National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Silicon Graphics, Inc.
Trusted IRIX/CMW Version 6.5.13
with patches 4354, 4451, 4452, 4373, and 4473

Report Number: CCEVS-VR-02-0020

Dated: 10 May 2002

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

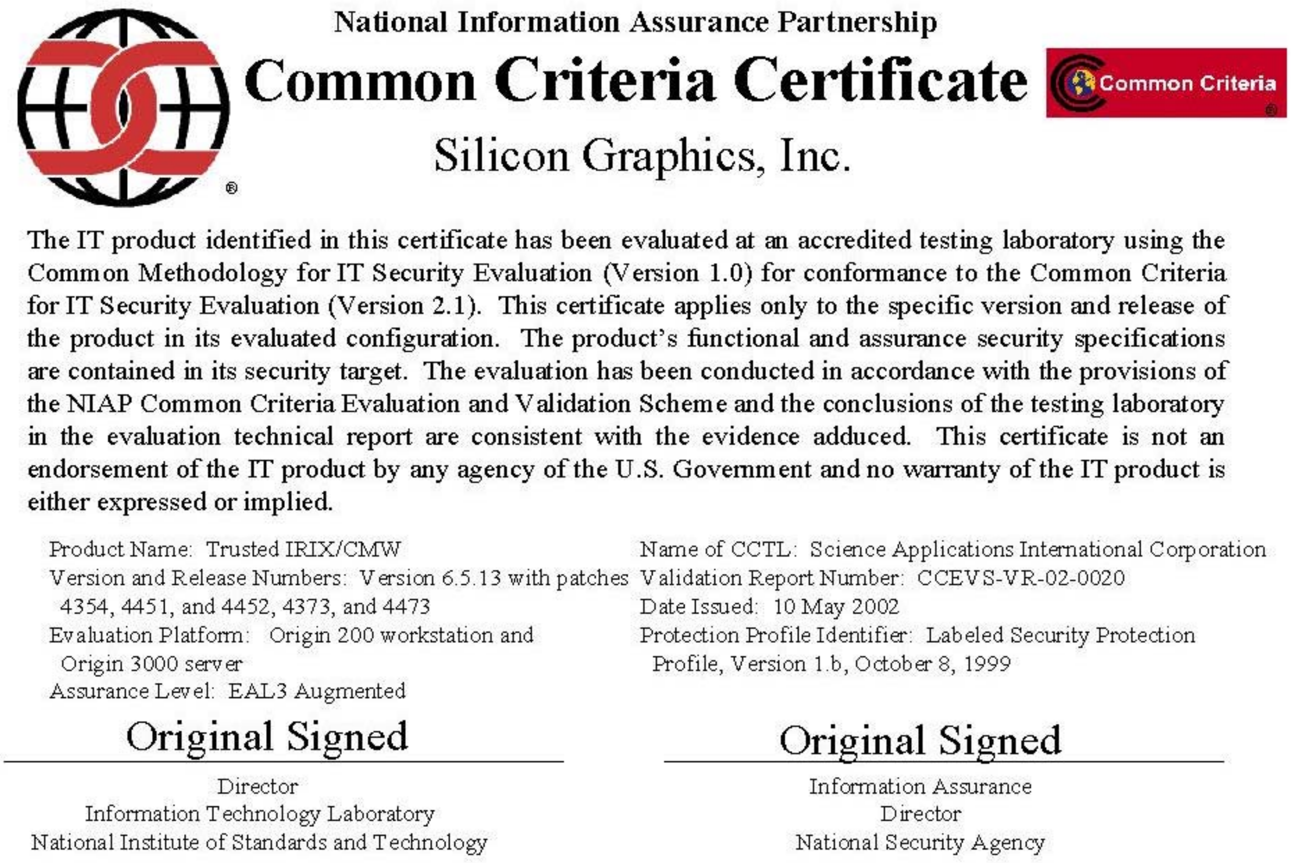
Validation Team

Bradford O'Neill
Frank Belvin
Jean Hung
The MITRE Corporation
Bedford, Massachusetts

Janine Pedersen
National Security Agency
Ft. George G. Meade, Maryland

Common Criteria Testing Laboratory

Science Applications International Corporation
Columbia, Maryland



National Information Assurance Partnership

Common Criteria Certificate

Silicon Graphics, Inc.

