UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P148

Sun Solaris

Version 8

with AdminSuite Version 3.0.1

Issue 1.0

November 2000

UK IT Security Evaluation and Certification Scheme
Certification Body, PO Box 152
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 is a UNIX-based operating system which can be configured from a number of workstations and servers to form a single distributed system. AdminSuite 3.0.1 provides tools to configure security aspects of Solaris 8. Both Solaris 8 and AdminSuite 3.0.1 have been developed by Sun Microsystems Inc.

Solaris 8, with AdminSuite 3.0.1, 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 and Intel Pentium platforms. It has also met the requirements of the Controlled Access Protection Profile.

Originator	**CESG** Certifier
Approval	**CESG** Technical Manager of the Certification Body
Authorisation	**CESG** Senior Executive UK IT Security Evaluation and Certification Scheme
Date authorised	21 November 2000

(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
ITSEC	Information Technology Security Evaluation Criteria
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 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. Solaris 8 Security Target,
Sun Microsystems Inc.,
S8.0_101/ts2_101, Issue 1.0, 28 July 2000.

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. Endorsed Interpretation UK/2.1/003,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, January 2000.

j. LFL/T120 Evaluation Technical Report 1,
Logica CLEF,
CLEF.24831.30.1, Issue 1.0, 17 January 2000.

k. LFL/T120 Evaluation Technical Report 2,
Logica CLEF,
CLEF.24831.30.2, Issue 1.0, 1 June 2000.

l. LFL/T120 Evaluation Technical Report 3,
Logica CLEF,
CLEF.24831.30.3, Issue 1.0, 31 July 2000.

m. Solaris 8 Security Release Notes,
Sun Microsystems Inc.,
Issue 0.8, 9 October 2000.

n. Solaris 8 Documentation CD,
Sun Microsystems Inc.,
Part No. 704-6899-10, Revision A, February 2000.

o. Certification Report No. 95/56, Sun Solaris 2.4 SE,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, November 1995.

p. Certification Report No. P101, Sun Solaris 2.6 SE,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, January 1999.

q. Solaris 2.6SE Security Target,
Sun Microsystems Inc.,
S2.6_101, Version 1.0, 17 June 1998.

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria evaluation of Sun Solaris 8, with AdminSuite 3.0.1, to the Sponsor, Sun Microsystems Inc., and is intended to assist prospective consumers when judging the suitability of the IT security of the products 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 Version 8 First Customer Shipment (FCS)
- AdminSuite Version 3.0.1 FCS

with patches:

- 108875-07 and 108879-02 for SPARC platforms
- 108876-07 and 108881-02 for Pentium platforms

The Developer was Sun Microsystems Inc.

4. Solaris 8 is a highly-configurable UNIX-based operating system which has been developed to meet 'System High' operation including the use of Access Control Lists (ACLs). It meets the requirements of the Common Criteria (CC) Controlled Access Protection Profile (CAPP) [d], which are equivalent to those of the C2 class of the Trusted Computer System Evaluation Criteria. A Solaris 8 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. AdminSuite 3.0.1 provides tools to allow administrators to configure the security aspects of the Solaris 8 system.

6. The evaluated products are hereinafter referred to as:

a. 'The Solaris 8 operating system' and 'AdminSuite' where distinction is made between them.

b. 'Solaris 8' where they are referred to jointly. The products are also jointly identified as the Target of Evaluation (TOE).

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

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

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

TOE Scope

10. The Solaris 8 operating system was evaluated with AdminSuite 3.0.1 installed.

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

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

13. 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`.

14. Both 32bit and 64bit SPARC-based architectures were evaluated.

15. The evaluated configuration addressed both IPv4 and IPv6.

16. None of the following were evaluated:

    a. the impact of configuring Solaris 8 without installing or using AdminSuite 3.0.1 (ie using the user command interface);

    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. section 8 of the Security Target [c], as discussed below under 'Security Policy Model';

    d. patches 108652-16 and 109320-01 (for SPARC platforms) and 108653-16 and 109321-01 (for Pentium platforms), as discussed below under 'Vulnerability Analysis';

    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. role based access control (with the exception of that used by AdminSuite);

j. printer-related functionality; and

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

17. The TOE was evaluated for hardware platforms representative of the following currently available ranges:

a. single and multi-processor Sun SPARC platforms using the Ultra-I, Ultra-II and Ultra-IIi family of processors; and

b. single processor PCs using the Intel Pentium II and Intel Pentium III processor families.

