UK ITSEC SCHEME CERTIFICATION REPORT NO. P104

Trusted Solaris 2.5.1

Running on Sun Ultra SPARC-1 Workstation

Issue 1.0

October 1998

UK IT Security Evaluation and Certification Scheme
Certification Body, PO Box 152
Cheltenham, Glos GL52 5UE
United Kingdom

RECOGNITION AGREEMENT OF
INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES

The Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Agreement Group and as such:

- indicates that it is the issuer's claim that this certificate is a conformant certificate as defined in this Agreement; and

- therefore gives grounds for confidence, though it cannot in itself guarantee, that the certificate is a conformant certificate and that it will in practice be recognised by the other Members of the Agreement Group.

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.

Trademarks:

CERTIFICATION STATEMENT

Trusted Solaris 2.5.1 is a highly-configurable UNIX-based trusted operating system which has been developed by SUN Microsystems Federal Inc., to meet a number of operational requirements for secure computing, including:

- "Multi-Level" Operations supported through F-B1 functionality with the addition of Trusted Networking and Windowing; and

- "System High" Operation supported via enhanced F-C2 functionality, including the use of Access Control Lists and Trusted Advisory Labelling.

Trusted Solaris 2.5.1 has been evaluated under the terms of the UK ITSEC Scheme and has met the requirements of ITSEC Assurance Level E3 and Functionality Classes F-B1 and F-C2 when running on the Sun Ultra SPARC-1 workstation as specified in Annex B.

Originator	**CESG** Certifier
Approval	**CESG** Head of the Certification Body
Authorisation	**CESG** Senior Executive UK ITSEC Scheme
Date authorised	30 October 1998

THIS PAGE IS INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE IS INTENTIONALLY LEFT BLANK

ABBREVIATIONS

CDE	Common Desktop Environment
CESG	Communications-Electronics Security Group
CLEF	Commercial Evaluation Facility
DAC	Discretionary Access Control
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
ITSEC	Information Technology Security Evaluation Criteria
ITSEM	Information Technology Security Evaluation Manual
MAC	Mandatory Access Control
NFS	Network File System
NIS+	Network Information Service
SEF	Security Enforcing Function
SIN	Scheme Information Notice
SoM	Strength of Mechanisms
SPARC	Scalable Processor Architecture
TCB	Trusted Computer Base
TCSEC	Trusted Computer Systems Evaluation Criteria
TOE	Target of Evaluation
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 3.0, 2 December 1996.

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 2.5.1 Security Target,
EC.22740.ST / ts2_101, Version 6.0, 6 August 1998

d. Harmonised Information Technology Security Evaluation Criteria,
Commission of the European Communities,
CD-71-91-502-EN-C, Version 1.2, June 1991.

e. Information Technology Security Evaluation Manual,
Commission of the European Communities,
Version 1.0, 10 September 1993.

f. Manual of Computer Security Evaluation, Part I, Evaluation Procedures,
UK IT Security Evaluation and Certification Scheme,
UKSP 05, Issue 3.0, October 1994.

g. Manual of Computer Security Evaluation, Part III, Evaluation Techniques and Tools,
UK IT Security Evaluation and Certification Scheme,
UKSP 05, Issue 2.0, 30 July 1997.

h. Evaluation Technical Reports
ETR1- CLEF.22740.30.1, Version 1.0, 5 February 1997
ETR2- CLEF.22740.30.2, Version 1.0, 14 July 1997
ETR3- CLEF.22740.30.3, Version 1.0, 13 October 1997
ETR4- CLEF.22740.30.4, Version 1.0, 25 June 1998
ETR5- CLEF.22740.30.5, Version 1.0, 07 August 1998

i. Trusted Computer Systems Evaluation Criteria,
Department of Defense, United States of America,
DOD 5200.28-STD, December 1985.

j. Scheme Information Notice No. 052, F-B1 Functionality Class,
UK IT Security Evaluation and Certification Scheme,
SIN No. 052, Issue 2.0, 28 January 1997.

k. Scheme Information Notice No. 053, F-C2 Functionality Class,
UK IT Security Evaluation and Certification Scheme,
SIN No. 053, Issue 1.0, 24 April 1996.

l. Trusted Solaris User Guide (805-806-10)

m. Trusted Solaris Reference Manual (805-8005-10)

n. Trusted Solaris Developers Guide (805-8014-10)

I. INTRODUCTION

Intended Audience

1. This Certification Report states the outcome of the IT security evaluation of Trusted Solaris Version 2.5.1 to the Sponsor, SUN Microsystems Federal Inc., and is intended to assist potential users when judging the suitability of the product for their particular requirements.

