122-B

CERTIFICATION REPORT No. CRP243

Hewlett-Packard HP-UX 11i

Version 3

running on HP 9000 and HP Integrity platforms

Issue 1.0

March 2008

UK Certification Body
CESG, Hubble Road
Cheltenham, 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 in this report are those of the Qualified Certification Body which issued them 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

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 Version 3
Platform	HP 9000 and HP Integrity platforms
Description	HP-UX 11i is Hewlett-Packard's UNIX-based operating system, delivering an end-to-end, scalable, manageable, and secure infrastructure for developing, deploying, and brokering mission-critical services.
CC Part 2	Extended
CC Part 3	Conformant
EAL	EAL4 augmented by ALC_FLR.3
SoF	SoF-Medium
PP Conformance	CAPP, RBAC
CLEF	LogicaCMG[1]
Date Certified	26 March 2008

The *IT Security Certified* logo which appears above:

- confirms that this certificate has been issued under the authority of a party to an international Recognition Agreement ('RA') 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 RA.

The judgements[2] 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. 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 upon those judgements by a third party.

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 [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 carried out properly and that no *exploitable* vulnerabilities have been found in the evaluated configuration of the TOE. It is not an endorsement of the product.

Trademarks:

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

[1] Note that LogicaCMG changed its name to Logica on 27 February 2008. For further information please refer to: http://www.logica.com/logicacmg+becomes+logica/400010974.

[2] All judgements contained in this Certification Report are covered by the Recognition Arrangement.

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria security evaluation of HP-UX 11i Version 3 to the Sponsor, Hewlett-Packard, as summarised in the Certification Statement, 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 **EAL 4** augmented by ALC_FLR.3 on 26 March 2008:

   - **HP-UX 11i Version 3**

4. The Developer was Hewlett Packard.

5. HP-UX 11i Version 3 is an Operating System based on UNIX. The evaluated product may execute on a single HP 9000 Server or HP Integrity Server or on an nPartition of HP 9000 or HP Integrity Server, which may be connected to other HP 9000 Servers and HP Integrity Servers via a local Ethernet network, each executing the same version of the TOE and under the same administrative control. The TOE may also be connected to other CAPP-conformant systems, such as PCs or workstations, under the same administrative control and on the same local network.

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’.

7. An overview of the TOE and its security architecture can be found in Chapter IV ‘TOE Security Architecture’. Configuration requirements are specified in Section 2.3 of [ST].

Protection Profile Conformance

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

   - Controlled Access Protection Profile (CAPP);
   - Role Based Access Control [RBAC].

9. The Security Target [ST] also includes objectives and security functions additional to those of the protection profiles.

Security Claims

10. The Security Target [ST] fully specifies the TOE's Security Objectives, the Threats and OSPs which these Objectives support and the Security Functional Requirements (SFRs) and Security Functions that elaborate the Objectives. All of the SFRs are taken from CC Part 2 [CC2], [CAPP] and [RBAC]; use of these facilitates comparison with other evaluated products.

11. Section 6.2 of the Security Target [ST] makes security functionality claims for the TSF grouped under the following categories:

    - Audit (AUD);
    - Identification and Authentication (IA);
    - Discretionary Access Control (DAC and ACLs);
    - Role Based Access Control (RBAC);
    - Object Reuse (OBJ_REUSE);
    - Protection Functions (PROT).

12. The TOE security policies are detailed in [ST]. The OSPs that must be met are specified in Section 3.3 of [ST].

13. The environmental assumptions related to the operating environment are detailed in Chapter III under 'Environmental Requirements'.

Strength of Function Claims

14. The minimum Strength of Function (SoF) was claimed to be SoF-Medium. This is claimed for the password checking mechanism. The Evaluators have determined that these claims were met.

15. The Security Target [ST] states that the claimed minimum SoF for the password checking mechanism, SoF-medium, is consistent with the CAPP Security Functional Requirement FIA_SOS.1 as justified in CAPP Section 7.5 [CAPP].

16. The CAPP security functional requirement FIA_SOS.1 states that the password checking mechanism should meet the following:

    - For each attempt to use the authentication mechanism, the probability that a random attempt will succeed is less than one in 1,000,000.
    - 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.
    - Any feedback given during an attempt to use the authentication mechanism will not reduce the probability below the above metrics.

