Guidance Supplement for Oracle® Solaris 11.1

March 2014
Version 0.7

Security Evaluations
Oracle Corporation
500 Oracle Parkway
Redwood Shores, CA 94065

Guidance Supplement for Oracle Solaris 11.1

Version 0.7

Author: Oracle Corporation

Contributors: Corsec Security

RESTRICTED RIGHTS LEGEND

Use, duplication or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of DFARS 252.227-7013, Rights in Technical Data and Computer Software (October 1988).

Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065.

The information in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. Oracle Corporation does not warrant that this document is error free.

Table of Contents

CHAPTER

1 Introduction

The Target of Evaluation (TOE) is the Oracle Solaris 11.1 SRU5.5. The TOE is a highly configurable UNIX-based Operating System optimized to quickly and securely deploy services in traditional enterprise data centers and large scale internet (or cloud) environments. It includes services such as resource management and network virtualization to provide optimal performance with low overhead in both physical and virtualized environments. TOE provides a sophisticated security system that controls the way users access files, protect system databases, and use system resources. Key high-level security services of TOE include kernel protection, login protection, and data protection.

1.1 Purpose

This document provides guidance on the secure installation and secure use of the TOE for the Common Criteria (CC) Evaluation Assurance Level EAL4+ evaluated configuration. This document provides clarifications and changes to the Oracle documentation and should be used as the guiding document for the installation and administration of the TOE in the CC evaluated configuration. The official Oracle documentation should be referred to and followed only as directed within this guiding document. Oracle documentation is available for download at http://docs.oracle.com.

Table 1 below lists the guidance documents relevant to the use of the TOE. Table 2 lists other documents relevant to the installation of the TOE.

Table 1 TOE Guidance Documents

Document Name	Description
Oracle Solaris 11 Security Guidelines, Part No: E29014–02, February 2013	Provides an overview of Oracle Solaris security features and the guidelines for using those features to protect the TOE.
Oracle Solaris Administration: Security Services, Part No: E29015–03, February 2013	Explains how to administer security features on the TOE
Oracle Solaris 11.1 Desktop Administrator's Guide, Part No: E28056-02, February 2013	Describes how to administer the Oracle Solaris Desktop and its components.
Solaris 11 XScreenSaver Manual, 28-Sep-2011	Information on the XScreenSaver program.
Trusted Extensions Configuration and Administration, Part No: E29017–01, October 2012	Explains how to enable, configure, and maintain the Trusted Extensions (TX) feature of the TOE.
Trusted Extensions User Guide, Part No: E29018-01, October 2012	Describes how to work in a multilevel environment when the TX feature is enabled.
Oracle Solaris 11.1 Administration: Oracle Solaris Zones, Oracle	Describes resource management, Oracle

Document Name	Description
Solaris 10 Zones, Resource Management, Part No: E29024-01	Solaris Zones, and Oracle Solaris 10 Zones (Solaris10 branded zones).
Securing the Network in Oracle Solaris 11.1, Part No: E28990-02, February 2013	Explains how to secure the link and IP[1] layer on a Solaris Network.
Working With Naming and Directory Services in Oracle® Solaris 11.1, Part No: E29002-01	Discusses the use of naming and directory services in the TOE.
MIT Kerberos Documentation (http://web.mit.edu/kerberos/krb5-current/doc/)	Provides information on administration, use and concepts of Kerberos.
Man pages section1M: System Administration Commands, Part No: E29031	Reference information (man pages) for TOE administration commands.
Man pages section4: File Formats, Part No. E29042	Reference information (man pages) for various file formats.
Man pages section5: Standards, Environments and Macros, Part No: E29043	Reference information (man pages) for various miscellaneous subjects, including headers, environments, macro packages, character sets, and standards

Table 2 Installation Documents

Document Name	Description
Installing Oracle Solaris 11.1 Systems, Part No: E28980–01, October 2012	Provides instructions for installing the TOE. This guide describes how to install from live media, use the text installer, and perform client installations over the network.
Creating and Administering Oracle Solaris 11.1 Boot Environments, Part No: E29052–01, October 2012	Provides instructions to create and administer multiple boot environments on the TOE.
Adding and Updating Oracle Solaris 11.1 Software Packages, Part No: E28984–02 February 2013	Describes the Oracle Solaris Image Packaging System (IPS) tools used to install, upgrade, and remove software packages for the TOE.

Along with the above-referenced documentation, additional supporting documentation for the TOE is available in the Oracle Solaris 11.1 Information Library: http://docs.oracle.com/cd/E26502_01/.

1.2 Target Audience

The audience for this document consists of the end-user, the Oracle development staff, the CC Evaluation Laboratory staff, and the Government Certifier.

[1] IP – Internet Protocol

1.3 Evaluated TOE Configurations

Figure 1 depicts the sample deployment of the TOE.

