# UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME


122-B

## COMMON CRITERIA CERTIFICATION REPORT No. P182

**Sun Microsystems, Inc.**

**Solaris** TM

**Version 8 2/02**

Issue 1.0

April 2003



UK IT Security Evaluation and Certification Scheme
Certification Body, PO Box 144
Cheltenham, Glos GL52 5UF
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.

# CERTIFICATION STATEMENT

Solaris 8 2/02 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 by Sun Microsystems Inc.

Solaris 8 2/02 has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met 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 platforms. It has also met the requirements of the Controlled Access Protection Profile.

| | |
|---|---|
| **Originator** | **CESG**<br>Certifier |
| **Approval and Authorisation** | **CESG**<br>Head of the Certification Body<br>UK IT Security Evaluation<br>and Certification Scheme |
| **Date authorised** | 7 April 2003 |

(This page is intentionally left blank)

# TABLE OF CONTENTS

(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 |
| FCS | First Customer Shipment |
| OSP | Organisational Security Policy |
| SFR | Security Functional Requirement |
| SoF | Strength of Function |
| TOE | Target of Evaluation |
| TSF | TOE Security Functions |
| TSFI | TOE Security Functions Interface |
| 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 5.0, July 2002.

b. The Appointment of Commercial Evaluation Facilities,
UK IT Security Evaluation and Certification Scheme,
UKSP 02, Issue 3.0, 3 February 1997.

c. Solaris 8 2/02 Security Target,
Sun Microsystems Inc.,
S8.0 2/02, Version 1.0, 19 March 2002

d. Controlled Access Protection Profile,
U.S. National Security Agency,
Version 1.d, 8 October 1999.

e. Common Criteria Part 1,
Common Criteria Interpretations Management Board,
CCIMB-99-031, Version 2.1, August 1999.

f. Common Criteria Part 2,
Common Criteria Interpretations Management Board,
CCIMB-99-032, Version 2.1, August 1999.

g. Common Criteria Part 3,
Common Criteria Interpretations Management Board,
CCIMB-99-033, Version 2.1, August 1999.

h. 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.

i. LFL/T152 Evaluation Technical Report,
Logica CLEF,
336.EC25669:30.1, Issue 1.0, 29 July 2002.

j. LFL/T152 Evaluation Technical Report 2,
Logica CLEF,
CLEF.25569.30.2, Issue 1.1, 10 February 2003.

k. LFL/T152 Evaluation Technical Report 3,
Logica CLEF,
CLEF.25569.30.3, Issue 1.1, 21 February 2003.

l. Solaris 8 2/02 Security Release Notes,
Sun Microsystems Inc.,
Issue 0.2, 22 November 2002.

m. Solaris 8 2/02 Documentation CD,
Sun Microsystems Inc.,
Part No. 705-0075-10, Revision A, March 2002.

n. 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.

o. Solaris 8 Security Target,
Sun Microsystems Inc.,
S8.0_101/ts2_101, Issue 1.0, 28 July 2000.

# I. EXECUTIVE SUMMARY

## Introduction

1. This Certification Report states the outcome of the Common Criteria evaluation of Sun Solaris 8 2/02 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 Products

3. The versions of the products evaluated were:

- Solaris 8 2/02 (also known as Solaris 8 Update 7)

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

4. Solaris 8 2/02 is a highly-configurable UNIX-based operating system which has been developed to meet 'System High'[1] operation including the use of Access Control Lists (ACLs). It meets the requirements of the Common Criteria (CC) Controlled Access Protection Profile (CAPP) [d]. A Solaris 8 2/02 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.

5. Further identification of the evaluated TOE, including the SPARC platforms on which it was evaluated, follow below under 'TOE Scope'.

6. Specification of the evaluated configuration, including the TOE's supporting guidance documentation, is given in Annex A.

7. An overview of the TOE's security architecture can be found in Annex B.

## TOE Scope

8. The TOE was evaluated with the Common Desktop Environment (CDE) Version 1.4 installed. CDE is required for some tasks, particularly administration.