Identification of Target of Evaluation

2. The version of the product evaluated was:

Trusted Solaris 2.5.1. running on Sun Ultra SPARC-1 workstation.

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

3. Trusted Solaris 2.5.1 is a highly configurable UNIX based operating system which has been developed to meet 'System High' and 'Multi Level' requirements.

4. System High Operation is supported via enhanced F-C2 functionality, including the use of Access control lists and Trusted Advisory Labelling.

5. Multi-Level Operations are supported through F-B1 functionality with the addition of Trusted Networking and Windowing.

6. A Trusted Solaris 2.5.1 system consists of a number of workstations and servers linked together to form a single distributed system. Users share the resources of multiple workstations and servers connected together in a single Trusted Computer Base (TCB).

Evaluation

7. The evaluation was carried out in accordance with the rules of the UK IT Security Evaluation and Certification Scheme which is described in United Kingdom Scheme Publication (UKSP) 01 and UKSP 02 [References 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.

8. The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [c], which users are advised to read. The criteria against which the TOE was judged are described in the IT Security Evaluation Criteria (ITSEC) [d]. This describes how the degree of assurance is expressed in terms of the levels E0 to E6 where

E0 represents no assurance. The methodology used is described in the IT Security Evaluation Manual (ITSEM) [e] and UKSP 05 [f, g].

9. The Certification Body monitored the evaluation which was carried out by the Logica UK Commercial Evaluation Facility (CLEF). The evaluation was completed in August 1998 when the CLEF submitted a final Evaluation Technical Report (ETR) [h] to the Certification Body which, in turn, produced this Certification Report.

10. The Target Assurance Level for the product, as required by the Security Target [c], was E3, together with ITSEC [d] Functionality Class F-B1 as described in Scheme Information Notice (SIN) No. 052 [j], and Functionality Class F-C2 as described in SIN No. 053 [k]. The claimed Strength of Mechanism was High when all passwords are generated by Trusted Solaris 2.5.1 and Medium when the passwords are generated by the users.

General Points

11. Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with higher assurance levels) that exploitable vulnerabilities remain undiscovered. Prospective users of the TOE are reminded that the security functionality evaluated is that claimed in the Security Target [c]. This functionality may not necessarily meet all the threats that a user has identified in a particular operating environment. The assumed threats, intended method of use and environment are as stated in the Security Target. The TOE should only be used in its evaluated configurations (as indicated in Annex B) and in accordance with the recommendations and caveats contained in this report. It is the responsibility of purchasers to ensure that Trusted Solaris 2.5.1 meets their requirements.

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

II. EVALUATION FINDINGS

Introduction

13. The evaluation of Trusted Solaris Version 2.5.1 followed the generic Evaluation Work Programme described in the ITSEM [e] with work packages structured around the evaluator actions described in the ITSEC [d]. The results of this work were reported in the ETR [h] under the ITSEC headings. This Certification Report summarises the assurance results in relation to the security functionality claimed in the Security Target [c].

Correctness – Construction

14. This aspect of the evaluation examined both the development process (ie the Security Target, the Architectural and Detailed Designs, the Implementation) and the environment in which it takes place. The results were as follows:

a. The final version of the Security Target [c] described the Security Enforcing Functions (SEFs) provided by the TOE, and contained a product rationale identifying its method of use and intended environment; it also described how the product's functionality was appropriate for that method of use and was adequate to counter the assumed threats.

b. The Architectural Design properly described the general structure of the TOE, together with any external interfaces and supporting hardware or firmware; it also clearly detailed how the SEFs of the TOE are provided and how the TOE is separated into security enforcing and other components.

c. The final version of the Detailed Design identified all security mechanisms, described all SEFs and other security relevant functions, mapped SEFs to mechanisms and components, documented interfaces adequately and enabled the relationships between levels of specification to be identified.

d. The correctness of the implementation was satisfactory, ie all security enforcing and security relevant functions offered in the Detailed Design were identifiable in the source code and test documentation and the associated tests were repeatable.

e. Repeating an agreed sample of the Sponsor's functional tests on Sun Ultra SPARC-1 workstations produced no differences in the test results.

f. The configuration control, programming standards and security aspects of the Developer's working environment were satisfactory.

