C2 Security in IRIX 5.3 and 6.1

E.J. McCauley, Trusted Products Manager

This is a technical note describing the C2 Security features in the IRIX™ 5.3 and 6.1 operating systems. The document is organized around the Orange Book description of a C2 level system. It is a revision of a previous document describing the C2 feature content in the 5.0 versions of IRIX.

Executive Summary

The IRIX™ 5.3 and 6.1 operating systems incorporate security features from the Trusted IRIX/B 4.0.5 EPL™ operating system. These features are designed to meet the C2 level of trust as defined by the Orange Book (DOD 5200.28-STD, *Department of Defense Trusted Computer Systems Evaluation Criteria*). This document describes these features in terms of the Orange Book C2 criteria.

Trusted IRIX/B 4.0.5EPL has been formally evaluated by the National Computer Security Center (NCSC) to meet the B1 level of trust, and is listed in the Spring 1995 edition of the NCSC Evaluated Products List. As part of its formal evaluation by the NCSC, extensive analysis of the security features has been done, including the preparation of over 3000 pages of submittal documentation. Much of this analysis is applicable to a C2 level system, since a B1 level system incorporates all of the C2 features. Where appropriate, references to the Trusted IRIX/B system documentation are presented. This documentation can be made available on request to customers contemplating local evaluations or with other needs. It should be noted that the NCSC evaluation is of a version of Trusted IRIX/B based in IRIX 4.0.5H.

NCSC policy has been to permit only one evaluation to be in progress for a given company, and to discourage new evaluations at the C2 level in favor of the more important (to DoD) B level evaluations. Therefore, the IRIX 5.3 and 6.1 operating system cannot be formally classified as C2 level systems, since this requires the evaluation of the system. Nevertheless, the IRIX 5.3 and 6.1 operating system security features were designed to meet the C2 requirements. We believe that these systems could be evaluated at the C2 level. SGI has and will continue to accept problem reports on errors or omissions of C2 features and will remedy defects in an appropriate manner.

This document is organized around the descriptions in the Orange Book. It draws upon elements of the *Trusted IRIX/B - B1 Correspondence Guide*, submitted to NCSC as part of the evaluation.

IRIX 5.3 and IRIX 6.1 Background

IRIX 5.3 was released in late 1995 as an all platforms release. It is an upgrade to the IRIX 5.0 baseline first released in March, 1993. Starting with IRIX 5.0, security features originally developed for Trusted IRIX/B were incorporated into the main software baseline, and have been generally available to the SGI customer base as optionally installed, bundled products. The most significant of these has been the incorporation of the auditing mechanism from Trusted IRIX/B.

IRIX 6.1 is a revision of IRIX 5.3 to support 64 bit operation of user programs and the IRIX kernel itself. IRIX 6.1 is available only on the Power Challenge, Power ONYX and Power Indigo2 systems. Its feature content is the union of IRIX 5.3 (basic OS, commands and utilities), IRIX 6.0.1 (64 bit kernel, compilers and selected utilities), and IRIX 6.0.1 with XFS (new 64 bit file system). IRIX 6.1 is currently in Beta test, with a planned release in Summer 1995. Since IRIX 6.1 incorporates the feature content of IRIX 5.3, it has picked up the audit functionality present in 5.3. Modifications have been made to adapt to the 64 bit internals of the IRIX 6.1 kernel.

An all platforms release from a 6.1 baseline with the incorporation of selected new functionality is planned for late 1995. Tentatively this will be designated IRIX 6.2. As with IRIX 6.1, it will incorporate the C2 features from prior releases.

C2 Requirements and How IRIX 5.3/6.1 Meets Them

Class (C2): Controlled Access Protection

Systems in this class enforce a more finely grained discretionary access control than (C1) systems, making users individually accountable for their actions through login procedures, auditing of security-relevant events, and resource isolation. The following are minimal requirements for systems assigned a class (C2) rating:

2.2.1 Security Policy

2.2.1.1 Discretionary Access Control

The TCB shall define and control access between named users and named objects (e.g., files and programs) in the ADP system. The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects by named individuals, or defined groups of individuals, or by both, and shall provide controls to limit propagation of access rights. The discretionary access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable *of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.*

Ref: Trusted IRIX/B - Discretionary Access Control Requirements and Design (des.27.-dac.mm)

The IRIX 5.3/6.1 operating system enforces standard UNIX™ Discretionary Access Control. The implementation for the IRIX 4.x environment has been analyzed in the referenced document (des.27.dac.mm). The IRIX 5.3/6.1 support of DAC is essentially the same, although the details of the implementation differ. The DAC checking in the IRIX system includes checks made for access of each of the system objects:

- file system objects (files, directories, pipes, FIFOs, symbolic links and process files)
- System V intra-process communication objects (shared memory, messages, semaphores)

Since the DAC features in IRIX 5.3/6.1 are essentially the same as the DAC features in Trusted IRIX/B, and these features in Trusted IRIX/B have been accepted as sufficient for a B1 level system, the DAC features in IRIX 5.3/6.1 meet the C2 requirements.

