Certification Report

EAL 4+ Evaluation of Sun Microsystems Inc.

Solaris™ 10 Release 11/06

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document Number: 383-4-56-CR
Version: 1.0
Date: 6 November 2007
Pagination: i to v, 1 to 11

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 2.3*, for conformance to the *Common Criteria for IT Security Evaluation, Version 2.3*. This certification report, and its associated certificate, apply only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment (CSE), or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the CSE, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment (CSE)

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO Standard 17025, General requirements for the accreditation of calibration and testing laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is CGI Information Systems and Management Consultants Incorporated, located in Ottawa, Ontario.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) to which the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 6 November 2007, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list at http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html and on the official Common Criteria Program website at http://www.commoncriteriaportal.org.

This certification report makes reference to the following trademarked names:

- Java, Netra, Solaris, Sun Fire and Ultra are trademarks of Sun Microsystems, Inc, in the United States and other countries.
- AMD and AMD-64 are trademarks of Advanced Micro Devices, Inc., in the United States and other countries.
- SPARC is a trademark of SPARC International, Inc., in the United States and other countries.

TABLE OF CONTENTS

Executive Summary

Solaris™ 10 Release 11/06 (hereafter referred to as Solaris™ 10 11/06), from Sun Microsystems Inc., is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4+ evaluation.

Solaris™ 10 11/06 is a highly configurable operating system conformant to the Controlled Access Protection Profile (CAPP), Version 1.d, October 8, 1999 and to the Role Based Access Control Protection Profile (RBAC PP), Version 1.0, July 30, 1998.

CGI Information Systems and Management Consultants Incorporated is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed in October 2007, and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for Solaris™ 10 11/06, the security requirements, and the level of confidence (evaluation assurance level) to which it is asserted that the product satisfies its security requirements. Consumers are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the Evaluation Technical Report (ETR)[1] for this product provide sufficient evidence that it meets the EAL 4+ assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 2.3*, for conformance to the *Common Criteria for IT Security Evaluation, version 2.3*. The following augmentation is claimed: ALC_FLR.3 - Systematic flaw remediation.

CSE, as the CCS Certification Body, declares that the Solaris™ 10 11/06 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list.

[1] The Evaluation Technical Report is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 + evaluation is Solaris™ 10 Release 11/06 (hereafter referred to as Solaris™ 10 11/06), from Sun Microsystems Incorporated.

2 TOE Description

Solaris™ 10 11/06 is a highly configurable operating system conformant with the Controlled Access Protection Profile (CAPP), Version 1.d, October 8, 1999 and with the Role Based Access Control Protection Profile (RBAC PP), Version 1.0, July 30, 1998.

The TOE comprises Solaris™ 10 11/06 running on workstations and servers forming a distributed system. Such systems are typical of personal, workgroup, and enterprise computing systems used by multiple users for controlled shared access to data.

Section 2 of the ST provides a detailed TOE description.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Solaris™ 10 11/06 is identified in Sections 5.1 and 5.2 of the Security Target (ST).

4 Security Target

The ST associated with this Certification Report (CR) is identified by the following nomenclature:

Title: Solaris™ 10 11/06 Security Target
Version: 1.3
Date: September 11, 2007

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 2.3*, for conformance to the *Common Criteria for IT Security Evaluation, version 2.3*. Solaris™ 10 11/06 is:

a) Common Criteria Part 2 conformant, with security functional requirements based only upon functional components in Part 2;
b) Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3; and

c) Common Criteria EAL 4 augmented, containing all security assurance requirements from EAL 4 package, as well as ALC_FLR.3 - Systematic flaw remediation.

Solaris™ 10 11/06 is conformant to the Controlled Access Protection Profile (CAPP), Version 1.d, October 8, 1999 and to the Role Based Access Control Protection Profile (RBAC PP), Version 1.0, July 30, 1998.

6 Security Policy

Solaris™ 10 11/06 security policy details can be found in Section 6.1 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Solaris™ 10 11/06 should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will help to ensure the proper and secure operation of Solaris™ 10 11/06.