The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.1). This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Product Name: Trusted IRIX/CMW
Version and Release Numbers: Version 6.5.13 with patches 4354, 4451, and 4452, 4373, and 4473
Evaluation Platform: Origin 200 workstation and Origin 3000 server
Assurance Level: EAL3 Augmented

Name of CCTL: Science Applications International Corporation
Validation Report Number: CCEVS-VR-02-0020
Date Issued: 10 May 2002
Protection Profile Identifier: Labeled Security Protection Profile, Version 1.b, October 8, 1999

Original Signed

Director
Information Technology Laboratory
National Institute of Standards and Technology

Original Signed

Information Assurance
Director
National Security Agency

Table of Contents

LIST OF FIGURES

LIST OF TABLES

1 EXECUTIVE SUMMARY

This report documents the NIAP validators' assessment of the CCEVS evaluation of SGI Trusted IRIX Version 6.5.13, hereinafter referred to as Trusted IRIX. It presents the evaluation results, their justifications, and the conformance result.

The evaluation was performed by Science Applications International Corporation (SAIC) and was completed on 10 May 2002. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by SAIC and submitted to the validators. The evaluation determined the product conform to the CC Version 2.1, Part 2 and Part 3 to meet the requirements of **EAL 3 with augmentation**, resulting in a "pass" in accordance with CC Part 1 paragraph 175. Evaluation Assurance Level (EAL) 3 has been augmented with the Security Policy Modeling (ADV_SPM.1) requirement. The Target of Evaluation (TOE) also conforms to the Labeled Security Protection Profile, version 1.b.

The Trusted IRIX system under evaluation is a system of Silicon Graphics Computer Systems, Inc. (SGI) Origin200 workstations and Origin 3000 servers connected via an Ethernet. These UNIX-based, multi-user, multi-tasking workstations provide high-performance, general-purpose computing. The processor of the workstation and server is the SGI MIPS R12000.

The Trusted IRIX operating system is a security-enhanced version of the IRIX operating system. In addition to the IRIX identity-based discretionary access control (DAC) on system resources, Trusted IRIX controls access to system resources based on the sensitivity and integrity labels of each resource. Trusted IRIX supports a set of access control policies; an identification and authentication capability to mediate and validate requests for entry into the system; an audit trail capability; and networking capability. The administrator guidance documents and product release notes provide the administrator with specific instructions to ensure that the product is installed in an appropriate environment.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, reviewed selected evaluation evidence, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that SAIC's findings are accurate, the conclusions justified, and the conformance results correct.

Disclaimers: The information contained in this Validation Report is not an endorsement of Trusted IRIX by any agency of the U.S. Government and no warranty of Trusted IRIX is either expressed or implied.

2 IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Accreditation Program (NVLAP) accreditation.

The NIAP Validation Body assigns validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List. Table 1 provides information needed to completely identify the product, including:

- the Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated,

- the Security Target (ST), describing the security features, claims, and assurances of the product,

- the conformance result of the evaluation,

- the organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Trusted IRIX Version 6.5.13 with Patches 4354, 4451, 4452, 4373, and 4473
Protection Profile	Labeled Security Protection Profile (LSPP), version 1.b, October 8, 1999
Security Target	SGI Trusted IRIX/CMW Version 6.5.13, Security Target Version 1.9
Evaluation Technical Report	Evaluation Technical Report for the IRIX version 6.5.13, with Patches 4354, 4451, and 4452, and the Trusted IRIX/CMW version 6.5.13, with Patches 4354, 4451, 4452, 4373, and 4473, Version 0.2, April 11, 2002.
Conformance Result	Part 2 conformant, Part 3 augmented, and EAL 3
Version of CC	CC Version 2.1 [1], [2], [3], [4] and all applicable National and International Interpretations effective on February 13, 2001
Version of CEM	CC Version 1.0 [5], [6] and all applicable National and International Interpretations effective on February 13, 2001
Sponsor	Silicon Graphics, Inc.
Developer	Silicon Graphics, Inc.
Evaluators	Science Applications International Corporation Ms. Cynthia Reese Ms. Shukrat A. Abbas Mr. James L. Arnold Jr Ms. Farideh Moghadami Ms. Evencie Pierre Government Participants Ms. Marvella Towns
Validators	Mr. Bradford O'Neill (The MITRE Corporation) Mr. Frank Belvin (The MITRE Corporation) Ms. Jean Hung (The MITRE Corporation) Mrs. Janine Pedersen (NSA)

3 SECURITY POLICY

Trusted IRIX is a security-enhanced version of IRIX. . In addition to the IRIX identity-based discretionary access control (DAC) on system resources, Trusted IRIX's mandatory access control (MAC) policy controls access to system resources based on the sensitivity and integrity labels of each resource. The MAC policy is based on the Bell and LaPadula [1] model and the Biba [2] model. Trusted IRIX supports the access control policies; an identification and authentication capability to mediate and validate requests for entry into the system; an audit trail capability; and networking capability. Trusted IRIX supports a least privilege mechanism. The SuperUser privileges have been broken out into a set of distinct capabilities, which can be granted and relinquished through a set of inheritance rules.

