COMMON CRITERIA CERTIFICATION REPORT No. P176

Hewlett-Packard HP-UX (11i)

Version 11.11
September 2001 release with specified patches
running on HP 9000 platforms

Issue 1.0

February 2003

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

EAL4
CAPP

HP-UX (11i)
Version 11.11
September 2001 release with specified patches
running on HP 9000 platforms

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.

HP-UX (11i)   **EAL4**
Version 11.11   **CAPP**
September 2001 release with specified patches
running on HP 9000 platforms

CERTIFICATION STATEMENT

Hewlett Packard's HP-UX Version 11.11 is Hewlett Packard's implementation of UNIX. The product may execute on a single HP 9000 server or be connected to other HP 9000 servers executing identical versions of the product to form a local distributed system.

HP-UX Version 11.11 September 2001 release with specified patches 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, when running on HP 9000 platforms as specified in Annex A. It has also met the requirements of the Controlled Access Protection Profile.

Originator	**CESG** Certifier
Approval and Authorisation	**CESG** Technical Manager of the Certification Body
Date authorised	28 February 2003

EAL4
CAPP

HP-UX (11i)
Version 11.11
September 2001 release with specified patches
running on HP 9000 platforms

(This page is intentionally blank)

HP-UX (11i)
Version 11.11
September 2001 release with specified patches
running on HP 9000 platforms

EAL4
CAPP

TABLE OF CONTENTS

EAL4
CAPP

HP-UX (11i)
Version 11.11
September 2001 release with specified patches
running on HP 9000 platforms

(This page is intentionally blank)

HP-UX (11i)   **EAL4**
Version 11.11   **CAPP**
September 2001 release with specified patches
running on HP 9000 platforms

ABBREVIATIONS

ACL	Access Control List
CAPP	Controlled Access Protection Profile
CC	Common Criteria
CCIMB	Common Criteria Interpretation Management Board
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
FSO	File System Object
HFS	High-speed File System
HP	Hewlett Packard
ITSEC	Information Technology Security Evaluation Criteria
JFS	Journalled File System
NFS	Network File System
NIS	Network Information Service
OSP	Organisational Security Policy
PAM	Pluggable Authentication Module
PA-RISC	Precision Architecture - Reduced Instruction Set Computer
SAM	System Administration Manager
SFR	Security Functional Requirement
SOF	Strength of Function
TCB	Trusted Computing Base
TCSEC	Trusted Computer System Evaluation Criteria
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
UKSP	United Kingdom Scheme Publication

EAL4
CAPP

HP-UX (11i)
Version 11.11
September 2001 release with specified patches
running on HP 9000 platforms

(This page is intentionally blank)

HP-UX (11i)   **EAL4**
Version 11.11   **CAPP**
September 2001 release with specified patches
running on HP 9000 platforms

REFERENCES

a.   HP-UX Version 11.11 Security Target,
      Hewlett Packard Limited,
      HPUX11CC-TR-01, Issue 4.0, September 2002.

b.   Common Criteria for Information Technology Security Evaluation,
      Part 1: Introduction and General Model,
      Common Criteria Interpretation Management Board,
      CCIMB-99-031, Version 2.1, August 1999.

c.   Common Criteria for Information Technology Security Evaluation,
      Part 2: Security Functional Requirements,
      Common Criteria Interpretation Management Board,
      CCIMB-99-032, Version 2.1, August 1999.

d.   Common Criteria for Information Technology Security Evaluation,
      Part 3: Security Assurance Requirements,
      Common Criteria Interpretation Management Board,
      CCIMB-99-033, Version 2.1, August 1999.

e.   Controlled Access Protection Profile,
      US National Security Agency,
      Version 1.d, 8 October 1999.

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

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

h.   Common Methodology for Information Technology Security Evaluation,
      Part 2: Evaluation Methodology,
      Common Evaluation Methodology Editorial Board,
      CEM-99/045, Version 1.0, August 1999.

i.   Evaluation Technical Report, HP-UX Version 11.11,
      CMG CLEF,
      111761/T53/1, Issue 1.0, September 2002.

j.   Certification Report 97/76, HP-UX Version 10.10
      UK IT Evaluation and Certification Scheme,
      Issue 1.0, January 1997.