7.1 Secure Usage Assumptions

The following secure usage assumptions, which are consistent with the ST, were made during the evaluation of Solaris™ 10 11/06:

a) Each individual user has a unique user ID;
b) Those responsible for the Solaris™ 10 11/06 must configure minimum password length for normal users to be at least 6 but no more than 8 characters;
c) Rights for users to gain access and perform operations on information are based on their membership in one or more roles (and the profiles that accompany these roles). These roles are granted to the users by the Administrator. These roles accurately reflect the users job function, responsibilities, qualifications, and/or competencies within the enterprise;
d) A limited set of users is given the rights to "create new data objects" and they become owners for those data objects;
e) The system administrative personnel are neither careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the administrator documentation; and
f) Authorized users possess the necessary authorization to access at least some of the information managed by the Solaris™ 10 11/06 and act in a cooperative manner in a benign environment.

7.2 Environmental Assumptions

The following environmental assumptions, which are consistent with the ST, were made during the evaluation of Solaris™ 10 11/06:

a) All software and hardware, including network and peripheral cabling is approved for the transmission of the most sensitive data held by the system. Such items are physically protected against threats to the confidentiality and integrity of the data transmitted;

b) The processing resources of Solaris™ 10 11/06 are located within controlled access facilities which will prevent unauthorized physical access;

c) Physical controls are in place to alert system authorities to the physical presence of attackers within the controlled space;

d) If the product comprises more than one platform, then all platforms are administered from a central point;

e) All bridges and routers correctly pass data without modification;

f) All connections to peripheral devices reside within the controlled access facilities. Internal communication paths to interfaces points such as terminals are adequately protected; and

g) Any other systems with which the Solaris™ 10 11/06 communicates are under the same management control and operate under the same security policy constraints.

For more information about the Solaris™ 10 11/06 security environment, refer to Section 3 of the ST.

7.3 Clarification of Scope

As described in the ST, where specific threats to distributed systems need to be countered, the following clarifications apply:

a) Data transferred between platforms may be disclosed to, or modified by, unauthorized users or processes either directly or indirectly (e.g. through spoofing of workstation/server identity).

b) Compromise of assets may occur through improper administration or operation of the Solaris™ 10 11/06. For example, users could be assigned to roles that are not commensurate with their duties, giving them inappropriate authorizations.

These threats are not countered by Solaris™ 10 11/06 and are assumed to be countered by the measures within the environment.

8 Architectural Information

The Solaris™ 10 11/06 is an operating system that comprises the following main subsystems:

Kernel. The Kernel subsystem supports the security functionality of the product. Detail on security functionality can be found in Section 2.4 of the ST.

Kernel V Inter-Process Communications (SVIPC). Solaris™ 10 11/06 implements System V IPC (Inter Process Communication) that allows effective communication between processes. Three mechanisms are provided: Semaphores; Message Queues; and Shared Memory. The Semaphore mechanism allows processes to synchronize their execution using mutually exclusive access to critical sections. The Message Queue mechanism allows cooperating processes to send and receive formatted data between themselves. The Shared Memory mechanism allows processes to attach (map) system memory spaces to their virtual address spaces and share these attached system spaces.

File Systems. The File System component provides a system call interface used to access the variety of file system types supported by Solaris™ 10 11/06. The system call interface provides a consistent set of operations which can be performed on all the file system types.

Audit. The Audit subsystem collects extensive auditing information about security related actions taken or attempted by users, ensuring that users are accountable for their actions. For each such action or event an audit record is generated containing: date and time of the event, user, security attributes and success or failure. Detail on Audit can be found in Section 2.4.6 of the ST.

Identification and Authentication (I&A). The I&A subsystem provides identification and authentication as a built-in feature using the Pluggable Authentication Module (PAM) based on usernames and passwords. Detail on I&A can be found in Section 2.4.3 of the ST.

Lightweight Directory Access Protocol (LDAP). The LDAP subsystem maintains a central database of name services information for workstations and servers within a Domain.

Trusted Startup. The Trusted Startup subsystem ensures a secure transition from run level 0 (the power-down state) to the system run level.

Trusted Windowing. The Trusted Windowing subsystem provides the user with a choice of desktop environments. Solaris™ 10 11/06 includes both the Common Desktop Environment (CDE) windowing environment and Sun Java™ Desktop System (JDS) Operating Environment.

