

Trusted Solaris™ 8 Operating Environment

A Technical Overview



Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303
1 (800) 786.7638
1.512.434.1511

Copyright 2000 Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, California 94303 U.S.A. All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, Java, Solaris, Solaris Management Console, Solstice AdminSuite, and Trusted Solaris are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

RESTRICTED RIGHTS: Use, duplication, or disclosure by the U.S. Government is subject to restrictions of FAR 52.227-14(g)(2)(6/87) and FAR 52.227-19(6/87), or DFAR 252.227-7015(b)(6/95) and DFAR 227.7202-3(a).

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright 2000 Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, Californie 94303 Etats-Unis. Tous droits réservés.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, Java, Solaris, Solaris Management Console, Solstice AdminSuite, et Trusted Solaris sont des marques de fabrique ou des marques déposées, ou marques de service, de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

CETTE PUBLICATION EST FOURNIE "EN L'ETAT" ET AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, N'EST ACCORDEE, Y COMPRIS DES GARANTIES CONCERNANT LA VALEUR MARCHANDE, L'APTITUDE DE LA PUBLICATION A REPENDRE A UNE UTILISATION PARTICULIERE, OU LE FAIT QU'ELLE NE SOIT PAS CONTREFAISANTE DE PRODUIT DE TIERS. CE DENI DE GARANTIE NE S'APPLIQUERAIT PAS, DANS LA MESURE OU IL SERAIT TENU JURIDIQUEMENT NUL ET NON AVENU.



Please
Recycle



Adobe PostScript

Contents

Overview	1
Design Goals	2
Trusted Solaris Software Capabilities	2
What's New	4
Administration	5
Roles	7
Rights Profiles	8
Authorizations	8
Privileges	9
Processes and Privileges	10
Network Services	11
Name Services	11
IPv6	11
Trusted Solaris Software Features	12
How Trusted Solaris Software Enforces Access Control Policy	12
Discretionary Access Control (DAC)	12
Mandatory Access Control (MAC) Enforces System-Wide Access Control	13
Dominance Relationships Between Labels	14
Administrative Labels	15
How Labeled Files Are Stored	15
Labeled Printing	16
Trusted Networking and Interconnectivity	16

Controlling Device Access	16
Device Allocation	16
Device Label Ranges	17
Trusted Common Desktop Environment (CDE)	17
Cut and Paste and Drag and Drop	17
Trusted Mail	18
Trusted Path	18
Audit Trails	18
Pluggable Authentication Module (PAM)	19
Certified Trusted Systems	19
Appendix	21
How the Trusted Solaris Operating Environment Helps Implement a Security Policy	21

Overview

The Trusted Solaris™ 8 Operating Environment — an extension of the Solaris™ 8 Operating Environment — is designed for deployments where enhanced security and policy enforcement is of key importance. The Trusted Solaris 8 Operating Environment layers additional security capabilities on top of the existing Solaris 8 Operating Environment, extending the inherent security features in both server and desktop environments. Trusted Solaris 8 software can be deployed across the full line of Sun™ multiprocessor servers and workstations while running unmodified, off-the-shelf Solaris applications. Both the Solaris 8 and Trusted Solaris 8 platforms use the same administrative interface — Solaris Management Console™ software. Administrators familiar with Solaris 8 administration should be comfortable with the Trusted Solaris administration tools because the only differences are the security extensions offered by the Trusted Solaris platform.

While trusted computing systems and operating environments were originally developed to meet government and military security requirements, today commercial operations such as network service providers, banks, educational institutions, and others are increasingly interested in enhancing safeguards for their information technology (IT) assets. The Trusted Solaris 8 Operating Environment leverages the proven reliability, availability, and scalability of the established OS leader for Global 2000 Internet deployments — the Solaris 8 Operating Environment — and further strengthens its security capabilities.

Design Goals

The Solaris Operating Environment has a long history of successful worldwide evaluations by government-sponsored evaluation programs. Trusted Solaris 8 software is currently undergoing evaluation against the Common Criteria at the EAL4 level with the Labeled Security Protection Profile (LSPP — equivalent to the Orange Book – Trusted Computer System Evaluation Criteria (TCSEC) B1 class). In a trusted systems evaluation, the features of a product must meet a specified set of criteria. It is expected that certification will be completed in the first half of 2001.

The Trusted Solaris 8 Operating Environment is designed to extend the demanding, government-style security requirements into commercial environments. For commercial users, this enables administrators to exert greater control over the actions and capabilities of users and operational personnel. Trusted Solaris 8 software uses the role-based-access control (RBAC) model, and continues to provide the features and functionality that enables separation and compartmentalization of users and data, depending on their roles and rights.

Trusted Solaris 8 servers can be used in Solaris 8 network environments; they appear to users as any other server on such a network. For example, a Domain Name Service (DNS) server using Trusted Solaris 8 software running in an Internet service provider (ISP) network would still provide name services to all users entitled to them. However, administrative or other non-authorized access to this DNS server would be protected by the extended security features of the Trusted Solaris 8 Operating Environment.