9. Both networked and standalone authentication and file access were addressed.

[1] By contrast with a multi-level system in which not all users are cleared to see the highest labelling of data, 'System High' gives the owner of a specific data object discretion to determine which other users be allowed access to the data.

10. The following filesystem types were addressed by the evaluation:

    a. the standard Solaris UNIX filesystem, `ufs`, without the Trusted Solaris attributes;

    b. the standard remote filesystem access protocol, `nfs` (v2 and v3);

    c. the MS-DOS formatted filesystem `pcfs`; and

    d. the High Sierra filesystem for CD-ROM drives, `hsfs`.

11. Only 64-bit mode operation was evaluated.

12. The evaluated configuration addressed IPv4 and IPv6.

13. None of the following were evaluated:

    a. the impact of not installing or not using CDE (eg using a more basic installation option, or using the alternative Open Windows environment);

    b. remote networked booting;

    c. unbundled products used to perform network backup services;

    d. remote administration of the server (using a Remote System Control card or networked System Controller board);

    e. Web Based Enterprise Management Services;

    f. Dynamic Host Configuration Protocol support;

    g. role based access control;

    h. printer-related functionality; and

    i. support for non-default authentication options (eg using smartcards).

14. The TOE was evaluated for the following Sun SPARC platforms, all using UltraSPARC III+ processors.

    a. SunBlade 2000 (as detailed in Annex A);

    b. SunFire V880 (as detailed in Annex A); and

    c. SunFire mid-frame family (as detailed under ‘Platform Issues’).

15. A fuller discussion of the consideration given to hardware and firmware platforms, including the OpenBoot PROM firmware used with the SunBlade 2000 and SunFire V880 platforms, and the System Controller board used with the SunFire mid-frame family machines, is given below under ‘Platform Issues’.

**Protection Profile Conformance**

16. The Security Target [c] claimed conformance to CAPP [d].

17. The Security Target contains no TOE security objectives or TOE Security Functional Requirements (SFRs) additional to those of CAPP [d]. The environmental security objectives are equivalent to those of CAPP, but are refined for the environment assumed for Solaris 8 2/02. An additional IT environment SFR is specified, relating to use of the OpenBoot PROM and System Controller board.

18. The TOE assurance requirement of Evaluation Assurance Level 4 (EAL4) exceeded, and was thus more than necessary to conform to, the EAL3 requirement of CAPP [d].

**Assurance**

19. The Security Target [c] specified the assurance requirement for the evaluation. Predefined Evaluation Assurance Level EAL4 was used. CC Part 3 [g] describes the scale of assurance given by predefined levels EAL1 to EAL7. An overview of CC is given in CC Part 1 [e].

**Strength of Function Claims**

20. The minimum Strength of Function (SoF) was SoF-medium. This was claimed in respect of the password authentication function, used either on attempting to gain access to the system or on attempting to change a password to a new one. 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.

21. 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.

22. The OpenBoot PROM and System Controller board were considered only as platform components, and as such the SoF claims did not extend to their password authentication mechanisms.

**Security Policy**

23. The TOE meets the Discretionary Access Control (DAC) policy associated with the Organisational Security Policy (OSP) P.DAC specified by the Security Target [c].

**Security Claims**

24. 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 CAPP [d] SFRs which require no tailoring for Solaris 8 2/02, where the Security Target merely references CAPP for their full specification. The Security Target also specifies OSPs which are met by the objectives.

25. Most of the SFRs are taken from CC Part 2 [f]; use of this standard facilitates comparison with other evaluated products. All extended SFRs, ie those not taken directly from CC Part 2, are inherited from CAPP [d], as identified in Section 8 of CAPP.

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

- Discretionary Access Control (DAC)
- Object re-use
- Identification and Authentication
- Auditing

27. The consumer familiar with Solaris 8 First Customer Shipment (FCS), which was previously certified by the UK IT Security Evaluation and Certification Scheme [n], will observe that the security claims of Solaris 8 2/02 are equivalent[2] to those of Solaris 8 FCS, specified in the Solaris 8 FCS Security Target [o], with variations existing primarily in respect of:

a. The TOE Security Functions Interface (TSFI). The product no longer incorporates the AdminSuite GUI which had been used for certain administrative functions, the Command Line Interface now being used in its place.

b. The hardware platforms specified for evaluation.

