TCB).

This Solaris 9 ST is based on the previous Solaris 8 02/02 security target with the appropriate changes.

1.3 CC Conformance

This ST is conformant with the following:

- Controlled Access Protection Profile version 1.d [CAPP].
- Role Based Access Control Protection Profile version 1 [RBAC]

This ST is CC Part 2 extended and Part 3 conformant, augmented by ALC_FLR.3, with a claimed Evaluation Assurance Level of EAL4+ (see section 7.3.3).

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] and [RBAC].
- Appendix A contains information about TOE supported hardware platforms

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 Solaris 9 system. Some administrative tasks require the use of the *root* username and password so that they can become the superuser (with a user ID of 0).

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.

CB: Certification Body, a part of CSE (Communications Security Establishment) overseeing and monitoring evaluations in Canada.

Common Components: These relate to components of the mid-frame family that share the same or functionally similar hardware such as CPU, memory, Compact PCI Card, SC, I/O assemblies, etc.

Dynamic Reconfiguration (DR): This is the process of dynamically reconfiguring system boards, removing them or installing them onto a system while the Solaris operating environment is running. DR software is part of the Solaris Operating Environment and supports Multiple Domaining or Dynamic System Domains feature.

Dynamic System Domains: see Multiple Domain

FCS: First Customer Shipment.

High End Server platforms: For the purposes of this security target this means the Sunfire 12K and 15K servers.

IARR: Impact Analysis and Rationale Report, the document which shows platform equivalency across the SunFire mid-frame range of servers.

Low-end/Entry-Level platforms: For the purposes of this security target this means the following product models: Sunblade 150, 1500 and 2000 Workstations, Sunblade B100s server, Sunfire V100, V120, V210, V240, V250, 280R, V440, V480, V880 and V880z servers.

Mid-frame/Mid-range platforms: For the purposes of this security target this means the Sunfire V1280, 3800, 4800, 4810 and 6800 servers.

Multiple Domain (MD): This is a hardware configuration feature whereby a system may be logically partitioned into one or more domains. Each domain is a self-contained server of one or multip[le system boards, contains CPU, memory, I/O, boot-disk. network resources and runs a single instance of the Solaris Operating Environment.

Object: In Solaris 9, 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.

Peripherals: This term should be taken to mean (optional) storage, communications or printing devices that can be used with the TOE platforms.

Platform: Refers to servers, workstations or both when contextually appropriate.

PP: Protection Profile.

Product: The term product is used to define all hardware and software components that comprise the distributed Solaris 9 system.

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

SB: Sun Blade, a name given to a family of workstation products.

SC: System Controller, the component in the mid-frame platforms that boots up the ToE, and performs similar functions to that of an Open BootPROM

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.

Server: A computer/device which provides/manages information or services to computers on a network.

SF: Security Function OR (alternatively) SunFire, a name given to a family of servers, dependent upon context.

SFR: Security Functional Requirement

SMC: Sun Management Console, a secure system management GUI for SPARC administration

SoF: Strength of Function

SPARC: The name given to the processor family that is incorporated into the platforms identified in this security target.

SRN: Security Release Notes, see references.

Subject: There are two classes of subjects in Solaris 9:

- *untrusted subject* - this is a Solaris 9 process running on behalf of some user, running outside of the TCB (for example, with no privileges).
- *trusted subject* - this is a Solaris 9 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 Solaris 9 product which are connected/networked together and configured to form a usable system.

System Controller: This is an embedded system consisting of the system controller board and the system controller software (own processor, memory, etc.) which provides communication pathways between the platform system components and additionally performs functions replicating those of an ‘Open Boot PROM’.

Target of Evaluation (TOE): The TOE is defined as the Solaris 9 operating system, running and tested on the hardware and firmware specified in this Security Target. The BootPROM firmware forms part of the TOE Environment (see section 5.4).

TSF: TOE Security Function.

TSP: TOE Security Policy.

User: Any individual/person who has a unique user identifier and who interacts with the Solaris 9 product.

Workstation: A workstation is a computer intended for individual use that is more capable, powerful and faster than a personal computer.

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.

TOE Description 2

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

Solaris 9 is a highly-configurable UNIX-based operating system which has been developed to be compliant with the Controlled Access and Role Based Protection Profiles. Originally developed to meet the requirements of the C2 class of the U.S. Department of Defence (DoD) Trusted Computer System Evaluation Criteria (TCSEC), it now meets specific equivalent Protection Profiles developed within the Common Criteria Project.

A Solaris 9 system consists of a number of workstations and/or servers linked together to form a single distributed system. Users share the resources of multiple workstations and/or servers connected together in a single, distributed Trusted Computing Base (TCB).

2.3 Evaluated Configurations

2.3.1 Target of Evaluation

This section defines the software that comprise the ToE and the Servers/Workstations that the software runs on.

2.3.1.1 ToE Certification Platforms:

Note that the UltraSPARC IIi, IIIi and III Low-End platforms use an OpenBoot PROM. SunFire MidFrame and High-End platforms make use of the System Controller component to perform similar tasks to the OpenBOOT PROM. Both the OpenBoot PROM and System Controller are outside of the scope of this evaluation. The OpenBootPROM and System Controller are protected by a password commensurate *with the appropriate SoF requirement for the environment. The Administrator is responsible for selecting passwords of appropriate strength to meet the Security Target requirements.*

Workstations and Servers:

The target of evaluation is a (distributed) operating system product running on:

- Platform 1: Entry Level workstations and servers utilizing an UltraSPARC III, UltraSPARCIIIi or UltraSPARCIIi processor in a single or multiple configuration. Various configurations of these platforms are possible and the evaluation scope includes all possible combinations/permutations through the testing of CB appropriate configurations. An [IARR], Impact Analysis and Rationale Report, will show platform equivalency across the SunFire midframe family.
- Platform 2: The SunFire mid-frame and high-end family offering Dynamic Reconfiguration and Multiple Domaining as defined in Section 1.5. Various configurations of these platforms are possible and the evaluation scope includes all possible combinations/permutations through the testing of CB appropriate configurations. An [IARR], Impact Analysis and Rationale Report, will show platform equivalency across the SunFire midframe family.

Please refer to Appendix A for tables illustrating the hardware configurations available for use. Note that within each platform group, the processor speed associated with each model is dependant upon what was or is offered by the vendor.

2.3.1.2 Software

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

- Solaris 9 8/03, August 2003 (Also known as Update 4).
- Sun Management Console 2.1 (SMC)

The TOE documentation is supplied on CD-ROM and on SUN’s website: http://www.sun.com/software/security/securitycert.

2.3.2 File systems

The following filesystem types are supported:

- the standard Solaris UNIX filesystem, ufs, without the Trusted Solaris attributes;
- the standard 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 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 attributes inferred from the underlying process’ DAC attributes.

2.3.3 Configurations

The evaluated configurations are defined as follows.

