



**UK IT SECURITY EVALUATION AND
CERTIFICATION SCHEME**



122-B

COMMON CRITERIA CERTIFICATION REPORT No. P170

Sun Microsystems, Inc.

Trusted Solaris™

Version 8 4/01

Issue 3.0

March 2004

© Crown Copyright 2004

Reproduction is authorised provided the report
is copied in its entirety

UK IT Security Evaluation and Certification Scheme, Certification Body,
CESG, Hubble Road, Cheltenham GL51 0EX
United Kingdom

**ARRANGEMENT ON THE
MUTUAL RECOGNITION OF COMMON CRITERIA CERTIFICATES
IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY**

The Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements contained in the certificate and Certification Report are those of the Qualified Certification Body which issued it and of the Evaluation Facility which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party. *

* Whilst the Arrangement has not yet been extended to address ALC_FLR.3 (systematic flaw remediation), a working agreement exists amongst Parties to the Arrangement to recognize the Common Evaluation Methodology ALC_FLR supplement (Reference [v] in this report) and the resultant inclusion of ALC_FLR.3 elements in certificates issued by a Qualified Certification Body.

Trademarks:

The following trademarks are acknowledged:

Sun, Sun Microsystems, Solaris and NFS are trademarks or registered trademarks of Sun Microsystems, Inc.

All SPARC trademarks are trademarks or registered trademarks of SPARC International, Inc.

UNIX is a registered trademark of The Open Group.

Intel and Pentium are registered trademarks of the Intel Corporation.

CERTIFICATION STATEMENT

Trusted Solaris 8 4/01 is a UNIX-based operating system which can be configured from a number of workstations and servers to form a single distributed system. It has been developed to meet the requirements for secure computing, including 'Multi-Level' and 'System High' operation. It has been developed by Sun Microsystems Inc.

Trusted Solaris 8 4/01 has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the Common Criteria Part 3 augmented requirements of Evaluation Assurance Level EAL4, augmented with ALC_FLR.3, for the specified Common Criteria Part 2 extended functionality in the specified environment when running on the specified Sun SPARC and Intel Pentium platforms. It has also met the requirements of the Labeled Security Protection Profile, Controlled Access Protection Profile and Role-Based Access Control Protection Profile.

Certification to the EAL4 Evaluation Assurance Level was previously completed in June 2002. This certification was updated to include the ALC_FLR.1 (basic flaw remediation) augmentation in December 2003, and has now been updated to include the ALC_FLR.3 (systematic flaw remediation) augmentation. Details of the ALC_FLR.3 certification update are given by Annex C (other points within the report are those made at the time of the original EAL4 certification).

Originator	J C Longley Certifier
Approval and Authorisation	P. Fischer Head of the Certification Body UK IT Security Evaluation and Certification Scheme.
Date authorised	30 March 2004

(This page is intentionally left blank)

TABLE OF CONTENTS

CERTIFICATION STATEMENT	iii
TABLE OF CONTENTS	v
ABBREVIATIONS	vii
REFERENCES	ix
I. EXECUTIVE SUMMARY	1
Introduction.....	1
Evaluated Product.....	1
TOE Scope	2
Protection Profile Conformance	3
Assurance Requirement	4
Strength of Function Claims	4
Security Policy.....	5
Security Claims.....	5
Evaluation Conduct.....	6
Certification Result.....	6
General Points.....	6
II. EVALUATION FINDINGS	9
Introduction.....	9
Delivery	9
Installation and Guidance Documentation.....	9
Strength of Function	10
Vulnerability Analysis	11
Testing	11
Platform Issues.....	12
Assurance Maintenance Issues	14
III. EVALUATION OUTCOME	15
Certification Result.....	15
Recommendations	15
ANNEX A: EVALUATED CONFIGURATION	17
ANNEX B: PRODUCT SECURITY ARCHITECTURE	21
ANNEX C: FLAW REMEDIATION AUGMENTATION	29

(This page is intentionally left blank)

ABBREVIATIONS

ACL	Access Control List
CAPP	Controlled Access Protection Profile
CC	Common Criteria
CDE	Common Desktop Environment
CEM	Common Evaluation Methodology
CESG	Communications-Electronics Security Group
CLEF	Commercial Evaluation Facility
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ITSEC	Information Technology Security Evaluation Criteria
LSPP	Labeled Security Protection Profile
MAC	Mandatory Access Control
OSP	Organisational Security Policy
RBAC	Role-Based Access Control
RBACPP	Role-Based Access Control Protection Profile
SFR	Security Functional Requirement
SMC	Solaris Management Console
SoF	Strength of Function
TOE	Target of Evaluation
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy
UKSP	United Kingdom Scheme Publication

(This page is intentionally left blank)

REFERENCES

- a. Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 4.0, February 2000.
- b. The Appointment of Commercial Evaluation Facilities,
UK IT Security Evaluation and Certification Scheme,
UKSP 02, Issue 3.0, 3 February 1997.
- c. Trusted Solaris 8 4/01 Security Target,
Sun Microsystems Inc.,
TS8_101, Issue 2.0, June 2002.
- d. Labeled Security Protection Profile,
U.S. National Security Agency,
Version 1.b, 8 October 1999.
- e. Controlled Access Protection Profile,
U.S. National Security Agency,
Version 1.d, 8 October 1999.
- f. Role-Based Access Control Protection Profile,
National Institute of Standards and Testing,
Version 1.0, 30 July 1998.
- g. Common Criteria Part 1,
Common Criteria Interpretations Management Board,
CCIMB-99-031, Version 2.1, August 1999.
- h. Common Criteria Part 2,
Common Criteria Interpretations Management Board,
CCIMB-99-032, Version 2.1, August 1999.
- i. Common Criteria Part 3,
Common Criteria Interpretations Management Board,
CCIMB-99-033, Version 2.1, August 1999.
- j. Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Criteria Evaluation Methodology Editorial Board,
Version 1.0, CEM-099/045, August 1999.

