122-B

CERTIFICATION REPORT No. CRP251

Hewlett-Packard HP-UX 11i v3 Update 3

Virtual Server Operating Environment (VSE-OE)

running on HP 9000 Servers and HP Integrity Servers

Issue 1.0

November 2009

CESG Certification Body
IACS Delivery Office, CESG
Hubble Road, Cheltenham
Gloucestershire, GL51 0EX
United Kingdom

CERTIFICATION STATEMENT

The product detailed below has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the specified Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.	
Sponsor:	Hewlett-Packard
Developer:	Hewlett-Packard
Product and Version:	HP-UX 11i v3 Update 3 Virtual Server Operating Environment (VSE-OE)
Platform:	HP 9000 Servers and HP Integrity Servers
Description:	HP-UX 11i v3 Update 3 is Hewlett-Packard's implementation of a POSIX-compliant UNIX-based Operating System
CC Part 2:	Extended
CC Part 3:	Augmented
EAL:	EAL4 augmented by ALC_FLR.3 (Systematic Flaw Remediation)
PP Conformance:	COTS Compartmentalized Operations Protection Profile - Operating Systems (CCOPP-OS) [PP]
CLEF:	Logica
CC Certificate:	CRP251
Date Certified:	27 November 2009

The evaluation was performed in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in UK Scheme Publication 01 [UKSP01] and 02 [UKSP02P1], [UKSP02P2]. The Scheme has established a Certification Body, which is managed by CESG on behalf of Her Majesty's Government.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [ST], 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 1 [CC1] and 3 [CC3], the Common Evaluation Methodology [CEM] and relevant Interpretations.

The issue of a Certification Report is a confirmation that the evaluation process has been performed properly and that no *exploitable* vulnerabilities have been found in the evaluated configuration of the TOE. It is not an endorsement of the product.

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 [CCRA] 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[1] contained in the certificate and in this report are those of the Qualified Certification Body which issued them and of the Evaluation Facility which performed the evaluation. There is no implication of acceptance by other Members of the Arrangement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed by a third party upon those judgements.

MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES

The SOG-IS MRA logo which appears below:

- confirms that the certificate has been issued under the authority of a party to an international Mutual Recognition Agreement (MRA) [MRA] designed to ensure that security evaluations are performed to high and consistent standards;
- indicates that it is the claim of the evaluating party that its evaluation and certification processes meet all the conditions of the MRA.

The judgements[1] contained in the certificate and in this report are those of the Qualified Certification Body which issued them and of the Evaluation Facility which performed the evaluation. Use of the logo of this Agreement does not imply acceptance by other Members of liability in respect of those judgements or for loss sustained as a result of reliance placed by a third party upon those judgements.

CCRA logo **CC logo** **SOG-IS MRA logo**

[1] All judgements contained in this Certification Report, are covered by the CCRA [CCRA] and the MRA [MRA].

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of HP-UX 11i v3 Update 3 Virtual Server Operating Environment (VSE-OE) to the Sponsor, Hewlett-Packard (HP), as summarised on page 2 'Certification Statement' of this report, 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 [ST], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

3. The following product completed evaluation to CC **EAL4** augmented by ALC_FLR.3 (Systematic Flaw Remediation) on 27 November 2009:

   - **Hewlett-Packard HP-UX 11i v3 Update 3 Virtual Server Operating Environment (VSE-OE) running on HP 9000 Servers and HP Integrity Servers**

4. The Developer was Hewlett-Packard.

5. HP-UX 11i v3 Update 3 is Hewlett-Packard's implementation of a UNIX-based operating system that executes on the entire range of PA-RISC based HP 9000 and Itanium-based HP Integrity servers.

6. The evaluated configuration of this product is described in this report as the Target of Evaluation (TOE). Details of the TOE Scope, its assumed environment and the evaluated configuration are given in Chapter III 'Evaluated Configuration' of this report.

7. An overview of the TOE and its product architecture can be found in Chapter IV 'Product Architecture' of this report. An overview of the Configuration requirements is specified in Section 1.4.2 of [ST].

Protection Profile Conformance

8. The Security Target [ST] is certified as achieving conformance to the following protection profile:

   - COTS Compartmentalized Operations Protection Profile - Operating Systems [PP]

   Note that [PP] is conformant to the Controlled Access Protection Profile (CAPP) [CAPP] and the Role Based Access Control (RBAC) Protection Profile [RBAC].

Security Claims

9. The Security Target [ST] fully specifies the TOE's Security Objectives, the Threats which these Objectives counter and the Security Functional Requirements (SFRs) that elaborate the Objectives. Most of the SFRs are taken from CC Part 2 [CC2]; use of this standard facilitates comparison with other evaluated products. The other SFRs originate from the COTS Compartmentalized Operations Protection Profile - Operating Systems [PP].

10. The TOE security policies are detailed in ST [ST]. The Organisational Security Policies (OSPs) that must be met are specified in [ST] Section 3.3.