15. The above findings enabled the Evaluators to conclude that the TOE fully met the requirements for ITSEC E3 in respect of its Security Target, Architectural and Detailed Designs, Implementation and Development Environment.

Correctness – Operation

16. The Evaluators checked and confirmed that:

a. the operational documentation adequately described the SEFs relevant to end users and administrators and how to operate the TOE in a secure manner;

b. the delivery and configuration documentation described the delivery arrangements from the development environment to the customer and the required system generation aspects;

c. the startup and operation documentation adequately described the procedures for secure start-up and operation and, where relevant, for the deactivation or modification of SEFs; and

d. the information supplied described how these procedures maintain the security of the TOE.

17. The Evaluators concluded that the operational documentation and the operational environment satisfied the requirements for ITSEC E3.

Effectiveness – Construction

18. This aspect of the evaluation dealt with:

a. the suitability of the TOE's SEFs to counter the threats identified in the Security Target [c];

b. the ability of the SEFs and mechanisms to bind together in a way that is mutually supportive and provides an integrated and effective whole;

c. the ability of the TOE's security mechanisms to withstand direct attack; and

d. the question of whether known security vulnerabilities in the construction of the TOE could, in practice, compromise its security.

19. The Evaluators were satisfied that:

a. the Suitability Analysis confirmed that all the threats listed in the Security Target [c] were adequately countered by one or more of the stated SEFs and mechanisms;

b. the Binding Analysis demonstrated that it was not possible for any SEF or mechanism to conflict with or contradict the intent of any other SEFs or mechanisms;

c. the procedural measures in the Sponsor's Security Target [c] and the Developer's operational documentation [l, m, n] were sufficient to prevent all known construction vulnerabilities from being exploited;

d. penetration testing did not reveal any exploitable vulnerabilities in the TOE that were not satisfactorily corrected or neutralised;

e. penetration testing did not identify any exploitable vulnerabilities associated with the use of the TOE beyond 2000 AD; and

f. the Strength of Mechanisms (SoM) Analysis listed all the security enforcing mechanisms identified as critical within the TOE, and the minimum strength ratings of the user password mechanism was Medium (for user generated passwords) and High (for system generated passwords) as claimed.

20. As a result of the above findings, the TOE is adjudged fully to have met the requirements for ITSEC E3 in respect of Suitability, Binding, SoM and Construction Vulnerability.

Effectiveness – Operation

21. This work involved:

a. checking that the TOE can be used in a secure manner and assessing whether known vulnerabilities in its operation could, in practice, compromise its security; and

b. checking the List of Known Vulnerabilities in the operation of the TOE, as supplied by the Sponsor, and assessing the impact of these vulnerabilities and the measures proposed to counter their effects.

22. The evaluation confirmed that:

a. the TOE could not be configured or used in a manner which was insecure but which an administrator or end-user would reasonably believe to be secure;

b. the countermeasures proposed by the Sponsor in the List of Known Vulnerabilities in Operational Use were entirely satisfactory; and

c. a number of exploitable vulnerabilities, revealed by comprehensive penetration testing but not identified by the Sponsor, had all been technically addressed or could be successfully overcome by procedural measures documented in the Security Target[c] and / or the operational documentation [l, m, n].

23. The TOE thus meets the requirements for ITSEC E3 in respect of Ease of Use and Operational Vulnerability.

Specific Functionality

24. The Evaluators concluded that all the functionality claimed in the Security Target [c] (including Functionality Classes F-B1 and F-C2 as described in SIN No. 052 [j] and SIN No. 053 [k] respectively), had been met. This included functionality claims for:

- Identification and Authentication
- Access Control
- Audit
- Accountability
- Administration
- Object Reuse

25. This evaluation used the Functionality Classes F-B1 and F-C2 as defined in SIN No. 052 and SIN No. 053. This version [j, k] resolves some known inconsistencies in Functionality Classes F-B1 and F-C2 defined in Annex A of ITSEC (both internal and with respect to the Trusted Computer Systems Evaluation Criteria (TCSEC) [i] B1 and C2 requirements), and also takes into account official TCSEC interpretations relevant to B1 and C2. Compliance with the ITSEC version does not guarantee compliance with SIN No. 052 or SIN No. 053; however, compliance with SIN No. 052 and SIN No. 053 guarantees compliance with the ITSEC version.