- k. LFL/T143 Evaluation Technical Report 1,
Logica CLEF,
CLEF.24888.30.1, Issue 1.0, 11 September 2001.
- l. LFL/T143 Evaluation Technical Report 2,
Logica CLEF,
CLEF.24888.30.2, Issue 1.0, 5 December 2001.
- m. LFL/T143 Evaluation Technical Report 3,
Logica CLEF,
CLEF.24888.30.3, Issue 1.0, 14 March 2002.
- n. Trusted Solaris 8 4/01 Release Notes,
Sun Microsystems Inc.,
Part Number 816-1043-10, November 2001.
- o. Trusted Solaris 8 4/01 AnswerBook CD,
Sun Microsystems Inc.,
CD Part Number 704-7949-10, Revision A, November 2001.
- p. Trusted Solaris Reference Manuals (volumes 1 to 4),
Sun Microsystems Inc.,
Part Number 816-1052-10, November 2001.
- q. Certification Report No. P101, Sun Solaris 2.6SE,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, January 1999.
- r. Certification Report No. P104, Trusted Solaris 2.5.1,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, October 1998.
- s. Common Criteria Certification Report No. P148, Sun Solaris Version 8 with AdminSuite
Version 3.0.1,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, November 2000.
- t. Common Criteria Certification Report No. P170, Sun Microsystems, Inc., Trusted Solaris
Version 8 4/01,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, June 2002.
- u. Trusted Solaris 8 4/01 Security Target,
Sun Microsystems Inc.,
TS8_101, Issue 3.1, 12 November 2003.

- v. Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology, Supplement: ALC_FLR – Flaw Remediation,
Common Criteria Evaluation Methodology Editorial Board,
CEM-2001/0015R, Version 1.1, February 2002.
- w. LFL/T154 Evaluation Technical Report 2,
LogicaCMG CLEF,
309.EC200582:30.2.2, Issue 1.0, 11 December 2003.
- x. Common Criteria Certification Report No. P170, Sun Microsystems, Inc., Trusted Solaris
Version 8 4/01,
UK IT Security Evaluation and Certification Scheme,
Issue 2.0, December 2003.

(This page is intentionally left blank)

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria evaluation of Trusted Solaris 8 4/01, to the Sponsor, Sun Microsystems Inc., and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

2. Prospective consumers are advised to read this report in conjunction with the Security Target [Reference c] which specifies the functional, environmental and assurance evaluation requirements.

Evaluated Product

3. The version of the product evaluated was:

Trusted Solaris 8 4/01

This product is also described in this report as the Target of Evaluation (TOE). The Developer was Sun Microsystems Inc.

4. Trusted Solaris 8 4/01 is a highly-configurable, UNIX-based operating system which has been developed to meet:

- a. 'Multi-Level' operation through Mandatory Access Control (MAC) functionality, including the use of sensitivity labels; and
- b. 'System High' operation through Discretionary Access Control (DAC) functionality, including the use of Access Control Lists (ACLs).

It meets the requirements of the Common Criteria (CC) Labeled Security Protection Profile (LSPP) [d] and Controlled Access Protection Profile (CAPP) [e], which are respectively equivalent to those of the B1 and C2 classes of the Trusted Computer System Evaluation Criteria.

5. The Security Target [c] also draws attention to configuration options for:

- a. Multi-Level operation with display of sensitivity labels either enabled or disabled (on a per-user basis).
- b. Single-Level operation. This involves use of one level only of sensitivity label, and is effectively equivalent to System High operation.

6. A set of administrative roles can be established to provide the basis for security management. In this respect Trusted Solaris 8 4/01 also meets the requirements of the Role-Based Access Control Protection Profile (RBACPP) [f].

7. A Trusted Solaris 8 4/01 system consists of a number of workstations and servers linked together to form a single distributed system. Users share the resources of multiple workstations and servers in a single, distributed trusted computing base.
8. Further identification of the evaluated TOE follows below under 'TOE Scope'.
9. Specification of the evaluated configuration, including the TOE's supporting guidance documentation and the SPARC and Pentium platforms on which it was evaluated, is given in Annex A.
10. An overview of the TOE's security architecture can be found in Annex B.

TOE Scope

11. The evaluated build of Trusted Solaris 8 4/01 is identified by the operating system CD part numbers specified in Annex A.
12. The Trusted Solaris 8 4/01 operating system is supplied with the Solaris Management Console (SMC), which uses the mechanisms of the Common Desktop Environment (CDE) to provide a range of GUI-based administration tools. The TOE was thus evaluated with SMC and CDE Version 1.4 installed.
13. Both networked and standalone authentication and file access were addressed.
14. The various filesystem types listed in section 2.3.2 of the Security Target [c] were addressed by the evaluation.
15. Only 64-bit mode operation was evaluated for SPARC-based machines, and only 32-bit mode operation of applications for Pentium machines.
16. The evaluated configuration addressed IPv6.
17. None of the following were evaluated:
 - a. the impact of configuring Trusted Solaris 8 4/01 without installing or using SMC (ie using the user command interface for administration);
 - b. the impact of not installing or not using CDE (eg using a more basic installation option, or using the alternative Open Windows environment);
 - c. use of diskless workstations;
 - d. use of NIS (as distinct from NIS+);
 - e. remote networked booting;
 - f. unbundled products used to perform network backup services;

- g. Web Based Enterprise Management Services;
 - h. Dynamic Host Configuration Protocol support;
 - i. support for non-default authentication options (eg using smartcards); and
 - j. interoperability with TrustedSolaris 2.5.1 or Solaris 8.
18. The TOE was evaluated on hardware platforms of the following types specified in Annex A:
- a. single and dual-processor Sun SPARC platforms using Ultra-II, Ultra-IIe and Ultra III processors; and
 - b. single processor PCs using the Intel Pentium III processors.
19. Significant exclusions from the set of evaluated platform ranges were as follows:
- a. Sun SPARC platforms using processors other than UltraSPARCs;
 - b. the Remote Service Control component (available on some SPARC platforms);
 - c. multi-domain operation (available on some SPARC platforms); and
 - d. multi-processor Intel Pentium platforms.
20. For the Sun SPARC platforms, the security of the Version 4.2.4 OpenBoot PROM firmware was evaluated. However, the range of PC BIOS firmware available for use with Pentium processors was not evaluated.
21. A fuller discussion of the consideration given to hardware and firmware platforms is given below under 'Platform Issues'.