18. Significant exclusions from the set of evaluated platform ranges were as follows:

a. Sun SPARC platforms using the SuperSPARC processor;

b. the Remote Service Control component (available on some SPARC platforms);

c. the Sun Enterprise E10000 platform (on account of its multi-domain capability); and

d. multi-processor Intel Pentium platforms.

19. For the Sun SPARC platforms, the security of the Version 3 OpenBoot PROM firmware was evaluated. However, the range of PC BIOS firmware available for use with Pentium processors was not evaluated.

20. A fuller discussion of the consideration given to hardware and firmware platforms is given below under ‘Platform Issues’.

Protection Profile Conformance

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

22. 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. An additional IT environment SFR is specified, relating to use of the OpenBoot PROM.

23. 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 Requirement

24. The Security Target 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 (where EAL0 represents no assurance). An overview of CC is given in CC Part 1 [e].

Strength of Function Claims

25. 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.

26. 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.

27. 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.

28. The SoF claims did not extend to the algorithms used in the process for certifying the Sun website which is recommended below under 'Delivery'.

Security Policy

29. The TOE security policy is evident from Sections 1 to 7 of the Security Target [c]. It meets the Organisational Security Policies (OSPs) specified by the Security Target.

Security Claims

30. 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, where the Security Target merely references CAPP for their full specification. The Security Target also specifies OSPs which are met by the objectives.

31. 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.

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

- Discretionary Access Control (DAC)
- Object re-use

- Identification and Authentication
- Auditing

33. The consumer familiar with Solaris 2.6SE, which was previously certified by the UK IT Security Evaluation and Certification Scheme to the Information Technology Security Evaluation Criteria (ITSEC) assurance level E3 [p], will observe that the security claims of Solaris 8 are equivalent to those of Solaris 2.6SE, specified in the Solaris 2.6SE Security Target [q]. However, there is some variation in the expression of the claims in order to comply with CC requirements and to confirm conformance to CAPP [d].

Evaluation Conduct

34. 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 jointly managed by the Communications-Electronics Security Group (CESG) and the Department of Trade and Industry 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.

35. 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 [g] and the Common Evaluation Methodology (CEM) [h].

36. Much of the Solaris 8 functionality and supporting evaluation deliverables content remained unchanged from that of Solaris 2.4SE and Solaris 2.6 SE, both of which had previously been certified by the IT Security Evaluation and Certification Scheme to the ITSEC E3 assurance level, as reported in their respective Certification Reports [o, p]. For the evaluation of Solaris 8, the Evaluators addressed every CEM [h] EAL4 work unit but made some use of Solaris 2.4SE and Solaris 2.6SE evaluation results where these were valid for both Solaris 8 and the CEM requirements.

37. 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) [l] to the Certification Body in July 2000. Following a request for further information, the Certification Body produced this Certification Report.

Certification Result

38. For the certification result see the ‘Evaluation Outcome’ section.

General Points

39. 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.

40. 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.

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

II. EVALUATION FINDINGS

Introduction

42. The evaluation addressed the requirements specified in the Security Target [c] The results of this work were reported in the ETRs [j, k, l] under the CC Part 3 [g] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with the subsequent assurance maintenance and re-evaluation of the TOE.

Security Policy Model

43. UK interpretation UK/2.1/003 [i] was followed, allowing Sections 1 to 7 of the Security Target [c] to be taken as providing the Informal Security Policy Model. The additional security policy guidance material provided by the Sponsor in Section 8 of the Security Target was not evaluated.

Delivery

44. 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.