17. In addition, the Security Target 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.

Evaluation Conduct

18. The TOE SFRs and the security environment, together with much of the supporting evaluation deliverables, remained mostly unchanged from those of HP-UX 11i Version 2, which had previously been certified [CR] by the UK IT Security Evaluation and Certification Scheme to the CC EAL4 assurance level. For the evaluation of HP-UX 11i Version 3, the Evaluators made reuse of the previous evaluation results where appropriate.

19. The Certification Body monitored the evaluation which was carried out by the LogicaCMG Commercial Evaluation Facility (CLEF). The evaluation addressed the requirements specified in the Security Target [ST]. The results of this work, completed in December 2007 were reported in the Evaluation Technical Report [ETR].

Conclusions and Recommendations

20. The conclusions of the Certification Body are summarised in the Certification Statement on page 2.

21. Prospective consumers of HP-UX 11i Version 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.

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

23. 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 [ECG], section 5.10, 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

24. This Certification Report is only valid for the evaluated TOE. This is specified in Chapter III 'Evaluated Configuration'.

25. 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 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 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. 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 by a Scheme-approved Assurance Continuity process.

II. TOE SECURITY GUIDANCE

Introduction

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

Delivery

27. 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 in delivery.

28. For the evaluated product, the TOE consumer should order part BA491AA, option A54, using the following contact email address:

common_criteria_inquiries@cup.hp.com

29. 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.

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 Configuration documentation is as follows:

- Evaluated Configuration Guide [ECG];
- Installation and Update Guide, [INSTALL];
- Read Before Installing or Updating HP-UX 11i Version 3, [README];
- Release Notes [REL];
- HP Systems Partitions Guide Administration for nPartitions, [PARTITION].

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 files to be found on the product's delivery disks).

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

- Manual Pages, [MANPAGES];
- Evaluated Configuration Guide, [ECG];
- Managing Systems and Workgroups, [MSW];
- Using HP-UX, [USING];
- System Administrator's Guide: Security Management, [SAG_SEC];
- Software Distributor Administration Guide, [SDAG].

Flaw Remediation

34. 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.

35. 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.

36. 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 CDs and/or noting them in an updated Evaluated Configuration Guide [ECD].

III. EVALUATED CONFIGURATION

TOE Identification

37. The TOE is HP-UX 11i Version 3, which consists of HP-UX 11i v3 Mission Critical Operating Environment plus a number of patches identified in the Evaluated Configuration Guide [ECG].

TOE Documentation

38. The relevant guidance documentation for the evaluated configuration is identified above under 'Installation and Guidance Documentation'.

39. All the required documentation is provided on [INSTANT] and [CC_SUPP].

TOE Scope

40. The TOE Scope is defined in [ST] Section 1.2.2. In summary the TOE:

- executes on a single HP Computer or on an nPartition of HP Computer, which may be connected to other HP Computers via a local area network, each executing the same version of the product. The product may also be connected to other CAPP-conformant systems, such as PCs or workstations, under the same administrative control and on the same local area network;
- does not include virtual partitions (VPARs) but may be configured to use hardware partitions (nPartitions);
- supports user interaction via any of the supported Shells (including the POSIX, Bourne, C and Korn Shells);
- supports the HFS and VxFS File Systems, but excludes Online VxFS;
- includes Pluggable Authentication Modules (PAM), with the default configuration for authentication consisting of user identity and password;
- executes with CDE and X-Windows disabled and excludes the use of a restricted configuration of the System Management Homepage (Restricted SMH);
- includes socket based network functions but excludes network applications, such as NFS, peer authentication, encryption, sendmail(1M), mail(1), and NIS;
- supports only the following secure network applications: ftp(1), telnet(1), rexec(1), and rlogin(1).

41. The following are excluded from the evaluation.

- The Online VxFS file system;
- X-Windows;
- Network applications other than those listed above (e.g. NFS and NIS).

42. HP-UX 11i v3 provides a Controlled Access with RBAC operating system in both stand-alone and networked environments. The TOE provides one or more processes and attached peripheral and storage devices to be used by users to perform a variety of functions requiring controlled, shared access to processing capability and information.