EAL4
CAPP

HP-UX (11i)
Version 11.11
September 2001 release with specified patches
running on HP 9000 platforms

k.   Certification Report No. P111, HP-UX Version 10.20,
        UK IT Evaluation and Certification Scheme,
        Issue 1.0, February 1999.

l.   Evaluation Technical Report, HP-UX Version 10.10,
        Admiral Management Services Ltd,
        5295C/T8.15/1, Issue 1.0, December 1996.

m.   Evaluation Technical Report, Annex I, HP-UX Version 10.20,
        Admiral Management Services Ltd,
        7115A/T15/1, Issue 1.0, December 1998.

n.   UKSP 14 Addendum: EAL4 Delta Evaluation,
        UK IT Security Evaluation and Certification Scheme,
        Issue 2.C, 21 March 2000.

o.   Trusted Delivery,
        Hewlett Packard,
        Version 2.0, 8 August 1996.

p.   HP-UX 11*i* Installation and Update Guide,
        Hewlett Packard,
        5185-6511, Edition 3, September 2001.

q.   Common Criteria HP-UX 11*i* Evaluated Configuration Guide,
        Hewlett Packard,
        5990-3527, Edition 8, November 2002.

r.   Managing Systems and Workgroups: A Guide for HP-UX System Administrators,
        Hewlett Packard,
        B2355-90742, Edition 5, June 2001.

s.   Using HP-UX,
        Hewlett Packard,
        B2355-90164, Edition 1, December 2000.

t.   Multi-Platform Rationale,
        Hewlett Packard,
        HPUX11CC-TN-01, Issue 1.0, 12 February 2002

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

v.   Strength of Function Analysis,
        Hewlett Packard,
        HPUX11CC-TP-01, 15 May 2002.

HP-UX (11i)   **EAL4**
Version 11.11   **CAPP**
September 2001 release with specified patches
running on HP 9000 platforms

I.   EXECUTIVE SUMMARY

Introduction

1.   This Certification Report states the outcome of the Common Criteria (CC) security evaluation of HP-UX Version 11.11 to the Sponsor, Hewlett Packard Limited, 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 :

     HP-UX Version 11.11 September 2001 release with the patches identified in Annex A

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

4.   HP-UX Version 11.11 is Hewlett-Parkard's implementation of UNIX. When running in an 'evaluated configuration' (as described in paragraph 2.2 of the Security Target [a]), it meets the requirements of the CC Controlled Access Protection Profile (CAPP) [e], which is equivalent to class C2 of the Trusted Computer System Evaluation Criteria (TCSEC) [u].

5.   Annex A provides details of the evaluated configuration of the TOE.

6.   Annex B provides an overview of the TOE's security architecture.

TOE Scope

7.   Section 2.2 of the Security Target [a] provided details of an 'evaluated configuration' of HP-UX Version 11.11. In summary:

     a.   the TOE executes on any single 64-bit computer system from the family of HP 9000 servers (for a fuller discussion of the consideration given to hardware platforms see 'Platform Issues' below);

     b.   the TOE supports user interaction via any of the supported Shells (including the POSIX, Bourne, C and Korn Shells);

     c.   The TOE supports the HFS and JFS file systems;

     d.   the TOE includes Pluggable Authentication Modules (PAM) with default configuration for authentication consisting of user identity and password;

EAL4   **HP-UX (11i)**
CAPP   **Version 11.11**
September 2001 release with specified patches
running on HP 9000 platforms

e.   the TOE executes with HP-VUE and X-Windows disabled and excludes the use of a restricted configuration of the System Administration Manager (SAM);

f.   the TOE includes socket based network functions and the following network applications (other network applications, such as NFS and NIS are excluded):

- ftp(1)
- rexec(1)
- rlogin(1)
- telnet(1)

8.   The following are excluded from the evaluation:

a.   The Online JFS file system;

b.   HP-VUE;

c.   X-Windows; and

d.   network applications other than those listed at paragraph 7.f above.

9.   The version of the TOE that was subject to evaluation was HP-UX 11.11 September 2001 release with patches identified in Annex A. The evaluated configuration of the TOE is described in Annex A.

Protection Profile Conformance

10.   The Security Target [a] claimed conformance to CAPP [e].

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

Assurance

12.   The Security Target [a] specified the assurance requirements for the evaluation. The predefined Evaluation Assurance Level EAL4 was used. CC Part 3 [d] describes an increasing 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

13.   The Security Target [a] states that the claimed minimum Strength of Function (SOF) for the password-checking mechanism is SOF-medium. Section 8.2.5 of the Security Target states that this claim is consistent with the CAPP [e] Security Functional Requirement (SFR) FIA_SOS.1 as justified in CAPP Section 7.5.

14.   The CAPP [e] security functional requirement FIA_SOS.1 states that the password-checking mechanism should meet the following:

HP-UX (11i)   **EAL4**
Version 11.11   **CAPP**
September 2001 release with specified patches
running on HP 9000 platforms

    a.   For each attempt to use the authentication mechanism, the probability that a random attempt will succeed is less than one in 1,000,000;

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

    c.   Any feedback given during an attempt to use the authentication mechanism will not reduce the probability below the above metrics.

15.   The password-checking mechanism is the only security mechanism for which a SOF claim is made in the Security Target [a].