**Evaluation Conduct**

28. 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 the Communications-Electronics Security Group (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.

29. 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

[2] Whilst the wording of security function ENF.2 has been changed from Solaris 8 FCS, this constitutes nothing more than a clarification of what was evaluated for both Solaris 8 FCS and Solaris 8 2/02.

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 [g], the Common Evaluation Methodology (CEM) [h] and relevant interpretations.

30. The claimed security functionality for Solaris 8 2/02 remained unchanged from that of Solaris 8 FCS, which had previously been certified by the IT Security Evaluation and Certification Scheme to the CC EAL4 assurance level, as reported in the Certification Report [n]. For the evaluation of Solaris 8 2/02, some re-use was therefore made of Solaris 8 FCS evaluation results where these were valid for both Solaris 8 2/02 and the requirements of CEM [h] and its associated interpretations. However evaluation work was repeated for those EAL4 work units impacted by changes to the TOE and the associated evaluation deliverables.

31. 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) [k] to the Certification Body in February 2003. The Certification Body then produced this Certification Report.

**General Points**

32. 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.

33. 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 certification. Consumers (both prospective and existing) should check regularly for themselves whether any security vulnerabilities have been discovered since this report was issued and, if appropriate, should check with the Vendor to see if any patches exist for the products and whether such patches have been evaluated and certified.

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

(This page is intentionally left blank)

# II. EVALUATION FINDINGS

## Introduction

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

## Delivery

36. 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.

37. All TOE software and documentation components identified in Annex A are obtainable on CD, with the exception of the Security Release Notes [l]. CD delivery is recommended where possible. However the Security Release Notes are available only from Sun's website (at address http://www.sun.com/software/solaris/securitycert/index.html)

38. 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.

39. The primary considerations governing the security of web-based delivery of the Security Release Notes [l] are as follows:

a. Standard procedures associated with a well managed consumer web interface should be followed; and

b. The Security Release Notes are downloaded as a `pdf` file.

40. Should software components be downloaded from Sun's website, eg any security patches which may subsequently be made available, further considerations regarding the security of their delivery are as follows:

a. The potential for spoofing of the Sun website is reduced by the fact that Sun manages the associated Domain Name Servers. However, to guard against the risk of importing malicious code from a local spoof site when attempting to download patches, it is recommended that the following procedure be followed to authenticate the Sun website:

i the web browser should be configured to use Secure Sockets Layer Version 3;

ii patches are downloaded from web address http://access1.sun.com/solarissolve/, which supports site authentication;

iii the secure session option is selected when downloading patches; and

iv clear confirmation should be obtained, using the web browser tools, that Sun's certificate is authenticated by Thawte Server Certification Authority (or a root authority certifying this).

b. The compound threat of vulnerabilities introduced in the course of web-based delivery and then exploited in the operational environment of the TOE is not considered relevant to the 'non-hostile working environment' and protection against 'inadvertent or casual attempts to breach the system security' claimed by the Security Target [c].

**Installation and Guidance Documentation**

41. The Security Release Notes [l] 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 Security Release Notes reference other product documentation where appropriate.

42. Further product documentation, held on the Solaris 8 2/02 AnswerBook CD [m], is accessed on-line, after installation on a Solaris system. This documentation comprises the following items:

a. Solaris 8 Installation Collection;

i. Solaris 8 (SPARC) Installation Guide;
ii. Solaris 8 Advanced Installation Guide;

b. Solaris 8 System Administrator Collection;

i. System Administration Guide – Volume 1;
ii. System Administration Guide – Volume 2;
iii. System Administration Guide – Volume 3;
iv. SunSHIELD Security Module Guide;

c. Solaris 8 User Collection;

i Solaris Common Desktop Environment User's Guide;
ii Solaris Advanced User's and System Administrator's Guide; and

d. Solaris 8 Reference Manual Collection (including the man pages, which are also available on-line with the operating system).