11. The environmental assumptions related to the operating environment are detailed in Chapter III (in 'Environmental Requirements') of this report.

Flaw Remediation

12. In addition to the EAL4 evaluation, the evaluators also assessed the Common Criteria Part 3 assurance component ALC_FLR.3, Systematic Flaw Remediation, and found that the TOE met this requirement.

13. The Evaluated Configuration Guide [ECG] includes instructions to users to check for reported flaws at the HP IT Resource Center (ITRC) site. It also describes a free alerting service which users can subscribe to.

14. As a result of their Flaw Remediation process, HP may include additional security patches to the delivery process for the TOE, including them on the delivered DVDs and/or noting them in an updated Evaluated Configuration Guide [ECG].

Evaluation Conduct

15. The TOE's SFRs and the security environment, together with much of the supporting evaluation deliverables, remained mostly unchanged from that of HP-UX 11i v3, which had previously been certified [CR] by the UK IT Security Evaluation and Certification Scheme to the CC EAL4 assurance level, against the protection profiles CAPP and the RBAC PP (which CCOPP-OS is conformant with), and version 2.3 of the Common Criteria. Therefore, for the evaluation of HP-UX 11i v3 Update 3 against CCOPP-OS [PP], the Evaluators made some reuse of the previous evaluation results where appropriate.

16. The CESG Certification Body monitored the evaluation which was performed by the Logica Commercial Evaluation Facility (CLEF). The evaluation addressed the requirements specified in the Security Target [ST]. The results of this work, completed in November 2009, were reported in the Evaluation Technical Report [ETR].

Conclusions and Recommendations

17. The conclusions of the CESG Certification Body are summarised on page 2 'Certification Statement' of this report.

18. Prospective consumers of HP-UX 11i v3 Update 3 should understand the specific scope of the certification by reading this report in conjunction with the Security Target [ST]. The TOE should be used in accordance with the environmental assumptions specified in the Security Target. Prospective consumers are advised to check that the SFRs and the evaluated configuration match their identified requirements, and to give due consideration to the recommendations and caveats of this report.

19. The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration. Chapter II 'TOE Security Guidance' of this report includes a number of recommendations regarding the secure receipt, installation, configuration and operation of the TOE.

20. In addition, the Evaluators' comments and recommendations are as follows:

- Although the ECG allows a password of 6 to 8 characters and account lockout after 1 to 10 failed login attempts, the Evaluators and the CESG Certification Body recommend that the administrator should set password lengths to 8 characters and should set account lockout to occur after no more than 3 consecutive failed login attempts.

- 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-based operating system with added security features. As noted in [ECG], section 5.11, whilst a large number of POSIX-compliant programs will work adequately, legacy programs may be unaware of the security features in the TOE and, so, may harm the configuration of the system.

Disclaimers

21. This report is only valid for the evaluated TOE. This is specified in Chapter III 'Evaluated Configuration' of this report.

22. Certification is *not* a guarantee of freedom from security vulnerabilities. There remains a small probability (smaller with higher Evaluation Assurance Levels) that exploitable vulnerabilities may be discovered after an evaluation has been completed. This report reflects the CESG Certification Body's view at the time of certification.

23. Existing and prospective consumers should check regularly for themselves whether any security vulnerabilities have been discovered since the ETR was issued and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether those patches have further assurance.

24. The installation of patches for security vulnerabilities, whether or not those patches have further assurance, should improve the security of the TOE. However, note that unevaluated patching will invalidate the certification of the TOE, unless the TOE has

undergone a formal re-certification or is covered under an approved Assurance Continuity process by a CCRA certificate-authorising Scheme.

25. All product or company names used in this report are for identification purposes only and may be trademarks of their respective owners.

II. TOE SECURITY GUIDANCE

Introduction

26. The following sections provide guidance that is of particular relevance to purchasers of the TOE.

Delivery

27. For the evaluated product, the TOE consumer should order part BA929AA with option code A54 using the following contact e-mail address:

    common_criteria_inquiries@cup.hp.com.

28. The relevant software disks are securely shrink-wrapped and then despatched to the TOE consumer by a trusted courier. The TOE consumer receives a packing list which includes the Purchase Order Number, an internal HP Order Number and a list of boxes with their contents. Each box is sealed with a label which includes both of the order numbers, the box number and its contents.

29. On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised during delivery.

30. Patches for the TOE may be sent out to consumers using the trusted delivery procedures 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 TOE consumers are recommended to request delivery of the patches from HP using the trusted procedure described above for delivery of the operating system.

Installation and Guidance Documentation

31. The Installation and Secure Configuration documentation is as follows:

- Evaluated Configuration Guide [ECG];
- Installation and Update Guide [INSTALL];
- Common Criteria Supplementary DVD [CC_SUPP];
- Release Notes (Update 3 Release) [REL];
- System Administrator's Guide: Overview [SAG_OVER];
- System Administrator's Guide: Configuration Management [SAG_CFG];
- System Administrator's Guide: Logical Volume Management [SAG_LVM];

- HP Systems Partitions Guide Administration for nPartitions [NPARS];
- Compartment Login Using Secure Shell (SSH) [CMPT_SSH];
- Software Distributor Administration Guide [SDAG];
- HP-UX Virtual Partitions Administrator's Guide [VPARS];
- Patch Management User Guide for HP-UX 11.x Systems [PATCH];
- Read Before Installing or Updating HP-UX 11i v3 [README];
- Using HP-UX [USING].