16.   In addition, the Security Target (paragraph 6.3) states that the product implements a modified one-way DES algorithm to satisfy the password encryption algorithm specified. This cryptographic mechanism is publicly known and as such it is the policy of the national authority for cryptographic mechanisms, CESG, not to comment on its appropriateness or strength.

Security Policy

17.   The TOE security policy is provided in the Security Target [a].

18.   The Security Target [a] states the Organisational Security Policies (OSPs) for the TOE, as follows, and states that they are fully conformant with CAPP [e]:

    a.   P.AUTHORIZED_USERS

    b.   P.NEED_TO_KNOW

    c.   P.ACCOUNTABILITY.

Security Claims

19.   The Security Target [a] fully specifies the TOE's security objectives, the OSPs which these objectives support and the SFRs and TOE Security Functions (TSF) to elaborate the objectives.

20.   All of the SFRs are taken from CAPP [e]. CAPP draws its SFRs from CC Part 2 [c] with some deviations, including extensions, applied that are described as 'Notes' in Section 8 of CAPP; use of CC Part 2 facilitates comparison with other evaluated products.

21.   The Security Target [a] makes security functionality claims for the TSF grouped under the following categories:

- identification and authentication
- access control
- audit
- object reuse
- protection functions.

EAL4

CAPP

HP-UX (11i)
Version 11.11
September 2001 release with specified patches
running on HP 9000 platforms

Evaluation Conduct

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

23.   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 that baseline.

24.   Both parts of the evaluation were performed in accordance with CC Part 3 [d], the Common Evaluation Methodology (CEM) [h] and the appropriate Common Criteria Interpretation Management Board (CCIMB) interpretations.

25.   HP-UX had been evaluated and certified, previously, to ITSEC assurance level E3 both at Version 10.10 [j] and then at Version 10.20 [k]. The TOE is derived from HP-UX Version 10.20 and while there are a number of new Security Functions, many of the Security Functions remained unchanged from previous versions of the product. Accordingly, the Evaluators made use of previous evaluation results where possible. For this evaluation of HP-UX Version 11.11, the Evaluators addressed every CEM [h] EAL4 work unit but made use (with guidance provided in [n]) of the evaluation results [l, m] from the ITSEC E3 evaluations where these were valid for the CEM requirements.

26.   The Certification Body monitored the evaluation, which was performed by the CMG Commercial Evaluation Facility (CLEF). The evaluation was completed when the CLEF submitted the Evaluation Technical Report (ETR) [i] to the Certification Body in September 2002. The Certification Body then produced this Certification Report.

General Points

27.   The evaluation addressed the security functionality claimed in the Security Target [a] with reference to the assumed operating environment specified by the Security Target.

28.   The evaluated configuration is specified in Annex A. Prospective consumers are advised to check that it matches their identified requirements and to give due consideration to the recommendations and caveats of this Certification Report.

29.   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

HP-UX (11i)   **EAL4**
Version 11.11   **CAPP**
September 2001 release with specified patches
running on HP 9000 platforms

associated patches exist for the product and whether such patches have been evaluated and certified.

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

EAL4
CAPP

HP-UX (11i)
Version 11.11
September 2001 release with specified patches
running on HP 9000 platforms

(This page is intentionally blank)

HP-UX (11i)   **EAL4**
Version 11.11   **CAPP**
September 2001 release with specified patches
running on HP 9000 platforms

II. EVALUATION FINDINGS

Introduction

31.   The evaluation addressed the requirements specified in the Security Target [a]. The results of this work were reported in the ETR [i] under the CC Part 3 [d] headings.

32.   The following sections note considerations of particular relevance to either consumers or those involved with the subsequent assurance maintenance and re-evaluation of the TOE.

Delivery

33.   Secure delivery of the TOE is described in the Delivery Procedures [o] (available from HP), which describe the process of releasing the TOE to consumers.

34.   After the consumer places an order for the product, the consumer is sent a letter confirming the order. This letter contains a unique security handle. The consumer contacts HP with this handle, which is checked prior to shipping the CD to the consumer. With the CD is a letter on HP-headed notepaper which contains full details of the CD and of the security handle. The CD is sent securely shrink-wrapped by trusted couriers.

35.   Patches may be sent out to consumers using the trusted delivery procedures described above or they may be downloaded from the HP support website. The website requires a user ID and password. Note, however, that there is no inherent security in the download of patches from the HP support website and consumers are recommended to request delivery of the patches from HP using the trusted procedure described for delivery of the operating system.

36.   On receiving the TOE, the consumer is recommended to check that it is the evaluated version and to check that the security of the TOE has not been compromised during delivery.