Mandatory Access control

Trusted IRIX's MAC policy for sensitivity and integrity is implemented with labels. Each protected resource has associated with it a label that has two components: a sensitivity and an integrity component. These labels are used to determine access to a resource in accordance with the system's MAC policy. This policy defines a dominance relationship between the labels. Sensitivity labels define the secretness or classification of files and resources and the clearance level of users. A sensitivity label is composed of a sensitivity level and possibly some number of sensitivity categories.

While the sensitivity labels identify whether a user is cleared to view certain information, integrity labels identify whether data is reliable enough for a specific user to see. An integrity label is composed of an integrity grade and some number of integrity divisions. SGI uses the integrity component of the label as a TOE identification and isolation mechanism. All software components of the TOE are labeled with a system high integrity level. Therefore, this integrity level in the label identifies the resource as being within the TOE. Also, all system processes that run as part of the TOE execute with system high integrity. Administrators may have this integrity level as part of their label, but it is not within the range available to other users. Thus, users do not have the ability to write a program that can be executed by an administrator. The Trusted IRIX MAC policy does not allow any user to modify a TOE file and no administrator to invoke a program that is not in the TOE

The access-control enhancements to Trusted IRIX allow the administrator to set up levels of clearance and related categories of files and other resources, and to assign each user a clearance (or range of clearances). Through this system of access controls, the administrator can custom tailor a user's environment so that the particular user has access only to those files and resources he or she needs to complete required tasks.

Discretionary Access Control

Trusted IRIX supports traditional file permission bits working in concert with the more versatile Access Control Lists (ACLs).. Discretionary Access Control (DAC) permissions are defined by the user who owns the file in question. For example, if a user has a personal file in his or her home directory, that user can set the DAC permissions to allow no other users on the system to view, copy, or edit that file. Default DAC permissions for newly created files are set via the umask command.

Thus, to gain access to a file that was created by another user, a user must not only have the proper MAC clearance, but must have set the DAC permissions on the file to allow others to access it. DAC permissions should be set in accordance with site security policies.

Default DAC permissions for newly created files depend on the umask and on any default ACL entries found in the containing directory.

Identification and Authentication

The Identification and Authentication (I&A) mechanism controls user access to the system. In common terms, the I&A mechanism is the login procedure. This subsystem is always active if the system is running, and it is impossible to have any contact with the system without first logging in through the I&A system.

The improved I&A facilities of Trusted IRIX allow the administrator to be certain that the people on the system are authorized users and that private password integrity is maintained to the highest possible levels.

Under Trusted IRIX, encrypted passwords are stored separately from other user identification information. This separate location is hidden from normal user access, so the process of a systematic dictionary encryption hunt for a password is precluded. User clearance information is also stored in a hidden or shadow file. Under Trusted IRIX, the /etc/passwd file does not contain the encrypted password; only the shadow password file contains that information.

Individual users may have a range of security levels available that have been predetermined by the administrator. The user is not always required to log in at the highest assigned level, thus allowing the flexibility to log in at a level appropriate for a given task.

System Audit Trail

A foundation of Trusted IRIX is the system audit trail. The system audit trail provides a means for the system administrator to oversee each important event that is taking place on the system. The audit trail is useful for tracking changes in sensitive files and programs and for identifying inappropriate use of the system.

The audit trail is generated by additional code in the operating system kernel that notes specific important events, such as file creation, file changes, file removal, invocation of programs, and the login and logout events.

The audit subsystem allows the administrator to create a dynamic record of the system's activity. Audit records of security relevant events are generated on each workstation of the Trusted IRIX system. These records contain the initial login identifier of the user who initiated the audited event and allow the administrator to hold each user strictly accountable for his or her actions. Trusted IRIX commands allow the system administrator to selectively audit events. SGI provides tools to reduce the audit logs for analysis. The audit system is completely configurable at any time by the audit administrator.

Audit information must be carefully gathered and protected so that actions affecting security can be traced to the responsible party. Trusted IRIX records the occurrences of security-relevant events in an audit log. For each event audited, the system records the date and time of the event, the initiating user, the type of event, the success or failure of the event, and the name and security classification of the files or programs used.

Object Reuse Policy

To preclude accidental disclosure of data, display memory and long-term data storage are subject to an object reuse policy and implementation. For example, all system memory is always automatically cleared before it is allocated to another program. Surrendered disk space is also cleaned before it is reallocated.

