White Paper

Multilevel Security (MLS) by Trusted IRIX™

This white paper describes the multilevel security capability present in SGI Trusted IRIX system software. This document is intended to help customers decide whether Trusted IRIX meets their MLS or other critical security needs. It articulates general and fundamental features of Trusted IRIX systems and the value-add proposition in using them. The reader will find that SGI Trusted IRIX provides a compelling, robust, and flexible security scheme that satisfies most users demanding cyber-security requirements. As always, SGI personnel are ready to answer specific questions on your setup.

Additional technical publications available from SGI regarding Trusted IRIX:

Trusted IRIX™ CMW Security Administration Guide
Trusted IRIX™ CMW Security Features User's Guide

1.0 Abstract

The SGI Trusted IRIX CMW security-enhanced feature set provides an environment for users to do their ordinary and necessary work while enforcing a multilevel security policy crafted by site security administration. Trusted IRIX CMW provides a strict security framework so that when application programs run on the system and users attempt to access files, their access is limited to data permitted by the MLS policy.

MLS operating systems compartmentalize user interactions according to specific security labels. User and process labels contain two main elements: sensitivity level and sensitivity category. This access structure extends above and beyond classical user permission and group permission schemes available in standard UNIX®. These additional operational restrictions need not be hostile to the average or even novice user. Users can continue to execute policy-abiding functions while unauthorized accesses are disallowed before data is compromised. Trusted IRIX CMW is a significant improvement over conventional secured operating systems derived from the standard UNIX kernel and it is fully integrated with the SGI® IRIX® operating system. High-performance capabilities available in SGI IRIX—such as real-time response guarantee, nonuniform shared-memory architecture (NUMAflex™), storage area networks (SANs), and others—continue to be operational in Trusted IRIX CMW. Because MLS is a fully integrated feature, it will not adversely affect your system's performance.

Trusted IRIX CMW and IRIX are developed to conform to functional requirements set forth in the Common Criteria for IT Security Evaluation (ISO Standard 15408) protection profiles. Labeled Security Protection Profile (LSPP) is derived from the U.S. National Computer Security Center 5200.28-STD Department of Defense Trusted Computer Systems Evaluation Criteria (TCSEC—Orange Book) for a B1-level trusted operating system. Controlled Access Protection Profile (CAPP) is based on a TCSEC C2 security level. Today, Trusted IRIX is evaluated at the assurance level of an LSPP system. IRIX is evaluated at the assurance level of a CAPP system. Formal certification for Trusted IRIX and IRIX was achieved in May 2002.

2.0 Trusted Operating System

The MLS framework present in a Trusted IRIX CMW system asserts three fundamental security aspects: policy, accountability, and assurance. Trusted IRIX CMW is fully configurable to your site's security policy requirements.

The security administrator is able to program the site's own security clearance definitions and limitations, permitted special operational capabilities, file access control lists, and choice of password protection scheme. Trusted IRIX CMW allows for auditing and monitoring of key and site-defined operational events, such as file access and modification, network access and modification, invocation of programs, login and logout, and unauthorized attempted accesses to files. The audit log could be used to discover malicious intent.

In addition to MLS labels, Trusted IRIX CMW provides other discretionary file-access control mechanisms. Optionally, access control lists (ACLs) can be attached to files. ACLs specify what group(s) and what user(s) are allowed to read or write the corresponding file. This provides access control granularity to the user account or accounts.

The trusted host enforces the following security policies:

- Identification and authentication (I&A): The identification and authentication mechanism controls user access to the 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. After a successful login has been established, the user may change the clearance of his or her process during the course of the login session. When this happens, all open file descriptors of the process are closed and all objects cleared to prevent declassification or violation of the security policy. All changes of clearance are audited.

- Mandatory access control (MAC): Mandatory access control allows the system administrator to set up policies and accounts that will allow each user to have full access to the files and resources he or she needs, but no access to other information and resources not immediately necessary to perform assigned tasks. Under MAC, access permission cannot be passed from one user to another, like it can in traditional UNIX systems, which use discretionary access control. Each label attached to system objects that are used for access control has two parts: the sensitivity label and the integrity label shown in figure 1.