Unresolved Issues

26. The Evaluators reported a number of issues in minor Evaluation Observation Reports (EORs) which did not impact on the assurance of the TOE. It is suggested that the Developer address these issues in the next release of the product. Those that remain unresolved are as follows:
EOR 018-3, EOR 045-6, EOR 048, EOR 051-2, EOR 051-3, EOR 051-5, EOR 083, EOR 085, EOR 086, EOR 089.

27. EOR 018-3 noted that net_nofloat privilege could override automatic floating of the object information label. However, the use of net_nofloat was not indicated in the detailed design and it is not substantially used in the product.

28. EOR 083 noted that a part of the configuration control was not documented although it appeared to be implemented satisfactorily.

29. EOR 085 noted that although the password changing via the front panel is audited and satisfies the requirements for SEF Audit 6 the process is not accurately described in the design documentation.

30. EOR 086 noted that although the TOE correctly does not permit the use of the *passwd* command, this is not accurately described in the documentation.

31. EOR 089 noted that the Evaluator's functional test DAC.2_F2 showed that a user can change the group attribute of an object to one of which they are a member without privilege. This is contrary to parts of the documentation.

32. The Developer satisfactorily tested all functionality and mechanisms apparent at the detailed design and source code levels respectively. The following minor EORs highlight certain combinations of detailed functionality where the Evaluators were not able to identify tests from the Developer's documentation.

33. EOR 045-6 noted that the Evaluators could not find evidence of functional testing to check that the audit events AUE_GETMSG and AUE_GETPMSG are generated as per SEF Audit 2.

34. EOR 048-1 noted that the Evaluators could not find evidence of functional testing to check that the audit event AUE_IOCTL is generated as per SEF Audit 2 when ioctl(2TSOL) operates on network endpoints.

35. EOR 048-2 noted that the Evaluators could not find evidence of functional testing of the checks performed by kill(2TSOL) before sending out a signal, to cover part of the functionality for SEF DAC.9.

36. EOR 048-3 noted that the Evaluators could not find evidence of functional testing of the use of file_dac_read privileges to override the restriction on link(2TSOL) that the subject must have DAC read access to the object to which a link is being created.

37. EOR 051-2 noted that the Evaluators could not find evidence of functional testing to check that the proc_owner privilege allows a subject to open a process file which has the setUID or setGID bits set.

38. EOR 051-3 noted that the Evaluators could not find evidence of functional testing to check that if a process requires to read a window resource, read_window checks that the subject's user ID is equal to the resource's user ID or it has win_dac_read privilege.

39. EOR 051-5 noted that the Evaluators could not find evidence of functional testing to show that umount(2TSOL) checks that the subject owns the root directory of the file-system to be mounted or has the file_owner privilege, before unmounting the filesystem.

THIS PAGE IS INTENTIONALLY LEFT BLANK

III. CONCLUSIONS

Certification Results

40. After due consideration of the ETR [h], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that Trusted Solaris Version 2.5.1 running on Sun Ultra SPARC-1 workstations in networked mode, meets the requirements of ITSEC Assurance Level E3 and Functionality Classes F-B1 and F-C2, with a minimum SoM of Medium for user generated passwords and a minimum SoM of High for system generated passwords.

41. The Evaluators did not identify any exploitable vulnerabilities associated with the use of the TOE beyond 2000 AD.

Recommendations

42. The product should only be used in accordance with the intended environment and method of use described in the Security Target [c]. Particular care should be taken that the product is configured and used in accordance with the operational documentation [l, m, n].

43. Potential users of the product should understand the specific scope of the Certification by reading this report in conjunction with the Security Target [c]. Only the relevant evaluated product network configuration should be installed.

THIS PAGE IS INTENTIONALLY LEFT BLANK

ANNEX A: SUMMARY OF THE SECURITY TARGET

Introduction

1. The Security Target is given in [c]. The Product Rationale is summarised below.

Product Rationale

Intended Method of Use

2. Trusted Solaris 2.5.1 is intended for use in organisations who need to safeguard sensitive information and who require security features unavailable in standard commercial operating environments.

3. Trusted Solaris allows both the system and individual users to be configured either as single or multi-level. The appearance that Trusted Solaris 2.5.1 presents to users can also be configured, as it is possible to enable or disable the display of both information labels and sensitivity labels (on a per user basis). It should be noted however, that even with sensitivity labels disabled, the underlying security mechanisms uphold the multi-level security policy even though the user is unaware of it. Thus, Trusted Solaris 2.5.1 can be configured to appear to end users as, for example a multi-level F-B1 system or a system-high F-C2 system.