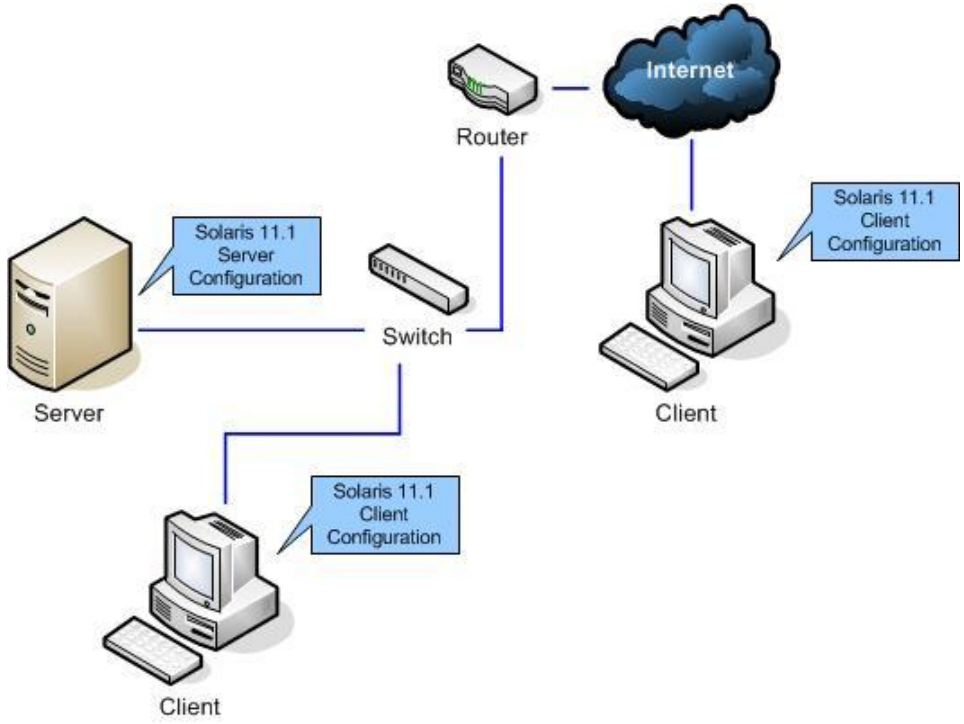
Router
Internet
Solaris 11.1 Server Configuration
Switch
Server
Solaris 11.1 Client Configuration
Client
Solaris 11.1 Client Configuration
Client

Figure 1 Sample Deployment Configuration of the TOE

The sample deployment shown in Figure 1 shows multiple instances of the TOE. All instances of the TOE are connected on a Local Area Network (LAN) provided by a network switch or a part of a Wide Area Network (WAN). One instance of the TOE is configured as a server connected to the LAN, and the other is a client configuration. A router provides an Internet gateway that allows restricted inbound and outbound connections. As part of the WAN, an instance of the TOE, configured as a client, communicates with a TOE in server configuration through a remote connection.

1.4 Assumptions

The writers of this document assume the following:

- 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.
- All connections to and from remote trusted Information Technology (IT) systems and between physically-separate parts of the TOE Security Functionality (TSF) not protected by the TSF itself are physically or logically protected within the TOE environment to ensure the integrity and confidentiality of the data transmitted and to ensure the authenticity of the communication end points.

- Any modification or corruption of security-enforcing or security-relevant files of the TOE, user or the underlying platform caused either intentionally or accidentally will be detected by an administrative user.
- The TSF is managed by one or more competent individuals. The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation.
- All remote IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions, are assumed to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality.
- All remote IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to be under the same management control and operate under security policy constraints compatible with those of the TOE.
- It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.
- Users are sufficiently trained and trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their user data.

CHAPTER

2 Installation Procedure

This section describes the installation procedure notes and changes.

2.1 Introduction

This section provides guidance for how to properly step through the installation instructions referenced in Table 2, along with additions and changes to the instructions contained therein, in order to allow the installer to properly install the evaluated configuration of the TOE.

2.2 Secure Installation

Note: Throughout this section the reader will be instructed to read certain passages from referenced documents. Unless otherwise stated, such instructions refer to the documents listed in Table 1 and Table 2.

2.2.1 Phase 1 – Initial Preparation

Before the administrator begins the installation, he should make certain that he has all the necessary components as listed below.

Components Required for the TOE Installation Configuration

The following components are required for the TOE installation:

- Hardware platform on which the TOE can be installed – either x86 or SPARC[2]-based system, with these minimum system requirements:
  - Memory – minimum 512 MB[3]
  - Disk space – minimum 30 GB[4]
- The TOE downloaded from the Oracle Software Delivery Cloud at https://edelivery.oracle.com. The right ISO image depending on the platform (X86 or SPARC) should be downloaded for installation.