2.2.1.2 Object Reuse

All authorizations to the information contained within a storage object shall be revoked prior to the initial assignment, allocation, or reallocation to a subject from the TCB's pool of unused storage objects. No information, including encrypted representations of information produced by a prior subject's actions is to be available to any subject that obtains access to an object that has been released back to the system.

Ref: Trusted IRIX/B - System Call Security Analysis, Section 3, Object Reuse (ana.11.-syscalls.mm)

IRIX 5.3/6.1 follows the same principles of object reuse that Trusted IRIX/B 4.0.5 EPL does, although some implementation details differ. In general, the system does not clear deallocated blocks of disk or memory as they are deallocated. Rather, it ensures that the space is either cleared or refilled on re-allocation (e.g. memory pages), or is inaccessible until it has been written (file data blocks). Details of the object reuse mechanisms are described in the referenced document. Since these object reuse mechanisms have been accepted as sufficient for the B1 evaluation of Trusted IRIX/B, IRIX 5.3/6.1 meets the C2 requirements for object reuse.

2.2.2 Accountability

2.2.2.1 Identification and Authentication

The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The TCB shall protect authentication data so that it cannot be access by any unauthorized user. The TCB shall be able to enforce individual accountability by providing the capability to *uniquely identify each individual ADP system user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.*

Ref: Trusted IRIX/B - Identification and Authentication Subsystem Requirements and Design (des.16.ianda.mm), Trusted IRIX/B - Requirements and Design of the X11R4 Window System (des.21.x.mm), Trusted IRIX/B - System Administrative Data Design (des.33.sadd.mm)

Although the Trusted IRIX/B environment has a more extensive data base for I&A (for example, it must maintain information about user clearances), many of the basic principles apply to the standard IRIX environment. In the commercial environment, there is a dialectic between security and ease of use. SGI systems have historically had their default configurations set up for maximum ease of use for use in benign environments. When systems are installed in less benign environments, the administrator is advised to follow the steps outlined in the IRIS Advanced Site and Server Administrator's Guide for enhancing the security of the system. To meet the requirements of this section, the local administrator of an IRIX 5.3/6.1 system must invoke the *pwconv* utility which removes the encrypted passwords from the vulnerable /etc/passwd file, and places them in an shadow password file which is inaccessible to unprivileged programs. Assuming that the system administrator follows the guidance on system security in the IRIS Advanced Site and Server Administrator's Guide and other applicable material such as release notes and security advisories from SGI, an IRIX 5.3/6.1 system would meet the requirements for C2 level Identification and Authentication.

2.2.2.2 Audit

The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data.The TCB shall be able to record the following types of events: use of identification and authentication mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects, actions taken by computer operators and system administrators and/or system security officers, and other security relevant events. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record.For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object.The ADP system administrator shall be able to selectively audit the actions of any one or more users based on individual identity.

Ref: Trusted IRIX/B Security Audit Trail Subsystem Requirements and Design (des.12.satsubsys.mm)

The IRIX 5.3/6.1 system incorporates the Security Audit Trail Subsystem from Trusted IRIX/B. New audit capture points have been added to the IRIX 5.3/6.1 system to reflect additional functionality. The basic concept is to generate an audit record at each security relevant event. A system daemon, satd, selectively captures these records under the control of an audit capture mask which may be manipulated by the system administrator while the system is running. Raw audit records are stored in files for subsequent processing. Trusted programs can generate audit records using system calls. Trusted shell scripts can generate audit records by using the sat_echo program. Administrators can select audit records with the sat_select program which produces a file in the same format as the original input log file, containing only the selected records. These may be displayed using the program sat_interpret or summarized with sat_summarize. Approximately 70 distinct audit record types are supported by the system (not all of them are relevant for the C2 level, as some of them deal with MAC events). The list was defined by the B1 requirements so fully meets the C2 requirements.

2.2.3 Assurance

2.2.3.1 Operational Assurance

2.2.3.1.1 System Architecture

The TCB shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). Resources controlled by the TCB may be a defined subset of the subjects and objects in the ADP system. The TCB shall isolate the resources to be protected so that they are subject to the access control and auditing requirements.