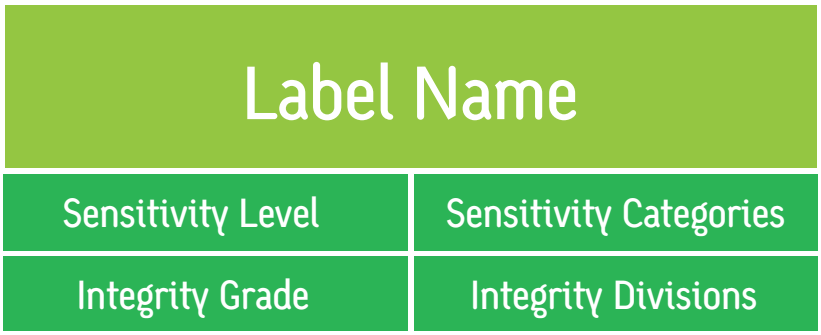

Fig. 1. Sensitivity and Integrity Labels

Sensitivity Label Components: 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. There are 256 hierarchical sensitivity levels available for the administrator to create security classifications. In a commercial environment, this label attribute could be used to classify, for example, levels of a management hierarchy. Each file or program has one hierarchical sensitivity level. A user may be allowed to use several different levels, but only one level may be used at any given time. Over 65,000 sensitivity categories are available for files and programs. For example, categories could include information sorted by subject matter such as geography, demography, astronomy, and others. Each file or user can be a member of any number of categories or of no categories.

Integrity Label Components: 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. There are 256 hierarchical grades to classify the reliability of information. For example, data could be classified as an unreliable rumor or as an absolute, confirmed fact. There are over 65,000 divisions available to classify information based on its source. The source implies probable integrity of the data. For example, sources of data could be divided into Canadian government, U.S. government, CBS News, Hearst Publications, and others. In the commercial environment, data sources could be trade shows, press releases, conversational, Dataquest, and the like.

- Access control lists: Users can specify, on a person-by-person basis, who may access their files and directories. The purpose of this feature is to provide a finer level of control than is allowed through traditional discretionary access control. ACLs are a standard feature of IRIX.

- System audit trail: The foundation of Trusted IRIX CMW is the system audit trail. The audit subsystem allows the system administrator to keep a precise log of all system activity. The system audit trail provides the means for the system administrator to oversee each important event occurring on the system. The audit trail is useful for tracking changes in sensitive files and programs and for identifying inappropriate use of the system.

- Capability-based privilege mechanism: This mechanism determines the privilege based on the set of effective capabilities for a given process. Also, it is how capabilities are assigned to a process or an executable file, and how a process manages its capabilities. This mechanism is utilized to grant very specific, controlled privileges to specific functions without granting access to key user accounts.

- Object reuse policy (object scrubbing): 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 cleared before it is reallocated. Object scrubbing is a standard feature of IRIX.

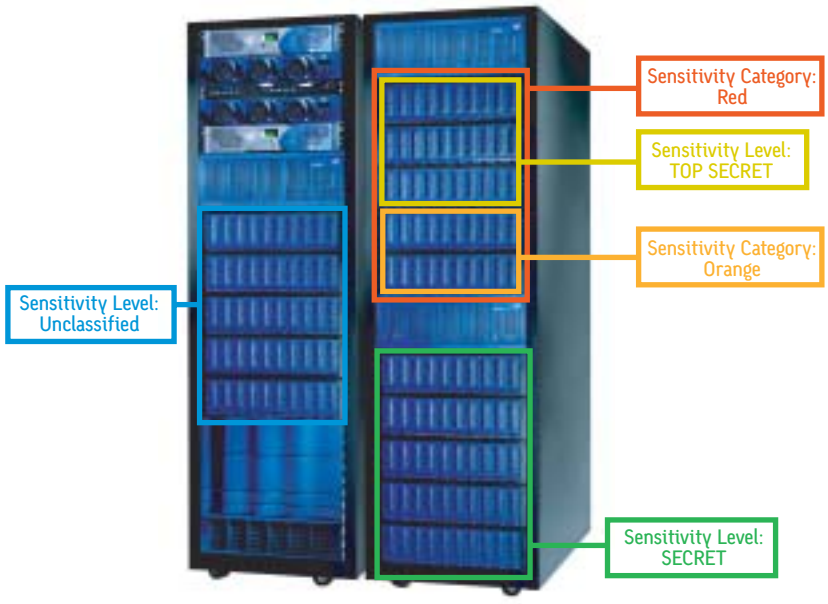

Fig. 2. Safe information sharing or strict information segregation? Multilevel security by SGI Trusted IRIX. Figure shows an example of MLS deployment on an SGI® Origin® 300 server.

3.0 Trusted Networking

Trusted IRIX CMW supports trusted networking by supporting data labeling. Data is labeled when it is imported or exported from the MLS system. Trusted IRIX CMW enforces the established security policy for the data. The Trusted Security Information Exchange (TSIX) standard was created to allow various trusted-operating-system vendors to interoperate. Under TSIX networking, labeling occurs at two levels. First, at the network level, IP security options (RIPSO or CIPSO) are used to route traffic. Second, at the session manager level, Security Attribute Modulation Protocol and Security Attribute Token Mapping Protocol are used to send all the security attributes required to enforce security policy between systems on the network.