4 ASSUMPTIONS AND CLARIFICATION OF SCOPE

4.1 Usage Assumptions

The evaluation made the following assumptions concerning product usage:

- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instruction provided by the TOE documentation.
- Authorized users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.
- Procedures exist for granting users authorization for access to specific security levels.
- Procedures exist for establishing the security level of all information imported into the system, for establishing the security level for all peripheral devices (e.g., printers, tape drives, disk drives) attached to the TOE, and marking a sensitivity label on all output generated.
- Procedures exist for the administrator to ensure that all internal representations of security levels are consistent between all machines.
- The TOE must operate under a single management domain with each TSF sharing the same identification and authentication database.

4.2 Environmental Assumptions

The evaluation made the following environmental assumptions:

- The processing resources of the TOE will be located within controlled access facilities which will prevent unauthorized physical access.
- The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
- Any other systems with which the TOE communicates are assumed to be under the same management control and operated under the same security policy constraints. LSPP-conformant TOEs are applicable to networked or distributed environments only if the entire network operates under the same constraints and resides within a single management domain. There are no security requirements which address the need to trust external systems or the communications links to such systems.
- All connections to peripheral devices reside within the controlled access facilities. LSPP-conformant TOEs only address security concerns related to the manipulation of the TOE through its authorized access points. Internal communication paths to access points such as terminals are assumed to be adequately protected.

4.3 Clarification of Scope

All TOE security objectives were derived from the ST's organizational security policies and the ST did not list any threats. Therefore, there are no threats that were not countered by the TOE.

5 ARCHITECTURAL INFORMATION

The system under evaluation is a system of Silicon Graphics Computer Systems, Inc. (SGI) Origin200 workstations and the Origin 3000 servers connected via an Ethernet. The workstations and servers run the Trusted IRIX operating system. The processor of the workstation and server is the SGI MIPS R12000.

The Origin 3000 Series is a family of modular computer server systems. The various internal components of the various Origin 3000 servers and their functions are divided into separate units called "bricks". These bricks are housed in short or tall rack enclosures. The Origin200 workstation is a multiprocessor system that consists of one or two chassis, which are called modules. The Origin200 GIGAchannel uses an additional chassis to provide extra peripheral device interfaces. In the evaluated configuration, the following peripherals can be attached to a computer system: fixed disk drives, SCSI tape drive, CD-ROM drive, floppy disk drive, and network interface. In addition, a dumb terminal and/or dumb printer can be attached to an Origin200 computer system.

Trusted IRIX is a UNIX-based multi-user, multi-tasking operating system that supports the following security policies: discretionary access control; mandatory access control; identification and authentication; auditing, and object reuse. The services provided by the Trusted IRIX system have been divided into logical subsystems. Each subsystem is responsible for policy enforcement or for maintaining information used by other subsystems for policy enforcement. Figure 1 Architectural Overview presents an architectural overview of the product. A more detailed description of each subsystem may be found in Annex A. The subsystems are organized into following three portions: hardware, kernel-mode, and user-mode.

The Trusted IRIX system executes instructions in two broad domains. Commands and applications execute in user-mode. In this mode, the memory management system and hardware restrictions on instruction execution isolate processes from each other, from operating system control data, and from direct hardware access. This establishes a strong separation of the instruction streams and data contained in one process from those found in another process.

A process may initiate an operating system request from user-mode through the system call trap mechanism. A system call trap is a software interrupt operation that causes a context switch from user-mode into kernel-mode. In kernel-mode, only defined code sequences are executed to perform the requested function. This kernel code sequence, however, has unrestricted direct access to kernel control data and the hardware.