Trusted Solaris Software Capabilities

Over the past decades, computer systems have become corporate-wide resources, essential to the day-to-day operation of a business and other organizations. A wide range of sensitive data, such as personnel and payroll records, marketing and sales plans, new product information, and so on is stored on these systems. Considerable cost, damage, and loss can be caused by hostile or unauthorized access and use of this information.

To protect information, firewalls and other methods are often used as gatekeepers to control external access to a system. However, these methods might not be sufficient. For example, an external attacker could gain access through the firewall and gather information from servers on the internal domains. The Trusted Solaris 8 Operating Environment provides methods for limiting *external* access, as well as extensive *internal* protection against intruders and misuse by:

- *Limiting access to system data and resources.* The Trusted Solaris 8 Operating Environment allows controls to be set on all potential interactions with its programs, utilities, and file access. Both identity-based and label-based policies are enforced, which means users get the access and functionality they need, while at the same time the system is protected from unauthorized use.
- *Eliminating superuser.* Superuser functions are divided into multiple roles, making it far more difficult for compromising key individuals to penetrate the network. In the Trusted Solaris 8 Operating Environment, root (the superuser account) is used only at installation time to construct other roles, such as the primary administrator. Root is never used as a login account.
- *Independent certifying authority.* Trusted Solaris 8 software is in evaluation by a third party to validate that its security functions operate correctly to established standards and conventions.
- *Preventing “eavesdropping” in the window environment.* In conventional environments, an intruding program can capture keystrokes typed in other windows. The Trusted Solaris Operating Environment provides a “trusted” path that protects entered data, which is particularly important for protecting passwords. Passwords can also be protected through Trusted Solaris software’s facilities for requiring password changes and for generating random passwords.
- *Augmented security auditing.* Actions that may affect security or sensitive files can be monitored. Administrators may generate usage reports by user, file, data, and time to detect suspicious activity.
- *Preventing spoofing programs.* Untrusted applications cannot be displayed on the desktop during administrative sessions. Visible indication that a user session is valid is provided by a trusted stripe graphic appearing in a reserved area at the bottom of the screen.
- *Protecting devices against unauthorized users.* Devices provide a means for adding and removing information from a Trusted Solaris system. Administrative screens are included to control data flow through device allocation and device label ranges.

In many cases, misuse by authorized users is the dominant source of security violations. Trusted Solaris software helps reduce misuse by providing the means for configuring a security policy into a system. This offers the ability to control the access and handling of information, including tools for facilitating the administration, operation, and monitoring of a system. For information on developing and implementing a security policy, see the Appendix at the end of this document.

What's New

The Trusted Solaris 8 Operating Environment offers the same protection, security level, and functionality as its predecessor, the Trusted Solaris 7 Operating Environment. This includes Orange Book B1 security capabilities, support for the Intel Architecture, 64-bit support, and support for Sun's entire SPARC™ product line.

Trusted Solaris 8 Operating Environment offers improved ease-of-use features, such as simplified software installation and setup and comprehensive integration capabilities. Trusted Solaris 8 software also offers performance and availability improvements. Availability is increased through a smaller, more stable kernel design and increased load balancing across multiple processors. Performance is now comparable to similar Solaris 8 platform installations.

New features in this release include:

- Administration — New Java™ administration tools support a wide range of increased features for comprehensive and easy-to-use remote management of the Trusted Solaris 8 Operating Environment with fine-grain access control
- Network Services — Supports the latest networking protocols and adheres to all major industry standards, including NIS, NIS+, and IPv6 protocols
- Performance — Optimizations such as attribute caching and a new label daemon result in improved system throughput

Administration

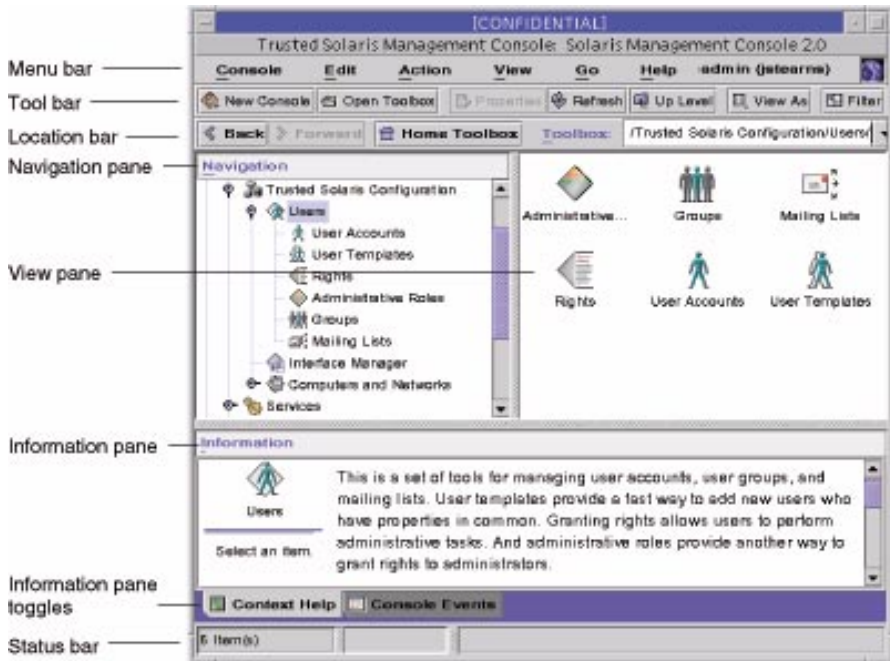


FIGURE 1 The Solaris Management Console application environment provides access to families of GUI-based administration tools, enabling administration of items in the system databases.