Installation and Guidance Documentation

37.   Secure installation, generation and startup of the TOE are described in the Installation and Update Guide [p], the Common Criteria Evaluated Configuration Guide [q], and the Administrator Guide [r].

38.   The Evaluated Configuration Guide [q] should be read first, as it details the steps that must be followed to install the TOE in its evaluated configuration. The Evaluated Configuration Guide references out to the Installation and Update Guide [p] and the Administrator Guide [r], as appropriate.

39.   When the installation of the TOE is complete, the Man Pages can then be accessed.

40.   Administrator guidance for the TOE is provided in the Installation and Update Guide [p], the Common Criteria Evaluated Configuration Guide [q], the Administrator Guide [r] and the Man Pages. User guidance is provided in [s].

EAL4
CAPP

HP-UX (11i)
Version 11.11
September 2001 release with specified patches
running on HP 9000 platforms

Strength of Function

41.   The SOF claim for the TOE is identified above under the heading 'Strength of Function Claims'.

42.   Based on their examination of all the evaluation deliverables, the Evaluators confirmed that there were no other probabilistic or permutational mechanisms in the TOE.

43.   The Evaluators examined the assertions, assumptions and analysis presented in the Developer's Strength of Function Analysis [v] and confirmed that the SOF claim of SOF-medium for the TOE is upheld.

Vulnerability Analysis

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

Platform Issues

45.   The TOE was tested on the hardware platforms specified in Annex A.

46.   In addition, the Evaluators confirmed their agreement with the Developer's Multi-platform rationale [t] that the results of the evaluation would be applicable to other hardware platforms. As a result of their examination of this rationale, the Evaluators considered the evaluation outcome should apply to all of the additional platforms identified in paragraph 11 of Annex A.

47.   All of the platforms identified in the Developer's Multi-platform rationale [t] are based on HP's Precision Architecture - Reduced Instruction Set Computer (PA-RISC) architecture version 2.0. The hardware in the HP 9000 platforms varies according to the processor version, processor speed, number of processors, amount of memory, I/O expandability, I/O buses and types of I/O adapters as allowed by the PA-RISC architecture. The Developer's Multi-platform rationale discusses each of these hardware variations in the context of the assurance requirements and provides justification that none of the variations affect the evaluation results.

HP-UX (11i)   **EAL4**
Version 11.11   **CAPP**
September 2001 release with specified patches
running on HP 9000 platforms

III. EVALUATION OUTCOME

Certification Result

48.   After due consideration of the ETR [i] produced by the Evaluators, and the conduct of the evaluation as witnessed by the Certifier, the Certification Body has determined that the TOE meets the CC Part 3 [d] conformant requirements of Evaluation Assurance Level EAL4, for the specified CC Part 2 [c] extended functionality, when running on HP 9000 platforms as specified in Annex A. It has also met the requirements of the Controlled Access Protection Profile [e].

49.   The Certification Body has also determined that the TOE meets the minimum SOF claim of SOF-medium for the password-checking mechanism given above under the heading 'Strength of Function Claims'.

Recommendations

50.   Prospective consumers of the TOE should understand the specific scope of the certification by reading this report in conjunction with the Security Target [a].

51.   The TOE should be used in accordance with a number of environmental considerations, as specified in the Security Target [a].

52.   The TOE should be delivered, installed, configured and used in accordance with the supporting guidance documentation [o - s] included in the evaluated configuration.

53.   Only the evaluated TOE configuration should be installed.   That for which EAL4 assurance has been demonstrated is specified in Annex A, with further relevant information given above under the headings 'TOE Scope' and 'Evaluation Findings' above.

54.   Prospective consumers, and authorised administrators should be aware of certain issues arising from the use, on the TOE, of POSIX-compliant utilities that do not handle all security attributes. This arises from the fact that the TOE is a POSIX-compliant UNIX operating system with added security features. As noted in [q, section 7.7], whilst a large number of POSIX-compliant programs will work adequately, legacy programs that are unaware of the security features in the TOE and, so, may harm the configuration of the system. See, also, [r] for more details.

EAL4
CAPP

HP-UX (11i)
Version 11.11
September 2001 release with specified patches
running on HP 9000 platforms

(This page is intentionally blank)

HP-UX (11i)   **EAL4**
Version 11.11   **CAPP**
September 2001 release with specified patches
running on HP 9000 platforms   **Annex A**

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1.   The TOE is uniquely identified as:

HP-UX Version 11.11 September 2001 release with the patches identified in Table A1.

TOE Documentation

2.   The guidance documents evaluated were:

- Trusted Delivery [o]
- HP-UX 11i Installation and Update Guide [p]
- Common Criteria HP-UX 11*i* Evaluated Configuration Guide [q]
- Managing Systems and Workgroups: A Guide for HP-UX System Administrators [r].
- Using HP-UX [s]

3.   Further discussion of the guidance documents is provided above under the heading 'Installation and Guidance Documentation'.