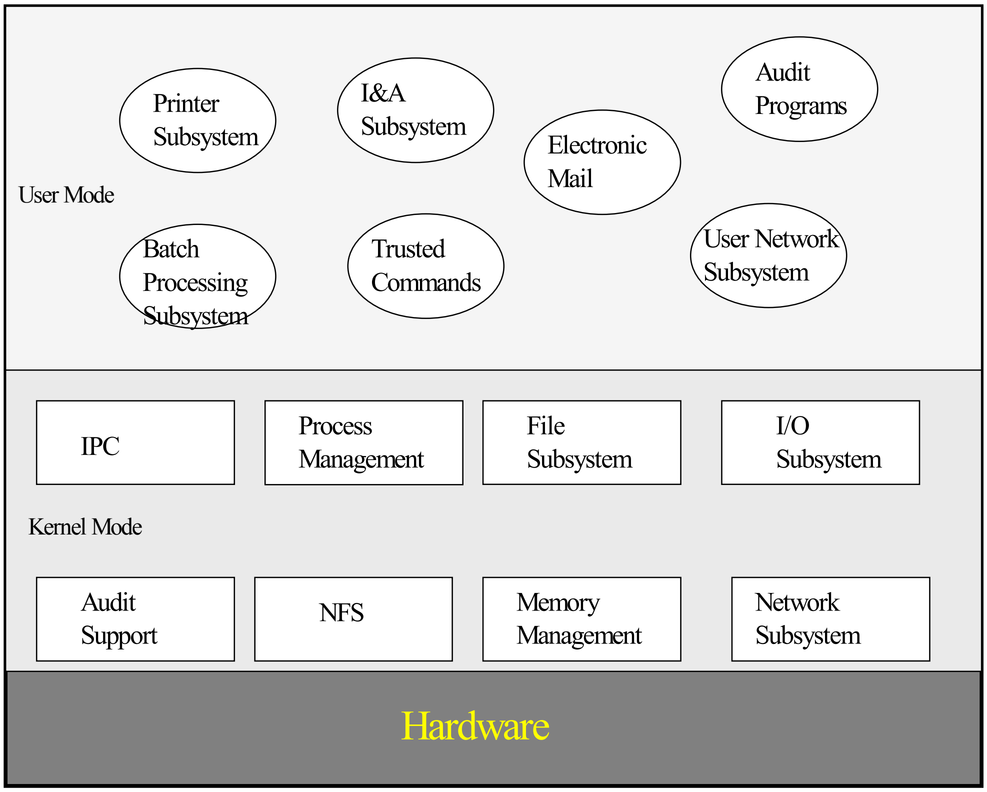


Figure 1: Architectural Overview

6 DOCUMENTATION

This section provides a complete listing of the documentation provided with the product by the developer to the consumer.

1) Administrative Guidance
   a. Trusted IRIX/CMW Security Administration Guide, 007-3299-005, August, 2001
   b. IRIX Admin: Backup, Security, and Accounting, 007-2862-004
   c. Trusted IRIX/CMW Security Administration Guide Release Notes for Release 6.5.13 Common Criteria Evaluation
   d. IRIX 6.5 man pages (only commands referenced in the Administrative Guidance)
2) User Guidance
   a. Trusted IRIX/CMW Security Features User's Guide, 007-3300-003
   b. Trusted IRIX/CMW Security Features User's Guide Release Notes for Release 6.5.13 Common Criteria Evaluation, version 1.0
   c. IRIX 6.5 man pages (only commands referenced in the User Guidance)
3) Delivery and Installation
   a. IRIX/Trusted IRIX Delivery and Installation, Revision 3.0, 4/9/02

7 IT PRODUCT TESTING

7.1 Developer Testing

The developer maintains a suite of tests to demonstrate that the product satisfies the claims that were made in the Security Target. This testing was primarily accomplished through the use of an automated test suite. The test driver executes individual test scripts and saves their output to a file. The test driver then compares the each test's output to its golden file and will report any significant differences as a test failure. The test's output contains enough information to describe what action took place, the current environment including the subject and object details, and the result. The golden output file is an output file from previous test execution that contains the expected output for the test. The developer manually examined each golden file to confirm that the test's objectives were satisfied. The automated tests were supplemented with a small number of manual tests.

The developer used a gray box methodology. Basic tests were run against every external security function interface. One interface was used for more extensive testing of the capability, MAC, DAC, and audit mechanisms. Auditing records, where required, were captured for a successful case and an unsuccessful case. In general, to demonstrate the expected test behavior both the successful and unsuccessful outcomes are executed. System calls and commands which modify security attributes of objects also included functionality tests. The implementation of these tests demonstrates the effect of the function when successfully called. The majority of tests fall under one of the following categories:

- The calling process has MAC access to the object or the appropriate MAC capability.
- The calling process has DAC access to the object or the appropriate DAC capability.
- The calling process has the required capabilities to perform the action, in addition to MAC or DAC capabilities that may be required.
- An audit record is generated when performing the action.
- The function creates a new object or modifies an object's attributes.

7.2 Evaluator Testing

The evaluators performed almost all of the tests in the developer's test suite. The evaluation team installed the Trusted IRIX operating system on two computer systems: an Origin200 workstation and an Origin 3000 server. The team ran all tests in developer's automated test suite on both the Origin200 and the Origin 3000 computer systems. The team executed all of the automated NFS tests using the Origin200 as the client and the Origin 3000 as the server. The evaluation team also performed a representative sample of the manual tests on the Origin 200. Approximately 20% of the manual tests, covering 8 subsystems, were executed. The team examined the test output to confirm that the actual test results were consistent with the expected results.