In the Trusted Solaris 8 Operating Environment, the Solaris Management Console 2.0 administration tools replace Solstice AdminSuite™ 2.3 tools. This tool is virtually identical to the Solaris Management Console tool used in the Solaris 8 Operating Environment Update 3, with additional tabs and fields available to administer the Trusted Solaris environment. The same terminology and user management database are used in both environments. Trusted Solaris attributes are optional, and do not cause incompatibilities in the Solaris 8 Operating Environment.

The Solaris Management Console client can run anywhere on the network, while the server runs on the name server. There are two types of clients: the GUI-based clients depicted in Figure 1, and a command-line interface (CLI).

Both GUI and CLI interfaces are capable of remote role assumption, which means that Solaris 8 and Trusted Solaris 8 software roles can perform cross-platform administration. For greater security, Trusted Solaris servers can be configured to restrict role assumption from untrusted hosts. The Solaris Management Console environment uses Java technology, and is built with a client/server architecture.

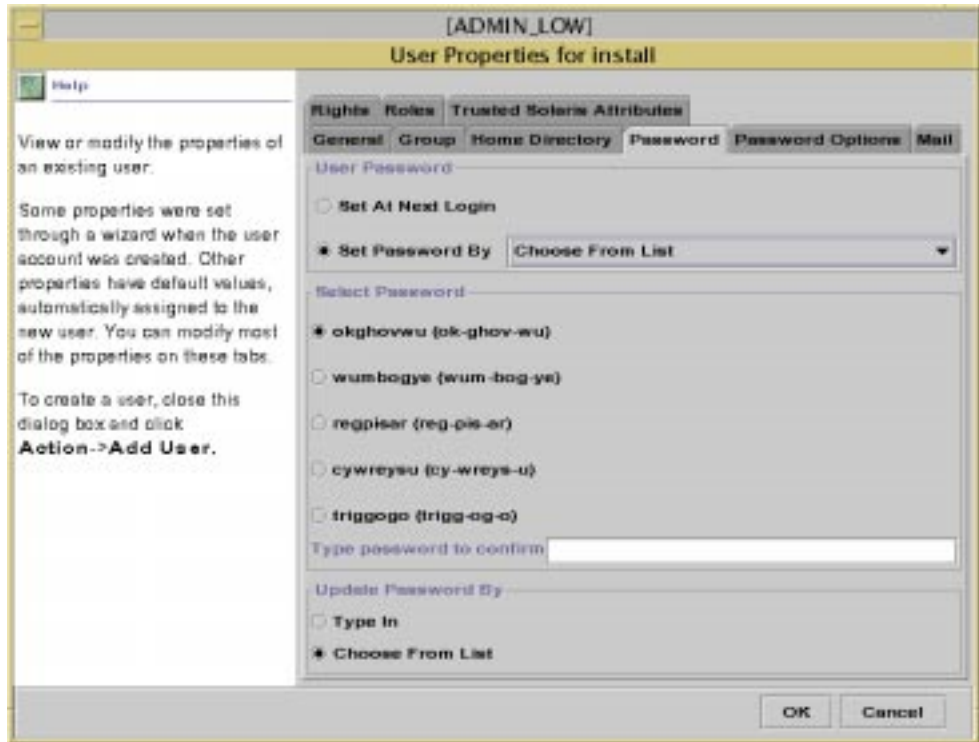


FIGURE 2 In Trusted Solaris software, the password tab enables the administrator to set a user's password as well as specify how a user changes his/her password in the future. When setting a user's password, the administrator can either type in a password or select a password from the list of system generated passwords.

Roles

A role is a special user account that gives a user access to specific applications as well as the authorizations and privileges necessary for running them. All users who can assume the same role have the same role home directory, operate in the same environment, and have access to the same files. Users cannot log in directly to a role; they must log into their user account prior to assuming a role to ensure that the user's real UID is recorded for auditing. Another restriction to facilitate auditing is that a user cannot assume any other role directly from a role. Assuming a role requires users to authenticate themselves by providing the role password. The user is then granted access to a dedicated role workspace where the user can then run trusted applications.