Ref: Trusted IRIX/B - System Hardware Configurations (con.26.hardware.mm), Trusted IRIX/B - System Call Security Analysis (ana.11.syscalls.mm), Trusted IRIX/B - Uncle Art's Big Book of IRIX, esp. Section 2, Memory Management (des.34.irix.dir), Trusted IRIX/B - System Integrity (tes.25.integrity.mm)

The IRIX operating system kernel is protected from modification while running through the memory management unit of the CPU. These are described in the MIPS Processor Architecture manuals, as well as being summarized in the above referenced documents. The memory management unit also provides isolation of user processes from each other. The disk files of the TCB are protected by standard UNIX DAC permissions. (Trusted IRIX/B has an additional mandatory integrity mechanism which is the mathematical dual of the mandatory access control mechanism.) The IRIX 5.3/6.1 environment actually meets the B1 requirements for System Architecture (these require distinct address spaces in addition to the C2 requirements), so is fully compliant with the C2 requirements.

2.2.3.1.2 System Integrity

Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

Ref: Trusted IRIX/B - System Integrity (tes.25.integrity.mm)

IRIS systems have two types of diagnostic environments to verify that the system operates correctly with respect to the security requirements. The first is in the Power On diagnostics which are run as the system is turned on. These check the basic functioning of the CPU and peripherals. The second is the IRIS Diagnostic Executive (IDE) which includes extensive tests of the memory management unit, which is the fundamental mechanism for providing process isolation. The integrity requirement is primarily a hardware and diagnostic requirement. B1 and C2 have identical requirements in this area. The same diagnostics used to meet this requirement for Trusted IRIX/B at the B1 level are available with IRIX 5.3/6.1, so the IRIX 5.3/6.1 environment meets the C2 requirements.

2.2.3.2 Life-Cycle Assurance

2.2.3.2.1 Security Testing

The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. Testing shall be done to assure that there are no obvious ways for an intruder to bypass or otherwise defeat the security protection mechanisms of the TCB. Testing should also include a search for obvious flaws that would allow violation of resource isolation, or that would permit unauthorized access to the audit or authentication data.

The Trusted IRIX/B test documentation is applicable to that system only, since most of it focuses on tests which would not operate correctly on a system without all of the security features of Trusted IRIX/B (notably MAC). However, the standard testing for the commercial versions of the IRIX system does do extensive testing of the protection features of the system, since this behavior is an important part of the system interfaces. The system functionality testing includes the POSIX 1003.1 / FIPS-151 test suite, the X/Open Portability Guide, Issue 4 (XPG4) test suite, the Generic SVR4 Applications Binary Interface test suite, a number of X11 test suites (xtest, xgbench, xcrash), and a growing list of specific tests for problems which have been fixed in prior releases. These tests meet the requirements for security testing at the C2 level.

2.2.4 Documentation

2.2.4.1 Security Features User's Guide

A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

Elements from the Trusted IRIX/B Security Features User's Guide have been incorporated into the IRIX Advanced Site and Server Administrator's Guide, which also contains additional information on security aspects of system administration.

2.2.4.2 Trusted Facility Manual

A manual addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility. The procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event shall be given.

Elements of the Trusted IRIX/B Security Administration Guide have been integrated into the IRIS Advanced Site and Server Administrator's Guide in fulfillment of this requirement.

2.2.4.3 Test Documentation

The system developer shall provide to the evaluators a document that describes the test plan, test procedures that show how the security mechanisms were tested, and the results of the security mechanisms' functional testing.

This material is contained in the test logs from the commercial tests mentioned above. Were the system to be under evaluation at the C2 level, the test documentation would consist of the assertions being tested (all of the above mentioned tests are assertion based), and the results. There are no known security failures in the tests applied to IRIX 5.3 / 6.1. Of particular note is the fact that the system has been formally tested and accepted as compliant with the XPG4 requirements, which include extensive tests of the DAC features.

2.2.4.4 Design Documentation

Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB. If the TCB is composed of distinct modules, the interfaces between these modules shall be described.

Ref: Trusted IRIX/B - Philosophy of Protection (ana.35.ppd.mm), Trusted IRIX/B - System Call Security Analysis (ana.11.syscalls.mm), Trusted IRIX/B - Program Security Analysis (ana.11.programs.mm)

The commercial versions of the IRIX system contain only DAC, so much of the Trusted IRIX/B Philosophy of Protection document is not pertinent. However, the DAC is common, so the requirements in this area are met with the Trusted IRIX/B documents. Also common are many of the user mode programs that provide support to the TCB and must be made part of it. These have been analyzed for Trusted IRIX/B, and this analysis also generally applies to the commercial versions of the IRIX system. Since the Trusted IRIX/B documents cover the design of the C2 level features (these features are a subset of the B1 features), the IRIX 5.3/6.1 environment meets the C2 requirements for design documentation.