- When installing the product, the entire distribution should be selected;
- No additional SMC add-ons should be installed;
- Minimum physical memory and disk configurations provided for the hardware in the tables above are provided with the Solaris 9 08/03 documentation and may not be sufficient for all applications. For components which must be installed separately from the Solaris Installation please consult that component’s installation guide to determine requirements.
- the CDE windowing environment must be used in preference to OpenWindows;
- Solaris 9 supports the use of IPv4 and IPv6, however IPv6 is not part of the TOE.
- support for DHCP is not included;
- 64 bit architectures are included;
- Web Based Enterprise Management Services (WBEM) are not included;
- Network, Web Start, Jumpstart, Flash, DVD and CD installations are all supported;
- the default configuration for identification and authentication only. Support for other authentication options e.g. smartcard authentication, is not included in the evaluation configuration;
- if the system console is used, it must be connect directly to the server/workstation and afforded the same physical protection as the server/workstation.
- The evaluated configuration may include the optional installation and deployment of the Sun Java System Application Server version 7.0 (SJAS). No additional security claims are made for SJAS.

The product comprises one or more of the above listed servers and/or workstations (and optional peripherals) running the above listed system software (a platform running the above listed software is referred to as a “TOE platform” below).

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

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

If the product is configured with more than one TOE platform, then the LDAP naming service must be used and the LDAP naming server(s) must be TOE platforms.

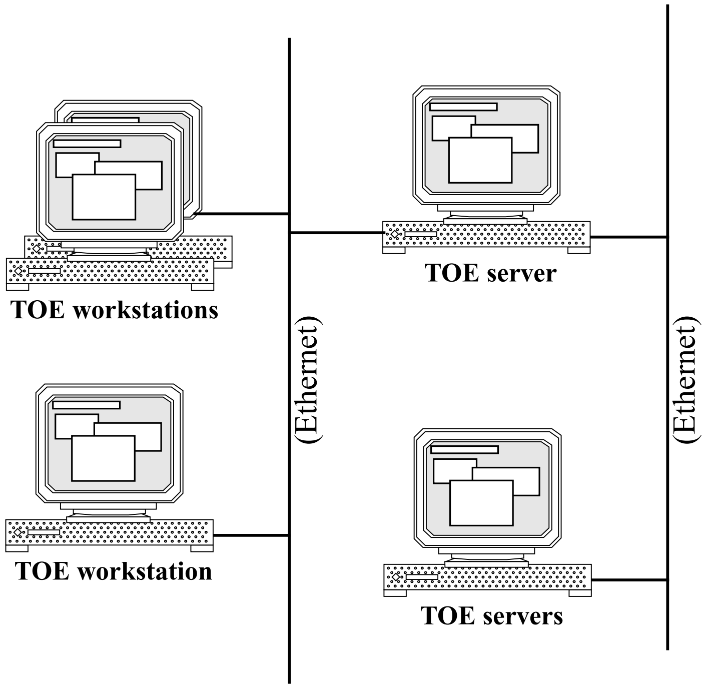

Table 1: Typical Evaluation Configuration

2.4 Summary of Security Features

The primary security features of the product are:

- Discretionary Access Control;
- Object Reuse;
- Identification and Authentication;
- Roles and Profiles;
- Security Management
- Auditing; and
- Enforcement.

These primary security features are supported by kernel and process domain separation and reference mediation, which ensure that the features are always invoked and cannot be bypassed.

2.4.1 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.

2.4.2 Object Reuse

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

2.4.3 Identification and Authentication

Solaris 9 provides identification and authentication based upon an unique user identifier and user password combination.

2.4.4 Roles and Profiles

Solaris 9 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 authorizations 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.

2.4.5 Security Management

The management of the security critical parameters of the TOE is performed by administrative users. A set of commands that require root privileges are used for system management. Security parameters are stored in specific files that are protected by the access control mechanisms of the TOE against unauthorized access by users non-administrative users.

2.4.6 Auditing

Solaris 9 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 and time of the event, user, security attributes and success or failure. This audit trail can be analyzed to identify attempts to compromise security and determine the extent of the compromise.

2.4.7 Enforcement

The Solaris 9 security policy is enforced in a manner which ensures that the organizational policies are upheld in the target environment i.e. the integrity of the TSF is protected, kernel and process domain separation is enforced and bypass of the security functions is prevented.

This Page Intentionally Left Blank

TOE Security Environment 3

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 lists 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 organizational 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/server, including data in transit between workstations/servers.

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

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

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

The threats listed below are grouped according to whether or not they are countered by the TOE. Those that are not countered by the TOE are countered by environmental or external mechanisms.

3.2.1 Threats countered by the TOE

[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.

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 unauthorized user of the TOE gains access to the system, thereby gaining unauthorized access to information.

An unauthorized user of the TOE could gain access to the system by impersonating an authorized user, or by gaining access to an unattended platform at which an authorized 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 unauthorized access to information.

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

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

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

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

3.2.2 Threats to be countered by measures within the TOE environment

The following threats apply in environments where specific threats to distributed systems need to be countered.

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

3.3 Organizational Security Policies

The TOE complies with the following organizational security policies:

[P.AUTH] Only those users who have been authorized 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 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.

3.4 Assumptions

This section indicates the minimum physical and procedural measures required to maintain security of the TOE. 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.LDAP_DOMAINS] It is assumed that, if the product comprises more than one platform, all platforms are administered from a central point within each LDAP directory domain.

LDAP 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 organization.

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

This Page Intentionally Left Blank

Security Objectives 4

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.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 released 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 organizational 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 the 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 analyzed 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 [noac] 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 platform 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 platform 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 Solaris 9 operating system is “booted” during system start-up.

Note: The above applies to both workstations and server. 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.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 platform, all such platforms are administered from a central point within each LDAP 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 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.

c. If a system console is used, it must be connected directly to the machine, and must be afforded the same physical protections as the server or workstation. Access onto the system console is protected by user identification and authentication mechanisms. Access to the eeprom is protected by an eeprom password.

d. For the MidFrame and E15K platforms, the system controller must be connected directly to the server, and must be afforded the same physical protections as the server. The system controller will not be accessible via a network connection. Access onto the system controller is protected by an SC password.

[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.SERIAL_LOGIN] Those responsible for the TOE shall implement procedures to ensure that users clear the screen before logging off where serial login devices (e.g.VT100) are used.

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 platforms is secured from disclosure, interruption or tampering.

This Page Intentionally Left Blank

Security Requirements 5

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 [CAPP] and [RBAC] where these are derived from either PP. An Asterick (*) after the elements's name indicates that one or more operations on that element are completed in this ST.