The evaluators performed some independent product testing of their own design. Through analysis of the developer's test suite, the evaluators determined that the developer testing was thorough enough to confirm that the TOE provided the functionality claimed in the ST with only a few exceptions. Hence, the evaluators did not develop a large number of independent tests. Based on a review of the subsystem specifications and the developer's test suite, the evaluation team identified specific functionality for additional independent testing. The team tests demonstrated functionality across nine of the twelve security functions described in the Security Target. Included in the nine, were the MAC, DAC, audit, and identification and authentication functions. The evaluation team also developed penetration tests based upon their review of the vendor's vulnerability assessment, wherever needed, to confirm the non-exploitability of potential vulnerabilities that had been noted in the course of the evaluation. This included testing, in support of the SOF analysis, to confirm that the rate at which repeated non-automated password guesses could be made was not unacceptably high.
Test procedures and expected results were developed for each test. After each test was performed, the evaluators confirmed that the actual results matched the expected results.

The evaluation team reviewed all of the security functions and the mapping between security functions and tests and concluded all security functions were appropriately tested. The evaluators also manually examined each golden file to confirm that the test's objectives were satisfied. The results of the evaluation team tests and the evaluation penetration tests demonstrated the product behaved as claimed in the Security Target. The testing found that the product was implemented as described in the functional specification and did not uncover any undocumented interfaces or other security vulnerabilities.

8 EVALUATED CONFIGURATION

The TOE hardware consists of Origin200 workstations and Origin 3000 servers connected via Ethernet. The TOE was evaluated for two basic hardware configurations. In both configurations the Trusted IRIX operating system was installed and configured according to the Installation and Delivery document. In one configuration, the hardware was an Origin200 workstation. In the other, the hardware was an Origin 3000 server. The network interfaces for both hardware configurations were evaluated. The physical Ethernet/IP network components were not evaluated and are regarded as an internal communication path that must be adequately protected. The environmental and usage assumptions described in this report are applicable to all evaluated configurations.

9 RESULTS OF THE EVALUATION

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 2.1 [1], [2], [3] [4] and CEM version 1.0 [5], [6] and all applicable National and International Interpretations in effect on November 21, 2000. The evaluation determined the product to be Part 2 conformant, and to meet the Part 3 Evaluation Assurance Level (EAL 3) requirements. The details of the evaluation are recorded in Evaluation Technical Report [8] which is controlled by SAIC.

9.1 Evaluation of the Trusted IRIX Security Target (ST) (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Trusted IRIX product that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluation team ensured the ST is consistent and compliant with the LSPP.

9.2 Evaluation of the CM capabilities (ACM)

The evaluation team applied each EAL 3 ACM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to control and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, and the CM documentation. The procedures reduce the risk that security flaws exist in the TOE implementation or TOE documentation.

9.3 Evaluation of the Delivery and Operation documents (ADO)

The evaluation team applied each EAL 3 ADO work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely.

9.4 Evaluation of the Development (ADV)

The evaluation team applied each EAL 3 ADV work unit, and the ADV_SPM.1 work units. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a high-level design document and a subsystem specification per subsystem. Section 5, Architectural Information, includes a description of each subsystem. The collection of subsystem specifications and the high-level design document describe the external interfaces of the TOE and the architecture of the TOE in terms of internal subsystems. The subsystem specifications and the high-level design document were determined by the evaluation team to sufficiently meet the requirements of a functional specification and a high-level design. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

Additionally, the evaluation team ensured that the Trusted IRIX security policy model document clearly describes the security policy rules which were found to be consistent with the design documentation.

9.5 Evaluation of the guidance documents (AGD)

The evaluation team applied all AGD EAL 3 CEM work units. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE.

9.6 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied all ALC EAL 3 CEM work units. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance.

9.7 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied all EAL 3 ATE CEM work units. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the subsystem specifications (functional specification and high-level design specification). The evaluation team performed a sample of the vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

Vulnerability Assessment Activity (AVA)

The evaluation team applied all AVA EAL 3 CEM work units. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the vendor strength of function analysis and the vendor vulnerability analysis, and the evaluation team's misuse analysis and performance of penetration tests.

9.8 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of a subset of the vendor tests suite, independent tests, and penetration test also demonstrate the accuracy of the claims in the ST.

10 VALIDATOR COMMENTS

The CC's ADV and ATE assurance requirements ensure that the TOE performs as described in its design documents and that the design documents are consistent with claims made in the ST. For the Trusted IRIX evaluation the functional specifications for the TSFI consisted of subsystem specifications supplemented by the traditional UNIX “man” pages with the subsystem specifications given precedence. Therefore, the “man” pages that are provided to the end-user should not be viewed as authoritative. Furthermore, the subsystem specifications did not explicitly reference the POSIX P1003.1e standard. Therefore, any statements regarding the implementation of POSIX P1003.1e features (e.g., capabilities and access control lists) are for informational use only and do not imply that the TOE was tested for conformance with the POSIX P1003.1e standard.