Protection Profile Conformance

22. The Security Target [c] claimed conformance to LSPP [d], CAPP [e] and RBACPP [f].
23. The Security Target contains no TOE or environmental security objectives additional to those of LSPP [d] and RBACPP [f]. However the environmental security objectives equivalent to those of LSPP are significantly refined for the environment assumed for Trusted Solaris 8 4/01.
24. Section 5 of the Security Target identifies those TOE Security Functional Requirements (SFRs) additional to one or both of LSPP [d] and RBACPP [f]. An additional IT environment SFR is specified, relating to use of the OpenBoot PROM.

25. The TOE assurance requirement of Evaluation Assurance Level 4 (EAL4) exceeded, and was more than necessary to conform to, the EAL3 and EAL2 augmented requirements of LSPP [d] and RBACPP [f] respectively.

26. It is noted that CAPP [e] is a subset of LSPP [d].

Assurance Requirement

27. The Security Target [c] specified the assurance requirement for the evaluation. Predefined Evaluation Assurance Level EAL4 was used. CC Part 3 [i] describes the scale of assurance given by predefined levels EAL1 to EAL7 (where EAL0 represents no assurance). An overview of CC is given in CC Part 1 [g].

Strength of Function Claims

28. The minimum Strength of Function (SoF) was SoF-medium. This was claimed in respect of the password authentication function, used on attempting to gain access to the system at the following times:

- a. initially;
- b. after a user-initiated 'lockscreen';
- c. after an inactivity period 'lockscreen'; and
- d. on attempting to change a password to a new one.

29. Two specific metrics were also claimed for this function:

- a. for each attempt to use the mechanism, the probability that a random attempt will succeed is less than one in 1,000,000; and
- b. for multiple attempts to use the mechanism during a one minute period, the probability that a random attempt will succeed is less than one in 100,000.

30. Trusted Solaris 8 4/01 passwords may either be specified directly by the user, or assigned by the administrator with the use, at the SMC, of the product's random, pronounceable password generator. In each case the above claims relate to the password space. However the claims do not involve the random number generator incorporated in the password generator, as it is the policy of the national authority for cryptographic mechanisms, the Communications-Electronics Security Group (CESG), for no claim to be made on the appropriateness or strength of random number generators.

31. The SoF claims did not extend to the hashing algorithm used to encrypt stored passwords, as the stored passwords are also protected by the access control mechanisms and the Security Target [c] assumes that TOE administrators are competent and trustworthy.

32. The OpenBoot PROM for SPARC platforms was considered only as a platform issue, and as such the SoF claims did not extend to its password authentication mechanism.

Security Policy

33. The primary access control policies for the TOE are those of MAC and DAC. The TOE accordingly meets the Organisational Security Policies (OSPs) P.CLASSIFICATION and P.DAC specified by the Security Target.

34. The basic MAC and DAC rules may be overridden by authorizations associated with administrative roles, and the RBAC policy extends to the effect of these authorisations. The RBAC policy is evident from the detail of the security claims.

Security Claims

35. The Security Target [c] specifies the TOE's security objectives, the threats which these objectives counter and the SFRs and security functions which elaborate the objectives. All are fully specified in the Security Target, with the exception of LSPP [d], CAPP [e] and RBACPP [f] SFRs which require no tailoring for Trusted Solaris 8 4/01, where the Security Target merely references the relevant Protection Profile for their full specification. The Security Target also specifies OSPs which are met by the objectives.

36. The Security Target [c] specifies a 'non-hostile' threat environment, with focus thus given to 'inadvertent or casual attempts to breach the system security'.

37. Most of the SFRs are taken from CC Part 2 [h]; use of this standard facilitates comparison with other evaluated products. All extended SFRs, i.e. those not taken directly from CC Part 2, are inherited from LSPP [d] and CAPP [e] as identified in Section 8 of each Protection Profile.

38. Claims are primarily made for security functionality in the following areas:

- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Object Re-use
- Identification and Authentication
- Trusted Path
- Privileges and Authorizations
- Roles and Profiles
- Auditing

Evaluation Conduct

39. The evaluation was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in United Kingdom Scheme Publication 01 (UKSP 01) and UKSP 02 [a, b]. The Scheme has established a Certification Body which is managed by CESG on behalf of Her Majesty's Government. As stated on page ii of this Certification Report, the Certification Body is a member of the Common Criteria Recognition Arrangement, and the evaluation was conducted in accordance with the terms of this Arrangement.

40. The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [c], which prospective consumers are advised to read. To ensure that the Security Target gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3 [i] and the Common Evaluation Methodology (CEM) [j].

41. Much of the Trusted Solaris 8 4/01 functionality and supporting evaluation deliverables content remained unchanged from that of Trusted Solaris 2.5.1 and Solaris 8, which had previously been certified by the IT Security Evaluation and Certification Scheme to the ITSEC E3 and CC EAL4 assurance levels respectively, as reported in their Certification Reports [r, s]. The Evaluators thus drew extensively on the results of the two previous evaluations but revalidated these results for Trusted Solaris 8 4/01 for the various CEM [j] EAL4 work units.

42. The Certification Body monitored the evaluation which was carried out by the Logica Commercial Evaluation Facility (CLEF). The evaluation was completed when the CLEF submitted the final Evaluation Technical Report (ETR) [m] to the Certification Body in March 2002. Following a request for clarification of technical issues relating to the evaluation results and the TOE, the Certification Body produced Issue 1.0 of this Certification Report [t].

Certification Result

43. For the certification result see the 'Evaluation Outcome' section.

General Points

44. The evaluation addressed security functionality claimed in the Security Target [c] with reference to the assumed operating environment specified by the Security Target. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and to give due consideration to the recommendations and caveats of this report.

45. Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with greater assurance) that exploitable vulnerabilities may be discovered after a certificate has been awarded. This Certification Report reflects the Certification Body's view at the time of the original EAL4 certification. Consumers (both prospective and existing) should check regularly for themselves whether any security

vulnerabilities have been discovered since Issue 1.0 of this report [t] was issued and, if appropriate, should check with the Vendor to see if any patches exist for the product and what assurance exists for such patches.

46. The issue of a Certification Report is not an endorsement of a product.

(This page is intentionally left blank)

II. EVALUATION FINDINGS

Introduction

47. The evaluation addressed the requirements specified in the Security Target [c]. The results of this work were reported in the ETRs [k, l, m] under the CC Part 3 [i] headings. The following sections note considerations that are of particular relevance to consumers.

Delivery

48. On receipt of the TOE, the consumer is recommended to check that the evaluated versions of its constituent components have been supplied, and to check that the security of the TOE has not been compromised in delivery.

49. All TOE software and documentation components identified in Annex A are all available on CD, and this is the recommended delivery method. A number of components are additionally available from Sun web sites; considerations governing the security of web-based delivery are as given by the Solaris 8 Certification Report [s].

50. The following measures provide security for CD delivery:

- a. CDs are read-only;
- b. CDs are supplied shrink-wrapped in a box sealed with tamper-evident tape;
- c. CDs carry the Sun logo and Solaris trademark; and
- d. the packing slip accompanying the CDs can be compared with the separately supplied invoice.

Installation and Guidance Documentation

51. The Release Notes [n] identify and discuss all security considerations relevant to users and administrators in a comprehensive but concise manner, and it is thus recommended that these be consulted first on all questions relating to the secure installation, configuration, startup and operation of the TOE. The Release Notes reference other product documentation where appropriate.

52. Further product documentation, held on the Trusted Solaris 8 4/01 AnswerBook CD [o], is accessed on-line, after installation on a Solaris system. This documentation comprises the following items:

- a. Trusted Solaris 8 4/01 Roadmap;
- b. Trusted Solaris 8 4/01 Installation and Configuration Guide;
- c. Trusted Solaris 8 4/01 Administration Overview;
- d. Trusted Solaris 8 4/01 Administrator's Procedures;

- e. Trusted Solaris 8 4/01 Audit Administration;
- f. Trusted Solaris Label Administration;
- g. Trusted Solaris User Guide; and
- h. Compartmented Mode Workstation Labeling: Encodings Format.

53. The Trusted Solaris 8 4/01 AnswerBook CD [o] also contains the following items:

- a. Trusted Solaris 8 4/01 Transition Guide.

This outlines the differences between Solaris 8 4/01, SMC 2.0 and their use in Trusted Solaris 8 4/01.

- b. Trusted Solaris Developer's Guide.

This describes how to develop applications for Trusted Solaris 8 4/01. Whilst it adds to the reader's understanding of the product's interfaces, the environmental objective that only system administrators should be allowed to introduce new software into the system and the potential risk which might be introduced by a poorly engineered application should be noted.

54. In addition the Trusted Solaris References Manuals [p] (volumes 1 to 4¹) provide the man pages which describe all user commands and interfaces. These are supplied on the operating system CDs.

55. A further form of guidance material is given by the SMC on-line help.

Strength of Function

56. SoF claims for the password authentication mechanism were as given above under 'Strength of Function Claims'. Confirmation of these claims was based on an analysis of password space, which was in turn based on the following considerations:

- a. For user supplied passwords:
 - i. the constraint imposed by the TOE in forcing users to select passwords including at least two alphabetic characters and one numeric or special character within the first 6 characters; and
 - ii. the recommendation that users should choose non-obvious passwords of at least 8 characters.
- b. For passwords assigned by the administrator with use of the random pronounceable password generator: the constraint imposed by the TOE that passwords will contain at least two and at most five vowels and that system dictionary words will not be chosen.

¹ Volumes 5 to 9 were not evaluated; volumes 1 to 4 are used most frequently and were found to contain sufficient information for the evaluated security functionality.

- c. The environmental objective that only system administrators should be allowed to introduce new software into the system, and the further recommendation that they restrict the use of compilers to a set of authorised users, in order to minimise the risk of automated guessing attacks.

57. Whilst the strength of the random number generator incorporated within the password generator was not specifically assessed, the evaluators noticed no obvious weakness from the evidence of the sequence of passwords generated when testing the TOE.

Vulnerability Analysis

58. The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process.

59. The Evaluators noted the environmental objective that only system administrators should be allowed to introduce new software into the system, and further recommended that they restrict the use of compilers to a set of authorised users, in order to minimise the risk of trojan horse attacks.

Testing

60. The TOE was tested using the TOE Security Functions Interface (TSFI) provided by the Trusted Solaris 8 4/01 operating system calls and the SMC functions, documented by the supporting guidance material.

61. The Developer performed tests using the full TSFI. The Developer's testing also exercised:

- a. all security functions specified in the Security Target [c], including those which have no direct interface and thus have to be exercised indirectly; and
- b. all high level design subsystems identified in Annex B.

62. The Developer's testing was performed using both an automated test suite and additional manual tests:

- a. The automated test suite exercised the TSFI. It included some tests prompting for manual input which needed to be made before return of control to the test suite. The test suite recorded the test results.
- b. Additional manual tests ensured that all aspects of the security functions specified in the Security Target [c] were exercised.

63. The Evaluators performed the following independent testing:

- a. A test for each security function specified in the Security Target [c], different from those performed by the Developer, was devised wherever possible. Independent tests were thus performed for a large proportion of security functions.