CLASS	FAMILY	COMPONENT	ELEMENT	[CAPP] 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	

Table 2: Security Functional Requirements

CLASS	FAMILY	COMPONENT	ELEMENT	[CAPP] PARAGRAPH	[RBAC] PARAGRAPH
FDP	FDP_ACC	FDP_ACC.1	FDP_ACC.1.1*	5.2.1.1	5.1.2
		FDP_ACF.1	FDP_ACF.1.1* FDP_ACF.1.2* FDP_ACF.1.3* FDP_ACF.1.4*	5.2.2.1 5.2.2.2 5.2.2.3 5.2.2.4	5.1.2
	FDP_RIP	FDP_RIP.2	FDP_RIP.2	5.2.3.1	
		FDP_RIP.2 (Note 1)	FDP_RIP.2	5.2.4.1	
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.1	FIA_UAU.1.1* FIA_UAU.1.2	5.3.3.1 5.3.3.2	
		FIA_UAU.2	FIA_UAU2.1		5.1.3
		FIA_UAU.7	FIA_UAU.7.1	5.3.4.1	
	FIA_UID	FIA_UID.1	FIA_UID.1.1* FIA_UID.1.2	5.3.5.1 5.3.5.2	
		FIA_UID.2	FIA_UID.2.1		5.1.3
	FIA_USB	FIA_USB.1	FIA_USB.1.1*	5.3.6.1 5.3.6.2 5.3.6.3	5.1.3

Table 2: Security Functional Requirements

CLASS	FAMILY	COMPONENT	ELEMENT	[CAPP] PARAGRAPH	[RBAC] PARAGRAPH
FMT	FMT_MSA	FMT_MSA.1	FMT_MSA.1.1*	5.4.1.1	5.1.4
		FMT_MSA.2	FMT_MSA.2.1		5.1.4
		FMT_MSA.3	FMT_MSA.3.1* FMT_MSA.3.2*	5.4.2.1 5.4.2.2	5.1.4 5.1.4
	FMT_MTD	FMT_MTD.1	FMT_MTD.1.1	5.4.3 5.4.4 5.4.5 5.4.6	5.1.4
		FMT_MTD.3	FMT_MTD.3.1		5.1.4
	FMT_REV	FMT_REV.1	FMT_REV.1.1 FMT_REV.1.2* FMT_REV.1.1	5.4.7.1 5.4.7.2 5.4.8.1	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
	FMT_SMF	FMT_SMF.1	FMT_SMF.1.1		
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 5.1.5 5.1.5
FTA	FTA_LSA	FTA_LSA.1	FTA_LSA.1.1		5.1.6
	FTA_TSE	FTA_TSE.1	FTA_TSE.1.1		5.1.6
	FTA_SSL	FTA_SSL.1	FTA_SSL.1.1* FTA_SSL.1.2*		
		FTS_SSL.2	FTA_SSL.2.1* FTA_SSL.2.2*		

Table 2: Security Functional Requirements

5.1.1 Protection Profile SFRs Tailored for This Security Target

The elements that are tailored for this security target are indicated by a * after the element's name in the table above. These tailored elements are given below, with the new material underlined. The remaining SFRs in the table above are to be used for this security target exactly as they appear in [CEM-2], [CAPP] and [RBAC].

5.1.1.1 Security Audit (FAU)

[CAPP] 5.1.5.1 The TSF shall provide the ability to perform searches of audit data based on the following attributes: FAU_SAR.3.1

a. User identity;

b. type of audit event and audit class.

[CAPP] 5.1.6.1 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. audit class.

[CAPP] 5.1.8.1 The TSF shall generate an alarm to the authorized administrator if the audit trail exceeds or meets 100% occupancy. FAU_STG.3.1

Note: An alarm is generated once 100% of the allocated audit space is reached. This disk space may be exceeded in certain circumstances e.g. by auditable actions taken by authorized administrators.

[CAPP] 5.1.9.1 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

5.1.1.2 User Data Protection (FDP)

[CAPP] 5.2.1.1 The TSF shall enforce the Discretionary Access Control Policy on processes acting on the behalf of users, filesystem objects and all operations among subjects and objects covered by the DAC policy. FDP_ACC.1.1

[CAPP] 5.2.2.1 The TSF shall enforce the Discretionary Access Control Policy to objects based on the following: FDP_ACF.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

[CAPP] 5.2.2.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: FDP_ACF.1.2

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

[CAPP] 5.2.2.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rule: FDP_ACF.1.3

a. If a subject has an effective UID of 0, the TSF shall authorize access of the subject to any given filesystem object, even if such access is disallowed by FDP_ACF.1.2.

[CAPP] 5.2.2.4 The TSF shall explicitly deny access of subjects to objects based on no additional rules. FDP_ACF.1.4

5.1.1.3 Identification and Authentication (FIA)

[CAPP] 5.3.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: FIA_ATD.1.1

a. User Identifier;

b. Group Memberships;

c. Authentication Data;

d. Security-relevant Roles; and

e. login shell.

[CAPP] 5.3.3.1 The TSF shall allow the following TSF-mediated actions on behalf of the user to be performed before the user is authenticated FIA_UAU.1.1

a. select language;

b. select desktop or console login;

c. select remote host for login;

d. help for login function.

[CAPP] 5.3.5.1 The TSF shall allow the following TSF-mediated actions on behalf of the user to be performed before the user is identified. FIA_UID.1.1

a. select language;

b. select desktop or console login;

c. select remote host for login;

d. help for login function.

[CAPP] 5.3.6.1 The TSF shall associate the *following* user security attributes with subjects acting on the behalf of that user: FIA_USB.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.

[CAPP] 5.3.6.2 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

a. 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.

b. 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.

[CAPP] 5.3.6.3 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

a. The effective user identity associated with a subject can be changed to another user's identity via a command, provided that the effective user identity was 0, or successful authentication as the new user identity has been achieved;

b. When executing a file which has the set 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.

Application Note: The DAC policy is enforced based on the effective UID as described above. All auditable events are recorded with the audit ID, which contains the identity of the user at identification time. In this manner, all auditable events can be traced back to the person initially identified to the TOE and are not associated to another person who may at some time identify them self as the alternate identity.

5.1.1.4 Security Management (FMT)

[CAPP] 5.4.1.1 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 effective UID of 0. FMT_MSA.1.1

[RBAC] 5.1.4 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

[CAPP] 5.4.2.2 The TSF shall allow the authorized administrators and users authorized by the Discretionary Access Control Policy 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

[CAPP] 5.4.7.1 The TSF shall restrict the ability to revoke security attributes associated with objects within the TSC to users authorized to modify the security attributes by the Discretionary Access Control policy.$^{\text{FMT\_REV.1.1}}$

[CAPP] 5.4.7.2 The TSF shall enforce the rules: $^{\text{FMT\_REV.1.2}}$

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

b. Administrative users shall be able to revoke security-relevant authorizations 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.

Application Note: The DAC policy may include immediate revocation (e.g., Multics immediately revokes access to segments) or delayed revocation (e.g., most UNIX systems do not revoke access to already opened files). The DAC access rights are considered to have been revoked when all subsequent access control decisions by the TSF use the new access control information. It is not required that every operation on an object make an explicit access control decision as long as a previous access control decision was made to permit that operation. It is sufficient that the developer clearly documents in guidance documentation how revocation is enforced.

Rationale: This component supports the O.DISCRETIONARY_ACCESS objective by providing that specified access control attributes are enforced at some fixed point in time.