Trusted Admin Tools. The Trusted Admin Tools includes File Manager, which is a desktop application that enables users to create, locate, organize and work with files and directories

on the desktop, and Solaris™ Management Console (SMC), that provides the user a Graphical User Interface (GUI) and a set of tools to help in administering a distributed configuration.

9 Evaluated Configuration

The evaluated configuration for Solaris™ 10 11/06 comprises:

a) Platform 1: Entry Level workstations and servers using an UltraSPARC II, UltraSPARC IIe, UltraSPARC IIi, UltraSPARCIII, UltraSPARCIIIi, or UltraSPARC T1 processor in a single or multiple configuration.
b) Platform 2: The Netra™ 1280 and Sun Fire™ mid-frame and high-end family offering Dynamic Reconfiguration and Multiple Domaining using an UltraSPARC III Cu (copper based) or UltraSPARC IV processor.
c) Platform 3: AMD based processor systems: AMD Opteron 800, 1200, and 8000 series; AMD-64 100, 200, and 2000 series; AMD dual-core 1200 and 2000 series; AMD Opteron 285; and, Intel Xeon.

Appendix A of the ST provides the detailed evaluated configuration.

10 Documentation

The documentation for Solaris™ 10 11/06 consists of the following:

a) The Security Release Notes, Version 0.57, September 14, 2007;
b) The Delivery and Configuration Procedures, Version 0.5, November 27, 2006;
c) Solaris 10 11/06 Release and Installation Collection;
d) Solaris 10 Reference Manual Collection;
e) Solaris 10 System Administration Collection;
f) Solaris 10 User Collection;
g) Solaris 10 Release and Installation Collection;
h) Java Desktop System Release 3, User Documentation; and
i) Solaris 10 Common Desktop Environment User Collection.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Solaris™ 10 11/06, including the following areas:

Configuration management: The Solaris™ 10 11/06 evaluation made use of results from the previous Solaris™ 9 8/03 evaluation. The developer attests that configuration management (CM) has not changed since the Solaris™ 10 03/05 evaluation. Access to the CM system is still dictated by the same framework that was in place for the Solaris™ 10

03/05 and prior systems. There is no change in the CM system from Solaris™ 10 03/05, thus unauthorized access to the configuration items is prevented. The manual and automated tools and procedures described in the CM plan are still in use for Solaris™ 10 11/06 development and the CM system is still being used in conformance with the CM documentation provided. The configuration items are still being effectively maintained under the CM system.

Secure delivery and operation: The Solaris™ 10 11/06 evaluation made use of results from the previous Solaris™ 10 03/05 evaluation. The developer attests that secure delivery has not changed since the Solaris™ 10 03/05 evaluation. The evaluators examined and tested the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Design documentation: The evaluators examined design documentation for the Solaris™ 10 11/06 including the functional specification, high-level design, low level design, security policy model and source code. The evaluators concluded that the design documents completely and accurately describe all interfaces and security functions of the product and are internally consistent.

Guidance documents: The evaluators examined the Solaris™ 10 11/06 user and administrator guidance documentation and determined that it sufficiently and unambiguously described how to securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

Life-cycle support: The Solaris™ 10 11/06 evaluation made use of results from the previous Solaris™ 10 03/05 evaluation. The developer attests that Life-cycle support has not changed since the Solaris™ 10 03/05 evaluation.

Vulnerability assessment: The evaluators validated the developer's vulnerability, misuse and strength of function analyses. The Solaris™ 10 11/06 strength of function claims were validated through independent evaluator analysis. The evaluators performed an independent vulnerability analysis and developed tests that focused on potential vulnerabilities in Solaris™ 10 11/06.

All these evaluation activities resulted in **PASS** verdicts.

12 ITS Product Testing

Testing at EAL 4 consists of the following three steps: assessing the developer's tests in terms of coverage and depth, performing independent functional tests, and performing independent penetration tests.

12.1 Assessing Developer Tests

The evaluators verified that the developer had met their testing responsibilities by reviewing the developer's test plan, test approach, test procedure and test results, and examining their test evidence, as documented in the Evaluation Technical Report (ETR)[2].