Roles define an explicit job responsibility that requires special commands, actions, and any necessary privileges that should be isolated from normal users. Any number of roles can be created. The Trusted Solaris Operating Environment recommends four roles:

- **Primary Administrator** — The primary administrator is designed to be as powerful as necessary to accommodate situations that were unplanned for in the creation and implementation of the security policy. The primary administrator role is not used in normal system operations. It is designed to be used only when the security administrator role cannot accomplish a task, for example, adding a new role or profile with capabilities the security administrator does not have.
- **System Administrator** — The system administrator role performs standard UNIX® system administration tasks, such as adding new users; configuring user templates; modifying certain user properties; and configuring hosts, networks, routes, and printers. It can also make and restore backups and administer printing.
- **Security Administrator** — The security administrator (Information System Security Officer) is responsible for security tasks and decisions. This role manages security-relevant attributes, which includes labels, privileges, and network access, of users, networks, printers and other devices, and hosts. This role can modify default roles and profiles and add new roles, but cannot grant capabilities beyond those of the security administrator role itself.
- **System Operator** — The system operator role makes backups and administers printing.

These roles are configurable to address the unique requirements at each site.

Additionally, a root role is provided by default to perform the initial installation, including the construction of the primary administrator role, and initial installation and configuration of the operating environment. After configuration, the root role is not used for administration and should not be assigned to any user.

Rights Profiles

Trusted applications and authorizations can be grouped into packages called *rights profiles* for assignment to user or role accounts. The main purpose of a rights profile is to provide limited override power to a user or role who needs a specific capability. For example, a rights profile can be assigned to a user to read audit trail files, manage system files, and manage cron jobs, yet restrict the user from additional privileges.



The predefined rights profiles can be modified by the security administrator to accommodate any organizational situations.

Authorizations

An *authorization* is a discrete right granted to a user or role that is checked by certain trusted applications to determine whether the user is permitted to execute a restricted function. For example, the Solaris 8 File Manager enables the superuser to change file ownership; Trusted Solaris 8 software requires the Change File Owner authorization.

An authorization has both a name (for example, `solaris.file.chown`), which is used internally, and a short description (for example, `Change File Owner`), which appears in the graphical interfaces. By convention, authorization names begin with the reverse order of the Internet name followed by the subject area, any subarea, and the function, all separated by periods (or dots), for example, `com.xyzcorp.device.access`. The exceptions to this convention are authorizations from Sun Microsystems, Inc., which use the prefix `solaris` instead of an Internet name. This representation enables administrators to apply authorizations in a hierarchical fashion using a wildcard (*) to represent any strings to the right of a dot.

The authorizations provided in the Trusted Solaris environment include the ability to manage processes, configure name services, assign roles, view, manage, and delete devices, and so on.

Privileges

A *privilege* is a discrete right granted to an application to perform an operation that would otherwise be prohibited in the Trusted Solaris Operating Environment. For example, applications cannot normally open data files unless they have the proper file permission. In the Trusted Solaris environment, the `file_dac_read` privilege gives an application the ability to override the file permissions for reading a file.

The Trusted Solaris 8 Operating Environment provides more than 70 privileges that can be applied to applications to override security policy. Categories of privileges include:

- File System Security — For overriding file system restrictions on user and group IDs, access permissions, labeling, ownership, and file privilege sets
- System V Interprocess Communication (IPC) Security — For overriding restrictions on message queues, semaphore sets, or shared-memory regions
- Network Security — For overriding restrictions on ports, sending broadcast messages, or specifying security attributes (such as labels, privileges on a message, or network endpoint defaults)
- Process Security — For overriding restrictions on auditing, labeling, ownership, clearance, user IDs, or group IDs
- System Security — For overriding restrictions on auditing, workstation booting, workstation configuration management, console output redirection, device management, file systems, creating hard links to directories, increasing message queue size, increasing the number of processes, workstation network configuration, third-party loadable modules, or label translation
- Window Security — For overriding restrictions on colormaps, reading to and writing from windows, input devices, labeling, font paths, moving data between windows, X server resource management, or direct graphics access (DGA) X protocol extensions

The Trusted Solaris 8 Operating Environment enforces the security principle called *least privilege*. Least privilege reduces the risk that occurs in standard operating systems when programs running as root are exempt from all policy controls. Trusted Solaris 8 software divides the unlimited power of a program running as root into many distinct privileges that can be tightly controlled.

Using privileges, an administrator can give a program the power to bypass some aspect of the security policy, such as *discretionary access control (DAC)* restrictions, without giving the program more power than it needs. Additionally, administrators can restrict the use of privileged programs to those users who can be trusted to use the privileges in an appropriate manner.

Processes and Privileges

The Trusted Solaris 8 Operating Environment determines which privileges a process can enable based on the allowed and forced privilege attributes assigned to the application file, and the inheritable privilege attributes assigned in the rights profile.

- The *allowed privilege* attribute satisfies one condition necessary for a privilege to be effective. If an allowed privilege for an application is not set, the privilege cannot be applied under any conditions. The *forced privilege* attribute applies the privilege for all users running that application. Note that if the executable file is modified, all allowed and forced privileges are removed.
- The *inheritable privilege* attribute is assigned to an application within a rights profile. Only users who have been assigned that rights profile are granted the privilege for that application. Inheritable privilege attributes for an application are assigned by using the Rights Manager. An inheritable privilege is applied when the process is launched by one of the trusted launchers. For the terminal environment Trusted Solaris 8 software provides three trusted launchers corresponding to the Bourne, Korn, and C shells; for the desktop, the Workspace Menu, the Front Panel, and the Application Manager interpret rights for actions; and for remote environments, the Solaris Management Console legacy application tool interprets rights. An application can also pass inheritable privileges to any child applications, provided that the particular privilege is allowed in the child application.