5.1.1.5 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 to modify their own authentication data;

d. *[CAPP] 5.4.9.1* Roles for the Object Owners.$^{\text{FMT\_SMR.1.1}}$

e. *[RBAC] 5.1.4* Restrictions on Roles for the Object owner and administrator FMT_SMR.2.1

[RBAC] 5.1.4 The TSF shall be able to associate users with roles.$^{\text{FMT\_SMR.2.2}}$

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. *[RBAC] 5.1.4* The set of RBAC administrative roles can modify security attributes for all objects under the control of the TOE.$^{\text{FMT\_SMR.2.3}}$

5.1.1.6 Trusted Recovery

[RBAC] 5.1.5 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 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. *[RBAC] 5.1.5* 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

5.1.1.7 Protection of the TOE Security Functions (FPT)

[CAPP] 5.5.1.1 The TSF shall run a suite of tests <u>at the request of an authorized administrator</u> to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF. FPT_AMT.1.1

5.1.1.8 Specification of Management Functions

[CEM-2] Note below: The TSF shall be capable of allowing the administrative user to perform the following management functions: FMT_SMF.1

a. Object security attributes management

b. Management of user accounts and roles (create, delete, modify)

c. Authentication data management

d. Management of security settings

e. Audit administration

NOTE: This security functional requirement has been added as a result of AIS 32, Final Interpretation 065. The security functional requirement was added because a dependency from FMT_MSA.1 and FMT_MTD.1 to this new component has been defined in ASI 32, Final Interpretation 065.

5.1.1.9 TOE Access

[CEM-2] 501 The TSF shall lock an interactive session after an <u>administrator-defined time interval of user activity</u> 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: <u>the user must be successfully re-authenticated.</u> FTA_SSL.1.2

[CEM-2] 501 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

5.2 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+ [CC]. Assurance is augmented by ALC_FLR.3 Systematic Flaw Remediation.

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 either the OpenBoot PROM or the System Controller. Refinements to the CC Part 2 functional component are identified by emboldened text. The functionality provided by this firmware/SC is specified as follows:

5.4.1 Ultrasparc Workstations, SunFire V880, SunBlade 2000

The **OpenBoot PROM on UltraSPARC II workstations, V880, and SunBlade 2000** shall restrict the ability to modify the behavior of the boot strapping process to users who know the valid PROM password.FMT_MOF.1.1:1

Application Note: In fully secure and command-secure modes, the valid (booting) password is required in order to configure the PROM operating modes, passwords or boot parameters as required by the [SRN].

5.4.2 SunFire MidFrames, E15K

The **System Controller on the SunFire MidFrame and E15K platforms** shall restrict the ability to modify the behavior of the boot strapping process to users who know the valid SC password.FMT_MOF.1.1:2

Application Note: A valid (booting) password is required in order to configure the SC operating modes, passwords or boot parameters as required by the [SRN].

This Page Intentionally Left Blank

TOE Summary Specification 6

6.1 IT Security Functions

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

- IA.1
- IA.11

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 platforms in the system.

Within 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 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, real user ID, saved user ID;
- effective group ID, real group ID, saved group ID, supplemental groups; and
- audit user ID.

The Solaris 9 discretionary access controls use the effective user ID and effective group ID for policing a subject's access rights over objects that have fixed or implicit permissions to within a process context.

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 Subject to DAC.8 the access permissions on an owner controlled object can be modified only by a subject that owns the object.

DAC.2 No subject may change the owner or group of an owner controlled object unless it has a uid of 0, or optionally is the owner of the object.

Note that Solaris 9 can be configured to allow the modification of owner and group of a owner controlled object by the owner, or can be configured to be POSIX compliant whereby only the root user (uid 0) can modify ownership, and the owner can change the group only to one which they are a member of. The functioning of both of these modes should be assessed during the evaluation of the TOE.

DAC.3 Subject to DAC.1, a subject may assign any combination of the following access modes to an owner controlled 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* or *nfs* 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 is limited to regular files held on ufs and nfs filesystems. This includes hard links but excludes device special files, pipes and symbolic links. However, the regular files referenced by symbolic links can still be controlled by ACLs.

DAC.6 Whenever a subject requests access to an owner controlled 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.7 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.8 Subjects may only override discretionary access control if they have a uid of 0.

6.1.2 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.

6.1.3 Identification and Authentication

<u>Password Authentication</u>

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 of the user's subjects shall be those specified by the authentication data.

<u>Password Protection</u>

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.9 On entry, passwords shall not be displayed in cleartext.

IA.10 User passwords are always stored in encrypted form.

Note: This SF does not apply to BOOTPROM or System Controller passwords (which are not user passwords, and are beyond the scope of this security target).

IA.11 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; and

- by a user supplying a new password.

Note: In respect of [CAPP_5.4.7.2] requirements; The administrator can use the Administration tools to revoke access rights, security relevant authorizations and forcibly log off users if required.

6.1.4 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)
- identification of the server/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;
- name 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.

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;
- 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;
- name of the user account being modified; and
- 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;
- name of the user account or object being modified;
- type of attribute; and
- success or failure of the attempt.

Audit.7 The assuming of uid 0 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 involved (if any).

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.
- the privilege or role granted

Audit.9 The allocation or re-allocation of any reconfigurable hardware component on a platform via the dynamic reconfiguration capability is auditable. The following information is recorded for each event audited:

- date;
- time;
- user identity - audit ID and effective user ID;
- name of the hardware component; and
- type of action.
- Note that this Security Function applies to the SunFire MidFrame and E15K platforms configured in multi-domain mode. If an attempt is made to execute the command which supports the dynamic reconfiguration feature, all other platforms and the SunFire MidFrames and E15K platforms configured in single-domain mode will generate audit records indicating that the command is not applicable to the machine.

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;
- name of the object and device; and
- 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.

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.

Audit Data Storage

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

Audit.21 If another server/workstation of the product is being used as an audit server, and this audit server becomes unavailable, the (local) server/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 server/workstation of the product takes over as an audit server;

or

- if no server/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.

6.1.5 Administration

Profiles

Solaris 9 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 authorizations 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 privilege that the action shall be performed with;
  - The real and effective user ID and the 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 real and effective user ID and the real and effective group ID that the command shall be executed with.
- A list of authorizations 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.

Roles

Roles are configurable with Solaris 9, allowing the 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.

6.1.6 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.

6.1.7 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.

6.2 Required Security Mechanisms

6.2.1 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 Medium. This mechanism supports the IT SFs IA.1 and IA.11.

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

6.3 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.

Table 4: How Assurance Requirements Will Be Met

Assurance components	Assurance Measure
ACM_AUT.1 Partial CM automation	Information on the automated CM tools will be provided in the Software Development Framework document
ACM_CAP.4 Generation support and acceptance procedures	Configuration Management procedures will be provided for Solaris 9.
ACM_SCP.2 Problem tracking CM coverage	As for ACM_CAP.4.
ADO_DEL.2 Detection of modification	Delivery procedures will be provided for Solaris 9.
ADO_IGS.1 Installation, generation, and start-up procedures	Installation, generation and start-up procedures will be provided for Solaris 9.
ADV_FSP.2 Fully defined external interfaces	The Solaris 9 MAN pages, which are relevant to the implementation of the security functions, will be provided to the evaluation and assessed against this assurance requirement.