43. The TOE provides user services directly or serves as a platform for networked applications and supports communications across an appropriately protected network.

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

TOE Configuration

45. The evaluated configuration of the TOE is defined in outline in [ST] Section 2.3 and in detail in Evaluated Configuration Guide [ECG].

46. The Sponsor provided a Multi Platform Rationale [MPR], in accordance with UK CC Interpretation UK/2.3/012 [UKI12], which extended the evaluation results to the platforms in Table 1.

Platform	Micro-Processor Type and Clock Frequency	Processors and Cores	Cells	Max. Memory	PCI slots	Max Internal Storage
rp3410-2	PA-8900 (800MHz)	1 (1-2)	N/A	6 GB	2	900 GB
rp3440-4	PA-8900 (800MHz/1.0GHz)	1-2 (1-4)	N/A	32 GB	4	900 GB
rp4410-4	PA-8900 (800MHz/1.0GHz)	1-2 (1-4)	N/A	128 GB	6	600 GB
rp4440-8	PA-8900 (800MHz/1.0GHz)	2-4 (2-8)	N/A	128 GB	6	600 GB
rp7420-16	PA-8800 (900MHz/1.0GHz) PA-8900 (1.0GHz/1.1 GHz)	1-8 (2-16)	1-2	128 GB	15	1.2 TB
rp8420-32	PA-8800 (900MHz/1.0GHz) PA-8900 (1.0GHz/1.1GHz)	1-16 (2-32)	1-4	256 GB	32	2.4 TB
Superdome	PA-8900 (1.1GHz)	2-64 (/4-128)	1-16	1 TB	192	N/A
BL60p	Itanium 2 (1.6GHz)	1-2 (1-2)	N/A	8 GB	0	293.6 GB
rx1620	Itanium 2 (1.6GHz)	1-2 (1-2)	N/A	16 GB	2	600 GB
rx2620	Itanium 2 (1.4GHz/1.6GHz)	1-2 (1-4)	N/A	32 GB	4	900 GB
rx3600	Itanium 2 (1.4GHz/1.6GHz)	1-2 (2-4)	N/A	96 GB	8	600 GB
rx4640	Itanium 2 (1.6GHz)	1-4 (1-8)	N/A	128 GB	6	600 GB
rx6600	Itanium 2 (1.4GHz/1.6GHz)	1-4 (2-8)	N/A	192 GB	8	1.2 TB
rx7620	Itanium 2 (1.5GHz/1.6GHz)	2-8 (2-16)	1-2	128 GB	15	584 GB
rx7640	Itanium 2 (1.42GHz/1.6GHz)	2-8 (2-16)	1-2	128 GB	15	1200 GB
rx8620	Itanium 2 (1.5GHz/1.6GHz)	2-16 (2-32)	1-4	256 GB	16	584 GB

Platform	Micro-Processor Type and Clock Frequency	Processors and Cores	Cells	Max. Memory	PCI slots	Max Internal Storage
rx8640	Itanium 2 (1.42GHz/1.6GHz)	2-16 (2-32)	1-4	256 GB	32	2400 GB
Superdome	Itanium 2 (1.6GHz)	2-64 (2-128)	1-16	1 TB	192	N/A

Table 1 - Evaluated Platforms

Environmental Requirements

47. The environmental assumptions for the TOE are stated in [ST] Section 3.

48. The TOE was evaluated running on platforms defined in Table 1 (in accordance with [MPR] and [UKI12]).

49. The threats countered by the environment are defined in [ST] Section 3.2.2. Procedural assumptions are defined in [ST] Section 3.1.1.

Test Configuration

50. The following configurations were used by the Developers and Evaluators for testing. Each server was available over a network from Windows XP Professional PCs or UNIX workstations. In each case a telnet session was established onto the server, from which access to the server could be gained.