Network Services

Name Services

Trusted Solaris 8 software supports the same name services as the Solaris 8 platform, NIS, and NIS+. In addition to the distributed databases in the Solaris 8 Operating Environment, additional trusted networking databases are provided. Remote administration is provided for all services.

IPv6

In addition to IPv4 protocols, the Trusted Solaris 8 Operating Environment supports IPv6 protocols. A single Trusted Solaris 8 system may be used in environments that have both IPv4 and IPv6 protocol traffic.

Trusted Solaris Software Features

How Trusted Solaris Software Enforces Access Control Policy

Trusted Solaris software protects information and other resources through discretionary access control, the traditional UNIX permission bits and access control lists set at the discretion of the owner, and *mandatory access control (MAC)*, a mechanism enforced by the system automatically that controls all transactions by checking the labels of processes and files in the transaction.

Discretionary Access Control (DAC)

DAC is a UNIX software mechanism that enables the owner of a file or directory to grant or deny access to other users. The owner assigns read, write, and execute permissions to the owner, the primary group to which the owner belongs, and a category for all other users. These are the standard UNIX permissions.

owner			group			other		
r	w	x	r	w	x	r	w	x

FIGURE 1 Owner Defined File Security

The file security provided by UNIX, while adequate for small numbers of groups, is not sufficient for larger systems and networks where files need to be shared by multiple groups or users. Addressing this problem, both Solaris and Trusted Solaris platforms provide a fine-grained form of discretionary access control called *access control lists (ACLs)*, which lets the owner assign permissions to specific users and groups.

Mandatory Access Control (MAC) Enforces System-Wide Access Control

The major deficiency of DAC is that users are responsible for securing their own data. Any user can forget or decide not to secure sensitive information, causing it to be vulnerable to inappropriate access.

The Trusted Solaris 8 Operating Environment provides a stronger access control with MAC because the system automatically enforces the access allowed each user. This mechanism is implemented by adding labels to each file, program, and device. When users begin sessions, they select the sensitivity level(s) they will operate at. Note that Trusted Solaris software uses this information as a factor in granting access to sensitive information, programs, or devices on the system. The selection of label determines which information the user can access during the session. Both discretionary and mandatory access controls can be overridden by privileges. In some cases, users may need authorizations as well.

Labels consist of one classification component and zero or more compartment components. The classification component indicates a hierarchical level of security such as *public* or *registered*. The compartment component represents a group of users who may need access to a common body of information. Some typical types of compartments are projects, departments, or physical locations.

For example, all files containing *registered*, *need-to-know*, *internal-use*, and *public* information are specifically assigned with the appropriate label. A user that has only been granted access to marketing documents with public access is totally unaware and unable to access internal-use, need-to-know, and registered human resource documents. This type of security is called *mandatory* because the system automatically controls and sets the access allowed for each user.

Most Trusted Solaris administrative files are assigned the administrative label ADMIN_LOW. Since no user can be assigned this label, these files can never be directly modified by users; they can only be changed by specific users with permission to operate at the ADMIN_LOW label.

The Trusted Solaris environment mediates all attempted security-related transactions. It compares the labels of the accessing entity, typically an application, and the entity being accessed, for example, a file, and then permits or disallows the transaction depending on which label is dominant (as described in the next section). Label values are assigned by the security administrator, and are also used to determine access to other system resources, such as devices, networks, framebuffers, and other hosts.

Dominance Relationships Between Labels

One entity's label is said to dominate another's if the following two conditions are met:

- The classification component of the first entity's label is equal to or higher than the second entity's classification component. (The security administrator assigns numbers to classifications in the `label_encodings(4)` file; these numbers are compared when determining dominance.)
- The set of compartments in the first entity includes all of the second entity's compartments. (The security administrator assigns bit sets to compartments in the `label_encodings(4)` file; these sets are compared when determining dominance.)

Two labels are equal if they have the same classification and the same set of compartments. If they are equal, they dominate each other and access is permitted. If one label has a higher classification, or if its compartments are a superset of the second label's compartments, or both, the first label is said to strictly dominate the second label.

Two labels are disjoint or noncomparable if neither label dominates the other.

The following table presents examples of label comparisons for dominance. In the example, `NEED-TO-KNOW` is a higher classification than `INTERNAL`. There are three compartments: `Eng`, `Mkt`, and `Fin`.