11 SECURITY TARGET

The Security Target, "Silicon Graphics, Inc. Trusted IRIX/CMW Version 6.5.13, Security Target Version 1.9, May 1, 2002", is included here by reference.

12 GLOSSARY

ACL	Access Control List
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
CI	Configuration Items
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
I&A	Identification and Authentication
I/O	Input/Output
IP	Internet Protocol
IPC	Interprocess Communications
LSPP	Labeled Security Protection Profile
MAC	Mandatory Access Control
MRA	Mutual Recognition Arrangement
NIAP	National Information Assurance Program
NIST	National Institute of Standards & Technology
NFS	Network File System
NVLAP	National Voluntary Laboratory Accreditation Program
OR	Observation Report
PP	Protection Profile
RISC	Reduced Instruction Set Computer
RPC	Remote Procedure Call
SAR	Security Assurance Requirement
SFR	Security Functional Requirements
SGI	Silicon Graphics, Inc
SMTP	Simple Mail Transfer Protocol
SOF	Strength of Function

ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TSF Interface
UDP	User Datagram Protocol
UID	User Identifier

13 BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.1.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, Version 2.1.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, Version 2.1.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[7] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001.

[8] Evaluation Technical Report for the IRIX version 6.5.13, with Patches 4354, 4451, and 4452, and the Trusted IRIX/CMW version 6.5.13, with Patches 4354, 4451, 4452, 4373, and 4473, Version 0.2, April 11, 2002.

[9] Silicon Graphics, Inc. Trusted IRIX/CMW Version 6.5.13, Security Target Version 1.9, May 1, 2002.

ANNEX A

Detailed Architectural Information

The services provided by the Trusted IRIX system are easiest to describe when divided into logical subsystems. Each subsystem is responsible for policy enforcement or for maintaining information used by other subsystems for policy enforcement. The following discussion provides a brief functional description of each major subsystem of Trusted IRIX. The discussion is divided into three portions – hardware, kernel-mode, and user-mode.

The Trusted IRIX system executes instructions in two broad domains. Commands and applications execute in user-mode. In this mode, the memory management system and hardware restrictions on instruction execution isolate processes from each other, from operating system control data, and from direct hardware access. This establishes a strong separation of the instruction streams and data contained in one process from those found in another process.

A thread within a share-group may initiate an operating system request from user-mode through the system call trap mechanism. A system call trap is a software interrupt operation that causes a context switch from user-mode into kernel-mode. In kernel-mode, the thread can only execute the kernel defined code sequence that follows from a system call. This kernel code sequence, however, has unrestricted direct access to kernel control data and the hardware.

A.1 Hardware

The evaluated hardware of the Trusted IRIX workstation is the Origin200 equipped with one or two disk drives and a dumb terminal connected to a serial interface. One or more workstations in a system may have tape drives and printers attached to them. The evaluated configuration of the Origin 3000 server consists of various internal components that are divided into separate units called "bricks". These bricks are housed in short or tall rack enclosures. The processor for the Origin200 and Origin 3000 is a MIPS R12000 processor.

A.2 Kernel-mode

A.2.1 Process Management

The Process Management subsystem maintains all processes and share-groups under the control of the Trusted IRIX system. It provides external operating system interfaces for creating a new process, changing its attributes, establishing a new execution image, and destroying the process. The process management subsystem also provides the means for delivering signals from one process to another and controlling the execution of a process from another process for the purpose of debugging and similar functions.

A.2.2 File Management

The file management subsystem provides a name space and storage management mechanism for Trusted IRIX objects that present an external interface based on the file abstraction. File management does not encompass operations on files across a network because these involve more complex negotiation between the local and the remote Trusted IRIX system. For the sake of clarity, this description segregates these responsibilities within the Network File System (NFS) subsystem. The file management subsystem does, however, play a crucial role in the Network File System operational model.

A.2.3 NFS

The NFS enables users to access files from remote hosts within the Trusted IRIX network using the same file system commands used to access local files. NFS uses the Remote Procedure Call (RPC) protocol to transfer file system commands from the requesting process (the client) to the host where file system is physically located (the server). The responses to these requests are then sent back by RPC.