- b. A sample of the Developer's tests was repeated to validate the Developer's testing. The sample included a representative range of tests, including tests relating to the security functions for which no additional tests could be devised. 47% of the Developer's tests were repeated, including both automated and manual tests.
- 64. The Evaluators also devised and performed penetration tests, wherever needed, to confirm the non-exploitability of potential vulnerabilities which had been noted in the course of the evaluation.
- 65. Testing, in support of the SoF analysis, to confirm that the rate at which repeated non-automated password guesses could be made was not unacceptably high, had been performed in the Solaris 8 evaluation [s]. The evaluators did not repeat this testing, having determined by analysis that the results remained valid for Trusted Solaris 8 4/01.
- 66. Remote authentication was tested using NIS+. Local authentication was tested with account data held locally in *passwd/shadow* files.
- 67. Multi-Level operation was tested for options to both enable and disable the display of sensitivity labels.
- 68. All filesystem types listed in section 2.3.2 of the Security Target [c] were exercised in the course of testing, internal filesystem types being exercised indirectly.
- 69. Test coverage of the hardware platforms was as outlined below under 'Platform Issues'.

Platform Issues

- 70. Secure operation of the TOE on the hardware platforms specified in Annex A was performed by both analysis and testing.
- 71. The Developer ran their full test suite on four combinations of SunBlade 1000 (NFS server, NIS+ master) and client platform. The SunBlade 1000 was additionally used for testing of standalone operation. These platforms were as specified in Annex A.
- 72. The Evaluators analysed the potential impact of the variations in platform characteristics on the 'Evaluation Outcome' stated below. A sample of the independent and penetration tests was run on each combination of SunBlade 1000 (NFS server and NIS+ master) and client platform, and on the SunBlade 1000 for standalone operation. Each sample included both a representative selection of tests and those which analysis had indicated might be most sensitive to platform variations. The various samples together included all Evaluator tests.
- 73. In addition the Evaluators confirmed their agreement with a Developer rationale that the SunFire 280R platform is equivalent to the SunBlade 1000 platform (for use as NFS server and NIS+ master, or for standalone operation) with respect to the 'Evaluation Outcome' stated below. In particular it was noted that the SunFire 280R and SunBlade 1000 both employ the UltraSPARCIII processor, Version 4.2.4 of the OpenBoot PROM (discussed below) and equivalent memory architectures, hard disk and ROM media drives, and Ethernet interfaces.

74. The following points were noted:
- a. A minimum memory of 256Mb (to support administrator SMC requests on NFS server, NIS+ master workstations) or 128Mb (on client workstations) and a minimum hard disk size of 2Gb are recommended.
 - b. There is a risk that slower processor speeds, memory sizes or hard disk sizes than those tested, for SPARC and Pentium machines respectively, may introduce performance degradation problems. No specific concerns of this nature were evident in the course of the evaluation. It is considered that the most significant risk of this type involves using less than the recommended memory or hard disk size.
 - c. Whilst each SPARC platform used for testing involved either a single or dual processor configuration, the overall testing result gives confidence in the use of either a single or dual processor configuration on any of the specified SPARC machines.
75. Re-use of the previous Solaris 2.6SE evaluation of the OpenBoot PROM for SPARC platforms was made for this evaluation. Version 3.5 was tested for Solaris 2.6SE. Version 4.2.4 is now available for use on the SPARC platforms specified in Annex A, but the Evaluators' analysis confirmed that the differences between versions 3.5 and 4.2.4 were not security relevant.
76. Recommendations for use of the OpenBoot PROM, originally made in the Solaris 2.6SE Certification Report [q], are as follows:
- a. environmental procedures should prevent or detect the removal of the OpenBoot PROM;
 - b. the OpenBoot PROM should be used in either command-secure or fully-secure mode (ie not configured to non-secure mode);
 - c. the PROM password should be a minimum of 5 characters, formed from a combination of alphabetic and/or numeric characters, not incorporating any meaningful words (ie not dictionary or recognisable words); and
 - d. the PROM password should only be known by the system administrator.
77. It was not considered practical to evaluate the range of PC BIOS firmware available for use with Pentium processors. However, the consumer is recommended to follow the environmental objective given by the Security Target [c], which requires consideration of:
- a. the protection which may be obtained through setting and enabling the BIOS boot password on the chosen platform; and
 - b. prevention of booting from a floppy drive, CD device or over a network where this is considered a threat.

Assurance Maintenance Issues

78. Consumers should note that assurance in derivatives of the TOE is maintained under the UK Assurance Maintenance Process. Details of the product releases currently covered by this process are provided on the UK Scheme website.

III. EVALUATION OUTCOME

Certification Result

79. After due consideration of the ETRs [k, l, m], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that Trusted Solaris 8 4/01 meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL4 for the specified Common Criteria Part 2 extended functionality in the specified environment when running on the specified Sun SPARC and Intel Pentium platforms, and that it meets the requirements of the Labeled Security Protection Profile, Controlled Access Protection Profile and Role-Based Access Control Protection Profile.

80. The password authentication mechanism meets the minimum strength of function of SoF-medium and the specific metrics given above under 'Strength of Function Claims'. This result is based on an analysis of password space. No comment is made in respect of the random number generator incorporated in the password generator.

Recommendations

81. Prospective consumers of Trusted Solaris 8 4/01 should understand the specific scope of the certification by reading this report in conjunction with the Security Target [c]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

82. Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above under 'TOE Scope' and 'Evaluation Findings'.

83. The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

84. The above 'Evaluation Findings' include a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

(This page is intentionally left blank)

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1. The TOE consists of :
Trusted Solaris 8 4/01 operating system (including SMC).
2. The Trusted Solaris 8 4/01 operating system is provided on the following CD sets:
 - For SPARC platforms:
 - i. CD, Part No. 704-7947-10, November 2001, Revision A; and
 - ii. CD, Part No. 704-7948-10, November 2001, Revision A.
 - For Pentium platforms:
 - i. CD, Part No. 704-7950-10, November 2001, Revision A; and
 - ii. CD, Part No. 704-7951-10, November 2001, Revision A.
3. The supporting guidance documents evaluated, which cover both platform types, were:
 - a. Trusted Solaris 8 4/01 Release Notes [n],
Part Number 816-1043-10, November 2001;
 - b. The Trusted Solaris 8 4/01 AnswerBook CD [o],
CD, Part No. 704-7949-10, November 2001, Revision A
Which comprises the following components:
 - i. Trusted Solaris 8 4/01 Roadmap,
Part Number 816-1039-10, November 2001;
 - ii. Trusted Solaris 8 4/01 Installation and Configuration Guide,
Part Number 816-1040-10, November 2001;
 - iii. Trusted Solaris 8 4/01 Administration Overview,
Part Number 816-1047-10, November 2001;
 - iv. Trusted Solaris 8 4/01 Administrator's Procedures,
Part Number 816-1048-10, November 2001;