Assurance components	Assurance Measure
ADV_HLD.2 Security enforcing high-level design	High-level Design will be provided for Solaris 9.
ADV_IMP.1 Subset of the implementation of the TSF	The source code for Solaris 9 will be provided to the evaluation.
ADV_LLD.1 Descriptive low-level design	Low-level Design will be provided for Solaris 9.
ADV_RCR.1 Informal correspondence demonstration	This correspondence information will be contained in the functional specification and design documents. The functional specification will map SFs 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 provided to the evaluation.
AGD_ADM.1 Administrator guidance	The Solaris 9 operational documentation relevant to an administrator will be provided.
AGD_USR.1 User guidance	The Solaris 9 operational documentation relevant to an end user will be provided.
ALC_DVS.1 Identification of security measures	Development security documentation will be provided for Solaris 9.
ALC_FLR.3 Life Cycle Support	Flaw remediation procedures are in place for Solaris, documents and other evidence will be provided.
ALC_LCD.1 Developer defined life-cycle model	The Life Cycle definition for Solaris 9 is documented in the Software Development Framework document.
ALC_TAT.1 Well-defined development tools	The tools used in the development of Solaris 9 are the same as for Solaris 8 FCS.
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 Solaris 8 02/02 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	The analysis of test depth will be presented to the evaluation in a form similar to that provided to the Solaris 8 02/02 evaluation. The existing coverage is against both High and Low level designs and should therefore be to a sufficient depth

Assurance components	Assurance Measure
ATE_FUN.1 Functional testing	The test documentation provided to the evaluation will be in a format similar to that provided to the Solaris 8 02/02 evaluation. The tests will be run on a range of platforms as specified in section 2.3.1.1.
ATE_IND.2 Independent testing - sample	Access will be provided to the TOE in its evaluated configuration on an appropriate set of platforms, together with all resources needed to repeat the developer's tests.
AVA_MSU.2 Validation of analysis	The Misuse Analysis, previously submitted for the EAL4 evaluation of Solaris 8 02/02, will be updated for Solaris 9.
AVA_SOF.1 Strength of TOE security function evaluation	The Strength of Function analysis, previously submitted for the EAL4 evaluation of Solaris 8 02/02, will be updated for Solaris 9.
AVA_VLA.2 Independent vulnerability analysis	The Developer Vulnerability Analysis, previously submitted for the EAL4 evaluation of Solaris 8 02/02, will be updated for Solaris 9 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.

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, organizational policies, assumptions and objectives is detailed in the following sections, and is summarized below.

Objectives	O.Authorisation	O.Dac	O.Audit	O.Residual_Info	O.Manage	O.Enforcement	O.Admin	O.Accountable	O.AuditData	O.AuthData	O.Boot	O.Consistency	O.Install	O.Info_Protect	O.Maintenance	O.Recover	O.Hierarchial	O.Duty	O.Role	O.Software_in	O.Serial_Login	O.Protect
T.Access_Info	✔	✔	✔	✔	✔	✔	✔			✔	✔	✔	✔	✔		✔			✔		✔	✔
T.Access_TOE	✔		✔		✔	✔	✔	✔	✔	✔	✔	✔	✔									
T.Modify	✔	✔	✔			✔	✔				✔	✔	✔	✔					✔			✔
T.Admin_Rights	✔		✔		✔	✔	✔	✔		✔	✔	✔	✔				✔	✔	✔	✔		
T.Transit													✔	✔								✔
P.Auth	✔				✔	✔				✔												
P.DAC		✔		✔	✔	✔																
P.Accountable	✔		✔		✔	✔	✔	✔	✔													
A. Password							✔						✔									
A.Protect														✔								✔
A.Admin							✔	✔	✔	✔	✔	✔	✔	✔	✔	✔				✔	✔	✔
A.User							✔	✔		✔												
A.Ldap_domains												✔										
A.Bridges&Routers														✔								✔

The OSPs are derived from the [CAPP] 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 and O.CONSISTENCY are general objectives which 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.CONSISTENCY is required to ensure that data is set up and maintained in a consistent manner across all platforms 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.

[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 compartmentalization 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 DAC, 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 O.DAC.

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.PROTECT - to ensure that data transmitted over network cabling is appropriately protected;

e. O.RECOVER - to ensure that information cannot be accessed by terminating the operation of a server/workstation (whether intentional or not);

f. O.SERIAL_LOGIN - to ensure that information is not seen by users who do not have a need to know when serial devices are being used;

[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 access functions.

O.MANAGE and O.ENFORCEMENT support this threat by ensuring:
- the database of authorized users is properly managed and maintained;
- the authorization 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 platforms. 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 O.DAC. O.MANAGE ensures that the administrative users can control access to the 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 supports this threat by ensuring the access control functions are always invoked and cannot be bypassed.

Role based access to the information is covered by the objectives O.DUTY and O.ROLE which ensure that only those users are assigned roles and only those uses 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.

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

O.DUTY provides the capability of enforcing separation of riles and O.HIERARCHIAL allows for the hierarchal 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.MANAGE and O.ENFORCEMENT support this threat 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.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 authorization 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 ensures that roles are properly defined.

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

Administrators must ensure that data transferred between platforms 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 platforms. 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.

7.2.2 Complete Coverage - Policy

This section provides evidence demonstrating coverage of the Organizational Security Policy by the IT security objectives.

[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 authorization functions are always invoked and cannot be bypassed.

O.AUTHDATA supports this policy by ensuring that authorization 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.

7.2.3 Complete Coverage - Environmental Assumptions

This section provides evidence demonstrating coverage of the environmental assumptions by security objectives.

[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.LDAP_DOMAINS] *It is assumed that, if the product comprises more than one platform, all platforms are administered from a central point within each LDAP domain.*

LDAP is installed and configured at installation time, and therefore objective O.CONSISTENCY 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)
	Authentication (FIA_UAU.1)
	User Authentication Before Any Actopn (FIA_UAU.2)
	Protected Authentication Feedback (FIA_UAU.7)
	User Identification Before Any Action (FIA_UID.2)
	User Identification (FIA_UID.1)
	TSF Initiated Screen Locking (FIA_SSL.1)
	User initiated locking (FTA_SSL.2)
O.DAC	Discretionary Access Control Policy (FDP_ACC.1)

Security Objective	Functional Component
	Discretionary Access Control Functions (FDP_ACF.1)
	User Attribute Definition (FIA_ATD.1)
	User-subject Binding (FIA_USB.1)
	Management of Object Security Attributes (FMT_MSA.1)
	Secure Security Attributes (FMT_MSA.2)
	Static Attribute Initialisation (FMT_MSA.3)
	Revocation of Object Attributes (FMT_REV.1)
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)
	Management of the Audit Trail (FMT_MTD.1)
	Management of the Audited Events (FMT_MTD.1)
	Reliable Time Stamps (FPT_STM.1)
O.RESIDUAL_INFO	Subject Residual Information Protection (FDP_RIP.2)
O.MANAGE	Audit Review (FAU_SAR.1)
	Restricted Audit Review (FAU_SAR.2)
	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)
	Management of Audit Events (FMT_MTD.1)
	Management of User Attributes (FMT_MTD.1)
	Management of Authentication Data (FMT_MTD.1)
	Revocation of User Attributes (FMT_REV.1)