TOE Configuration

4.   The TOE should be configured in accordance with the guidance documents [p - r] identified in paragraph 2 above.

Environmental Configuration

5.   Details of the TOE's environmental configuration are provided in Section 2.2 of the Security Target [a] and summarised above under the heading 'TOE Scope'.

6.   Further details of the hardware requirements are provided in Annex B under the heading 'Hardware and Firmware Dependencies'.

7.   The Evaluators performed their independent testing of the TOE on the following hardware platforms:

a.   Hewlett-Packard HP 9000 server rp5400 (L1000):

- PA8500 1.5MB cache 360 MHz CPU
- 256 MB RAM
- 18.2 GByte hard disk

b.   Hewlett-Packard HP 9000 server rp5400 (L1000):

- 2 x PA8500 1.5MB cache 360 MHz CPU
- 256 MB RAM
- 18.2 GByte hard disk

EAL4   **HP-UX (11i)**
CAPP   **Version 11.11**
                                   September 2001 release with specified patches
Annex A   **running on HP 9000 platforms**

8.   During the Evaluators' independent testing, the above machines were networked to allow testing of the network commands (*ftp*, *rexec*, *rlogin* and *telnet*) included within the TOE.

9.   The Developers conducted their testing on the hardware platforms identified in paragraph 7 above and on the following platforms:

   a.   Hewlett Packard HP 9000 server c3600:

   - PA8600 CPU, 552Mhz
   - 512MB RAM
   - 36 GB hard disk

   b.   Hewlett Packard HP 9000 server rp8400 (Keystone):

   - 2 * PA8700 CPU, 750Mhz
   - 512MB RAM
   - 36GB hard disk

10.   The version of the software that was used during the Developer's testing and during the Evaluators' independent testing and penetration testing was HP-UX 11.11 September 2001 release with the patches applied as identified in Table A-1.

11.   In addition, as discussed above under 'Platform Issues', the evaluation results were determined, through analysis, to hold for other HP 9000 servers. The complete list of HP 9000 servers for which the evaluation results hold is as follows::

   - rp2400 (A400), rp2450 (A500)
   - rp5400 (L1000), rp5430 (L1500), rp5450 (L2000), rp5470 (L3000)
   - rp7400 (N4000), rp7410
   - rp8400
   - Superdome
   - b2600, c3600, c3650, c3700
   - j5600, j6000, j6700

Patch Number	Version	Description
PHCO_22958	1.0	set_parms
PHCO_23083	1.0	newgrp(1) patch
PHCO_23263	B.11.11.15	HP AutoRAID Manager cumulative patch
PHCO_23333	1.0	LVM Virtual Array support
PHCO_23492	1.0	Kernsymtab Patch
PHCO_23510	1.0	gsp parser & dimm labels
PHCO_23774	1.0	Partition Commands cumulative patch
PHCO_23909	1.0	cu(1) patch
PHCO_23914	1.0	Enhancement support to Ultrium tape
PHCO_24173	1.0	ups_mond(1M) cumulative patch
PHCO_24777	1.0	mountall cumulative patch.
PHCO_24839	1.0	libpam_unix cumulative patch
PHCO_25111	1.0	lpspool subsystem cumulative patch

HP-UX (11i)   **EAL4**
Version 11.11   **CAPP**
September 2001 release with specified patches
running on HP 9000 platforms   **Annex A**