2.2.2 Phase 2 – Verification of the TOE

When the TOE is downloaded via Oracle's website, Oracle uses the Message Digest 5 (MD5) algorithm to verify the integrity of the data. To confirm the downloaded TOE's integrity, a customer can click the "View Digest" button to view the MD5 data for all the files displayed under the Media Pack. If the two values match, this indicates that the data has not been altered. Should the TOE fail the message digest hash procedure, the

[2] SPARC – Scalable Processor Architecture
[3] MG - Megabyte
[4] GB - Gigabyte

customer should download the TOE again and re-check the hash. If the failure persists, the customer should contact Oracle Customer Support.

After downloading the TOE, a customer may also verify the product version by running the following command *"pkg info entire"*. This will display the following information about the TOE:

Publisher: solaris

Version: 0.5.11 (Oracle Solaris 11.1 SRU 5.5)

If the version and build number displayed do not match with those ordered by the customer from the Oracle Software Delivery Cloud and confirmed via email as described, the customer should contact Oracle Customer Support.

2.2.3 Phase 3 – Installation

The evaluated configuration consists of the following Oracle Solaris software components/packages:

- Oracle Solaris 11.1 Text Installer image for 64-bit systems
- Oracle Solaris 11.1 SRU5.5 Repository image for 64-bit systems

In the evaluated configuration the TOE requires the following to be installed:

- Base Solaris Operating System
- Kerberos
- TX
- Zones

The guidance and installation documents referenced in Table 1 and Table 2 provide detailed instructions for installing the above functionality.

2.2.4 Phase 4 – Evaluated Configuration of the TOE

Once the TOE is properly installed as instructed above, the sections below describe the actions required to bring it into the evaluated configuration:

2.2.4.1 Disabling User Permissions to Run the xhost Command

The *xhost* command is used to add and delete host names or user names authorized to make connections to the TOE's X server, which controls access to system displays. Since host-based access control is excluded from the TOE, *xhost* must be made a 'root' only accessible command by the administrator changing the access permission on the executable files, by typing:

- *chmod* 744 /usr/openwin/bin/xhost
- *chmod* 744 /usr/X11/bin/xhost

2.2.4.2 Configuring the Audit Service

This section includes details about configuring the audit service. Refer to Chapter 22, 'Trusted Extensions Auditing', of *Trusted Extensions Configuration and Administration* for the role responsibilities for audit administration.

2.2.4.2.1 Configuring the Audit Plugins

The administrator decides in which format and where to collect audit records. There are three choices: store binary records locally, stream binary audit records to a remote protected repository by using the *audit_remote* plugin, or send audit record summaries to syslog by using the *audit_syslog* plugin. The default active plugin is *audit_binfile*, which stores binary audit records locally. The default storage directory is */var/audit*. There can be more than one plugin active. TOE administrator should also configure *audit_remote* and *audit_syslog* plugins, and specify which audit plugins are to handle the records placed in the audit queue.

2.2.4.2.2 Selecting Audit Events

By default, the TOE's audit service is configured to audit only login and logout events (the "lo" audit class); however it can be configured to record different classes of events based upon site policy. To group a set of related audit events, the audit service provides the ability for sites to define their own audit classes containing just those events that the site wants to audit. This is configured by an administrator by preselecting audit events to record on a system-wide and user-specific basis. The "Securing Users" section of *Oracle Solaris 11 Security Guidelines* explains how to audit significant events in addition to login/logout. It is required to audit administrative 'all' classes. (Refer to 'How to Preselect Audit Classes' in Chapter 28 of *Oracle Solaris 11.1 Administration: Security Services* for additional details.)

2.2.4.2.3 Setting Up the audit_warn Email Alias

The *audit_warn* script is run whenever the audit system detects a situation that requires administrative attention. By default, the *audit_warn* script sends email to an audit_warn alias and sends a message to the machine console. To set up this alias, see 'How to Configure the audit_warn Email Alias' in Chapter 28 of *Oracle Solaris 11.1 Administration: Security Services*.

It is required to set a disk utilization threshold for the audit directory of 1%. If this threshold is crossed (for the volume that includes */var/audit*), then a warning e-mail will be sent to advise the system administrator that audit events may be lost if the disk becomes full.

2.2.4.3 Configuring Network File System version 4

The evaluated configuration uses Network File System version 4 (NFSv4). The TOE administrator should mount NFS using the '*mount*' command. The Man page for the command *mount_nfs* lists the options to *mount* that are appropriate for NFS file systems. For example, the *sec* option lets an administrator specify the security mode (authentication mechanism) to be used on the NFS file system (refer to *nfssec* in *"Man pages section5: Standards, Environments and Macros"*, pg. 342 for the available security mode options). The sec mode should be set to krb5p in the evaluated configuration, since it provides the most secure file system sharing as all the traffic is encrypted. In the evaluated configuration the NFS server is configured as a Kerberos client. All clients that attempt to access files from a shared file system on the NFS server require Kerberos authentication.