Label 1	Relationship	Label 2
NEED-TO-KNOW Eng Mkt	(strictly) dominates	INTERNAL Eng Mkt
NEED-TO-KNOW Eng Mkt	(strictly) dominates	NEED-TO-KNOW Eng
NEED-TO-KNOW Eng Mkt	(strictly) dominates	INTERNAL Eng
NEED-TO-KNOW Eng Mkt	dominates (equals)	NEED-TO-KNOW Eng Mkt
NEED-TO-KNOW Eng Mkt	is disjoint from	NEED-TO-KNOW Eng Fin
NEED-TO-KNOW Eng Mkt	is disjoint from	NEED-TO-KNOW Fin
NEED-TO-KNOW Eng Mkt	is disjoint from	INTERNAL Eng Mkt Fin

Administrative Labels

The Trusted Solaris 8 Operating Environment provides two special labels for administration: ADMIN_HIGH and ADMIN_LOW. (These can be renamed in the `label_encodings(4)` file.) These labels are used to protect system resources and are intended for administrators rather than normal users.

- ADMIN_HIGH — The highest label, it dominates all other labels in the system and is used to protect system data, such as administration databases or audit trails, from being read. Users need to work at the ADMIN_HIGH label (typically in a role) or have the privilege to read up from their current label to read data labeled ADMIN_HIGH.
- ADMIN_LOW — The lowest label, it is dominated by all other labels in a system. Mandatory access control does not permit users to write data to files with labels lower than the subject's label. Thus, applying ADMIN_LOW to a file ensures that normal users cannot write to it, although they can read it. ADMIN_LOW is typically used to protect public executables and configuration files to prevent them from being modified — only a user working at ADMIN_LOW or with the privilege to write down would be able to write to these files. Typically, only an administrator would work at ADMIN_LOW.

When clearance and a minimum label are assigned to a user, they are defined with the upper and lower boundaries of the account label range in which that user is permitted to operate. If the administrator does not expressly set a user's clearance or minimum label, the defaults defined in the label encodings file take effect.

How Labeled Files Are Stored

In the Trusted Solaris Operating Environment, labels are automatically associated with all files and directories, and are stored as extended attributes of the file. These attributes are protected by privilege and mandatory controls.

In addition, special directories called *multilevel directories* (MLDs) allow files to be isolated by label in subdirectories called *single-level directories* (SLDs). SLDs are normally transparent to users and applications.

The purpose of MLDs is to enable applications that are running at different labels to write into what appears to be the same directory. For example, `/tmp` and the user's home directory are most often used by multiple applications. For that reason, they are MLDs. When applications write a file into an MLD, the file is actually being written into the SLD within the MLD that has the label at which the application is running. If a single-level directory corresponding to the label does not yet exist, the environment creates one automatically.

Home directories are MLDs, which means that applications can create files and folders at different labels within users' home directories. When user or role accounts change into their home directories, they do not need to be aware that they have actually changed into an SLD that is at the same label as their current workspace.

Labeled Printing

The administrator can arrange for labels, handling information, and other security information to print on the banner and trailer pages on a printer-by-printer basis. The Trusted Solaris 8 Operating Environment enables administrators to restrict the sensitivity of information that can be sent to individual printers. MAC is enforced when jobs are sent to a printer by comparing the label of the job to the printer's label range. Listing of print queues is restricted so users see only their own print jobs if the MAC checks are passed.

Trusted Networking and Interconnectivity

Hosts running the Trusted Solaris 8 Operating Environment can also share information with hosts running other trusted and standard operating systems, without compromising access controls on all communications. Administrators specify security attributes for each host and network. Certain attributes may be specified to control communications between Trusted Solaris 8 systems and other trusted systems. Trusted Solaris 8 software administrators can assign labels to standard operating system hosts, and communication between hosts on the network will follow the rules for dominance of these labels.

Default security attributes may be specified for hosts and networks that do not understand security or support these attributes. The Trusted Solaris 8 networking features use the specified attributes when enforcing the security policy.

Controlling Device Access

Because devices provide a means for the import and export of data to and from a Trusted Solaris system, they must be controlled to properly protect the data. The Trusted Solaris 8 Operating Environment allows data flow to be controlled through device allocation and device label ranges.

Device Allocation

Device allocation provides a method for controlling data when it is imported and exported, and prevents unauthorized user access to the information. In a Trusted Solaris system, the administrator decides which devices (if any) each user can use to import and export data, and sets those devices to be *allocatable*. The administrator then assigns (to selected users) the authorization needed to allocate each device. Users authorized to use a device must allocate the device before using it and deallocate the device when finished. Between the allocation and deallocation of a device, the user has exclusive use of it.

Device Label Ranges

To prevent users from copying sensitive information, each device has an associated label range that is assigned by an administrator. To use a device, the user must be currently operating at a label within the device's label range, or the access is denied. The user's current label is applied to data imported or exported while the device is allocated to the user. The label of exported data is displayed when the device is deallocated so that the user can physically label the medium containing the exported data.

Examples of devices that have label ranges include frame buffers, tape drives, diskette and CD-ROM drives, serial ports, network interfaces, and printers.

Trusted Common Desktop Environment (CDE)

With the Trusted Solaris 8 Operating Environment, users and administrators work within a trusted X11 window environment. The Solaris CDE environment is extended to provide transparent separation of data at multiple labels in an intuitive manner. Actions assigned to a user or role account are accessed through the Front Panel, Workspace menu, or Application Manager. Roles are protected from interference by other applications via special CDE workspaces, which are themselves protected by enforcing MAC, DAC, and trusted path policies. This prevents rogue applications from performing undesirable actions, such as capturing keystrokes or information contained in CDE windows.