Security Objective	Functional Component
	Security Management Roles (FMT_SMR.1)
	Specification of Management Functions (FMT_SMF.1)
	Management of Security Attributes (FMT_MSA.1)
	Secure Security Attributes (FMT_MSA.2)
	Static Attribute Initialization (FMT_MSA.3)
	Secure TSF Data (FMT_MTD.3)
	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)
O.DUTY	Security Roles (FMT_SMR.2)
O.HIERACHICAL	Security Roles (FMT_SMR.2)
O.ROLE	RBAC Policy (FDP_ACC.1)
	RBAC Functions (FDP_ACF.1)
	Management of Object Security Attributes (FMT_MSA.1)
	Static Attribute Initialisation (FMT_MSA.3)
	Management of User Attributes (FMT_MTD.1)
	Security Roles (FMT_SMR.2)
	Limitation on the Scope of Selectable Attributes (FTA_LSA.1)
	TOE Session Establishment (FTA_TSE.1)

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.1, FIA_UID.2 and FIA_UAU.2]. To ensure authorized access to the TOE, authentication data is protected [FIA_ATD.1, FIA_UAU.7 and FMT_MTD.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 uses 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]. The rules of the DAC policy must be defined [FDP_ACF.1]. The security attributes of objects used to enforce the DAC policy must be defined [FDP_ACF.1]. The security attributes of subjects used to enforce the DAC policy must be defined [FIA_ATD.1 and FIA_USB.1]. Authorized users must be able to control who has access to objects [FMT_MSA.1], that only secure values are set for security attributes [FMT_MSA.2] and be able to revoke that access [FMT_REV.1]. Protection of named objects must be continuous, starting from object creation [FMT_MSA.3].

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]. The audit trail must be protected so that only authorized users may access it [FAU_SAR.2]. The TSF must provide the capability to audit the actions of an individual user [FAU_SAR.3, FAU_SEL.1 and FIA_USB.1]. 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.3.1 and FMT_MTD.1] 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].

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.

Aspects that need to be managed must be defined [FMT_SMF.1]. 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 and FMT_REV.1]. The administrator must be able to review manage the audit trail

[FAU_SAR.1, FAU_SAR.3, FAU_SEL.1, FAU_STG.3, FAU_STG.4, FMT_MTD.1]. 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 organizational 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 [FMT_AMT.1]. The correctness of this objective is further met through the assurance requirements defined in the PP.

The TSF shall run a suite of self tests to demonstrate the correct operation of the TOE [FPT_TST.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 and FDP_ACF.1]. User and object security attributes required to enforce the RBAC policy must be securely managed [FMT_MTD.1, FMT_MSA.1 and FMT_MSA.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].

Table 3: 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_SMF.1	FMT_SMR.1	FPT_AMT.1	FPT_STM.1	FPT_TST.1
FAU_GEN.1																	✔	
FAU_GEN.2	✔									✔								
FAU_SAR.1	✔																	
FAU_SAR.2		✔																
FAU_SAR.3		✔																
FAU_SEL.1	✔												✔					
FAU_STG.1	✔																	
FAU_STG.3			✔															
FAU_STG.4			✔															
FDP_ACC.1					✔													
FDP_ACF.1				✔								✔						
FDP_IFC.1						✔												
FDP_IFF.2							✔					✔						
FDP_RIP.2																		
FIA_ATD.1																		
FIA_SOS.1																		
FIA_UAU.2										✔								
FIA_UAU.7									✔									
FIA_UID.2																		
FIA_USB.1								✔										
FMT_MSA.1				✔			✔							✔	✔			
FMT_MSA.2				✔							✔				✔			
FMT_MSA.3											✔			✔	✔			
FMT_MTD.1														✔	✔			
FMT_MTD.3													✔					
FMT_REV.1															✔			

Table 3: 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_SMF.1	FMT_SMR.1	FPT_AMT.1	FPT_STM.1	FPT_TST.1
FMT_SMF.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																		
FPT_TST.1																✔		
FTA_LSA.1																		
FTA_SSL.1									✔									
FTA_SSL.2									✔									
FTA_TSE.1																		

7.3.2 Requirements are Mutually Supportive and Internally Consistent

The above table identifies the dependencies of all functional components included in the ST. Required dependencies are indicated by the use if the checkmark: ✔

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

- 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.

ALC_FLR.3 introduces no additional dependencies.

7.3.3 Justification for Choice of Assurance Requirements

This security target claims an assurance rating of EAL4+. The security target has been based largely on [CAPP] and [RBAC] which specific security requirements for a product which is to be used in a non-hostile environment with a moderate risk to the assets. In such environments, an assurance level of EAL3 is recommended as stated in [CAPP].

This security target also contains the assurance requirements from the CC EAL4 assurance package augmented with ALC_FLR.3. The CC allows assurance packages to be augmented, which allows the addition of assurance components from the CC not already included in the EAL. Augmentation was chosen to provide the added assurance that is provided by defining flaw remediation procedures and correcting security flaws. This ST is based on solid rigorous commercial software development practices and has been developed for a generalized environment for a TOE that is generally available and does not need modification to meet the security needs specified in the ST.

The EAL chosen is based on the statement of the security environment and objectives defined in this ST. The sufficiency of the EAL chosen is justified based on the enhancements made to [CAPP] and [RBAC] which are detailed in Section 5.1. and the flaw remediation procedures defined in supplement ALC_FLR.3.

[CAPP] requires an EAL3 assurance rating. EAL4+ is a super-set of those requirements.

[RBAC] requires EAL2 assurance augmented with ADV_SPM.1.1 EAL4+ is a super-set 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 exceeds the [RBAC] requirement of SOF-basic and is consistent with [CAPP] 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 so as to satisfy the TOE security functional requirements. The table below shows the TOE security functions which together satisfy each security functional requirement. They are grouped under the relevant TOE security objective.

Table 5: SFR - IT SF Mapping

Security Functional Requirement	TOE Security Function(s) Rational to support the SFR
Audit Data Generation (FAU_GEN.1.1)	Audit.1 to Audit.11, Audit.15[a] Auditing procedures provide a record of auditable events.
Audit Data Generation (FAU_GEN.1.2)	Audit.1,2,3,4,5,6,8,11,21 Event records include date and time of the event, subject identity and the outcome (success or failure) of the event.
User Identity Generation (FAU_GEN.2.1)	Audit.1 to Audit.11 Auditing procedures identify each auditable event with the identity of the user that caused the event.
Audit Review (FAU_SAR.1.1)	Audit.19 Authorized administrators of the TOE have the capability to read all audit record information.
Audit Review (FAU_SAR.1.2)	Audit.19 Audit records are suitable for user interpretation.
Restricted Audit Review (FAU_SAR.2.1)	Audit.14 Audit data is protected so that access is limited to administrative users.
Selectable Audit Review (FAU_SAR.3.1)	Audit.19 Administrative users are able to selectively retrieve audit data based on, at a minimum, the identity of users, the type of audit event, and the audit class.
Selective Audit (FAU_SEL.1.1)	Audit.17, Audit.18 Administrative users are able to define the default system audit-mask that defines which audit classes are recorded by default. Only administrative users are 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.
Protected Audit Trail Storage (FAU_STG.1.1)	Audit.14 Audit data is protected against unauthorized deletion because access to it is limited to administrative users.
Protected Audit Trail Storage (FAU_STG.1.2)	Audit.14 Audit data is protected against modification.
Action in Case of Possible Audit Data Loss (FAU_STG.3.1)	Audit.23 The system shall notify an administrator of audit trail saturation.