- v. Trusted Solaris 8 4/01 Audit Administration,
Part Number 816-1049-10, November 2001;
 - vi. Trusted Solaris Label Administration,
Part Number 816-1050-10, November 2001;
 - vii. Trusted Solaris User Guide,
Part Number 816-1041-10, November 2001;
 - viii. Compartmented Mode Workstation Labeling: Encodings Format,
Part Number 816-1051-10, November 2001;
 - ix. Trusted Solaris 8 4/01 Transition Guide,
Part Number 816-1044-10, November 2001;
 - x. Trusted Solaris Developer's Guide,
Part Number 816-1042-10, November 2001; and
- c. Trusted Solaris Reference Manuals [p] (volumes 1 to 4), included on the operating system CDs specified above:
- Part Number 816-1052-10, November 2001.

Further discussion of the supporting guidance material is given above under 'Installation and Guidance Documentation'.

TOE Configuration

4. The following configuration was used for testing:
- a. A SunBlade 1000 workstation was configured as NFS server and NIS+ master, and was also used for testing of standalone operation. SunBlade 100, Enterprise 420R, Dell GX1 and Pixel USA workstations were configured as client machines. These platforms are specified below under 'Environmental Configuration'.
 - b. The system default run level of 3 was specified.
 - c. Use of the recommended administrative roles, outlined below in Annex B, was followed.
 - d. CDE Version 1.4 was installed.

Environmental Configuration

5. The hardware platforms used for testing were as follows:

Platform	Processor	Memory	Hard Drive	ROM Drive
SunBlade 1000 Model 2750	UltraSPARC III Dual 750MHz	2Gb	2 x 18.2Gb	DVD-ROM
SunBlade 100	UltraSPARC IIe 500MHz	512Mb	20Gb	DVD-ROM
Enterprise 420R	UltraSPARC II Dual 450MHz	2Gb	2 x 18.2Gb	CD-ROM
Dell GX1	Pentium III 600MHz	128Mb	8Gb	CD-ROM
Pixel USA	Pentium III 667MHz	128Mb	10Gb	CD-ROM

6. The workstations were connected via Ethernet using 10/100BaseT network connections (RJ45 interface).

7. In addition equivalence of a SunFire 280R platform to the SunBlade 1000 platform was determined through analysis, as discussed above under 'Platform Issues'.

8. Boot firmware is relevant to the security of the TOE. For this evaluation the adequacy of Version 4.2.4 of the OpenBoot PROM was confirmed, as discussed above under 'Platform Issues'.

(This page is intentionally left blank)

ANNEX B: PRODUCT SECURITY ARCHITECTURE

1. This annex gives an overview of Trusted Solaris 8 4/01 architectural features relevant to the security of the TOE. Further specification of the scope of evaluation is given in various sections above.

Major Architectural Features

Mandatory Access Control

2. Mandatory Access Control (MAC) is a system-enforced access control mechanism that uses sensitivity labels to enforce security policy. Sensitivity labels are used to represent the security level of users, files and other system objects. Generally MAC associates the programs a user runs with the security level (clearance or label) at which the user chooses to work in a session; it permits access to information, programs, and devices at the same or lower level only; and it prevents users from writing to files at lower levels. MAC is enforced according to a site's security policy and cannot be overridden without special authorization or privileges.

Discretionary Access Control

3. Discretionary Access Control (DAC) is a mechanism for controlling user access to files and directories. It leaves setting protections for files or directories to the owner's discretion. The two forms of DAC are the traditional UNIX permission bits and ACLs.

4. Permission bits let the owner set read, write and execute protection by owner, group and other users. In traditional UNIX systems, the superuser (root) can override DAC protection; for Trusted Solaris 8 4/01 the ability to override DAC is permitted for administrators and authorized users only. ACLs provide a finer granularity of access control, letting owners specify separate permissions for specific individuals and groups.

Object Reuse

5. Object-reuse functionality ensures that memory and other storage objects do not contain data when they are reallocated.

Identification and Authentication

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

Trusted Path

7. The trusted path mechanism provides a means for a user to access actions and commands that interact with the trusted computing base. The visible trusted path symbol acts as a non-bypassable communications path between the user and security-related software.

Privileges and Authorizations

8. There are usually cases for every security policy when a control must be overridden. In conventional UNIX systems, the superuser (root) has the ability to override all security policy. For Trusted Solaris 8 4/01 two separate mechanisms, authorizations and privileges, are used to confer security rights to users and processes. Authorizations apply to users; and the granting of an authorization to a user allows the user to perform an action that would otherwise be prohibited by the Trusted Solaris 8 4/01 security policy. Privileges apply to processes, and a process with an associated privilege can override a specific aspect of the security policy.

Roles and Profiles

9. In contrast to traditional UNIX systems, the superuser (root) is not all-powerful in Trusted Solaris 8 4/01. Rather, the ability to override protections can be broken into discrete capabilities and assigned to administrative roles so that no single user can compromise the system's security. A role is a special user account that gives the user access to certain applications with the authorizations, privileges, and effective User IDs/Group IDs necessary for performing the specific tasks.

10. With Trusted Solaris 8 4/01 users have access only to those applications needed to do their jobs. The administrator provides access by assigning one or more rights profiles to one or more user accounts or to roles. A rights profile is a special package of CDE actions, commands and authorizations.