Patch Number	Version	Description
PHCO_25311	B.11.11.15	HP Array Manager/60 cumulative patch
PHCO_25831	1.0	SCSI Ultra160 driver Online Addition script
PHCO_25870	1.0	cumulative SAM patch
PHCO_25887	1.0	Software Distributor Cumulative Patch
PHCO_26061	1.0	Kernel configuration commands patch.
PHCO_26951	1.0	itemap support for FireGL graphics cards
PHCO_27018	1.0	ugm cumulative patch
PHCO_27049	1.0	audit(5) man page patch
PHCO_27694	1.0	login(1) cumulative patch
PHCO_27704	1.0	audisp(1M) cumulative patch
PHCO_27752	1.0	audevent(1M) cumulative patch
PHKL_22857	1.0	SCSI Tape (stape) cumulative
PHKL_23203	1.0	Invalid 32-bit I/O blocks moved to iospace.
PHKL_23246	1.0	MO dev 4K sector size errors & FIFO panic
PHKL_23290	1.0	system_space.h header file patch
PHKL_23292	1.0	scsi_surface.h header file patch
PHKL_23293	1.0	assert.h header file patch
PHKL_23294	1.0	buf.h header file patch
PHKL_23295	1.0	debug.h header file patch
PHKL_23296	1.0	dnlc.h header file patch
PHKL_23297	1.0	io.h header file patch
PHKL_23298	1.0	ki_iface.h header file patch
PHKL_23299	1.0	pfdat.h header file patch
PHKL_23300	1.0	proc_debug.h header file patch
PHKL_23301	1.0	proc_iface.h header file patch
PHKL_23302	1.0	rw_lock.h header file patch
PHKL_23303	1.0	sem_alpha.h header file patch
PHKL_23304	1.0	sem_beta.h header file patch
PHKL_23305	1.0	sem_sync.h header file patch
PHKL_23306	1.0	sem_utl.h header file patch
PHKL_23307	1.0	spinlock.h header file patch
PHKL_23308	1.0	vas.h header file patch
PHKL_23309	1.0	vfd.h header file patch
PHKL_23310	1.0	vnode.h header file patch
PHKL_23311	1.0	inode.h header file patch
PHKL_23312	1.0	pci.h header file patch
PHKL_23314	1.0	spinlock.h header file patch
PHKL_23315	1.0	cpu.h header file patch
PHKL_23316	1.0	map.h header file patch
PHKL_23335	1.0	solve inode deadlock with mmap and pagefault
PHKL_23423	1.0	improper core dump msg
PHKL_23505	1.0	Support for more than 10 SD IOX-cabinets
PHKL_23625	1.0	Fix initial clock sync for SD derivatives
PHKL_23626	1.0	Fibre Channel Mass Storage Patch
PHKL_23666	1.0	SCSI IO Subsystem Cumulative Patch
PHKL_23810	1.0	Enable SCSI floppy for 64 bit computers
PHKL_23957	1.0	Boot panic (w/Fiber Ch. & Gig. Ethernet) fix
PHKL_24278	1.0	Softpower enablement for bladed servers
PHKL_24626	1.0	Cumulative USB Driver patch
PHKL_24824	1.0	par fans, cabtype, sinc, hwpath, cell info
PHKL_25166	1.0	early boot,Psets,vPar,Xserver,T600 HPMC
PHKL_25218	1.0	PDC Call retry,PDC_SCSI_PARMS,iCOD hang fix
PHKL_25610	1.0	New audio h/w support + cumulative fixes

EAL4
CAPP

Annex A

HP-UX (11i)
Version 11.11
September 2001 release with specified patches
running on HP 9000 platforms

Patch Number	Version	Description
PHKL_25770	1.0	stape kernel tunable cumulative patch
PHKL_25896	1.0	SCSI IO Cumulative Patch
PHKL_26233	1.0	VM-JFS ddlock, mmap,thread perf, user limits
PHKL_26425	1.0	Cumulative DLKM module load/unload patch
PHKL_26833	1.0	FXE perf, server patch, cumulative graphics
PHKL_27025	1.0	SCSI Ultra160 Driver with OLAR support
PHKL_27151	1.0	Syslog,HighTempAlerts,vPar,IntrMigr,PCI-X
PHKL_27152	1.0	I/O Cumulative, PA 8700 2.2, vPar, PCI-X
PHKL_27153	1.0	PCI cumulative patch, HPMCat boot, PCI-X
PHKL_27154	1.0	PA-8800
PHKL_27155	1.0	PA-8800 TLB optimization
PHKL_27156	1.0	PA-8800 p2p_bcopy optimization
PHKL_27219	1.0	adjtime(2) support for cpu speeds over 1 GHz
PHKL_27225	1.0	IDE/ATAPI cumulative patch
PHKL_27737	1.0	Enable Posix IPC syscalls to be audited
PHKL_27753	1.0	audit subsystem cumulative patch
PHKL_27949	1.0	shm_lock scaling; shm_open-shm_unlink audit
PHNE_22722	1.0	NTP timeservices upgrade plus utilities
PHNE_23275	1.0	Bind 8.1.2 Patch
PHNE_23289	1.0	mux4.h header file patch
PHNE_23594	1.0	Cumulative Mux and Pty Patch
PHNE_24130	1.0	inetd(1M) cumulative patch
PHNE_24492	1.0	LAN product cumulative patch
PHNE_25084	1.0	Cmulative STREAMS Patch
PHNE_25184	1.0	sendmail(1m) 8.9.3 patch
PHNE_25644	1.0	cumulative ARPA Transport patch
PHNE_26388	1.0	ONC/NFS General Release/Performance Patch
PHNE_27765	1.0	ftpd(1M) patch
PHNE_27777	1.0	r-commands cumulative mega-patch
PHSS_22898	1.0	HP aC++ -AA runtime libraries (aCC A.03.30)
PHSS_25983	1.0	B1000/B2000/C3X00/J5X00/J6000/J7000 5.0 FW
PHSS_26138	1.0	OV EMANATE14.2 Agent Consolidated Patch
PHSS_26492	1.0	CDE Base Periodic Patch
PHSS_26493	1.0	CDE Applications Periodic Patch
PHSS_26577	1.0	Xserver cumulative patch
PHSS_26799	1.0	Tachyon TL Fibre Channel Driver Patch
PHSS_26947	1.0	EMS & HA Monitors (A.03.20.01) patch
PHSS_27182	1.0	OV EMANATE14.2 snmpdm - subagent handling
PHSS_27812	1.0	Support Tool Manager Sep 2002 Patch