32. The Evaluated Configuration Guide [ECG] 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 the Installation and Update Guide [INSTALL] and a number of other minor documents (including Release Notes [REL] to be found on the products delivery disks: [INSTANT] and [CC_SUPP]).

33. The User Guide and Administration Guide documentation is as follows:

- System Administrator's Guide: Routine Management Tasks [SAG_MGMT];
- System Administrator's Guide: Security Management [SAG_SEC];
- Managing Systems and Workgroups [MSW];
- HP-UX Reference (Volumes 1 to 10) HP-UX 11i Version 3 [MAN_PAGES].

III. EVALUATED CONFIGURATION

TOE Identification

34. The TOE is HP-UX 11i v3 Update 3 Virtual Server Operating Environment (VSE-OE) plus a number of tools and patches identified in the Evaluated Configuration Guide [ECG] section 3.5 and provided on the HP-UX 11i v3 Common Criteria Supplementary Media DVD [CC_SUPP].

TOE Documentation

35. The relevant guidance documentation for the evaluated configuration is identified in Chapter II (in 'Installation and Guidance Documentation') of this report.

TOE Scope

36. The TOE Scope is defined in the Security Target [ST] Sections 1.4.1 and 1.4.2.

TOE Configuration

37. The evaluated configuration of the TOE is defined in [ECG] Section 2.1. It states that the TOE:

    a) executes on any single 64-bit computer system from the family of HP 9000 Servers and HP Integrity Servers that is supported on the September 2008 release of HP-UX 11i v3 Update 3 (hereinafter known as an 'HP Computer').

    b) executes on any nPartition of a cell-based HP server from the family of HP Computers that is supported on the September 2008 release of HP-UX 11i v3 Update 3. Cell-based servers may be configured as one single large system or as multiple smaller systems by configuring nPartitions. Each nPartition defines a subset of server hardware resources to be used as an independent system environment. An nPartition includes one or more cells assigned to it (with processors and memory) and all I/O chassis connected to those cells. All processors, memory, and I/O in an nPartition are used exclusively by the software running in the nPartition. For a server that supports nPartitions, the nPartition Configuration Privilege must be set to a non-default value to disable partition reconfiguring.

    c) executes on any vPartition within a server or any nPartition of a cell-based server that is supported on the September 2008 release of HP-UX 11i v3 Update 3. A server or an nPartition of a cell-based server may be configured as one single large system or as multiple smaller systems by configuring vPartitions running HP-UX Virtual Partitions (vPars) A.05.04 release. Each vPartition defines a subset of available hardware resources on a server or an nPartition to be used as an independent system environment. A vPartition includes one or more CPU-cores, a contiguous physical memory range in the multiple of configured granular size and one or more Local Bus Adapters (LBA). All processors, memory, and LBAs in a vPartition are used

exclusively by the software running in the vPartition. All vPartitions within a server or an nPartition of a cell-based server must be running the same version of the HP-UX Virtual Partitions (vPars) A.05.04 release and under the same administrative control.

d) executes on a single HP Computer or a vPartition of an HP Computer, or an nPartition of an HP Computer, which may be connected to other HP Computers via a local area network, each executing the same version of the product and under the same administrative control. The product may also be connected to other [CAPP] or CCOPP-OS [PP] conformant systems under the same administrative control and on the same local area network. No other processors may be connected to the product, either directly by hardwire connection (e.g. to implement a Cluster of HP Computers) or indirectly by, for example, a Wide Area Network or telephone cable to provide remote computer or network services.

e) must be patched as specified in [ECG] table 3.1, and configured and operated as detailed there.

f) may use either serial line or Guardian Service Processor connections to the system console. GSP connections are assumed to be over a private, isolated LAN, with a suitable GSP password configured, in order to provide appropriate protection of the system console.

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

h) supports the HFS and VxFS File Systems, but excludes Online VxFS.

i) includes Pluggable Authentication Modules (PAM), with the default configuration for authentication consisting of traditional user identity and password. Although the PAM framework permits other authentication modules, such as authentication through NT domain servers, Lightweight Directory Access Protocol (LDAP) or Distributed Computing Environment (DCE), to be used, these are not included in the evaluated configuration.

j) executes with CDE and X-Windows disabled and excludes the use of a restricted configuration of the System Management Homepage (Restricted SMH).

k) includes socket based network functions but excludes network applications, such as Network File System (NFS), peer authentication, encryption, sendmail(1M), mail(1), and NIS.