11. Trusted Solaris 8 4/01 is supplied with a preconfigured Root role. This is required for initial configuration, but its use thereafter is not generally recommended. The following four discrete roles are recommended:

a. System Admin :

For performance of standard UNIX system administration tasks:

- Addition of new users
- Configuration of user templates
- Modification of certain user properties
- Configuration of hosts, networks, routes, and printers
- Making and restoring backups and administering printing (if it is desired to combine the System Admin and System Operator roles)

b. Security Admin:

Responsible for security tasks and decisions:

- Administration of labels
- Modification of security-relevant attributes of users, networks, printers and other devices and hosts
- Configuration of host templates

- Modification of default roles and profiles and addition of new roles, but without granting capabilities beyond those of the Security Admin role itself
- c. Primary Admin:
- For use only when the Security Admin role cannot accomplish a task, eg adding a new role or profile with capabilities that the Security Admin role does not have
- d. System Operator:
- For use in making and restoring backups and administering printing

Auditing

12. Trusted Solaris 8 4/01 provides auditing functionality for capturing user activity and other events on the system, storing this information in the audit trail files, and producing system activity reports to fulfill site security policy. Should a breach of security occur, a site can use the audit records to determine how the breach occurred and which user or users were involved.

Networking and Standalone Options

13. Trusted Solaris 8 4/01 can be used networked or standalone.
14. With networked use, a master-client mode of operation is available for authentication and file access functions, and by implication for other functions such as auditing.
- a. One or more workstations may act as an NIS+ master. In this respect, the workstation acts as a central server holding authentication information which is shared among other workstations. When an individual logs in as a user contained in the NIS+ database, the authenticating workstation is acting as an NIS+ client, obtaining authorisation information from the NIS+ master.
 - b. A workstation may share its file system using NFS. In this respect, the workstation that contains the file system and is sharing it is the file system master, while the other workstations may act as clients by remotely mounting the file system. Shared file systems may contain any type of data, eg application data, user data etc.
15. For standalone use, the NIS+ authentication facility is not available, so all users must have 'local' user accounts, and file systems cannot be shared.

Design Subsystems

16. Trusted Solaris 8 4/01 is decomposed into a number of high level design subsystems. Some overlap between subsystems exists in that many use mechanisms and sub-routines within the kernel, and are thus wholly or partially implemented as system calls or processes which operate in kernel space. Subsystems identified as TSP-enforcing within the scope of the evaluation are as follows.

Kernel

17. The Kernel addresses the following features: MAC, DAC, reference mediation, domain separation, abstract machine testing, processes, auditing, object reuse and privileges. It implements System V IPC objects used for interprocess communication.

Filesystem

18. The Filesystem subsystem addresses the following features: MAC, DAC, auditing and object reuse.

19. It includes different types of objects: regular files, directories, symbolic links, FIFOs, pipes (unnamed), UNIX domain socket rendezvous files, process files, pseudo-terminals, and device special files. Each object has these security attributes: owner and group; permissions; ACL; and sensitivity label. The file system also includes the network file system (NFS) component, which allows file system objects stored on remote machines to be mounted and accessed as if they were stored locally.

20. The file system is implemented in the kernel and is accessed via system calls. Other parts of the TOE, user programs and user commands use these system calls to view and manipulate the file system.

Devices

21. The term 'device' refers to any system entity that is accessed through the file system interfaces naming a device special file. Devices fall into two broad classes: (1) fixed-attribute devices, generally established as part of system installation, which further subdivide into the subclass of universally accessible devices and the subclass of trusted computing base internal devices; and (2) variable-attribute (or allocatable) devices that are normally inaccessible outside the trusted computing base but are made accessible or allocatable to users as appropriate, which further subdivide into devices allocated automatically or only on user request.

22. Since access to all devices is through the file-system interfaces, the Filesystem provides MAC and DAC controls.

Audit

23. The Audit subsystem provides a record of events for the purpose of auditing and accountability. Auditing involves generating audit records when specified events occur. The records accumulate chronologically in an audit trail. Each record contains information identifying the event, when it occurred, who caused it, and other relevant information. An audit record can arise from three places: generated by a user-level application such as login(1); generated by the kernel due to a system call by a user process; or generated due to an asynchronous event such as when a communication packet is rejected for a label mismatch.

I & A

24. The Identification and Authentication subsystem ensures that access to a Trusted Solaris 8 4/01 system is permitted to only users who were granted access by an administrator and who have properly identified and authenticated themselves. A user's initial login is based on the CDE login manager, dtlogin; and the login process runs from the trusted path so no user process can read or write to the screen during login. The authentication data is protected by MAC and DAC; and it is never sent to the audit trail. Users working on remote machines must be properly authenticated before access is granted.

Trusted Networking

25. Trusted Networking allows data to be transmitted between workstations via the network while upholding the security policy. Based on the networking functionality of Solaris 8 4/01, Trusted Networking includes enhancements to enforce MAC, DAC, object reuse and authentication.

26. The objects that provide networking capabilities are known as network endpoints, and there are two types: sockets and Transport Level Interfaces (TLIs). A socket is a network endpoint created by a subject to allow communication with other sockets; two subjects communicate by connecting their sockets to form a bidirectional channel. A TLI is natively streams-based and performs the same operations as a socket but with an interface designed to be compatible with AT&T UNIX.

27. The Remote Procedure Call component allows a subject (the server) to perform operations on behalf of another subject (the client) on a remote workstation. Trusted Solaris 8 4/01 allows services to be registered at different sensitivity labels.

NIS+

28. NIS+ provides a replicated database across an NIS+ domain, which comprises a central NIS+ server that stores and distributes the master database files and a number of NIS+ clients that use the data in the master database. The centralized database allows a user to login at any workstation on the NIS+ domain on which the user's identification and authentication data is stored.

Printing

29. The Printing subsystem extends the underlying Solaris printing services by providing unique job IDs for printer requests, configurable banner/trailer pages that contain the sensitivity label of the object being printed, auditing of certain conditions, maintenance and protection of security-sensitive job information and print data, and limiting of the status information that unauthorized users see. The Printing subsystem is designed to enforce the system's MAC and DAC policies from the time of request to the time of printing a physical page. As a device, a printer can be configured for a restricted sensitivity label range such that only eligible jobs (within the range) can be sent to that printer.

Email

30. The Trusted Solaris 8 4/01 Email subsystem provides TSP-enforcing functionality in the sendmail application. Treating each email message as a file with an associated sensitivity label, sendmail relies on the file system mechanisms to enforce MAC, DAC and auditing policies.