Another example of a *mount* command option is the *proto* option that is used to select the transport protocol that the NFS mount uses. By default, the transport protocol that the NFS mount uses is the first available Remote Directory Memory Access (RDMA) transport supported by both the client and the server. If no RDMA transport is found, then it attempts to use a Transmission Control Protocol (TCP) transport or, failing that, a User Datagram Protocol (UDP) transport, as ordered in the */etc/netconfig* file.

However in the evaluated configuration *proto* is set to the TCP in the TOE to provide connection-oriented service. The UDP protocol is not supported for NFSv4 and RDMA is not recommended.

See ‘Chapter 6 – Accessing Network File Systems (Reference)’ of *Oracle Solaris Administration: Network Services, Part No: 821-1454-10, November 2011* for more details on the *mount* command as it applies to NFS mounts.

2.2.5 Flaw Remediation

Oracle Solaris customers or partners can receive information on flaw remediation through the secure My Oracle Support portal to report security vulnerabilities or other flaws in the TOE. Other individuals, i.e. independent researchers, may email secalert_us@oracle.com with their discoveries. Refer to the below reference for additional information on Oracle security practices and flaw handling procedures.
http://www.oracle.com/us/support/assurance/overview/index.html

CHAPTER

3 Administrative Guidance

This section provides additional guidance not found in the guides listed in Table 1. Any clarifications, exclusions, or additions are detailed here to allow the TOE Administrator to properly configure and maintain the evaluated configuration of the TOE. The TOE Administrator should have successfully completed the installation procedures listed in section 2 before applying the guidance found in sections 3.1 and 3.2. All configurations of the TOE must follow this guidance.

3.1 Clarifications

This section provides clarification on user accounts, system access, and cryptographic services.

3.1.1 User Accounts

This section provides guidance on setting up secure defaults for user accounts and their environment.

3.1.1.1 Creating Roles

An administrator should create administrative roles based on rights profiles for the site and assign the roles to users. For information on doing this, see Chapter 9, ‘Using Role-Based Access Control (Tasks)’ of *Oracle Solaris Administration: Security Services*. The rights profiles on the TOE are designed to map to roles. For example, the System Administrator rights profile can be used to create the System Administrator role. To configure a role, see “How to Create a Role” on page 165 of *Oracle Solaris Administration: Security Services*. The following roles are typical of a TX site:

- root role – Created at TOE installation
- Security Administrator role – Created during or after initial configuration by the initial setup team

3.1.1.2 Setting Password Policy

The password policy is configured by default for the evaluated configuration. Specifically, user passwords by default must comply with the following syntax:

- Password length must be at least six characters long and have at least two alphabetic characters and one non-alphabetic character.
- Passwords must not be a member of the configured dictionary specified in the */etc/default/passwd* file. To configure the TOE to perform a dictionary check on passwords, the administrator generates a dictionary database specified by

the DICTIONLIST flag in */etc/default/passwd* (refer to the *passwd* Man page). This will ensure that a password is not a member of the configured dictionary.

- Old and new passwords must differ by at least the MINDIFF value specified in */etc/default/passwd*. If unspecified, the default is 3.

Passwords must not be a circular shift of the login name *(*NAMECHECK flag set to 'yes' in */etc/default/passwd,* as set by default*).*

However it is recommended to follow the steps on how to set stronger password constraints in the "Securing Users" section of Chapter 2 of *Oracle Solaris 11 Security Guidelines*. Specifically, by setting certain variables in the */etc/default/passwd* file, administrators can implement the following stronger password constraints:

- requiring a password of at least eight characters
- keeping a password history
- requiring users to change their passwords periodically
- requiring the password must contain at least one upper-case letter and one digit
- requiring a minimum difference between the characters in an existing and new password of 4 (instead of 3)

In the evaluated configuration, the default password policy must be configured to the above recommendation for TOE users including Kerberos principals to meet the security strength requirements. Administrators should refer to the *passwd* Man page for information on the authorizations required to perform various options of this command. Users should refer to Chapter 3 of *Trusted Extensions User's Guide* for instructions on how to change their password.

There is no default password policy in force by Kerberos, refer to section "Administering Kerberos Policies" in *Oracle Solaris 11.1 Administration: Security Services.*

The Oracle Solaris default password encryption algorithm is a SHA[5] 256 based algorithm. This must not be changed in the evaluated configuration.

3.1.1.3 Removing Unneeded Basic Privileges from Users

It is recommended, but not required, to follow the steps on how to remove unneeded basic privileges from users in the 'Securing Users' section of Chapter 2 of *Oracle Solaris 11 Security Guidelines*. Do not remove the "proc_fork" or the "proc_exec" privilege. Without these privileges, a user cannot use the system.

3.1.2 System Access

The actions described in this section configure the TOE to control access to the system and its services.