l) must be installed, set up and operated as described in [MSW], [NPARS], [VPARS], [INSTALL], [SAG_SEC], [MAN_PAGES], [REL], [README], [SDAG], [USING], [CC_SUPP] and [ECG].

m) has shadow passwords feature enabled, as described in section 2.4.5 of [SAG_SEC] and section 4.3 of [ECG].

n) has auditing enabled in multi-user mode, as described in chapter 10 of [SAG_SEC] and section 4.3 of [ECG].

o) has boot authentication enabled, as described in section 1.4 of [SAG_SEC] and section 4.3 of [ECG].

p) has compartmentalization feature enabled, as described in chapter 7 of [SAG_SEC] and section 4.3 of [ECG].

q) has procedures and processes in place to periodically run integrity checking tools, as described in chapter 6 of [MSW] and section 4.3 of [ECG].

r) supports only the following secure network applications (other network applications and services, such as NFS and NIS, are excluded):

- scp(1)
- sftp(1)
- ssh(1)

Environmental Requirements

38. The intended environment for the TOE is listed in [ECG] Section 2.3. It states that it is necessary that a comprehensive security policy is established for the site(s) in which the product is operated and that it is enforced and adhered to by all users of the product. The security policy is expected to include measures for:

- physical security - to restrict physical access to areas containing the product, HP Computer and associated equipment and to protect physical resources, including networks, media and hardcopy material, from unauthorized access, theft or deliberate damage;
- procedural security - to control the use of the HP Computer, associated equipment, the product and supported applications, and information stored and processed by the product, including use of the TOE's security features and physical handling of information;
- personnel security - to limit a user's access to the product to those resources, applications and information for which the user has a need-to-know and to distribute security related responsibilities among different users.

39. The Operational Assumptions for the TOE are listed in [ECG] Section 2.4. It states:

- The product, its users and environs comply with any applicable directives regarding physical, procedural or personnel security defined in the relevant site security policies (recommended in [ECG] Section 2.3).

- The product is being operated as an evaluated 'trusted configuration' and is adequately protected against physical threats (e.g. fire, flood, disruption to power supplies, temperature, humidity fluctuations, and electromagnetic emanations).

- The HP Computer, associated devices and equipment function correctly.

- The components of the TOE shall comply with any applicable TEMPEST standards.

40. The environmental IT configuration is outlined in a number of Method of Use (MOU) assumptions from [ECG] Section 2.4 which must be followed:

a) The product is installed, configured, used and maintained in accordance with the procedures and guidelines defined in [README], [REL], [NPARS], [VPARS], [INSTALL], [MSW], [SAG_SEC], [CC_SUPP] and [ECG]. (MOU_1)

b) The TOE is configured with shadow passwords enabled and with a minimum password length of 6 characters. (MOU_2)

c) The TOE is configured with auditing enabled for both single user mode and multi-user mode. (MOU_3)

d) The TOE is configured to suspend authorized user processes in the event that audit data cannot be recorded because all available file systems are full. (MOU_4)

e) Audit data is protected, by setting appropriate file protections on the audit data files, so that it cannot be accessed by unauthorized users. (MOU_5)

f) The authorized administrator will select appropriate audit events to be recorded by the TOE from time to time and will analyze the audit files to detect possible attacks. (MOU_6)

g) The authorized administrator ensures that audit data files are backed up before deleting them from the TOE. (MOU_7)

h) The TOE is configured with authentication enabled for single-user mode. (MOU_8)

i) Authentication data is protected, by setting appropriate file protections on the authentication data databases, so that it cannot be accessed by unauthorized users. (MOU_9)

j) Appropriate default file permissions are assigned to all user accounts so that newly created objects are protected from unauthorized access. (MOU_10)

k) Administrative users make use of the trusted facilities provided to maintain the TOE configuration and do not make use of general purpose editors to edit the configuration files (e.g. /etc/passwd) directly, except in the few instances where trusted facilities are not provided by the TOE. (MOU_11)

l) The authorized administrator ensures that site policies and procedures exist to formally approve the addition of new users, that only formally approved users may access the product, that maximum disk quotas on file-system are configured for the new users and their groups, that their membership in roles accurately reflects the user's job function, responsibilities, qualifications and/or competencies within the enterprise, and that user access is promptly removed when users no longer have a need to use the TOE. (MOU_12)

m) The TOE is configured with compartmentalization feature enabled and supports at least two site-definable compartments. (MOU_13)

n) The TOE is configured with the compartment login feature enabled and users are assigned to a compartment at login time. (MOU_14)

o) Subjects and objects which are maintained within the product, but are outside of the control of the TOE, are protected by other technical or procedural controls against the threats of unauthorized access which would violate the TOE's discretionary or mandatory objectives, including additional data entry and import/export controls external to the TOE. (MOU_15)

p) The integrity of the TOE and information that is stored or processed by the TOE is maintained by making appropriate use of the system integrity and recovery utilities, periodically, and after product or HP Computer failure. (MOU_16)

q) Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints. All connections to peripheral devices reside within the controlled access facilities. In a configuration of networked hosts executing the TOE, communication links are physically protected against the threats of eavesdropping or spoofing attacks. The authorized administrator ensures that each connected host is configured with its correct IP address(es) and that each host accepts only those packets addressed to it. (MOU_17)

r) Cell-based servers may be configured as one single large system or as multiple smaller systems by configuring nPartitions. PARPERM (Partition Reconfiguration Privilege) must be set to a non-default value on cell-based HP 9000 and HP Integrity server to disable partition reconfiguring. (MOU_18)

s) A server or an nPartition of a cell-based server may be configured as one single large system or as multiple smaller systems by configuring vPartitions. Virtual partition flexible administrative capability must be enabled to designate one virtual partition to have administration capabilities (Designated-Admin vPar). (MOU_19)

Test Configuration

41. The Developers used the following configuration for their testing:

Name	Model	CPU	Memory	Configuration
CARMEL	ia64 hp server rx1620	1 x Intel(R) Itanium 2 1.6 GHz, 3 MB	2040 MB	Compartments: INIT, cmpt_A, cmpt_B
HELENA	ia64 hp server BL870c	4 x Intel(R) Itanium 2 1.42 GHz, 12 MB	8161 MB	Compartments: INIT, cmpt_A, cmpt_B
OAKLEY	ia64 hp server rx2660	2 x Intel(R) Itanium 2 (1.59 GHz, 18 MB)	8169 MB	Compartments: INIT, cmpt_A, cmpt_B
TRACY	ia64 hp server rx3600	2 x Intel(R) Itanium 2 (1.59 GHz, 18 MB)	8159 MB	Compartments: INIT, cmpt_A, cmpt_B
SYDNEY	ia64 hp server rx8640 (Hard Partitions with virtual partitions)	2 x Intel(R) Itanium 2 (1.6 GHz, 18 MB)	48952 MB	**nPAR 0:** vPar0: INIT, cmpt_A, cmpt_B vPar1: INIT, cmpt_A, cmpt_B vPar2: INIT, cmpt_A, cmpt_B **nPAR 1:** INIT, cmpt_A, cmpt_B
LAWTON	9000/800/rp7420 (Hard Partition with Virtual Partitions)	1 x PA-RISC 8800 (900 MHz, 32 MB)	8157 MB	**nPAR 0:** vPar0: INIT, cmpt_A, cmpt_B vPar1: INIT, cmpt_A, cmpt_B vPar2: INIT, cmpt_A, cmpt_B
MORAGA	9000/800/rp3440	2 x PA-RISC 8800 (800 MHz, 64 MB)	4094 MB	Compartments: INIT, cmpt_A, cmpt_B
PINOLE US	ia64 hp server rx2620	2 x Intel(R) Itanium 2 (1.3 GHz, 3 MB)	2028 MB	Compartments: INIT, cmpt_A, cmpt_B

Table 1: Developer Systems

42. The Evaluators used all the systems identified above for the developers, plus the additional system below, for their testing:

Name	Model	CPU	Memory	Configuration
PINOLE UK	ia64 hp server rx2620	2 x Intel(R) Itanium 2 (1.3 GHz, 3 MB)	2036 MB	Compartments: INIT, cmpt_A, cmpt_B

Table 2: Evaluator Test Systems

IV. PRODUCT ARCHITECTURE

Introduction

43. This Chapter gives an overview of the TOE's main architectural features. Other details of the scope of evaluation are given in Chapter III 'Evaluated Configuration' of this report.

Product Description and Architecture

44. The TOE is Hewlett-Packard's implementation of a UNIX-based operating system that executes on the entire range of PA-RISC based HP 9000 and Itanium-based HP Integrity servers in both stand-alone and networked environment in multi-user mode of operations. On cell-based HP 9000 and HP Integrity platforms, the TOE can execute with hard partition (nPartition) and logical partition (vPartition) configurations. The architecture of the TOE is based on the traditional UNIX architecture however it includes various HP-UX specific enhancements.

TOE Design Subsystems

45. For the purposes of the evaluation the TOE Design was split into the following sub-systems for evaluator analysis:

- Memory Management;
- Process Management;
- File System, incorporating Discretionary Access Control (DAC);
- Audit;
- Identification and Authentication;
- Role Based Access Control (RBAC);
- Compartment Management, incorporating Mandatory Access Control (MAC);
- System Administration;
- Networking;
- Shells.