Table 5: SFR - IT SF Mapping

Security Functional Requirement	TOE Security Function(s) Rational to support the SFR
Prevention of Audit Data Loss (FAU_STG.4.1)	Audit.20, Audit.21 In the event of an audit storage failure the system will prevent auditable events, except those taken by the administrator.
Discretionary Access Control Policy (FDP_ACC.1.1)	DAC.6, Admin.2, Admin.3 The access permissions on an owner controlled object can be modified only by a subject that owns the object or by a user with uid 0.
Discretionary Access Control Functions (FDP_ACF.1.1)	DAC.3, DAC.4 Solaris file permissions ensure that no subject can change the owner or group of an owner controlled object unless it has a uid of 0, or optionally is the owner of the object
Discretionary Access Control Functions (FDP_ACF.1.2)	DAC.6 Solaris file permissions ensure that whenever a subject requests access to an owner controlled 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.
Discretionary Access Control Functions (FDP_ACF.1.3)	DAC.8, Admin.2, Admin.3 Solaris file permissions ensure that a subject cannot override discretionary access control unless they have a uid of 0
Discretionary Access Control Functions (FDP_ACF.1.4)	DAC.3, DAC.4, DAC.6. Whenever a subject requests access to an owner controlled object, the access permissions for that object will 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 will be used instead of the object's permission bits. Unix file permissions ensure that the changes to the object are allowable unless overridden by ACL.
Object Residual Information Protection (FDP_RIP.2.1)	OR.1, OR.2, OR.3 Solaris ensures that any previous content of a resource is made unavailable upon the allocation of the resource to all objects.
Subject Residual Information Protection (Note 1)	OR.1, OR.2, OR.3 Solaris ensures that any previous content of a resource is made unavailable upon the allocation of the resource to all subjects.
User Attribute Definition (FIA_ATD.1.1)	IA.1, IA.11 Solaris assures that users are assigned unique individual security attributes that are enforced throughout each session.
Strength of Authentication Data (FIA_SOS.1.1)	IA.1, IA.11[b] Solaris mechanisms exists which enforces standards of password management.

Table 5: SFR - IT SF Mapping

Security Functional Requirement	TOE Security Function(s) Rational to support the SFR
Authentication (FIA_UAU.1.1)	IA.1 User must authenticate identity at the beginning of each user session.
Authentication (FIA_UAU.1.2)	IA.1 No user actions are allowed until authentication has completed successfully.
User Authentication (FIA_UAU.2)	IA.1 No user actions are allowed until authentication has completed successful
Protected Authentication Feedback (FIA_UAU.7.1)	IA.9 Passwords are not displayed upon entry.
Identification (FIA_UID.1.1)	IA.1 Solaris makes an allowance for actions to be taken on behalf of the user prior to identification.
Identification (FIA_UID.1.2)	IA.1 Solaris requires each user be successfully identified before allowing any other actions on the behalf of that user.
Identification (FIA_UID.2)	IA.1 Solaris requires each user be successfully identified before allowing any other actions on the behalf of that user.
User-Subject Binding (FIA_USB.1.1)	IA.2 Audit ID data assigned to a user upon entry does not change as the user switches user ID’s and roles.
Management of Object Security Attributes (FMT_MSA.1.1)	DAC.1, DAC.2 Discretionary Access Control rules ensure restricted ability to modify the access control attributes associated with a named object.
Static Attribute Initialization (FMT_MSA.3.1)	DAC.7 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.
Static Attribute Initialization (FMT_MSA.3.2)	DAC.7 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.
Management of the Audit Trail (FMT_MTD.1.1)	Audit.14 Access to audit trail is limited to the administrator and therefore protected from unauthorized observation or modification.
Management of Audited Events (FMT_MTD.1.1)	Audit.16, 17, 18 Only the administrative user may initialize or change auditable events.

Table 5: SFR - IT SF Mapping

Security Functional Requirement	TOE Security Function(s) Rational to support the SFR
Management of User Attributes (FMT_MTD.1.1)	IA.11, Admin.1 Only the administrator can initialize user accounts and assign user profiles
Management of Authentication Data (FMT_MTD.1.1)	IA.10 Only the administrator can change user authentication data.
Management of Authentication Data (FMT_MTD.1.1)	IA.11 A user may change their own password.
Management of Authentication Data (FMT_MTD.3)	ENF.4 The TSF ensures that only secure values are accepted for user passwords
Specification of Management Functions (FMT_SMF.1.1)	IA.1, IA.11, DAC.1, DAC.8 TSF allows for the administrator to manage the system security attributes
Revocation of User Attributes (FMT_REV.1.1)	IA.11, DAC.1, DAC.2, Admin.1 Only the administrator can remove or delete user accounts
Revocation of Object Attributes (FMT_REV.1.2)	IA.11 Once a user has been removed from the system there is no way to authenticate.
Revocation of Object Attributes (FMT_REV.1.2)	DAC.6 Solaris file permissions ensure that only authorized users are able to revoke object attributes.
Security Management Roles (FMT_SMR.1.1)	DAC.1, DAC.2, IA.11, Admin.1 Solaris assigns a unique id to each user which enables the assignment of management roles. Only the administrator can assign roles to a user.
Security Management Roles (FMT_SMR.1.2)	DAC.2, DAC.8, IA.11, Audit.14, 16, 17, 18, 19, 22, 23, Admin.1 Solaris supports this requirement through the use of uid assignment and audit tracking
Restriction on Security Roles (FMT_SMR.2.1)	Admin.1, Admin.4, Admin.5 The TSF shall maintain the list of roles.
Restriction on Security Roles (FMT_SMR.2.2)	Admin.1, Admin.4, Admin.5 The TSF shall be able to associate users with roles.
Restriction on Security Roles (FMT_SMR.2.3)	Admin.4, Admin.5 Defined ability of users and administrators to modify security attributes and objects.
Abstract Machine Testing (FPT_AMT.1.1)	ENF.3 SUN provides a suite of Abstract machine tests for TOE users
Failure with Preservation of Secure State (FPT_FLS.1)	Fail.2 The TSF maintains the ability to preserve RBAC database information when the system experiences a failure

Table 5: SFR - IT SF Mapping

Security Functional Requirement	TOE Security Function(s) Rational to support the SFR
Manual Recovery (FPT_RCV.1)	Fail.1 The TSF will enter maintenance mode following a system failure, allowing the administrator to bring the system to a secure state before resuming operation.
Functional Recovery (FPT_RCV.4)	Fail.2 The TSF maintains the ability to preserve RBAC database information when the system experiences a failure
Reference Mediation (FPT_RVM.1.1)	ENF.1 Solaris validates all actions between subjects and objects before allowing the action to succeed
Domain Separation (FPT_SEP.1.1)	ENF.2 Solaris maintains a secure domain within the system kernel for trusted execution and the storage of trusted objects. This are is separate from untrusted activities within the TOE.
Domain Separation (FPT_SEP.1.2)	ENF.2 Solaris maintains a secure domain within the system kernel for trusted execution and the storage of trusted objects. This are is separate from untrusted activities within the TOE
Reliable Time Stamps (FPT_STM.1.1)	Audit.12 Solaris provides a reliable time stamp through it's audit mechanism.
TSF Self Test (FPT_TST.1)	ENF.3 The TOE shall allow an administrator to perform a self test to ensure that the underlying TSF is enforcing process separation

[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] Supplying a new password is stated in ITSF IA.11, 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.