Administrative control is extended to the trusted CDE desktop in the Trusted Solaris 8 Operating Environment. Administrators can control which applications and commands are available to each user, whether labels are displayed on windows, and policies for login and inactivity.

Cut and Paste and Drag and Drop

Trusted Solaris software enables authorized users to cut and paste or drag and drop text, binary data, and graphics between windows at different labels. A trusted selection confirmation tool mediates all such transfers. Before confirming a transfer during a cut and paste, users view the selected data. The trusted windowing system prevents unauthorized transfers and enables auditing of successful and failed transfers.

Trusted Mail

Users are notified about incoming mail through the Mail subpanel on the Front Panel. When the recipient clicks on a mail icon, a mail reader is displayed at the label of the incoming message, irrespective of the current workspace's label.

Mail can be received by an account only if the message is within the account's clearance. Mail can be sent to a host only if the message is within the label range of the host, as specified in the trusted networking databases. An administrative option exists to allow mail from administrators at the ADMIN_LOW label to be delivered to users at their minimum label.

Trusted Path

The trusted path ensures that users are not tricked by a hostile program into supplying information that might be used to penetrate the system. Through the trusted path menu, users perform security-sensitive tasks such as entering passwords to authenticate identity, changing passwords, or selecting labels. Additionally, authorized users authenticate themselves when assuming administrative roles.

A trusted screen stripe along the bottom of the screen gives reliable feedback to assure users that they are communicating within a trusted path. The screen stripe also provides continuous feedback about the labels of the currently active window and input from the keyboard.

A trusted path symbol appears at the left of the trusted stripe area whenever the user is performing any activity that may affect security. It cannot be forged; its presence indicates that the user is safely interacting with the security portion of the system. The only two times when a trusted stripe is not displayed are when the user initially logs in and during the authentication process for unlocking the display. At these times, no untrusted clients are allowed to connect to the window system. The trusted stripe can only be dismissed by a trusted process, preventing rogue clients from duplicating the screen appearance during these states.

Audit Trails

Auditing is a basic feature of the Solaris Operating Environment. All system actions that are auditable are defined as audit events. Groups of audit events are defined as belonging to audit classes. When an audited event occurs, the information defined for it is written as an audit record into the audit log. This log enables an administrator to track system activity and security violations, and assists in determining the cause and source of problems. Trusted Solaris software extends auditing to incorporate new events, information, and classes, as well as provide multilevel support for all auditable events.

Pluggable Authentication Module (PAM)

Originally developed by Sun and adopted by the Open Group for inclusion in CDE/Motif, PAM provides a pluggable model for system authentication mechanisms and other related services, such as password, account, and session management.

The security mechanisms accessible through PAM are implemented as dynamically loadable, shared software modules that can be installed by the administrator transparently to applications. PAM enables the administrator to configure the user authentication mechanism on a per-application basis. For example, a site may require S/Key password authentication for Telnet access, while allowing console login sessions with just password authentication.

With PAM, it is also possible to configure multiple authentication mechanisms for each application. For example, an administrator may want users to be authenticated by both Kerberos and RSA mechanisms. Finally, PAM enables users of these applications to supply a single password even though multiple authentication services may be in use.

The Trusted Solaris 8 platform extends the PAM support of Solaris 8 software by providing failed login account locking, trusted path checking, and machine-generated passwords. For environments that require custom password encryption or password generation algorithms, an integrator provides a shared library implementing those algorithms. This replaces the standard Trusted Solaris 8 algorithms without code changes.

Certified Trusted Systems

Trusted computer systems are those that have been built, evaluated, and certified as conforming to a specific set of security criteria. Historically, the United States has used the Trusted Computer System Evaluation Criteria (the Orange Book) for the evaluation of trusted operating systems, while France, Germany, the Netherlands, and the United Kingdom have used the Information Technology Security Evaluation Criteria (ITSEC) as the *defacto* European security evaluation criteria. There has been a move towards a common set of standards, referred to as the Evaluation Criteria for Information Technology Security Evaluation (the Common Criteria).

The Trusted Solaris 2.5.1 Operating Environment, a predecessor product to the Trusted Solaris 8 Operating Environment, was certified at the E3/F-B1 ITSEC level. Trusted Solaris 8 software has been submitted for Common Criteria evaluation at the EAL4 level with the Labeled Security Protection Profile (LSPP — equivalent to the Orange Book - TCSEC B1 class).

The Solaris 8 Operating Environment has been certified at the EAL4 level with the Controlled Access Protection Profile (CAPP — a superset of the Orange Book - TCSEC C2 class). This includes file and directory read and write controls, user authentication, auditing capabilities, and password management functionality. LSPP functionality adds multilevel security, such as secret and top secret, and mandatory access control (MAC).