43. The evaluators drew particular attention to the recommendations given by section 3.7.6 the Security Release Notes [l] regarding configuration of the audit_startup file to ensure capture of full audit information associated with use of commands for administrative functions which had previously been supported by the AdminSuite GUI.

**Strength of Function**

44. SoF claims for the password authentication mechanism were as given above under 'Strength of Function Claims'. Confirmation of these claims was based on the following considerations:

a. the constraint imposed by the TOE in forcing users to select passwords of at least 6 characters, including at least two alphabetic characters and one numeric or special character;

b. the recommendation that users should choose non-obvious passwords; and

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.

**Vulnerability Analysis**

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

46. 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**

47. The TOE was tested using the TSFI provided by the Solaris 8 2/02 operating system calls.

48. The Developer performed tests using the full TSFI. These tests 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.

49. The Developer's testing was performed using both an automated test suite, which generated a log of the tests' execution and results, and manual tests.

50. 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 the majority of security functions.

    b. To validate the Developer's testing, the automatic test suite was fully checked and re-run and the manual testing witnessed. All developer tests were thus either repeated or witnessed (subject to the considerations noted below under 'Platform Issues').

51. 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. This included 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.

52. Remote authentication was tested using NIS+. Local authentication was tested with account data held locally in *passwd/shadow* files.

53. The `ufs`, `nfs` and `hsfs` filesystem types were all exercised in the course of testing. The `pcfs` filesystem type was not specifically exercised. However, the design of the filesystem subsystem, which separates security-enforcing code and filesystem type-specific code into separate modules, is such that this introduces no significant risk.

54. The 4 'internal' filesystem types listed in the Security Target [c], `fd`, `namefs`, `doorfs` and `procfs`, were exercised indirectly in the course of testing.

55. Test coverage of the hardware platforms was as outlined below under 'Platform Issues'.

**Platform Issues**

56. Secure operation of the TOE on the range of hardware platforms discussed above under 'TOE Scope' was investigated through both analysis and testing.

57. The Developer ran their automated test suite on the standalone SunBlade 2000 machine and on all network configurations specified in Annex A. The Evaluators re-ran this automated test suite on the standalone SunBlade 2000 machine and on network configurations A, B and C. The Developers ran their manual tests, which were witnessed by the Evaluators, on network configurations A, B and C.

58. The Evaluators analysed the potential impact of the variations in platform characteristics on the 'Evaluation Outcome' stated below.

    a. A sample of the independent tests was run on the standalone SunBlade 2000 machine and on each network configuration specified in Annex A. Each sample comprised 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.

b. A similar approach was followed for penetration testing; however the evaluators considered that it was sufficient to run samples of the penetration tests on the standalone SunBlade 2000 machine and on network configurations A, B and C in order to adequately investigate the potential vulnerabilities.

59. In addition the Evaluators confirmed their agreement with a Developer Rationale that, with respect to the 'Evaluation Outcome' specified below, the SunFire 3800 and 6800 platforms specified in Annex A were representative of the range of SunFire mid-frame platforms quoted in the Security Target [c], which also includes SunFire 4800 and SunFire 4810 machines.

60. The following points were noted:

a. A minimum memory of 128Mb and a minimum hard disk size of 2.3Gb are recommended.

b. There is a risk that slower processor speeds, memory sizes or hard disk sizes than those tested may introduce performance degradation problems (note that the memory and hard disk sizes used for testing were greater than the recommended minima). 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.

61. The OpenBoot PROM, available for use on SunBlade 2000 and SunFire V880 platforms, and the System Controller board, which provides a similar bootstrapping facility for the SunFire mid-frame family, were treated as part of the TOE's environment, and as such were not fully evaluated. However the evaluators did consider the characteristics of these components, and performed a penetration test of the boot sequence on the SunBlade 2000 workstation (the equivalent penetration test was not run on the other platforms, which are server machines).