46. The TOE subsystems each implement one or more aspects of the following main security features:

a) **User Identification and Authentication** – All users of the TOE are authenticated and held accountable for their security related actions. Each user is uniquely identified by the TOE. The TOE records security related events and the user associated with the

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

b) **Discretionary Access Control (DAC)** – The TOE enforces Discretionary Access Control (DAC) policies between active entities (subjects) and passive entities (objects) based on subject identity and allowed actions on the object. The TOE implements DAC policies through both the traditional UNIX 'owner', 'group', and 'other' access mode permissions and a more granular access control list (ACL) mechanism controlled by the object's owner. Except for kernel daemon processes that operate directly on behalf of the kernel, all subjects are associated with an authenticated user identity, and all named objects are associated with identity based protection attributes.

c) **Mandatory Access Control (MAC)** – The TOE enforces Mandatory Access Control (MAC) policies between active entities (subjects) and passive entities (objects) based on the compartment label of the subject and allowed actions on the object. All subjects are associated with a compartment label. The subjects' compartment labels and the 'label' access restriction rules for the objects defined in a compartment access rule database are used as the basis for the MAC decisions, which control the access of subjects to the objects.

d) **Role Based Access Control (RBAC)** – The TOE implements Role Based Access Control (RBAC) which breaks up the traditional one system administrator ('superuser') into a number of roles. The users may be assigned role(s). Each role is associated with zero or more authorizations for a privileged operation on an object. For example, a network administrator has a role that permits configuring network cards.

e) **Security Audit** – The TOE provides mechanisms to record security relevant events. It allows detection of any attempts to bypass the protection mechanism. It acts as a deterrent against system abuses and exposing potential security breaches in the system. An authorized administrator may select the users and events for which audit record is collected from time to time.

f) **Resource Utilization** – The TOE implements resource allocation policies for system resources as a measure of resistance to resource depletion. Maximum amount of memory and disk space per user or subject can be set by an authorized administrator.

g) **Object Reuse Protection** – An object reuse protection mechanism ensures that information is not inadvertently transferred between subjects when objects are re-allocated.

h) **Trusted Recovery** – The TOE provides mechanisms for trusted recovery in the event of system failures or detected insecurities such as system database corruption.

i) **Environmental Constraints Based Access Control** – The TOE can allow or deny access based upon environmental constraints such as time-of-day and port-of-entry.

TOE Dependencies

47. The TOE dependency is as follows:

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

TOE Interfaces

48. The external TOE Security Functions Interface (TSFI) is described as follows:

- User Commands;
- Systems Administration Commands;
- System Calls;
- Library Functions;
- File Formats (such as TSF configuration files).

V. TOE TESTING

TOE Testing

49. The Developer's tests covered:

- all SFRs;
- all TOE high-level subsystems, as identified in Chapter IV (in 'TOE Design Subsystems') of this report;
- all Security Functions (SFs);
- the TSFI, as identified in Chapter IV (in 'TOE Interfaces') of this report.

50. The Developer's tests also included those TOE interfaces which are internal to the product and thus had to be exercised indirectly.

51. The Evaluators independently ran the Developer's test suites on the Developer's test systems located in Cupertino, California as described in Chapter III (in 'Test Configuration') of this report. The results were analysed and all anomalies were investigated to ensure none indicated security failures.

52. The Evaluators devised and ran a total of 42 independent functional tests, different from those performed by the Developer, on systems located in Cupertino, California and also at the Logica CLEF in Reading, UK. Some anomalies were found but subsequently resolved.

53. The Evaluators also devised and ran a total of 19 penetration tests to address potential vulnerabilities considered during the evaluation, on systems located in Cupertino, California and also at the Logica CLEF in Reading, UK. Exploitable vulnerabilities were detected but subsequently resolved.

54. The Evaluators' penetration tests utilised publicly available penetration testing tools, where appropriate, when analysing aspects such as network security. However, a significant amount of the penetration testing effort went into investigating functionality where such tools were inappropriate and therefore implementation specific testing techniques were developed.

55. The Evaluators finished running their penetration tests on 15th October 2009.

Vulnerability Analysis

56. The Evaluators' vulnerability analysis, which preceded penetration testing and was reported in [ETR], was based on public domain sources and the visibility of the TOE provided by the evaluation deliverables.

Platform Issues

57. The Sponsor provided a Multi Platform Rationale [MPR], in accordance with UK CC Interpretation UK/3.1/012 [UKI12]. As a result of their examination of this rationale, the Evaluators considered the evaluation outcome should apply to all of the platforms listed in Table 3 below which includes some platforms not listed as test platforms in Table 1 and Table 2.