Machine Name	Model	CPU	Memory	Firmware
Gilroy	ia64 hp server rx2620	2 Intel(R) Itanium 2 processors (1.6 GHz, 6 MB) 400 MT/s bus, CPU version A1	2040 MB	Firmware revision: 03.10 FP SWA driver revision: 1.18
thunk	ia64 hp server rx4640	8 Intel(R) Itanium 2 processors (1.1 GHz, 4 MB) 400 MT/s bus, CPU version B1	8183 MB	Firmware revision: 03.11
hpdfs046	ia64 hp server rx7620	6 Intel(R) Itanium 2 processors (1.1 GHz, 4 MB) 400 MT/s bus, CPU version B1	8175 MB	Firmware revision: 001.022 FP SWA driver revision: 1.18
hpdfs053	ia64 hp server rx7620	6 Intel(R) Itanium 2 processors (1.1 GHz, 4 MB) 400 MT/s bus, CPU version B1	4079 MB	Firmware revision: 001.022 FP SWA driver revision: 1.18
Chico	ia64 hp server rx2660	2 Intel(R) Itanium 2 9000 series processors (1.59 GHz, 18 MB) 532 MT/s bus, CPU version C2 4 logical processors (2 per socket)	8169 MB	Firmware revision: 01.05 FP SWA driver revision: 1.18

Machine Name	Model	CPU	Memory	Firmware
Oakley	ia64 hp server rx2660	2 Intel(R) Itanium 2 9000 series processors (1.59 GHz, 18 MB) 532 MT/s bus, CPU version C2 4 logical processors (2 per socket)	8169 MB	Firmware revision: 01.05 FP SWA driver revision: 1.18
Tracey	ia64 hp server rx3600	2 Intel(R) Itanium 2 9000 series processors (1.59 GHz, 18 MB) 532 MT/s bus, CPU version C2 4 logical processors (2 per socket)	8159 MB	Firmware revision: 02.03
Lawton0	9000/800/rp7420	3 PA-RISC 8800 processors (900 MHz, 32 MB) CPU version 5 6 logical processors (2 per socket) 1 PA-RISC 8800 processor (900 MHz, 32 MB) CPU version 4 2 logical processors (2 per socket)	8157 MB	Firmware revision: 22.2
Moraga	9000/800/rp3440	2 PA-RISC 8800 processors (800 MHz, 64 MB) CPU version 5 4 logical processors (2 per socket)	4094 MB	Firmware revision: 45.11

Table 2 - Developer Test Platforms

51. In addition to the platforms listed above the evaluators also had the TOE installed on another platform, listed below.

Machine Name	Model	CPU	Memory	Firmware
LCMG server	Ia64 HP server rx2620	2 Intel ® Itanium 2 Processors (1.3 GHz, 3 MB) 400 MT/s bus, CPU version A2	2036 MB	Firmware Revision: 03.17

Table 3 - Evaluator Platform

IV. PRODUCT ARCHITECTURE

Introduction

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

Product Description and Architecture

53. The TOE comprises a single product HP-UX 11i V3 plus relevant patches running on Hewlett-Packard's Precision 2.0 architecture (PA-RISC 2.0) or Intel® Itanium® 2 architecture.

54. 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.

55. The main security features of the product are:

- Audit;
- Identification and Authentication;
- Discretionary Access Control;
- Role Based Access Control;
- Object Reuse;
- Protection Functions.

Audit

56. The product is capable of collecting audit records for all security relevant events that occur. An authorized administrator may select the users and events for which audit data is collected from time to time.

57. Audit records may be viewed by an authorized administrator selectively for any period on the basis of criteria such as user name, event type and outcome.

58. Facilities are provided to enable the authorized administrator 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.

Identification and Authentication

59. 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.

60. The product supports an ordinary user role and an authorized administrator (administrative) role. An authorized administrator has ‘root privilege’ and is not constrained by the product’s security policies.

61. The product allows an authorized administrator to associate individual users with a privileged group, thus permitting a process acting on the user’s behalf to change the ownership of files.

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

Discretionary Access Control

63. 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.

64. 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.

65. The product implements 2 independent ACL mechanisms:

- HFS ACLs for the HFS File System;
- VxFS ACLs for the VxFS File System.

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

Role Based Access Control

67. In addition to the standard access control mechanisms, the TOE also provides a Role Based Access (RBAC) mechanism as an alternative to the all-or nothing security model of traditional root user-based systems. With RBAC, an authorized administrator can assign certain roles to non-root users or groups. Each role has certain authorizations composed of an operation and object. Non-root users can then execute commands or applications with elevated privileges that would otherwise be impossible. RBAC is a mechanism that maps users to certain permitted operations.