7.4.2 Justification for Compliance of Assurance Measures

Section 6.3 shows that all assurance requirements are met by an appropriate assurance measure.

The Security Functional Requirements outlined in section 7.4.1 are all met within the design of the Solaris Operating Environment. Tests have been developed and will be conducted which confirm that all of the TOE security functional requirements are met.

7.5 PP Claims and Rationale

7.5.1 PP Reference

The TOE meets all of the requirements of the Controlled Access Protection Profile, which is defined in [CAPP] and the Role Based Access Control Protection Profile which is defined in [RBAC].

7.5.2 PP Tailoring

The security functional requirements for the TOE are as defined in [CAPP] and [RBAC] with refinements as necessary and appropriate for a Security Target. These refinements are detailed in section 5.1.1.

7.5.3 PP Additions

There are no additional security functional requirements for the TOE beyond that defined in [CAPP] and [RBAC]. There is one additional security requirement for the IT environment which is detailed in section 5.4. This relates to the requirements placed on the SC or OpenBoot PROM in support of protecting the server/workstation in the environment.

There are no additional TOE security objectives to those contained in [CAPP] and [RBAC]. The security objectives for the TOE environment in this security target may be regarded as additional to those contained in [CAPP] and [RBAC], although they are deemed to be broadly equivalent, and refined due to the specific environment assumed for the Solaris 9 product.

7.5.4 PP Rationale

The objectives used in this Security Target are derived from [CAPP] 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 [CAPP] 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 [CAPP] and [RBAC] also. Because of the similarities between the objectives and SFRs contained in this Security Target and in [CAPP] and [RBAC], the justification provided in [CAPP] and [RBAC] is also appropriate for this Security Target.

Appendix A

A 1.1Platform 1 Configurations

Platform Specification	**Server E3500**	**Server E4500**	**Server E5500**	**Server E6500**	**Server E10K**	**Server E450**	**Server E420R**	**Server E250**	**Server E220R**
Operating Environment	Solaris 9 Operating Environment								
CPUs	1-8	1-14	1-14	1-30	4-64	1-4	1-4	1-2	1-2
Processor	UltraSPARC II					UltraSPARC II with onboard e-cache			
Clock speeds	167; 250, 336, 400, 464, 500 or 650 MHz					250, 300, 400, 450 or 480 Mhz			
I/O Slots (SBus/PCI)	2 SBus	3 SBus	3 SBus	2 SBus 2 PCI	4 SBus 6 PCI	10 PCI	4 PCI	4 PCI	4 PCI
Maximum Memory	2 GB	2 GB	2 GB	56 GB	64 GB	4 GB	4 GB	2 GB	2 GB
Max Storage	n/a	144 GB	144 GB	72.8 GB	2 TB	730 GB	72.8 GB	216 GB	72.8 GB

Platform Specification	**Ultrasparc 30**	**Ultrasparc 60**	**Ultrasparc 80**	**Ultrasparc 450**	**Sunblade 100**
Operating Environment	Solaris 9 Operating Environment				
CPUs	1	1-2	1-4	1-4	1
Processor	UltraSPARC-II				
Clock speeds	250, 300, 450 or 500 MHz				
I/O Slots (SBus/PCI)	4 PCI	4 PCI	4 PCI	10 PCI	2 PCI
Maximum Memory	2 GB	2 GB	4 GB	4 GB	2 GB
Max Storage	18 GB	72 GB	72 GB	730 GB	30GB

Platform Specification	**SunBlade 1000**	**SunBlade 2000**	**Netra 20**	**SunFire V280R**	**SunFire V480**	**SunFire V880**	**SunFire V880z**
Operating Environment	Solaris 9 Operating Environment						
CPUs	1-2	1-2	1-2	1-2	2 or 4	2 - 8	1-6
Processor	UltraSPARC III Cu 8MHz Cache						
Clock speeds	600Mhz, 750Mhz, 900MHz, 1015MHz, 1050MHz & 1200MHz						
I/O Slots (SBus/PCI)	4 PCI	4 PCI	4 PCI	4 PCI	6 PCI	9 PCI	9 PCI
Maximum Memory	8 GB	8 GB	8 GB	8 GB	32 GB	64 GB	48 GB
Max Storage	146 Gb	146 GB	146 GB	146 GB	3 TB	3 TB	73 TB

Platform Specification	**SunFire V210**	**SunFire V240**	**SunFire V250**
Operating Environment	Solaris 9 Operating Environment		
CPUs	1-2	1-2	1-2
Processor	UltraSPARC IIIi 8MHz Cache		
Clock speeds	900MHz, 1015MHz, 1050MHz & 1200MHz		
I/O Slots (SBus/PCI)	1 PCI	3 PCI	6 PCI
Maximum Memory	4 GB	8 GB	8 GB
Max Storage	146 GB	292 GB	292 GB

Platform Specification	**Sun Blade 150**	**Sun Fire V100**	**Sun Fire V120**	**Netra 120**	**Netra CT410**	**Netra CT810**	**Ultra Sparc 5**	**Ultra Sparc 10**
Operating Environment	Solaris 9 Operating Environment							
CPUs	1 (single processor only)							
Processor	UltraSparc IIi 512Kb L2 on-die cache							
Clock speeds	270, 300, 333, 360, 440, 550, or 650 Mhz							
I/O Slots (SBus/PCI)	3 PCI	0	1 PCI	1 PCI	2 PCI	6 PCI	3 PCI	4 PCI
Maximum Memory	2 GB	2 GB	4 GB	4 GB	4 GB	4 GB	512 Mb	1 GB
Max Storage	40 GB	80 GB	108 GB	72 GB	72 GB	144 GB	20 Gb	40 GB

A 1.2Platform 2 Configurations

Platform Specification	**Netra 1280**	**Sun Fire V1280**	**Sun Fire 3800**	**Sun Fire 4800**	**Sun Fire 4810**	**Sun Fire 6800**	**Sun Fire 12K**	**Sun Fire 15K**
Operating Environment	Solaris 9 Operating Environment							
CPUs	4-12	4-12	2-8	2-12		2-24	4-52	16-106
Processor	UltraSPARC III Cu							
Clock speeds	900 Mhz		900MHz, 1050MHz & 1200MHz					
System Board (CPU) Slots	N/A	N/A	2	3		6	9	18
I/O Slots (SBus/PCI)	6 PCI	6 PCI	12 cPCI	16 PCI or 8 cPCI		32 PCI or 16 cPCI	36 PCI	72 PCI
I/O Channel Bandwidth	24 GB per second per PCI/cPCI assembly							
Maximum Memory per domain	96GB	96GB	64 GB	96 GB		192 GB	288 GB	576 GB
Max Storage (all SunFire data center servers support external storage)	17.5 TB	17.5 TB	35 TB			77 TB	120 TB	250 TB
Sustained System Bandwidth	9.6 GB/sec						21.6 GB/sec	43.2 GB/sec

This Page Intentionally Left Blank