Platform	Processor / Module Type	Clock Speed	Cells	Processors / Cores per system	Max RAM	PCI slots	Internal Storage
rp3410	PA-8900 Single Core	800MHz	N/A	1P/1C	6GB	2	900GB
	PA-8900 Dual Core	800MHz	N/A	1P/2C	6GB	2	900GB
rp3440	PA-8900 Single Core	800MHz/1.0GHz	N/A	1P/1C-2P/2C	32GB	4	900GB
	PA-8900 Dual Core	800MHz/1.0GHz	N/A	1P/2C-2P/4C	32GB	4	900GB
rp4410	PA-8900 Single Core	800MHz/1.0GHz	N/A	1P/1C-2P/2C	128GB	6	600GB
	PA-8900 Dual Core	800MHz/1.0GHz	N/A	1P/2C-2P/4C	128GB	6	600GB
rp4440	PA-8900 Dual Core	800MHz/1.0GHz	N/A	1P/2C-4P/8C	128GB	6	600GB
rp7420	PA-8800 Dual Core	900MHz/1.0GHz	1-2	1P/2C-8P/16C	128GB	15	1.2TB
	PA-8900 Dual Core	1.0GHz1.1 GHz	1-2	1P/2C-8P/16C	128GB	15	1.2TB
rp7440	PA-8900 Dual Core	1.068GHz	1-2	1P/2C-8P/16C	128GB	15	1.2TB
rp8420	PA-8800 Dual Core	900MHz/1.0GHz	1-4	1P/2C-16P/32C	256GB	16	1.2TB
	PA-8900 Dual Core	1.0GHz/1.1GHz	1-4	1P/2C-16P/32C	256GB	16	1.2TB
rp8440	PA-8900 Dual Core	1.068GHz	1-4	1P/2C-16P/32C	256GB	16	2.4TB
Superdome	PA-8900 Dual Core						
	16 Processors	1.1GHz	1-4	2P/4C-16P/32C	512GB	48	N/A
	32 Processors	1.1GHz	1-8	2P/4C-32P/64C	1TB	96	N/A
	64 Processors	1.1GHz	3-16	6P/12C-64P/128C	2TB	192	N/A
BL860c	Itanium Single Core	1.6GHz	N/A	1P-2P	48GB	3	292GB
	Itanium Dual Core	1.42GHz/1.66GHz	N/A	1P/2C-2P/4C	48GB	3	292GB
BL870c	Itanium Dual Core	1.4GHz/1.6GHz	N/A	1P/2C-4P/8C	192GB	3	584GB
rx1620	Itanium Single Core	1.3GHz/1.6GHz	N/A	1P/1C-2P/2C	16GB	2	292GB
rx2620	Itanium Single Core	1.3GHz/1.6GHz	N/A	1P/1C-2P/2C	24GB	4	292GB
rx2660	Itanium Single Core	1.6GHz	N/A	2P/2C	32GB	3	1.2TB
	Itanium Dual Core	1.42GHz/1.66GHz	N/A	2P/4C	32GB	3	1.2TB
rx3600	Itanium Dual Core	1.42GHz/1.66GHz	N/A	2P/4C	196GB	8	1.2TB
rx4640	Itanium Single Core	1.5GHz/1.6GHz	N/A	1P/1C-4P/4C	128GB	6	584GB
	Itanium MX2	1.1GHz	N/A	2P/2C-8P/8C	128GB	6	584GB
rx6600	Itanium Dual Core	1.42GHz/1.6GHz	N/A	1P/2C-4P/8C	384GB	8	2.3TB
rx7620	Itanium Single Core	1.3GHz/1.5GHz	1-2	2P/2C-8P/8C	128GB	15	584GB
	Itanium MX2	1.1GHz	1-2	2P/2C-16P/16C	128GB	15	584GB
rx7640	Itanium Dual Core	1.4GHz/1.6GHz	1-2	2P/4C-8P/16C	256GB	15	1.2TB
rx8620	Itanium Single Core	1.5GHz/1.6GHz	1-4	2P/2C-16P/16C	256GB	16	584GB
	Itanium MX2	1.1GHz	1-4	2P/2C-32P/32C	256GB	16	584GB
rx8640	Itanium Dual Core	1.4GHz/1.6GHz	1-4	2P/4C-16P/32C	512GB	32	1.2TB
Integrity Superdome	Itanium Single Core						
	16 Processors	1.6GHz	1-4	2P/2C-16P/16C	512GB	48	N/A
	32 Processors	1.6GHz	1-8	2P/2C-32P/32C	1TB	96	N/A
	64 Processors	1.6GHz	2-16	4P/4C-64P/64C	2TB	192	N/A
	Itanium Dual Core						
	16 Processors	1.6GHz	1-4	1P/2C-16P/32C	512GB	48	N/A
	32 Processors	1.6GHz	1-8	1P/2C-32P/64C	1TB	96	N/A
	64 Processors	1.6GHz	2-16	2P/4C-64P/128C	2TB	192	N/A

Table 3: Evaluated Platforms

58. Installing the TOE on Hard Partitions (nPartition) and Logical Partitions (vPartition) is also covered by the evaluation. They were discussed in the Developer's Multi Platform Rationale [MPR] and the independent functional tests were run on combinations of nPartitions and vPartitions to ensure these specific platform technologies did not invalidate any evaluation results.

VI. REFERENCES

[CAPP] Controlled Access Protection Profile,
National Security Agency,
Version 1.d, October 8, 1999.

[CC] Common Criteria for Information Technology Security Evaluation,
(comprising Parts 1, 2, 3: [CC1], [CC2], [CC3]).

[CC1] Common Criteria for Information Technology Security Evaluation,
Part 1, Introduction and General Model,
Common Criteria Maintenance Board,
CCMB-2006-09-001, Version 3.1 R1, September 2006.