3.1.2.1 Setting Account Locking for Regular Users

It is required to follow the steps on how to set account locking for regular users in the 'Securing Users' section of Chapter 2 of *Oracle Solaris 11 Security Guidelines*.

The RETRIES parameter in the /etc/default/login file is the number of failed login attempts a user is allowed before being disconnected from the system and forced to reconnect. When LOCK_AFTER_RETRIES is set to 'YES' in */etc/security/policy.conf*, then the user's account is locked after this many failed retries (the account can only be unlocked by an administrator using the command *passwd* -u

[5] SHA – Secure Hash Algorithm

<username>). The value for security attribute 'RETRIES' is administrator configurable and there is not a specific setting required for the evaluated configuration. Users who can assume roles such as root, which are necessary to rescue the system, must have account locking turned off to prevent the denial of service.

3.1.2.2 Disabling Host-based Authentication for Solaris Secure Shell

Host-based authentication for Solaris Secure Shell (SSH) is not used in the evaluated configuration. It is disabled by default, but, if necessary, disable host based authentication as follows:

- On the local host (client), the HostbasedAuthentication keyword in the system-wide configuration file */etc/ssh/ssh_config* should be set to 'no'.
- On the remote host (server), the HostbasedAuthentication keyword in the system-wide server configuration file, */etc/ssh/sshd_config* should be set to 'no'.
- Also on the remote host, the IgnoreRhosts keyword in */etc/ssh/sshd_config* should be set to 'yes'. This forces users to enter a password when authenticating with SSH. If the IgnoreRHosts line does not appear in the file, the default setting of 'yes' is automatically applied, so no additional changes are needed.

3.1.2.3 Setting Default Screen Lock for Desktop Environment Users

The XScreenSaver program is used on the TOE to blank and lock a displayed screen after an administrator-configurable amount of time of inactivity to prevent others from using it. The *xscreensaver-demo* program is a graphical front-end to the XScreenSaver program for setting the parameters used by the background *xscreensaver* daemon. The *Blank After* field controls how long the user can be idle before the screen blanks. The user inactivity period is administrator configurable and there is not a specific setting required for the evaluated configuration. The *Lock Screen After* option controls the length of time between when the screensaver activates and the screen becomes locked. The default is 0, meaning that if locking is enabled, then a password will be required as soon as the screen blanks.

The Screensaver preference tool from the GNOME[6] GUI System menu is used to modify screensaver application preferences. To start the Screensaver preference tool, run the *xscreensaver-demo* command from the */usr/bin/* directory. To start the Screensaver preference tool from the System menu, choose System → Preferences → Screensaver. Refer to Chapter 7 'Managing Screensavers' of *Oracle Solaris 11.1 Desktop Administrator's Guide* and *Solaris 11 XScreenSaver Manual* for more information.

3.1.2.4 Disabling Unneeded Services

All services disabled in TOE by default are not part of the evaluated configuration unless explicitly enabled by authorized administrator as specified in this document. TOE user can run the command *svcs –a* to list the services enabled and disabled by default. In order to disable any unneeded services in TOE please refer to the steps described in "Securing the System" section of Chapter 2 of *Oracle Solaris 11 Security Guidelines.*.

3.1.2.5 Configuring X Window System

[6] GNOME – GNU Object Model Environment - the desktop environment and Graphical User Interface (GUI) for the TOE.

The X Window System, commonly referred to as X or X11, is a network-based graphical window system. The X Window System used in the TOE is the X11R7.7 release, an open source version developed by the X.Org Foundation. It consists of X servers and X clients. The TOE uses the Xorg X server and Xvnc X server (for remote administration) included with the X11R7.7 release of X Window System. Other X servers are available in Solaris 11.1 but are not used in the evaluated configuration.

The X clients supported in the evaluated configuration include the following: metacity window manager, xterm, Xscreensaver, GNOME and TigerVNC. Other available X clients are not included in the evaluated configuration. X Display Manager Control Protocol (XDMCP) displays the login screen and resulting session on a remote machine over a network interface. By default, XDMCP is disabled; this should be enabled in the evaluated configuration for remote administration. Refer to section "How to Configure a Trusted Extensions System with Xvnc for Remote Access" in *Trusted Extensions Configuration and Administration*.

In the evaluated configuration even though no trusted path between a user and TOE is claimed for remote access, it is recommended to secure the remote Xvnc sessions using TOE supported cryptographically protected trusted channels.

3.1.2.6 Configuring Solaris Secure Shell for Federal Information Processing Standards 140

SSH provides for remote login to the TOE as well as providing an encrypted and trusted channel for communication. SSH in Oracle Solaris is built on top of the Open Source toolkit, OpenSSL, which implements the Secure Sockets Layer and Transport Layer Security. Two distinct versions of the OpenSSL toolkit are available in Oracle Solaris:

- Version 1.0.0 is the default version that SSH runs on.
- Version 0.9.8 implements Federal Information Processing Standards (FIPS) 140, a U.S. government computer security standard for cryptography modules.