68. The TOE grants permissions to the authorized administrator for all operations, and denies permissions to non-root users on certain operations. This notion of privilege checking is

simple. But it is difficult to distribute the administrative responsibilities among a group of administrators, as they all need to have the access to the root account to perform any administrative action. For further details see the RBAC Protection Profile [RBAC].

Object Reuse Protection

69. Memory is allocated, managed, and access controlled, by a multitude of mechanisms, which ensure, for example, that when a page of memory is allocated to a process, only that process, or others that may have authorized access to that memory, can access that memory. Also, when memory is returned and made available for subsequent allocation, that page of memory is zeroed prior to subsequent allocation, to ensure no other process may access residual information contained therein as a result of its use by another process.

TOE Design Subsystems

70. Within the TOE there are four layers. These are:

- Hardware Trusted Computing (TCB) – which manages the execution of hardware instructions;
- Kernel TCB – executes privileged hardware commands and I/O;
- Non-Kernel TCB – contains executable and non-executable components which run in user mode;
- Untrusted programs and user commands.

Kernel TCB

71. The entire kernel software 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.

72. The kernel software is a collection of distinct logical subsystems, as follows:

- 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, enable memory sizes far in excess of actual hardware, for all processes. Further, this subsystem tracks all address space allocations to all processes, and prevents the unintended sharing of memory between processes, thereby maintaining address space integrity.
- Process Management - initiates processes, allocates and deallocates system resources, tracks and manages all processes within the system from point of initiation to final termination (for both kernel, and non-kernel processes).
- File System and Device Input/Output - provides for the creation, access, and manipulation of file system objects by other processes, and maintains device

independence for end user applications. This component provides the interface for low-level device I/O drivers and other processes.

- Inter Process Communications (IPC) Mechanisms - facilitate the synchronization of processes or events, and the sharing of information, between processes for both kernel and non-kernel processes.
- 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. A privileged application may also specifically request the kernel to generate a high-level audit record on its behalf.
- Access Mediation - enforces security policy for DAC 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.

73. 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

74. The non-kernel TCB contains executable and non-executable 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.

75. 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.

76. 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:

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

- TCB Databases, sets 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.
- Binary Libraries - containing the executable files for commands and user initiated actions.
- 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.
- Trusted Commands - 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.
- Batch Processing Programs - facilities that schedule the initiation and execution of programs at a future date.
- Role Based Access Control - an alternative to the all-or-nothing security model of traditional root user-based systems. With RBAC, an administrator can assign certain roles to non-root users or UNIX groups. Each role has certain authorizations composed of an operation and object.
- Aries Binary Translator - Software which emulates execution of PA-RISC applications on Itanium 2 systems.
- System Management Homepage - 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 SMH’s respective databases for use and interface by the foregoing components.

77. 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

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

TOE Interfaces

79. The external TSFI is described as follows:

- User Commands;
- Systems Administration Commands;
- System Calls;
- Library Functions;
- File Formats.

80. There are also internal interfaces between kernel and non-kernel software.

V. TOE TESTING

Test Configuration

81. The Developer’s tests covered all SFRs, all TOE high-level subsystems (as identified under ‘TOE Design Subsystems’), all SFRs and the TSFI (as identified under ‘TOE Interfaces’ in Chapter IV). The tests included those TOE interfaces which are internal to the product and thus had to be exercised indirectly.

82. The Developer ran their tests on several different platforms to support their arguments in [MPR]. Platforms used for testing are described in Table 2 in Chapter III.

83. The Evaluators devised and ran independent functional tests, different from those performed by the Developer. No anomalies were found. The Evaluators also devised penetration tests to address potential vulnerabilities considered during the evaluation. No exploitable vulnerabilities or errors were detected.

84. The Evaluators performed their testing at the Sponsor’s premises in Cupertino, United States of America, using the platforms listed in Table 2 in Chapter III and also at the LogicaCMG CLEF in Camberley, United Kingdom using the platform listed in Table 3 in Chapter III.