The policies enforced by trusted networking are as follows:

- Received packets must be within the label range of the host or network
- Delivered data must have a label dominated by the receiving process
- Trusted processes may themselves enforce appropriate policy

When using network services to log in to remote hosts, no provision is made for entering a label on the remote host. The user must conduct all transactions with the remote host at the current label on the local host. This restriction prevents compromise of data.

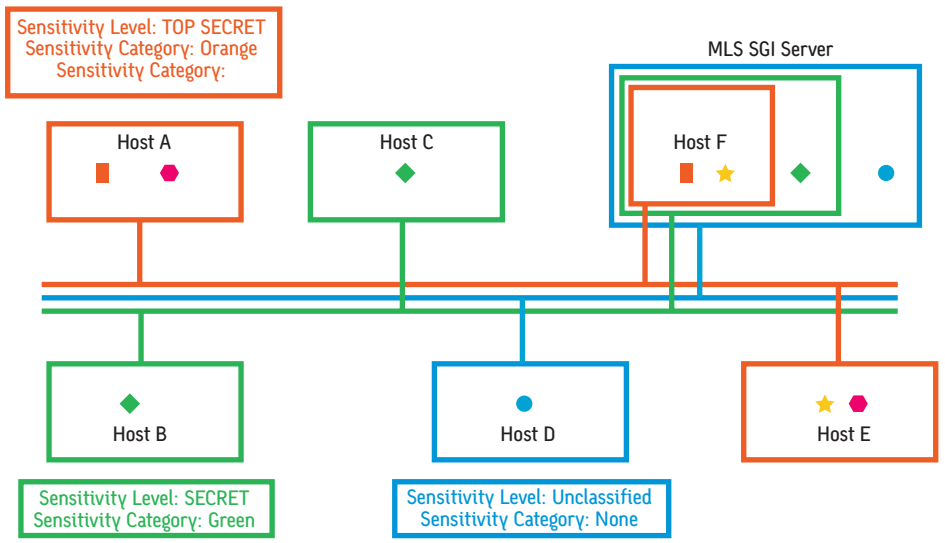

Fig. 3. Safe information sharing or strict information segregation? Multilevel security by SGI Trusted IRIX. Figure shows shows an example of a trusted network.

4.0 Why Use Trusted IRIX CMW?

- **Strict information segregation requirement**
  Distinct sources of information could be present and sharing the computing capability of a single host system. However, owners of the information may want to keep their data safe and private. This might be required because of legal, economical, or competitive considerations. An MLS scheme can be easily defined to guarantee against leaks of information.

- **Controlled information-sharing requirement**
  When distinct sources of information are present in a single host system, the owners of that data would want to keep it private unless strict clearance eligibility is met. Then, cross-reference and/or correlation analysis by specially cleared users could be made possible. An MLS policy scheme can meet privacy concerns and, at the same time, allow special and controlled intelligence analysis.

- **Customer space constraints**
  When floor space is an important consideration, an MLS scheme would allow two or more parties to share a single machine without risk of compromising the data. For example, the system may operate in a vehicle where users need to keep their information separate.

- **Infrastructure costs and/or energy savings**
  Trusted IRIX CMW on a single host controls data access for a network of systems. The alternative to sharing the single trusted host is to keep the data separated on different hosts, thus increasing the cost of operation, administration, and maintenance.

Other reasons why SGI provides the best trusted environment include:

- Experience: As a modified version of an existing operating system, many of the underlying features of Trusted IRIX have withstood the test of time. Designing a system that promotes ease of use was a paramount consideration in the creation of IRIX. In fact, IRIX development started more than 12 years ago, and this is the second time that Trusted IRIX is being evaluated to conform to the official governing security criteria.

- Flexibility and scalability: IRIX running on the SGI® NUMA architecture provides the highest level of customization available to satisfy the most difficult customer computing demands.

- Conformance to standards: IRIX® 6.5 is a fifth-generation 64-bit UNIX operating system compliant with industry standards such as UNIX® 95, X11 Motif®, OpenGL®, and COE.

- Richest feature set: IRIX has been instrumental in delivering high-performance computing, advanced graphics, high-bandwidth throughput, and real-time processing provided by IRIX and REACT/pro™. IRIX supports application binary compatibility for every IRIX 6.5 update for entry-level desktops to supercomputers.

Corporate Office
1600 Amphitheatre Pkwy.
Mountain View, CA 94043
(650) 960-1980
www.sgi.com

North America 1(800) 800-7441
Latin America (52) 5267-1387
Europe (44) 118.925.75.00
Japan (81) 3.5488.1811
Asia Pacific (65) 771.0290

3241 (11/05/2002) JI4136