The evaluated configuration uses SSH only in FIPS 140 (FIPS) mode, i.e., built on top of the Version 0.9.8 tookkit..

The administrator shall invoke FIPS mode on the command line by typing ssh -o "UseFIPS140 yes" *remote-host*. As an alternative, the administrator can configure sshd to run OpenSSL in FIPS mode by setting the variable UseFIPS140 to 'yes' in the configuration file */etc/ssh/ssh_config* and */etc/ssh/shhd_config*. The TOE supports SSH v2 on server and client side, and SSH v1 on client side. In the evaluated configuration the TOE should be configured to use SSHv2 on both server and client side. Refer to */etc/ssh/ssh_config*, */etc/ssh/sshd_config*; "Secure Shell and FIPS-140" section of chapter 15 'Using Secure Shell' in *Oracle Solaris Administration: Security Services*; and *sshd* and *ssh_config* Man pages for additional information.

3.1.2.7 Specifying Kerberos Encryption Algorithms

The Kerberos component is a client-server architecture that provides secure transfer of data over an insecure network. The service offers strong user authentication, as well as integrity and privacy. Authentication guarantees that the identities of both the sender and the recipient of a network transaction are true. The service can also verify the validity of data being passed back and forth and encrypt the data during transmission.

When a client logs into the TOE using Kerberos, the KDC[7] will create a session key and a ticket. The session key is part of the TGT[8] that is used for all further client communications with the KDC. Kerberos securely transports the session key, which can be AES[9] in CTS[10] mode with a key size of 256 or 128 or 3DES[11] in CBC[12] mode, and ticket with a 168-bit key using RSA[13] or DSA[14]. HMAC-SHA1[15] is also used for authentication of the session keys. Kerberos uses HMAC-SHA1 for integrity and AES 128 or 256 in CTS mode for privacy of NFS file transfers.

The administrative command *krb5kdc* allows an administrator to specify encryption algorithms for Kerberos. As described above, only 3DES and AES algorithms are used (DES[16] and ARCFOUR are not used in the evaluated configuration). The **-k** *masterenctype* option for *krb5kdc* specifies the encryption algorithm for Kerberos. The default value is des-cbc-crc. This must be changed to des3-cbc-sha1, aes128-cts-hmac-sha1-96, or aes256-cts-hmac-sha1-96. des-cbc-crc, arcfour-hmac-md5, and arcfour-hmac-md5-exp are not to be used.

3.1.3 Configuring FIPS Algorithms

All cryptographic services provided by the TOE, including key agreement, key exchange, symmetric and asymmetric encryption, hashing, message authentication, and random number generation services, are accessed via the Solaris Cryptographic Framework API[17]. This API is divided into a User-level and kernel-level Cryptographic Framework. The User-level API is accessible to applications running in the user area of memory on the TOE, while processes running in kernel space have access to the kernel-level API.

Kernel-level processes are able to access the kernel-level API directly. Any cryptographic functionality required by a kernel-level process is sent to the kernel-level API.

It is a requirement that the Solaris administrators and users only request FIPS 140-2 approved algorithms that are listed in the Oracle Cryptographic Framework FIPS Security Policies (Solaris Userland Cryptographic Framework Software FIPS 140-2 Security Policy and Solaris Kernel Cryptographic Framework Software FIPS 140-2 Security Policy) in the evaluated configuration. Each API provides an interface for processes to access cryptographic functionality, but does not actually implement any cryptographic functionality. The actual cryptographic functionality is implemented in separate libraries called providers implemented in the form of public-key cryptography standards (PKCS) #11-compliant plug-ins. The PKCS #11-compliant plug-ins in the evaluated configuration include *libmd.so.1* and *libsoftcrypto.so.1*. The OpenSSL[18] module is used exclusively by the SSH protocol in the evaluated configuration and does not present a public interface.

[7] KDC – Key Distribution Center
[8] TGT – Ticket Granting Ticket
[9] AES – Advanced Encryption Standard
[10] CTS – Ciphertext Stealing
[11] 3DES – Triple Data Encryption Standard
[12] CBC – Cipher Block Chaining
[13] RSA – Rivest, Shamir and Adleman
[14] DSA – Digital Signature Algorithm
[15] HMAC-SHA1 – Hash message authentication code using secure hash algorithm 1
[16] DES – Data Encryption Standard
[17] API – Application Programming Interface
[18] The OS provides two OpenSSL libraries. The publicly available OpenSSL library has been excluded from the evaluation. All references to OpenSSL refer only to the FIPS validated, private interface used exclusively for SSH.

libmd.so.1 is a publically available library on the TOE that provides hashing (SHA-1 and SHA-2[19]) and message authentication (HMAC[20] SHA-1 and HMAC SHA-2) functionality to cryptographic consumers. This library can be accessed via direct API call or through the Cryptoki interface which leverages *pkcs11_softoken.so.1*.