45. All TOE software and documentation components identified in Annex A are available on both CD and from the sun.com website, with the following exceptions:

a. the Solaris 8 operating system FCS software is available only on CD;

b. patches are available only from the website (at various addresses); and

c. the Security Release Notes [m] are available only from the website (at address http://www.sun.com/software/solaris/securitycert/index.html).

46. CD delivery is recommended wherever possible.

47. The following measures provide security for CD delivery:

a. CDs are write-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.

48. The primary considerations governing the security of web-based delivery are as follows:

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

b. 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).

c. The Security Release Notes [m] are downloaded as a `pdf` file.

d. The compound threat of vulnerabilities introduced in the course of web-based delivery and then exploited in the operational environment of the TOE (eg involving local spoofing of the address http://www.sun.com/software/solaris/securitycert/index.html) 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

49. The Security Release Notes [m] 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.

50. Further product documentation, held on the Solaris 8 documentation CD [n], is accessed on-line, after installation on a Solaris system. The AnswerBook2 application, which is also supplied on the CD, is used to access the documentation. The documentation comprises the following:

a. Solaris 8 User Collection;

   i Solaris 8 Advanced User's Guide;
   ii Solaris 8 Common Desktop Environment User's Guide;
   iii Solaris 8 Common Desktop Environment Advance User's and Administrator's Guide;

b. Solaris 8 System Administrator Collection;

c. SunSHIELD Basic Security Module Guide;

d. Solaris 8 Installation Guides;

i SPARC Platform Edition; and
ii Intel Platform Edition.

51. A further form of guidance material is given by the AdminSuite on-line help.

Strength of Function

52. 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

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

54. 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.

55. The Sponsor had identified vulnerabilities involving an X11 buffer overrun, a *netpr* buffer overrun and a *ufsrestore* buffer overflow. In all three cases procedural fixes are given by the Security Release Notes [m], and it is recommended that these be followed. The Sponsor has also made patches 108652-16 and 109320-01 (for SPARC platforms) and 108653-16 and 109321-01 (for Pentium platforms) available to fix the X11 buffer overrun and netpr buffer overrun vulnerabilities, but these patches were not evaluated.

Testing

56. The TOE was tested using the TOE Security Functions Interface (TSFI) provided by the Solaris 8 operating system calls, documented by the on-line man pages, and the AdminSuite functions, documented by the supporting guidance material.

57. The Developer performed tests using the full TSFI, with the exception of one interface which was subsequently tested by the Evaluators. 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.

58. The Developer's testing was performed using an automated test suite, comprising both fully automated tests and 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.

59. 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. 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. All fully automated tests were repeated, as were 83% of those requiring manual input.

60. 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.

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

62. 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.

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

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

Platform Issues

65. Secure operation of the TOE on the range of hardware platforms discussed above under 'TOE Scope' was performed by both analysis and testing.

66. The Developer ran their full test suite on all platforms specified in Annex A.

67. The Evaluators analysed the potential impact of the variations in platform characteristics on the 'Evaluation Outcome' stated below. All independent and penetration tests were first run on the combination of the Ultra 1 (NFS server, NIS+ master) and Ultra 10 platforms. A sample of the tests was then repeated on all the other platforms specified in Annex A, using the same Ultra 1 as NFS server and NIS+ master. The sample included both a representative selection of tests and those which analysis had indicated might be most sensitive to platform variations.

68. For the SPARC platforms, developer tests and evaluator tests were run in both 32 bit and 64 bit modes.

69. The following points were noted:

a. The slowest machine in the Ultra family, the Ultra 1, was tested. Slower Pentium speeds may introduce the risk of performance degradation problems. No concerns relating to higher processor speeds were evident in the course of the evaluation, but this was untested.

b. A minimum memory of 96Mb and, for configurations with fixed disks, a minimum disk size of 2Gb are recommended.

c. A security relevant problem was experienced in that the logout function did not always operate on the client Ultra 1 machine. All other security functions continued to operate correctly. It was suspected, but not confirmed, that this was due to the memory sizes on the Ultra 1 platforms being less than the recommended minimum. It is recommended that a local procedural instruction be issued to require powering down of the workstation in question before it is left unattended should this problem re-occur on machines with marginal resources.