Table A-1: patches applied to evaluated configuration

HP-UX (11i)   **EAL4**
Version 11.11   **CAPP**
September 2001 release with specified patches
running on HP 9000 platforms   **Annex B**

ANNEX B: PRODUCT SECURITY ARCHITECTURE

1.   This annex gives an overview of the product's main 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 this report and in Annex A.

Architectural Features

2.   The product may execute on a single HP 9000 Server or be connected to other HP 9000 Servers executing identical versions of the product to form a local distributed system.

3.   The product incorporates network functions but contains no network specific security requirements. Networking is covered only to the extent to which the product can be considered to be part of a centrally managed system that meets a common set of security requirements.

4.   The main security features of the product are:

- user identification and authentication
- discretionary access control (DAC), including access control lists
- auditing

Identification and Authentication

5.   All users of the product are authenticated and held accountable for their security related actions. Each user is uniquely identified by the product. The product records security related events and the user associated with the event.

6.   The product supports an ordinary *user* role and a *superuser* (administrative) role.

7.   A superuser has 'root privilege' and is not constrained by the product's security policies.

8.   An ordinary user does not have 'root privilege' and is constrained by the product's security policies.

9.   The product allows a superuser to associate individual users with a privileged group, thus permitting a process acting on the user's behalf to change the ownership of files.

10.   The authentication features are supported by constraints on user-generation of passwords and an encryption mechanism.

Discretionary Access Control

11.   All subjects are associated with an authenticated user identity, and all named objects are associated with identity-based protection attributes. These are used as the basis of DAC decisions, which control the access of subjects to objects.

12.   The product implements a DAC policy, which provides both the traditional UNIX 'owner', 'group', 'other' access mode permissions and a more granular Access Control List (ACL) mechanism, controlled by the object's owner.

EAL4
CAPP

HP-UX (11i)
Version 11.11
September 2001 release with specified patches
Annex B **running on HP 9000 platforms**

13. The product implements 2 independent ACL mechanisms:

- HFS ACLs for the HFS File System; and
- JFS ACLs for the JFS File System.

14. DAC is supported by object reuse mechanisms to ensure that information is not inadvertently transferred between subjects when objects are re-allocated.

Auditing

15. The product is capable of collecting audit records for all security relevant events that occur. A superuser may select the users and events for which audit data is collected from time to time.

16. Audit records may be viewed by a superuser selectively for any period on the basis of criteria such as user name, event type and outcome.

17. Facilities are provided to enable the superuser to manage audit log files and to ensure that audit data is retained during abnormal conditions. Note that audit records are buffered in memory before they are written to disk. In these cases it is likely that some of these records will be lost if the operation of the TOE is interrupted by hardware or power failures (see [a] paragraph 6.2.3.27).

Design Subsystems

18. The Trusted Computer Base is divided into Kernel and non-kernel software.

Kernel TCB

19. The entire kernel TCB executes in (hardware/privileged) kernel mode. This allows the kernel to execute privileged hardware instructions and perform low-level I/O. The kernel interface is via instruction trap. User/unprivileged processes call the trap instruction as an interface. There is no separate process that represents the kernel; rather, through the trap instruction, kernel functions are available to every process on the system.

20. The kernel TCB is a collection of distinct logical subsystems, and is summarized as follows:

a. Memory Management - Provides for access, allocation, deallocation, and control of all memory, for all processes, both kernel and non-kernel, within the system. Interfaces with the hardware for address translation, enabling memory sizes far in excess of actual hardware, for all processes. Further, this subsystem tracks all address space allocations to all processes, allows for the sharing of memory between processes, and prevents the sharing of memory between processes, thereby maintaining address space integrity.

b. Process Management - Initiates processes, allocates and deallocates system resources, tracks and manages all processes within the system from point of initiation

HP-UX (11i)   **EAL4**
Version 11.11   **CAPP**
September 2001 release with specified patches
running on HP 9000 platforms   **Annex B**

to final termination. This subsystem accomplishes the aforementioned for both kernel, and nonkernel processes.

c. File System and Device I/O - Provides for the creation, access, and manipulation of file system objects by non-TCB processes, and maintains device independence for end user applications. This component provides the interface for low-level device I/O drivers and non-TCB processes.

d. Inter Process Communications (IPC) Mechanisms - Facilitates synchronization of processes or events, and the sharing of information, between processes for both kernel and non-kernel processes.

e. Kernel Audit Support - Creates and writes Audit records for each of the user selected events and system calls to provide a complete audit trail of user space processes and services of the kernel TCB.

f. Access Mediation - This subsystem enforces security policy for Discretionary Access Control to file system objects (FSOs). Functionally, it determines the access rights of the requestor to FSOs, and compares the associated access rights to the security policy of the system, and/or as defined in ACLs, and enforces that policy, for each request.

