UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P199

Tru64 Unix 5.1A

Issue 1.0

February 2004

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

**ARRANGEMENT ON THE
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

Hewlett Packard Tru64 Unix (5.1A) is a multi-user operating system to be used for general purpose computing services, offering FTP and Telnet services.

Tru64 Unix (5.1A with patch kit common_criteria_cert_t64v51a) 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 EAL1 for the specified Common Criteria Part 2 extended functionality (executing on a single AlphaServer and accessed via a console or local network) when running on the platforms specified in Annex A.

Originator	**CESG** Certifier
Approval and Authorisation	**CESG** Technical Manager of the Certification Body UK IT Security Evaluation and Certification Scheme
Date authorised	9th February 2004

(This page is intentionally left blank)

TABLE OF CONTENTS

(This page is intentionally left blank)

ABBREVIATIONS

CAPP	Controlled Access Protection Profile
CC	Common Criteria
CEM	Common Evaluation Methodology
CESG	Communications-Electronics Security Group
CLEF	Commercial Evaluation Facility
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OSP	Organizational Security Policy
SFR	Security Functional Requirement
SoF	Strength of Functions
TOE	Target of Evaluation
UKSP	United Kingdom Scheme Publication

(This page is intentionally left blank)

REFERENCES

a. Security Target Tru64 UNIX (Version 5.1A), Hewlett Packard, Version 07, 28 January 2004

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

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

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

e. Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 4.0, February 2000.

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

g. 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.

h. Evaluation Technical Report, LogicaCMG Camberley, 117272/T6/1, October 2003.

i. Report on Additional Testing and a Discussion of Outstanding Matters, Reference 117272/T4.1/7, 9 January 2004

j. Controlled Access Protection Profile, NSA, Version 1.d, 8 October 1999

k. Evaluated Configuration for Version 5.1A, Tru64 UNIX Version 5.1A, January 2004, Hewlett-Packard Company, Version 10.

l. Compaq Tru64 UNIX Installation Guide, Part Number AA-RH8SD-TE, June 2001, Compaq Computer Corporation.

(This page is intentionally left blank)

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria security evaluation of Tru64 Unix (version 5.1A) to the Sponsor, Hewlett Packard, 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 a] which specifies the functional, environmental and assurance evaluation requirements.

Evaluated Product

3. The version of the product evaluated was 5.1A with patch kit:

    common_criteria_cert_t64v51a.

4. This product is also described in this report as the Target of Evaluation (TOE). The Developer was Hewlett Packard.

5. The TOE is a multi-user UNIX operating system to be used for general purpose computing services and executes on a single HP Alphaserver. The target environment is as a server providing applications support and secure file storage. Within the scope of this evaluation the only direct access to the TOE is via the console and a local network. The local network itself is assumed to be subject to appropriate security procedures but these are out of scope of the TOE.

6. The TOE offers FTP and Telnet services, constrained by the TOE's user authentication security functions, to unspecified clients connected via the network interfaces offered by the TOE.

7. Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

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

TOE Scope

9. The TOE is an 'evaluated configuration' of the product and the 'evaluated configuration guide' [k] must be followed exactly for this certification to be applicable. The guide explains how to constrain the system and some of these constraints are summarised here (but refer to the guide itself for the details).

10. The system console must be kept physically secure, with access being limited to authorised administrators. Administrators must not rely on setting password protection for root console access on reboot. The operating system must be patched (with common_criteria_cert_t64v51a) and policies set for passwords, auditing etc.

11. For incoming packets, the 'inetd' daemon must be configured only to respond to requests for Telnet & FTP services. The network, including clients of FTP & Telnet, is out of scope of the evaluation (but is assumed to be constrained by a similar security policy to that of the TOE, with the network users being accountable for their actions).

12. Administrators should take particular note of specific instructions in the evaluated configuration guide. For example, taking care that duplicate user IDs are not issued and (when changing users' passwords) not using the password button on the dxaccounts window.

13. Unwanted daemons, such as those for remote admin, SNMP and sendmail must be disabled.

14. X-Windows is configured as the graphical interface on the physically secure console, with remote sessions disabled.

Protection Profile Conformance

15. The Security Target [a] did not claim conformance to any protection profile.

Assurance

16. The Security Target [a] specified the assurance requirements for the evaluation. Predefined evaluation assurance level EAL1 was used. Common Criteria Part 3 [d] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1 [b].

Strength of Function Claims

17. No strength of function was claimed in the Security Target (and this is not required at EAL1) but the Evaluated Configuration Guide [k] does include details of minimum password lengths, maximum number of unsuccessful attempts etc.

Security Policy

18. The TOE security policies are detailed in the Security Target [a].

Security Claims

19. The Security Target [a] fully specifies the TOE's security objectives, the Organizational Security Policies (OSPs) which these objectives meet and Security Functional Requirements (SFRs) and security functions to elaborate the objectives. Most of the SFRs are taken from CC Part 2 [c]; use of this standard facilitates comparison with other evaluated products.

20. Some SFRs have modifications as defined in the CAPP [j]. The ST followed much of CAPP although full compliance was not claimed.

Evaluation Conduct

21. 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 [e, f]. 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.

22. The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [a], 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 [d] and the Common Evaluation Methodology (CEM) [g].

23. The Certification Body monitored the evaluation which was carried out by the Logica-CMG Commercial Evaluation Facility (CLEF). The evaluation was completed when the CLEF submitted the Evaluation Technical Report (ETR) [h] to the Certification Body in November, 2003. Following the CLEF response to a request for further information and further testing, the Certification Body then produced this Certification Report.

General Points

24. The evaluation addressed the security functionality claimed in the Security Target [a] 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.

25. 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.