70. 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. Different variants (ie versions 3.x.x) are now available for use on platforms in the range of SPARC platforms outlined above under 'TOE Scope', but the Evaluators' analysis confirmed that the differences were not security relevant.

71. Recommendations for use of the OpenBoot PROM, originally made in the Solaris 2.6SE Certification Report [p], 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.

72. 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 and Re-evaluation Issues

73. It is recommended that the patches 108652-16 and 109320-01 (for SPARC platforms) and 108653-16 and 109321-01 (for Pentium platforms), discussed above under 'Vulnerability Analysis', be included within the scope of any future assurance maintenance and re-evaluation activities.

74. If, for future purposes of assurance maintenance and re-evaluation, claims are to be maintained in respect of SPARC platforms for which the Ultra 1 is representative, it is recommended that tests be run to address the logout function concern noted above under 'Platform Issues' (eg by using a configuration with the recommended minimum memory size of 96Mb).

75. A single Observation Report, relating to a small deficiency in the Developer's test coverage, remained uncleared at the end of the evaluation. The Evaluators remedied this in their independent testing. However, in the event of subsequent assurance maintenance activity, the Developer is recommended to remedy this deficiency in the test suite used in the course of the assurance maintenance activities.

76. The development environment assessment gave primary focus to the AdminSuite development site, as AdminSuite exhibited the most significant changes made to the TOE in its derivation from the previously certified Solaris 2.6SE. For the Solaris 8 operating system development site, sufficient confidence in the proper application of configuration management and development security procedures was demonstrated by:

a. reference to checks previously made on the correct application of procedures at the times of the Solaris 2.4SE and Solaris 2.6SE evaluations;

b. confirmation that the procedures used for Solaris 2.4SE and Solaris 2.6SE remained in use for the Solaris 8 operating system, supported by the fact that the equivalent claim made for AdminSuite was confirmed; and

c. documentary evidence relating to the Solaris 8 operating system, encountered by the Evaluators in the course of the evaluation, which was found to be consistent with correct use of the procedures.

It is recommended however, that correct application of procedures be confirmed directly during a visit to the Solaris 8 operating system site, in the course of a subsequent assurance maintenance audit or a re-evaluation.

(This page is intentionally left blank)

III. EVALUATION OUTCOME

Certification Result

77. After due consideration of the ETRs [j, k, l], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that Solaris 8, with AdminSuite 3.0.1, 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 Controlled Access Protection Profile.

78. 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

79. Prospective consumers of Solaris 8, with AdminSuite 3.0.1, 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.

80. 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'.

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

82. 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 :

   a. Solaris version 8 operating system FCS,

   b. AdminSuite version 3.0.1 FCS,

   with patches:

   - 108875-07 and 108879-02 for SPARC platforms; and
   - 108876-07 and 108881-02 for Pentium platforms.

2. The Solaris 8 operating system FCS is provided on the following CD sets:

   - For SPARC platforms:

     i Solaris 8 Installation CD, Part No. 704-6897-10, February 2000, Revision A
     ii Solaris 8 Software 1 of 2 CD, Part No. 704-6898-10, February 2000, Revision A
     iii Solaris 8 Software 2 of 2 CD, Part No. 704-6972-10, February 2000, Revision A

   - For Pentium platforms:

     i Solaris 8 Installation CD, Part No. 704-6900-10, February 2000, Revision A
     ii Solaris 8 Software 1 of 2 CD, Part No. 704-6901-10, February 2000, Revision A
     iii Solaris 8 Software 2 of 2 CD, Part No. 704-6975-10, February 2000, Revision A

3. The AdminSuite FCS, for both platform types, is supplied on the following CD:

   Solaris 8 Admin Pack, Part No. 704-7144-10, March 2000, Revision A.