The evaluators reviewed the developer's test coverage and depth, and found them to be complete and accurate. The correspondence between tests identified in the developer's test documentation, and the functional specification and the high-level design was complete.

The evaluators executed a 25% sample of the developer's tests, comprising 5 separate test sets.

12.2 Independent Functional Testing

During the evaluation, the evaluators developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests. Independent testing concentrated on the following areas:

a) policy enforcement;

b) audit;

c) object reuse;

d) identification and authentication;

e) discretionary access control;

f) secure communications; and

g) session locking.

12.3 Independent Penetration Testing

After reviewing the technical specifications and product documentation, a flaw hypothesis methodology was used to develop a list of potential vulnerabilities of the TOE. Those vulnerabilities assessed as potentially exploitable by an attacker possessing a low attack potential were used to develop penetration test cases.

[2] The Evaluation Technical Report is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review

The following potential attack areas were assessed during the development of potential attack scenarios:

a. Generic vulnerabilities;
b. Bypassing;
c. Tampering;
d. Direct attacks; and
e. Misuse.

A total of 12 penetration attacks were developed and exercised against the TOE.

Penetration testing did not uncover any exploitable vulnerabilities for the Solaris™ 10 11/06 in its anticipated operating environment.

12.4 Conduct of Testing

Solaris™ 10 11/06 was subjected to a comprehensive suite of formally documented, independent, functional and penetration tests. The testing took place at the ITSET facility at CGI Information Systems and Management Consultants Incorporated, located in Ottawa, Ontario. The CCS Certification Body witnessed a portion of the independent testing. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in the ETR.

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that Solaris™ 10 11/06 behaves as specified in its ST and functional specification. The penetration testing resulted in a **PASS** verdict, as the evaluators were unable to exploit any of the identified potential vulnerabilities in Solaris™ 10 11/06 in its intended operating environment.

13 Results of the Evaluation

This evaluation has provided the basis for an **EAL 4+** level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

14 Evaluator Comments, Observations and Recommendations

As described in the ST and previous sections of this document, where specific threats to distributed systems need to be countered, such threats are not countered by the Solaris™ 10 11/06 and are assumed to be countered by measures within the environment. Consumers are advised to review the ST and ensure that their deployment environment is consistent with the defined intended environment.

15 Glossary

This section expands any acronyms, abbreviations and initializations used in this report.

Acronym/Abbreviation/Initialization	Description
CAPP	Controlled Access Protection Profile
CB	Certification Body
CC	Common Criteria for Information Technology Security Evaluation
CCEF	Common Criteria Evaluation Facility
CCRA	Common Criteria Recognition Arrangement
CCS	Common Criteria Evaluation and Certification Scheme
CDE	Common Desktop Environment
CEM	Common Methodology for Information Technology Security Evaluation
CR	Certification Report
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GUI	Graphical User Interface
I&A	Identification and Authentication
ISO	International Organisation for Standardisation
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
JDS	Java™ Desktop System
LDAP	Lightweight Directory Access Protocol
SMC	Solaris™ Management Console
SVIPC	Kernel V Inter-Process Communications
LDAP	Lightweight Directory Access Protocol
OS	Operating System
PALCAN	Program for the Accreditation of Laboratories Canada
PAM	Pluggable Authentication Module
PP	Protection Profile
RBAC	Role Based Access Control
ST	Security Target
TOE	Target of Evaluation
TSF	TOE security functions

16 References

This section lists all documentation used as source material for this report:

a) Canadian Common Criteria Evaluation and Certification Scheme (CCS) Publication #4, Technical Oversight, Version 1.0.

b) Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

c) Common Methodology for Information Technology Security Evaluation, Version 2.3, August 2005;

d) Controlled Access Protection Profile (CAPP), Version 1.d, October 8, 1999;

e) Role Based Access Control Protection Profile (RBAC PP), Version 1.0, July 30, 1998;

f) Solaris™ 10 11/06 Security Target, Version 1.3, 11 September 2007; and

g) Evaluation Technical Report of Solaris™ 10 11/06, Version 1.4, 30 October 2007.