62. The Evaluators' assessment resulted in the following recommendations for use of both the OpenBoot PROM and System Controller board:

a. environmental procedures should prevent or detect the removal of these platform components;

b. the boot password should only be known by the system administrator;

c. boot passwords commensurate with those used for the operating system itself should be applied, therefore:

i. passwords of at least 6 characters, including at least two alphabetic characters and one numeric or special character, should be chosen;

ii. non-obvious passwords should be chosen; and

d. as an alternative to use of these components, machines can be housed in physically secure areas (e.g. this might be desired for SunFire mid-frame machines, as the boot sequence was not tested for the System Controller board).

63. A further recommendation exists for the OpenBoot PROM, which should be used in either command-secure or fully-secure mode (ie not configured to non-secure mode).

# III. EVALUATION OUTCOME

**Certification Result**

64. After due consideration of the ETRs [i, j, k], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that Solaris 8 2/02 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 platforms, and that it meets the requirements of the Controlled Access Protection Profile.

65. The password authentication mechanism meets the minimum strength of function of SoF-medium and the specific metrics given above under 'Strength of Function Claims'.

**Recommendations**

66. Prospective consumers of Solaris 8 2/02 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.

67. 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'.

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

69. 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 :

   Solaris 8 2/02 operating system.

2. The Solaris 8 2/02 operating system is provided on the following CD set:

   a. CD, Part No. 704-7980-10, March 2002, Revision A;
   b. CD, Part No. 704-0005-10, February 2002, Revision A; and
   c. CD, Part No. 704-0006-10, February 2002, Revision A.

3. The supporting guidance documents evaluated were:

   a. Solaris 8 2/02 Security Release notes, issue 0.2 [l].

   b. The Solaris 8 2/02 AnswerBook CD [m]

      CD, Part No. 705-0075-10, March 2002, Revision A.

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. The SunFire 3800 machines were configured as NFS server and NIS+ master.

   b. The system default run level of 3 was specified.

   c. Each workstation had a local *root* account. Other accounts were created using NIS+.

   d. CDE version 1.4 was installed.

## Environmental Configuration

5. The TOE was evaluated for the Sun SPARC platforms specified above under 'TOE Scope', with testing performed on the SunBlade 2000 and SunFire V880 machines detailed below and on a representative selection of SunFire mid-frame family platforms as discussed above under 'Platform Issues'.

6. The hardware platforms used for testing were as follows

| Platform | Processors and Memory | Hard Disks | Boot Option |
|---|---|---|---|
| SunBlade 2000 | Dual 1015 MHz cpu, 512Mb memory | 18.2 Gb | OpenBoot PROM version 4.5.15 |
| SunFire V880 | 2 x 900 MHz cpu, 2Gb memory | 2 x 18Gb, 6 x36Gb | OpenBoot PROM version 4.6 |
| SunFire 3800 (configuration 1) | 1 board, comprising:<br>4 x 900 MHz cpu, 8 x 512Mb memory | 2 x 18 Gb | System Controller version 5.12.6 |
| SunFire 3800 (configuration 2) | 1 board, comprising:<br>2 x 900 MHz cpu, 2 x 512Mb memory | 2 x 18 Gb | System Controller version 5.12.6 |
| SunFire 6800 (configuration 1) | 6 boards, each comprising:<br>4 x 750 MHz cpu, 8 x 512 Mb memory | 9 Gb | System Controller version 5.12.6 |
| SunFire 6800 (configuration 2) | 2 boards, each comprising:<br>1 x 750 MHz cpu, 2 x 512 Mb memory | 9 Gb | System Controller version 5.12.6 |
| SunFire 6800 (configuration 3) | 1 board, comprising:<br>1 x 750 MHz cpu, 2 x 512Mb memory<br>and 1 board, comprising:<br>2 x 750 MHz cpu, 4 x 512Mb memory<br>and 1 board, comprising:<br>4 x 750 MHz cpu, 4 x 512Mb memory<br>and 1 board, comprising:<br>4 x 750 MHz cpu, 8 x 512Mb memory | 9 Gb | System Controller version 5.12.6 |

7. Standalone operation was tested using the SunBlade 2000 machine. Networked operation was tested using the following master-client platform combinations.