[CC2] Common Criteria for Information Technology Security Evaluation,
Part 2, Security Functional Components,
Common Criteria Maintenance Board,
CCMB-2007-09-002, Version 3.1 R2, September 2007.

[CC3] Common Criteria for Information Technology Security Evaluation,
Part 3, Security Assurance Components,
Common Criteria Maintenance Board,
CCMB-2007-09-003, Version 3.1 R2, September 2007.

[CCRA] Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security,
Participants in the Arrangement Group,
May 2000.

[CC_SUPP] HP-UX 11i v3 Common Criteria Supplementary DVD, Hewlett-Packard,
BA929AA option A54, November 2009.

[CEM] Common Methodology for Information Technology Security Evaluation,
Evaluation Methodology,
Common Criteria Maintenance Board,
CCMB-2007-09-004, Version 3.1 R2, September 2007.

[CMPT_SSH] Compartment Login Using Secure Shell (SSH),
Hewlett-Packard,
5992-5374, October 2008.

[CR] Common Criteria Certification Report No. CRP243,
UK IT Security Evaluation and Certification Scheme,
CRP243, Issue 1.0, March 2008.

[ECG] HP-UX 11i v3 Evaluated Configuration Guide,
Hewlett-Packard,
ECG_V1.8.doc, Version 1.8, October 2009.

[ETR] Evaluation Technical Report,
Logica CLEF,
LFL/T257/ETR, Issue 1.2, November 2009.

[INSTALL] HP-UX 11i v3 Installation and Update Guide,
Hewlett-Packard,
5992-4165, Issue 4, September 2008.

[INSTANT] HP-UX 11i Version 3 HP Instant Information DVD,
Hewlett-Packard,
B3921-10049, September 2008.

[MAN_PAGES] HP-UX Reference (Volumes 1 to 10) HP-UX 11i Version 3,
Hewlett-Packard,
February 2007.

[MPR] HP-UX 11i v3 Common Criteria Multi-Platform Rationale Against CCOPP-OS,
Hewlett-Packard,
MPR_V1.0.doc, Issue 1.0, May 2009.

[MRA] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates,
Management Committee of Agreement Group,
Senior Officials Group – Information Systems Security,
Version 2.0, April 1999.

[MSW] Managing Systems and Workgroups: A Guide for HP-UX System Administrators,
Hewlett-Packard,
B2355-90950, Issue 9, March 2006.

[NPARS] HP Systems Partitions Guide Administration for nPartitions,
Hewlett-Packard,
5991-1247B, February 2007.

[PATCH] Patch Management User Guide for HP-UX 11.x Systems,
Hewlett-Packard,
5992-0674, Issue 9, September 2008.

[PP] COTS Compartmentalized Operations Protection Profile – Operating Systems,
Hewlett-Packard,
Issue 2.0, June 2008.

[RBAC] Role Based Access Control (RBAC) Protection Profile,
US National Institute of Standards and Testing,
Version 1.0, July 30, 1998.

[README] Read Before Installing or Updating HP-UX 11i v3 September 2008,
Hewlett-Packard,
5992-4183, September 2008.

[REL] HP-UX 11i Version 3 September 2008 Release Notes (Update 3 Release),
Hewlett-Packard,
5992-4174, September 2008.

[SAG_CFG] HP-UX System Administrator's Guide: Configuration Management,
Hewlett-Packard,
5992-4607, Issue 3, September 2008.

[SAG_LVM] HP-UX System Administrator's Guide: Logical Volume Management,
Hewlett-Packard,
5992-4589, Issue 3, September 2008.

[SAG_MGMT] HP-UX System Administrator's Guide: Routine Management Tasks,
Hewlett-Packard,
5992-4616, Issue 4, September 2008.

[SAG_OVER] HP-UX System Administrator's Guide: Overview,
Hewlett-Packard,
5992-4580, Issue 3, September 2008.

[SAG_SEC] HP-UX System Administrator's Guide: Security Management,
Hewlett-Packard,
5992-3387, Issue 4, March 2008.

[SDAG] Software Distributor Administration Guide for HP-UX 11i v3,
Hewlett-Packard,
5992-2146, September 2007.

[ST] HP-UX 11i v3 Common Criteria Security Target Against CCOPP-OS,
Hewlett-Packard,
ST_V1.6.doc, Issue 1.6, October 2009.

[UKI12] Multi-platform TOEs,
UK IT Security Evaluation & Certification Scheme,
UK CC Interpretation UK/3.1/012, Version 1.0, 12 March 2007.

[UKSP00] Abbreviations and References,
UK IT Security Evaluation and Certification Scheme,
UKSP 00, Issue 1.5, October 2008.

[UKSP01] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.2, October 2008.

[UKSP02P1] CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4.1, October 2008.

[UKSP02P2] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 2.3, October 2008.

[USING] Using HP-UX,
Hewlett-Packard,
B2355-90164, September 1997.

[VPARS] HP-UX Virtual Partitions Administrator's Guide,
Hewlett-Packard,
T1335-90098, September 2008.