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

(This page is intentionally left blank)

II. EVALUATION FINDINGS

Introduction

27. The evaluation addressed the requirements specified in the Security Target [a]. The results of this work were reported in the ETR [h] and in additional report [i] under the CC Part 3 [d] headings. The following sections note considerations that are of particular relevance to consumers.

Delivery

28. The consumer should ensure that version 5.1A is requested. On receipt of the TOE, it is recommended that the consumer checks that the evaluated version has been supplied. Also, whilst EAL1 does not require evaluation of delivery mechanisms, it is recommended that the consumer checks for obvious signs of compromise.

Installation and Guidance Documentation

29. The installation guide [l] and the evaluated configuration guide [k] should be consulted by administrators installing the TOE. Man pages are available for users and the Security Manual and Sys Admin guide can be found at:

http://h30097.www3.hp.com/docs/

Strength of Function

30. No strength of function was claimed (see above under "Strength of Function Claims"). However, constraints such as minimum password lengths were tested as part of the evaluation (Annex B).

(This page is intentionally left blank)

III. EVALUATION OUTCOME

Certification Result

31. After due consideration of the ETR [h, i], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that Tru64 Version 5.1A (with patch: common_criteria_cert_t64v51a) running on AlphaServer platforms meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL1 for the specified Common Criteria Part 2 extended functionality, in the specified environment, when running on the platforms specified in Annex A, when constrained and configured as described in the evaluated configuration guide [k].

Recommendations

32. Prospective consumers of Tru64 Version 5.1A, should understand the specific scope of the certification by reading this report in conjunction with the Security Target [a]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

33. 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’.

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

(This page is intentionally left blank)

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1. The TOE consists of: The Tru64 Unix 5.1A operating system, supplied on CD (QA-6ADAA-H8) plus the patch:

   common_criteria_cert_t64v51a

TOE Documentation

2. The supporting guidance documents evaluated were: the installation guide [l] and the evaluated configuration guide [k].

TOE Configuration

3. This was covered by the earlier section on 'TOE scope' and by [k].

Environmental Configuration

4. Details of the hardware platforms used for testing are given in Annex C.

(This page is intentionally left blank)

ANNEX B: PRODUCT SECURITY ARCHITECTURE

1. This annex gives an overview of the main product architectural features that are relevant to the security of the TOE. Other details of the scope of evaluation are given in the main body of the report and in Annex A. The TOE security architecture is described in more detail in the Security Target [a], see this for more information.

Architectural Features

Subjects, Sessions & Privileges

2. A subject is an active entity generally in the form of a user process, it has a number of attributes associated with it, which are used by the TOE to control a user's access (privileges) via sessions and to enforce the TOE's security policies.

3. A user gains initial access to the product via a login, which involves authentication. A successful login results in the creation of a session, which consists of a group of processes (with appropriate attributes). After login, further sessions may be created (e.g. background jobs), which will inherit key security attributes from their parent session. A process with 'super-user' status is not constrained by the TOE's security policies.

4. Processes are associated with users, and this is used for auditing, which gives accountability of users.

Objects & Access Permissions

5. Objects are passive objects with access permissions defined for users and groups of users. Examples include: directories, files, pipes, symbolic links, devices, shared memory, message queues and semaphore sets. Note that DEC Windows objects are not included in the evaluated configuration and hence were not considered by the evaluation of the product.

6. Each object has an associated Access Control List (ACL) described in a bit more detail below.

Design Subsystems

Identification & Authentication

7. Attributes relating to user authentication are stored in the Protected Password Authentication database. Attributes relating to group membership are also stored within the filesystem.

8. Passwords must be at least 8 characters long in the evaluated configuration (with triviality checks) and a maximum of 5 attempts is set before the account is locked. The response to an invalid username and password is the same as for a valid username and invalid password.

Access Control

9. The TOE shall ensure that an Access Control List is associated with each object (subject to Discretionary Access Control). This consists of one or more entries that determine which users and groups can access the object, with each entry defining read, write and execute permissions. The ACL is checked before any subject makes a request to perform an action on an object.

Audit

10. The TOE maintains an audit trail in a standard file (protected as described as above). The super-user is responsible for determining what is written to (and read from) the audit trail. The minimum set of audit data to be collected is described in the Security Target [a].

Object re-use

11. When an object is initially assigned, allocated or reallocated to a subject from the TOE's pool of unused objects, the TOE ensures that the object contains no information for which the subject is not authorised.

12. Memory is cleared before being allocated to a process. Likewise, parts of files that have not previously been written to will either not be readable or will be cleared before access.

Hardware and Firmware Dependencies

13. The TOE implements its memory separation policy using standard hardware features.

ANNEX C: PRODUCT TESTING

IT Product Testing

1. All security relevant design sub-systems were tested i.e. Identification & Authentication, Access Control, Audit and Object Reuse. The tests were an independent verification of a subset of developer tests (as required for EAL1). No vulnerabilities were found. Although there were a few minor inconsistencies, these are not relevant if the instructions in the evaluated configuration guide [k] is followed.

Platform Issues

3. The developer provided a multi-platform rationale, which explained how the results of this evaluation are applicable to a subset of supported platforms. This subset is as follows:

AlphaServer platforms: 300, 400, 800, 1000, 1000A, 1200, 2000, 2100, 2100A, 4000, 4100, 8200, 8400, DS10, DS10L, DS20, DS20E, ES40, ES45, GS60E, GS80, GS140, GS160, GS320. The following platforms are limited to single partition use: GS80, GS160 and GS320.

An independent verification of a selection of developer tests was carried out using a DS20E Alphastation with 2x EV67 processors (667 MHz), 8MB Cache and 1 GB RAM. Network interface tests were carried out using an ES45 Alphaserver with 4x EV68 processors (1 GHz), 8MB cache, 16 GB RAM.

(This page is intentionally left blank)