| Network Configuration | Master | Client |
|---|---|---|
| A | SunFire 3800 (configuration 1) | SunBlade 2000 |
| B | SunFire 3800 (configuration 1) | SunFire V880 |
| C | SunFire 3800 (configuration 1) | SunFire 6800 (configuration 1) |
| D | SunFire 3800 (configuration 2) | SunFire 6800 (configuration 2) |
| E | SunFire 3800 (configuration 2) | SunFire 6800 (configuration 3) |

8. The machines were connected via Ethernet using cPCI Ethernet cards.

9. The Ipv6 option was set when configuring the TOE, but Ipv4 addresses were used. Both Ipv4 and IP46 capabilities were thus both tested; use of the Ipv4 option or Ipv6 addresses should introduce no significant risk.

# ANNEX B: PRODUCT SECURITY ARCHITECTURE

1. This annex gives an overview of Solaris 8 2/02 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**

Trust and Privilege

2. Solaris 8 2/02 consists of the system kernel and a set of independent processes which may execute both system and user applications. A process may be trusted or untrusted. This is supported by:

a. the Processor States feature, which enables the operating system to allocate the processor in either *user state*, in which only 'safe' instructions can be executed and there is no interference between processes, and *supervisor state*, in which any instructions can be executed and any memory accessed; and

b. the Memory Management feature, which enables every process to run in its own virtual memory space.

3. Solaris 8 2/02 uses the root superuser concept. By default, root is the only user provided with modify access, but additional users can be set up with administration type privilege to administer the product. The privileges associated with users are stored in the */etc/user_attr* file.

Filesystems

4. The filesystem types noted above under 'TOE Scope' are supported.

Networking and Standalone Options

5. Solaris 8 2/02 can be used networked or standalone.

6. 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.

7. 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**

8. Solaris 8 2/02 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 processor supervisor mode. Subsystems identified as TOE Security Policy enforcing within the scope of the evaluation are as follows.

Kernel

9. The Kernel addresses DAC, processes, audit, enforcement and object reuse. The kernel contains the System V IPC objects used for inter-process communication. Inter-process communication is supported by 3 mechanisms: semaphores, message queues and shared memory.

Filesystem

10. The Filesystem contains files, directories, symbolic links, FIFOs, pipes, domain socket rendezvous files, process files, pseudo terminals and device special files. Every file system object has security attributes relating to the owning user and group membership access permissions and may have an ACL. DAC is based on the permissions and ACL. The file system overlaps significantly with the kernel subsystem in that some of the file system functionality is implemented inside the kernel.

Audit

11. The Audit subsystem provides a record of events for the purposes of auditing and accountability. The auditable actions of an individual user can be reconstructed and analysed. The audit trail consists of a set of audit files. An audit file consists of a set of audit records. Tools are provided for audit analysis and printing. The audit trail is protected from unauthorised access by the DAC mechanism.

I & A

12. The Identification and Authentication subsystem ensures that access to the TOE is only granted to authorised users who are identified and authenticated, as configured by a system administrator. The TOE Security Functions (TSF) ensure that dtlogin is the only method by which a user can initially log on to Solaris. When users successfully login, the TSF will correctly set up all their security attributes. The authentication data is protected by DAC. A user may also login remotely, may change the effective user identifier to that of another user and may change the password; each of these activities are subject to a further authentication check (unless, in the case of remote login, the system has been configured to rely only on settings in the rhosts file).

Admin Tools

13. The Admin Tools subsystem provides functionality to allow administrators to configure the security aspects of the system.

NIS+

14. The Network Information Service+ subsystem maintains a central database of administrative information across all workstations within a NIS+ Domain. This administrative information is used to support the I&A component by providing a secure database for the identification and authentication data.

Startup

15. The Startup subsystem has 8 pre-defined run levels. System startup controls run level transition from level 0 to the level specified from the BOOTPROM or via the system default run level.

Windowing

16. The Windowing subsystem consists of the X server, window manager and the selection manager. It provides a Front Panel facility for users to control workspaces, applications, session exit and mail.

**Hardware and Firmware Dependencies**

17. The TOE uses standard hardware features to implement its Memory Management and Processor States features.

18. 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)