Method of Use Assumptions

4. The Security Target [c] lists 31 physical and procedural measures that are required to maintain security of the Trusted Solaris 2.5.1 product. It also warns that this is not a complete list, as specific measures may be required for different configurations and sites.

Assumed Threats

5. The threats are addressed in terms of the three modes of operation F-C2, F-C2 with advisory labels and F-B1.

a. F-C2

- Access to information for which a user does not have a need to know.
- Access by an unauthorised user to the system.
- Unauthorised modification or destruction of information.
- Unauthorised use of privileged facilities.
- Attempts to circumvent or modify TCB mechanisms.

- Abuse of trust/privilege by an authorised user.
- Attempts to breach the security policy go undetected.
- Masquerade of an insecure system as an authorised system to the user.

b. F-C2 with Advisory Labels

- Incorrect labelling of information within the system.
- Incorrect labelling of imported and exported information.
- Over classification of information by users.
- Unauthorised downgrading of information.

c. F-B1

- Access to information for which a user is not cleared.

Summary of Security Features

6. The Security Target [c] specifies a combined total of 115 SEFs for the following security features:

Access Control

7. Trusted Solaris 2.5.1 assigns Sensitivity Labels to objects (e.g. user processes and files), and these labels are used as the basis for Mandatory Access Control (MAC).

8. Trusted Solaris 2.5.1 assigns Information Labels to the information itself. These labels are adjusted automatically as the information changes.

9. In Trusted Solaris 2.5.1, Discretionary Access Control (DAC) restricts access to objects, such as files and is based on Access Control Lists and the standard UNIX permissions for user, group and others.

Privileges and Authorisation

10. Privileges are applied to programs (files) and are granted to a process when it executes the program. This allows user processes to be granted the minimum set of privileges to perform superuser tasks - the principle of least privilege.

11. Authorisations apply to users, and when granted will allow a user to assume a trusted facility management role or to perform an action that would otherwise be prohibited by the security policy.

Trusted Facility Management and Roles

12. Trusted Solaris 2.5.1 provides a number of trusted applications that allow for the creation of users; configuring of user security parameters; configuration of system security parameters; and the creation and maintenance of authorisations and user roles.

Auditing

13. Trusted Solaris 2.5.1 can record a range of audit data including the date and time of an event, user name, security attributes of files and whether the event was successful or not.

Multi-Level Secure Window Environment

14. Users interact with Trusted Solaris 2.5.1 through a multi-level secure window system based on the Common Desktop Environment (CDE). The CDE includes Information and Sensitivity labels on each window and a trusted path indicator to provide assurance that the user is interacting with a critical function. In addition, a number of CDE applications have been made security aware to enhance their operation under Trusted Solaris 2.5.1.

Network Security

15. Trusted Solaris 2.5.1 treats the system of work stations and servers linked together as a single security environment.

16. Trusted Solaris 2.5.1 utilises the Network Information Service (NIS+) which centrally stores and maintains the system-wide configuration data. It supports the internal network protocol, TSOL, to optimise internetworking of Trusted Solaris 2.5.1 workstations.

17. The Trusted Solaris 2.5.1 implementation of Network File System (NFS) provides transparent access to remote files while enforcing MAC and DAC and propagating security attributes.

Target Assurance Level

18. The Target Assurance Level for the product, as defined in the Security Target [c], was E3 as defined in ITSEC [d].

Target Functionality Class

19. The Target Functionality Classes for the product, as defined in the Security Target [c], were F-B1 and F-C2.

Claimed Minimum Strength of Mechanisms

20. The minimum SoM claimed for the product was Medium for the password mechanism using user generated passwords and High for system generated passwords.

ANNEX B: EVALUATED CONFIGURATION

Hardware

1. The evaluation results apply to the following platforms:

   a. Ultra Sparc 140 running at 167 MHz
   64 MB memory
   1 GB disk

   b. Ultra Sparc 140 running at 167 MHz
   64 MB memory
   1 GB disk
   UltraWide SCSI 4GB external disk
   UltraWide SCSI external CD-ROM
   UltraWide SCSI external QIC tape drive

Firmware

2. The TOE has the following firmware component :
   OpenBoot PROM version 3.5.0, 1997/01/06 18:05 with POST 3.10.6, 1996/10/18 10:19

Software

3. The TOE consists of Trusted Solaris Version 2.5.1. CD part no. 704-8118-10 Revision 50.

THIS PAGE IS INTENTIONALLY LEFT BLANK