Startup

31. The Startup subsystem has eight predefined run levels. The run level determines what state the system is in and what system services are available to users. System startup controls the run level transition from run level 0 (power down) to the level specified from the BootPROM or the system default run level. The component ensures that at startup no window other than the Login window is started; the trusted-path Login is presented for the first user interaction; and no user is allowed to login until a user authorized to enable logins has been authenticated.

Windowing

32. The Windowing subsystem consists of the Trusted X Server, which controls basic window operations and user input; the Selection Manager, which monitors the movement of data between windows; and the Trusted Window Manager, which manages the labeling of workspaces, windows and other graphical objects, the trusted path, and the 'lockscreen'. The subsystem also enforces MAC, DAC and auditing policies.

Admin Tools

33. Trusted Solaris 8 4/01 provides a variety of tools for administering and managing the system and its users. The SMC provides GUI-based tools for managing the system through various configuration databases. The Application Manager provides actions for editing other databases, such as the system defaults (vfstab) and label definitions (label_encodings), with a special version of the 'vi' editor. Administrators can also use other tools, such as the File Manager to set privileges and labels on executable files or the Device Allocation Manager to make device-administration capabilities available to roles. Finally, through rights profiles assigned to administrative roles, administrators have access to commands intended for restricted use.

Trusted Shells

34. Trusted Solaris 8 4/01 provides two special shells for interaction via a command line:
- a. The profile shell is a Bourne, Korn, or C shell that has been modified to grant roles and users access to those programs assigned to their rights profiles and to make security attributes available to commands. From a profile shell, a user can execute those commands and only those commands assigned to that user's profiles. All roles have a profile shell as their login shell. Profile shells do not execute commands for roles unless the commands are issued within the trusted path. Users may or may not be assigned a profile shell, either as a login shell or as a shell made available in a rights profile. An audit record is generated for each command executed in the profile shell.

- b. The system shell, which can only be run from the trusted path, enables commands in run control scripts to execute with privilege. For every command in the run control script, the system shell consults a rights profile for security attributes. If no specific profile is listed for the command, the shell consults the boot rights profile. Local to each computer, the boot and 'inetd' rights profiles specify commands that require security attributes during booting.

Hardware and Firmware Dependencies

35. The TOE uses standard hardware features to implement its Memory Management and Processor States features.
36. A secure startup capability is required to ensure that the correct operating system is loaded and executed as discussed above under 'Platform Issues'.

(This page is intentionally left blank)

ANNEX C: FLAW REMEDIATION AUGMENTATION

Introduction

1. This annex gives an overview of the ALC_FLR evaluation that was performed concurrently with Assurance Maintenance Audit No 2 in December 2003.

Assurance Requirement

2. The assurance requirement for the TOE, as defined in the updated Security Target [u], was EAL4 augmented with ALC_FLR.3 (systematic flaw remediation).

Evaluation Conduct

3. As part of the UK Assurance Maintenance Process, the ALC_FLR.3 component was evaluated by the LogicaCMG CLEF in accordance with the latest guidance detailed in the CEM Supplement on Flaw Remediation [v]. Following the submission in January 2004 of an ETR [w] that addressed ALC_FLR.3, the Certification Body produced Issue 3.0 of this Certification Report to confirm the Flaw Remediation outcome stated in that ETR. (Issue 2.0 of this Certification Report [x] had previously been produced to cover the earlier ALC_FLR.1 augmentation).

General Points

4. Certification of a Flaw Remediation Process acknowledges that there is no guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with greater assurance) that exploitable vulnerabilities may be discovered after an original certification.

5. Consumers (both prospective and existing) should check regularly for themselves whether any security vulnerabilities have been discovered and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether such patches have been:

- released in accordance with the evaluated flaw remediation procedures,
- incorporated into a later assurance maintained derivative, or
- evaluated and certified.

Flaw Remediation Procedures

6. Sun's flaw remediation process is coordinated by its Security Coordination Team, which receives and assesses bug reports and, where appropriate, issues security alerts and produces, checks and releases patches. Security alerts, patches and supporting information are made available from the www.sunsolve.sun.com website. Where one of Sun's local technical support centres is unable to answer a consumer request through the provision of straightforward security advice it will therefore typically refer the consumer to the Security Coordination Team (which may be contacted at email address security-alert@sun.com) or invite them to visit the sunsolve website.

7. Bug reports may be submitted by either Sun personnel or the consumer. Where the consumer wishes to do this they should contact the Security Coordination Team.
8. Security alerts, which contain information on vulnerabilities, workarounds and patches, are made available to the consumer from the SunSolve website. A process exists, as described on the website, whereby the consumer can subscribe to receive a weekly SunAlert newsletter which notes the latest updates to the alert information.
9. The patches themselves are available from the SunSolve website, which also offers:
 - a) Tools to locate a specific patch and the set of patches relevant to a specific release of Trusted Solaris 8;
 - b) Patch usage instructions; and
 - c) Temporary patches (T-patches) which are issued ahead of fully checked patches for use where a consumer requires a time-critical fix.

Delivery

10. Patches, and associated guidance, must be downloaded from the SunSolve website. Mechanisms which Sun provide to enable the consumer to check secure delivery include:
 - a) Use of digital signatures to check the authenticity of the download (Sun's certificate is authenticated by Baltimore Technologies, and it is possible to check this signature without using Sun's downloadable patch management tool); and
 - b) An MD5 fingerprint database for use in checking the integrity of the download

Certification Result

11. After due consideration of the ETR [w] produced by the Evaluators, and the visibility of the Flaw Remediation Process given to the Certifier, the Certification Body has determined that Trusted Solaris 8 4/01 meets the Common Criteria Part 3 augmented requirements of Evaluation Assurance Level EAL4 augmented with ALC_FLR.3, for the specified Common Criteria Part 2 extended functionality in the specified environment when running on the specified Sun SPARC and Intel Pentium platforms, and that it meets the requirements of the Labeled Security Protection Profile, Controlled Access Protection Profile and Role -Based Access Control Protection Profile.