Trusted Solaris 8 software meets many requirements beyond LSPP — such as trusted path, separation of roles, and enforcement of privilege. In TSCEC terms, all the B3 functionality is included except real-time audit alarming, but at a B1 level of assurance. Most notably lacking assurances are trusted recovery, TCB modularity and modeling, and covert channel analysis.

Appendix

How the Trusted Solaris Operating Environment Helps Implement a Security Policy

The Trusted Solaris Operating Environment provides a powerful means for organizations to provide better risk management of their computer data. Most corporations already practice some aspects of risk management for paper documents. For example, confidential documents may be printed on colored paper and discarded in locked containers whose contents are later shredded. Master documents, bank account numbers, and access codes are typically kept in fireproof safes. So without realizing it, most corporations have already established the basis for a security policy that protects — in some form — their computer data.

The first step in defining a corporate security policy is to draft a high-level management policy statement that establishes a framework and context for security within an organization. This policy defines the security measures necessary to safeguard a company's systems, networks, transactions, and data. For example, in the pharmaceutical industry, confidentiality and integrity of clinical trial data might be paramount; whereas in the financial industry, ensuring continuity of service and data integrity might be the most important objectives. The Trusted Solaris 8 Operating Environment provides several mechanisms for implementing security policy, ensuring confidentiality by restricting access to specific files on a user-by-user basis.

Next, a systematic analysis of an organization's information assets is made with regard to how sensitive the information is, and which communities of users need access to it. The sensitivity of information is broken down into broad rankings called *classifications: registered, need-to-know, internal use, and public*. The categorizing of users needing the information is used to create *compartments*, communities of users with a common information need. Examples of typical compartments might be engineering, QA, a project spanning disciplines, and marketing. Trusted Solaris software tags all users, processes, files, and other entities on the system with a *label*, which is composed of a classification and one or more compartments to indicate the security level.

Information such as trade secrets, vault and authorization codes, and lock and key information are typically protected by the highest nonadministrative classification. For example, the classification *registered* can be used to protect documents whose unintended disclosure could cause severe loss to a business or operation. In addition to computer security, attention should be given to physical security, for example, restricting the use of modems, removable media, and controlling access to devices. Trusted Solaris software delivers assistance in ensuring physical security by providing the means to control and restrict access to removable media and other devices.

The second highest nonadministrative classification, *need-to-know*, can be used to protect departmental information. This level typically consists of data that is private to a particular department, such as payroll information in finance and medical records in personnel. There may be legal requirements for securing this information. In the Trusted Solaris Operating Environment, all need-to-know information is invisible to anyone who is not specifically authorized to access it.

The next level of classification is *internal-use*. This level of protection varies from company to company, but typically consists of information that should only be disclosed to employees and partners of a company, such as policy and procedure manuals. Trusted Solaris software enables portions of a system to be made available to specific nonemployees without creating unintended vulnerabilities.

The lowest nonadministrative level is the *public* classification. This level covers information, such as product literature, brochures, and catalogs, that needs to be freely available to anyone, but whose integrity needs to be assured to prevent unauthorized alteration. This information is often provided to customers and interested parties via the Internet. Some examples of how labels are applied to information are shown in the following table.

Label	Typical Documents
Registered Engineering	patents, trade secrets
Need-to-Know Engineering	show stopper bugs
Need-to-Know Marketing	pending press releases
Internal-Use	schedules
Public	press releases, product literature

A careful and systematic examination of risks is needed, since perceptions often differ substantially from actual risks. Often the primary risk is found to be internal. For example, system administrators often are among the lowest paid individuals in an organization, yet have access to sensitive information otherwise limited to executives. Trusted Solaris software divides up this function into multiple roles, making it more difficult to compromise systems by corrupting key individuals.

Having evaluated the value of assets and determined potential risks, an implementation strategy for protecting assets can be developed. The objective is to make obtaining the data more expensive than its value, while spending the minimum amount required to protect it. The Trusted Solaris 8 Operating Environment provides a very cost-effective method to obtain excellent security for a modest increase in expense and time.

The next major step in security analysis is to determine which users should have access to which compartments of information. Each user in the organization will be assigned a clearance, consisting of a classification and one or more compartments, which sets an upper limit on the labeled information that the user may access. An example of user security analysis is illustrated in the table below. Clearances used in this example are shown with the users assigned the clearance.

Clearance	Users Assigned to the Clearance
Registered Engineering	Vice-president engineering
Need-to-Know Engineering	Engineering staff
Need-to Know-Marketing	Marketing staff
Internal-Use	Uncategorized employees
Public	All

In summary, establishing a corporate security policy involves the following:

- High-level management policy statement
- Systematic analysis of organizations assets
- Examination of risks
- Development of an implementation strategy

The Trusted Solaris Operating Environment facilitates implementation of a corporate security policy by enabling the set of rules that define the information sensitivity, and the measures used to protect the information from unauthorized access, to be applied to all of its data, devices, and users.

Additional information on creating a security policy can be found at www.sun.com/software/white-papers/wp-security-devsecpolicy/.



Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303

1 (800) 786.7638
1.512.434.1511

<http://www.sun.com/solaris>