*libsoftcrypto.so.*1 is a private library in the TOE that provides the following functions:

- data encryption and decryption
  - AES ECB[21], CBC, CFB[22], CCM[23], GCM[24], and CTR[25] with 128, 192, and 256-bit keys
  - 3DES CBC and ECB modes with 168-bit keys
- signature generation and verification
  - RSA with 1024, 2048, 4096, and 8192-bit keys
  - DSA with domain parameters of 1024 and 160-bits
  - Diffie-Hellman with 160, 224, 256, and 384-bit private keys and 1024, 2048, 4096, and 8192-bit public keys

This library can be accessed via a direct API call (*ucrypto)*[26] or through Cryptoki which leverages *pksc11_softoken.so.1*.

The libraries *libpkcs11.so.1* and *pkcs11_softtoken.so.1* provide access to the cryptographic provider plug-ins through the RSA defined PKCS #11 Cryptoki interface. Applications that would like to take advantage of the various cryptographic providers need to link to these libraries.

To manage the cryptographic providers, the TOE provides a management interface through *crytpoadm*, which can be used to manage the cryptographic provider plug-ins. Using the *cryptoadm* interface, an administrator can install, uninstall, enable, and disable cryptographic providers, which will determine the cryptographic services available to a software consumer, for example, Kerberos, Internet Key Exchange (IKE), or Internet Protocol Security (IPsec). FIPS mode must be appropriately enabled through this interface to comply with the evaluated configuration.

All cryptographic consumers besides SSH should use the PKCS #11 interface. In User Space, users and applications that wish to interact with these plug-ins call the PKCS #11 API, which determines which plug-in to use.

3.1.4 Enabling a Persistent Entropy Block

For instructions on enabling a persistent entropy block as well as the specific commands necessary to enable FIPS mode using *cryptoadm*(*1M)* refer to the below FIPS 140-2 Security Policies:

- Oracle Solaris Kernel Cryptographic Framework Software Version 1.0 and 1.1
- Oracle Solaris Userland Cryptographic Framework Software Version 1.0 and 1.1
- Oracle Solaris Kernel Cryptographic Framework with SPARC T4 and T5 Software Version 1.0 and 1.1; Hardware Version: SPARC T4 (527-1437-01) and T5 (7043165)

[19] SHA-2– Includes SHA-224, SHA-256, SHA-384, and SHA-512
[20] HMAC – Hash-based Message Authentication Code
[21] ECB – Electronic Code Book
[22] CFB – Cipher Feedback Mode
[23] CCM – CBC Counter Mode
[24] GCM – Galois/Counter Mode
[25] CTR – Counter Mode
[26] A small subset of the cryptographic algorithms is available via *ucrypto*

- Oracle Solaris Userland Cryptographic Framework with SPARC T4 and T5 Software Version 1.0 and 1.1; Hardware Version: SPARC T4 (527-1437-01) and T5 (7043165)

3.1.5 Configuring IPsec and IKE

The TOE implements IPsec with IKE v1. IPsec supports Authentication Header (AH) and Encapsulating Security Payload (ESP). AH provides data authentication, integrity, and replay protection through the use of a hash that is sent as a header of the packet. The following algorithms can be used for AH in the evaluated configuration:

- SHA1 (integrity only)
- HMAC-SHA1
- HMAC-SHA256
- HMAC-SHA384
- HMAC-SHA512
- AES-GMAC[27]128
- AES-GMAC192
- AES-GMAC256

ESP provides data confidentiality by encrypting the packet using the following algorithms:

- AES in CBC, CCM, or GCM mode with 128-, 192-, and 256-bit keys
- 3DES in CBC mode with 168-bit keys

These protocols can be used individually or together.

Administrators can use *ipsecconf* to configure system-wide IPsec policies. Policies perform a specific action when a packet matches the policy. Both the action and the match criteria are set with *ipsecconf.* Policies can also be added through the */etc/inet/ipsecinit.conf* file in the Service Management Facility (SMF) module.

Only AES and 3DES encryption algorithms are allowed to be used in IPsec policies for the evaluated configuration. Administrators must not configure IPsec rules that use Blowfish, RC4 [28], or MD5. The administration command *ipsecalgs* allows an administrator to specify authentication and encryption algorithms for IPsec. The *ipsecalgs* command can list the algorithms that each IPsec protocol supports. The *ipsecalgs* configuration is stored in the */etc/inet/ipsecalgs* file. Typically, this file does not need to be modified. However, if the file needs to be modified, use the *ipsecalgs* command. The file must never be edited directly. The supported algorithms are synchronized with the kernel at system boot by the svc:/network/ipsec/ipsecalgs:default service. The *ike.config*also allows algorithms to be set. For details on IPsec packet flow and how IPsec operates with other networking protocols see *Securing the Network in Oracle Solaris 11.1.*

IKE is used to securely exchange keys with a trusted external system in order to establish an IPsec connection. IKE automates key management for IPsec. IPsec and IKE are used in the evaluated configuration, but only with pre-shared keys. Preshared keys should be 128 bits or larger. IKE is disabled by default in the TOE and must be enabled for the evaluated configuration. See *Securing the Network in Oracle Solaris 11.1* IKE Key Negotiation and IKE Configuration Choices for Preshared Keys for details on the IKE process. IKE phase 1 operates in either Main Mode[29]..