Vulnerability Analysis

85. The Evaluators’ vulnerability analysis, which preceded penetration testing, was based on public domain sources and the visibility of the TOE provided by the evaluation deliverables.

Platform Issues

86. The TOE was tested on the hardware platforms specified above under 'Test Configuration', with each test being performed on a range of platforms.

87. In addition, the Evaluators confirmed their agreement with the Developer’s Multi Platform Rationale [MPR] that the results of the evaluation would be applicable to other stated 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 above under 'Test Configuration'.

88. All of the platforms identified in the Developer’s Multi Platform Rationale [MPR] are of two types based on:

    - the HP 9000 PA-RISC (Precision Architecture - Reduced Instruction Set Computer) architecture version 2.0;
    - HP's Integrity (Itanium 2) architecture.

89. HP-UX 11i v3 source code is structured to permit common source to be used on all supported platforms (both HP 9000 and HP Integrity). The few exceptions to this rule apply to the lowest level machine dependent kernel code.

90. The hardware in the HP 9000 and HP Integrity 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 and Itanium 2 architectures. The Developer's Multi Platform Rationale [MPR] 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.

VI. REFERENCES

[A&R] Abbreviations and References,
UK IT Security Evaluation and Certification Scheme,
Issue 1.3, March 2006.

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

[CC1] Common Criteria for Information Technology Security Evaluation,
Part 1, Introduction and General Model,
Common Criteria Maintenance Board,
CCMB-2005-08-001, Version 2.3, August 2005.

[CC2] Common Criteria for Information Technology Security Evaluation,
Part 2, Security Functional Requirements,
Common Criteria Maintenance Board,
CCMB-2005-08-002, Version 2.3, August 2005.

[CC3] Common Criteria for Information Technology Security Evaluation,
Part 3, Security Assurance Requirements,
Common Criteria Maintenance Board,
CCMB-2005-08-003, Version 2.3, August 2005.

[CC_SUPP] CD HP-UX 11i v3 February 2007 Common Criteria Supplementary CD,
Hewlett-Packard,
December 2007, 5013-8833.

[CEM] Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Criteria Maintenance Board,
CCMB-2005-08-004, Version 2.3, August 2005.

[CR] Common Criteria Certification Report No. P225
Hewlett-Packard HP-UX Version 11.23 (11i Version 2)
running on HP 9000 or HP Integrity platforms,
UK IT Security Evaluation and Certification Scheme,
CRP225, Issue 1.0, May 2006.

[ECG] Common Criteria HP-UX 11i v3 Evaluated Configuration Guide,
HP9000 and HP Integrity Computers,
Hewlett-Packard, Issue 1.1, December 2007.

[ETR] Evaluation Technical Report,
LogicaCMG CLEF,
LFL 310.EC201717:v3:30.1, Version 1.0, February 2008.

[INSTALL] HP-UX 11i v3 Installation and Update Guide, 1,
Hewlett Packard,
February 2007.

[INSTANT] HP-UX 11i Version 3 HP Instant Information DVD,
Hewlett-Packard,
February 2007.

[MANPAGES] HP-UX Reference (Volumes 1 to 9) HP-UX 11i Version 3,
Hewlett-Packard,
February 2007.

[MPR] Multi-Platform Rationale, HP-UX 11i v3 Common Criteria,
Hewlett-Packard,
Version 0.3, September 2007.

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

[PARTITION] HP System Partitions Guide: Administration for nPartitions,
Hewlett-Packard,
5991-1247B, February 2007.

[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,
Hewlett-Packard,
December 2007.

[REL] HP-UX 11i Version 3 Release Notes,
Hewlett-Packard,
February 2007.

[SAG_SEC] HP-UX System Administrator's Guide: Security Management,
Hewlett-Packard,
Issue 1, February 2007.

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

[ST] Security Target,
Hewlett Packard,
Version 1.9, December 2007.

[UKI12] Multi-platform TOEs,
UK IT Security Evaluation & Certification Scheme,
UK CC Interpretation UK/2.3/012, Version 1.0, 1 March 2007.

[UKSP01] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.1, March 2006.

[UKSP02P1] CLEF Requirements – Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4, April 2003.

[UKSP02P2] CLEF Requirements – Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 2.1, March 2006.

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

This page is intentionally blank.