A.2.4 Input/Output

The Input/Output (I/O) subsystem allows a process to transfer data to and from peripheral devices such as disks, tape drives, and printers. Each device in the system is represented by one or more device special files. Trusted IRIX uses the information in the device special file to locate the appropriate device driver, which handles the device-specific requests.

A.2.5 Memory Management

The memory management subsystem of Trusted IRIX provides a demand paged memory management model in which process memory consists of regions that, in turn consist of pages. A process may contain several regions including, but not limited to stack regions, data regions, executable text regions, memory mapped files, and shared data regions.
The memory management subsystem makes a strict distinction between a process, a share-group, and a share-group member-thread. The memory management subsystem in Trusted IRIX exists to provide four functions:

- allocation, release, and sharing of memory associated with share-groups,
- mapping of entities such as files into memory addressable space for easier manipulation,
- transparent movement of data between high speed local memory and lower speed, higher capacity storage devices (such as swap areas on disk), and
- enforcement of the boundaries between share-groups and between user-mode and kernel-mode processing.

A.2.6 Auditing

The Trusted IRIX system provides an auditing mechanism that allows user level processes in the administrative or system domain and kernel mechanisms to record security related activities by users and administrators. The audit mechanism provides a means for capturing, buffering, writing to disk, and filtering audit trail information. It does not define the contents of a given audit record. Only the subsystem in which a given event occurs knows the nature of any given security related event. For this reason, subsystems hold the responsibility for the content of specific audit record types.

A.2.7 Interprocess Communication

The Interprocess Communications (IPC) services offered by the kernel provide mechanisms for communication between processes. Trusted IRIX supports AT&T System V, BSD, and Trusted IRIX specific mechanisms. The IPC mechanisms allow communication on local machines as well as across the network.

A.2.8 Network

Included in the kernel is a set of network protocols. Users request services of trusted network applications to access and utilize the resources of all workstations in the system. These trusted applications use the kernel network protocols for their lower level communication services. Trusted IRIX implements Transmission Control Protocol (TCP), Internet Protocol (IP), User Datagram Protocol (UDP), and Ethernet in the kernel.

A.3 User-mode

A.3.1 User Network Services

The provision of network services to users requires two processes: a client process, which is invoked by a user, and a server process executing on a remote host. These client and server processes communicate with one another in the Internet communication domain. Under this model, the server process waits for requests to perform some service, while the client process asks the server to perform some service on its behalf. In the Internet domain, a server process generally sets up a socket on which it "listens" for incoming requests to perform a service. The network services in the evaluated configurations are: ftp, telnet, rlogin, rsh, echo, discard, chargen, daytime, and time.

A.3.2 Identification and Authentication

Trusted IRIX identification and authentication is performed using a user name and password. In the password based authentication model, the Interactive Login Services subsystem requires a user to specify a user name and a correct password before creating an initial process for the user. The password verifies the authenticity of the user name. The user name is then mapped to a user identifier (UID) for use in identifying the owner of the login session to the system. A user failing to provide a suitable user name and password is not allowed to log into the Trusted IRIX system.

A.3.3 Printer Subsystem

The Printing Services subsystem of Trusted IRIX provides controlled access to printing resources. It serves two important functions within the Trusted IRIX security model:
1. Controlling access to printers, print queues, and jobs to avoid unauthorized interference with or observation of printing requests and resources, and
2. Generating human readable labeling on printed output to uphold the MAC requirement that printed output must be labeled.

A.3.4 Batch Processing

The Trusted IRIX Batch Processing Services subsystem allows users to submit requests for either periodic or deferred processing. There are three modes of batch processing supported:
1. Once as soon as possible but not as part of the user's current login session (submitted through batch(1)),
2. Once at a user specified time in the future (submitted through at(1)), and
3. Persistent and periodic, at times specified by the user (submitted through crontab(1)).
These commands accept user input and create entries in queues under the control of the Batch Processing Services subsystem. A daemon called cron reads these queues and schedules jobs for execution. When a job's scheduled time of execution arrives, cron establishes a session for that job and initiates processing.

A.3.5 Electronic Mail Subsystem

Trusted IRIX uses the Internet Simple Mail Transfer Protocol (SMTP) for electronic mail. The sendmail process implements SMTP. For mail with a remote destination, the client sendmail uses Internet domain sockets to communicate with the remote sendmail process. The sendmail daemon listens on a known port and waits for a client to connect to the port and begin transmitting a mail message.

A.3.6 Trusted Commands

Trusted IRIX provides a set of commands to be used for system administration. These commands can be used to manage all aspects of the Trusted IRIX system, including commands to manage user accounts, audit configuration, device configuration, file system backup, and audit event viewing. These commands are used to manage the system and are trusted to perform correctly. The commands are documented in the administrator guide.