21.   All of the above subsystems provide the interface to the TCB hardware for all processes and objects for the definition and enforcement of the security policy, thereby ensuring system security.

Non-kernel TCB

22.   The non-kernel TCB contains executable and nonexecutable components. All executable components in the non-kernel TCB are trusted programs that run in user mode, which prevents them from executing privileged hardware instructions. Note that all non-kernel TCB components have discretionary access set to prevent unauthorized modification.

23.   Non-kernel TCB trusted programs consist of specific function-related code combined with common routines found in the system libraries. Although many of these libraries are dynamically linked at execution time, the locations of these libraries are specified by HP at compile time. These libraries are stored in files and memory that cannot be modified by untrusted users.

24.   The non-kernel TCB consists of a number of functions that support the operation of the system. The interface, just as any untrusted process, to the TCB, for protected services, is via an instruction trap. The functions are included as a part of the TCB because their operation supports the kernel TCB, and are necessary for administration of the system. The components of the non-kernel TCB are summarized as follows:

a. Audit programs - a collection of programs and functions that enables the auditing of processes and events, to a granularity of an individual user, of security relevant actions requested, or taken by the process.

EAL4
CAPP
Annex B

HP-UX (11i)
Version 11.11
September 2001 release with specified patches
running on HP 9000 platforms

    b.   System Call Libraries - a set of files containing the executable system calls and service routines invoked by the kernel TCB for accomplishing a trusted function on behalf of an untrusted process.

    c.   TCB Databases - set(s) of files operated upon, and/or used by the kernel, and non-kernel TCB for the enforcement of the security policy, and administration of the TCB.

    d.   Binary Libraries - contain the executable files for commands and user initiated actions

    e.   Trusted Processes - Support processes that provide an interface to call on components of the kernel TCB, or allow for modification of user or untrusted process access rights.

    f.   Trusted Commands - Commands that may be initiated by untrusted users, or processes, that are trusted to restrict initiation of the command to those entities that are authorized to do so.

    g.   Batch Processing Programs - Facilities that schedule the initiation and execution of programs at a future date.

25.   One of the major subsystems of the Non-Kernel TCB is the System Administration Manager. This facilitates the definition, maintenance, control, and implementation of the desired security policies to ensure system integrity of the trusted system. Through this subsystem, all access to system resources by all potential users, privileges associated therewith, as well as audit trails, are defined and maintained in SAMs respective databases for use and interface by the foregoing components.

26.   The non-kernel TCB also contains security databases, file system objects, and trusted libraries whose access is limited to specific users or groups.

Hardware and Firmware Dependencies

27.   The TOE relies on the correct operation of processor mode and memory separation mechanisms to ensure system security.

HP-UX (11i)
Version 11.11
September 2001 release with specified patches
running on HP 9000 platforms

EAL4
CAPP

Annex C

ANNEX C: PRODUCT TESTING

IT Product Testing

1.   The Evaluators performed independent functional testing on the TOE to confirm that it operates as specified. They also witnessed initiation of 2 of the 3 suites of Developer tests and of the Developer's suite of evaluation-specific tests and confirmed the results of a sample of 20% each of the Developer tests and of the Developer's suite of evaluation-specific tests to confirm the adequacy of the Developer's testing of all of the TSF, subsystems and TSFI.

2.   The Evaluators then performed penetration testing which confirmed the SOF claimed in the Security Target [a] for the password checking mechanism The penetration testing also confirmed that all identified potential vulnerabilities in the TOE have been addressed, i.e. that the TOE in its intended environment has no exploitable vulnerabilities.

Test Platforms

3.   The Evaluators and Developers conducted their testing on the hardware platforms identified under the heading 'Environmental Configuration' in Annex A.

EAL4　　　　　　　　　　　　　　　　　　　　　　　　**HP-UX (11i)**
CAPP　　　　　　　　　　　　　　　　　　　　　　　　**Version 11.11**
　　　　　　　　　　　　　September 2001 release with specified patches
Annex C　　　　　　　　　　　　　　　　**running on HP 9000 platforms**

(This page is intentionally blank)