4. The supporting guidance documents evaluated were:

   a. Solaris 8 Security Release notes, issue 0.6 [m], which covers both platform types.

   b. The AnswerBook 2 Application, providing supporting guidance documentation covering both platform types, supplied on the following CD:

      Solaris 8 Documentation CD, Part No. 704-6899-10, February 2000, Revision A. [n]

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

TOE Configuration

5. The following configuration was used for testing:

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

   b. The Sun Ultra 1 workstation equipped with two hard drives (specified below under 'Environmental Configuration') was configured as NFS server and NIS+ master,

   c. Each workstation had a local *root* account. Other accounts were created using NIS+. *root* was set up as the primary administrator for AdminSuite.

   d. For SPARC platforms, the 64 bit architecture was installed as the default bootup option, and the 32 bit architecture was invoked using the *boot kernel/unix* command.

Environmental Configuration

6. The TOE was evaluated for the Sun SPARC and Intel Pentium platform ranges specified above under 'TOE Scope', with testing performed on a representative selection of hardware platforms as discussed above under 'Platform Issues'.

7. The hardware platforms used for testing were as follows

Platform	Processor	Memory (Mb)	Hard Drive (Gb)	CD-RoM
Sun Ultra 1 Model 170	UltraSPARC I 166MHz	64	2 (Internal) 4 (External)	External
Sun Ultra 1 Model 170	UltraSPARC I 166MHz	64	2	-
Sun Ultra 10	UltraSPARC Iii 333MHz	128	4	Internal
Sun Enterprise E450	UltraSPARC II 300MHz	256	9	Internal
Sun Enterprise E4500	Dual UltraSPARC II 336MHz	256	9	Internal
Dell OptiPlex GXa	Pentium II 233MHz	128	17	Internal
Dell OptiPlex GX1	Pentium III 500MHz	96	3	Internal

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

9. The IPv6 option was set when configuring the TOE, but IPv4 addresses were used. Both IPv4 and IPv6 capabilities were thus both tested; use of the IPv4 option or IPv6 addresses should introduce no significant risk.

10. Boot firmware is relevant to the security of the TOE. For this evaluation, re-use was made of the previous Solaris 2.6SE OpenBoot PROM version 3 testing, as discussed above under ‘Platform Issues’.

(This page is intentionally left blank)

ANNEX B: PRODUCT SECURITY ARCHITECTURE

1. This annex gives an overview of Solaris 8 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. The Solaris 8 operating system 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. The Solaris 8 operating system uses the root superuser concept. By contrast AdminSuite uses role based access control. 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 configured within AdminSuite, and the corresponding Solaris 8 operating system entries 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 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. Networked workstations can be booted from local media or from a networked SPARC-based server.

8. Either IPv4 or IPv6 can be used to support networked operation.

9. For standalone use, the NIS+ authentication facility is not available, so all users must have 'local' user accounts, and file systems cannot be shared.

Architecture Bitsizes

10. The Solaris 8 operating system kernel can be run in either 32 or 64 bit modes when running on SPARC platforms. On Pentium platforms only the 32 bit version can be run.

11. Applications can be run as 32 bit or 64 bit as follows:

- 32 bit applications can be run on a 32 bit or 64 bit kernel
- 64 bit applications can be run only on a 64 bit kernel

Design Subsystems

12. Solaris 8 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 TSP enforcing within the scope of the evaluation are as follows.

Kernel

13. 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

14. 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 component overlaps significantly with the kernel component in that some of the file system functionality is implemented inside the kernel.

Audit

15. The Audit component 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

16. The Identification and Authentication component 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. Subject to successful authentication, a user may login remotely, may change the effective user identifier to that of another user and may change the password.

Admin Tools

17. The Admin Tools component provides tools to allow administrators to configure the security aspects of the system. These tools form the AdminSuite application consisting of AdminSuite Console (the top level GUI), Computer/Networks, Mounts/Shares, Groups Manager, Serial Manager, User Accounts Manager and File Manager.

NIS+

18. The Network Information Service+ component 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

19. The Startup component 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

20. The Windowing component 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

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

22. 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)