[27] GMAC – Galois Message Authentication Code

[28] RC4 – ARCFOUR encryption algorithm.

[29] IKE phase 1 operates in either Main Mode or Aggressive Mode. Aggressive Mode does not include authentication and is therefore not allowed in the evaluated configuration.

3.1.5.1 SSH and TCP/IP Forwarding

SSH should not be used for TCP/IP forwarding. An administrator disables this by changing the default value of the AllowTCPForwarding keyword in */etc/ssh/sshd_config* from ‘yes’ to ‘no’. Refer to “Keywords in Solaris Secure Shell” in Chapter 16 ‘Secure Shell (Reference)’ of *Oracle Solaris Administration: Security Services*.

3.1.6 IP Filter

The IP Filter service (*svc:/network/ipfilter*) is not enabled by default, meaning that network information flow control is allowed for all packets by default. An administrator must enable IP Filter using *ipf* to enable the firewall functions. An administrator may also define a new filter using *svc.ipfd* and enable it. This is done through the SMF module. Enabling the firewall functions allows administrators to assign more restrictive values for flow control attributes by creating rules to block packets according to the security attributes assigned.

Solaris IP Filter is installed with the Solaris OS. However, packet filtering is not enabled by default. Use the procedure described in *ipf(1M) man page* to activate the Solaris IP Filter feature. Also refer to “Configuring IP Filter” in Chapter 4 of *Securing the Network in Oracle Solaris 11.1*. Packet filter rules for the logical or physical network interface through which network data enters the TOE need to be created by an administrator based on IEEE[30] 802.1Q VLAN[31] tags and_TCP/IP information security attributes, including the following

- Source and destination IP address
- Source and destination TCP port number
- Source and destination UDP port number
- Network protocol of IP, IPv4, IPv6, TCP, UDP, ICMP[32], ARP[33], SCTP[34], and IPsec
- TCP header flags of SYN[35] and ACK[36]

The packet filter rules identify network data by matching it to the attributes defined above or by matching based on the state of a TCP connection. The rules also specify what to do with a packet if it matches the filter rule. This can include discarding the network data without any further processing (block) or allowing the network data to be processed unaltered by the TOE according to the routing information maintained by the TOE (pass).

3.1.7 CUPS

The default label_encodings file must be modified to have the Clearance words match the Sensitivity Label words for successfully accessing the print server from within a non-global zone. The default label_encodings file must be modified such that the Clearance word section in the file has exactly the same contents as the Sensitivity Label section.

3.1.8 Modifications to *syslog.conf* file

Audit records are records generated by the audit daemon (*auditd*) and are not generalized to */var/adm* or */var/log*. However some potential security information such

[30] IEEE – Institute of Electrical and Electronics Engineers
[31] VLAN – Virtual Local Area Network
[32] ICMP – Internet Control Message Protocol
[33] ARP – Address Resolution Protocol
[34] SCTP – Stream Control Transmission Protocol
[35] SYN – Synchronize
[36] ACK – Acknowledge

as *su* or *sudo* failures are logged into */var/adm/messages*. Thus in order to prevent leakage of any security information the following changes must be made to */etc/syslog.conf* file:

the line in *syslog.conf* that reads:
".err;kern.debug;daemon.notice;mail.crit   /var/adm/messages"*
must be edited to read:
".err;kern.debug;daemon.notice;auth.none;mail.crit   /var/adm/messages"*
and also uncomment the line that reads
#auth.notice   ifdef('LOGHOST', /var/log/authlog, @loghost')

Once the above change is made the loghosts should be properly configured in hosts(4) database.

3.1.9 LDAP

The TOE supports cryptographically protected trusted channels between itself and LDAP[37] directory server in the TOE environment. The TOE supports SASL/GSSAPI authentication method to bind to the LDAP directory servers, with this method the credential level must be configured to "Self" in order to correctly bind to the LDAP directory server. The TOE also supports IPsec protocol to establish a trusted channel between LDAP directory server and itself. The LDAP directory server in the environment should conform to the TOE supported schemas, detailed information about Oracle Solaris specific schemas are discussed in *"Working With Naming and Directory Services in Oracle® Solaris 11.1".*

3.2 Exclusions

The following product features and functionality are excluded from the TOE, and hence, they are not part of the evaluated configurations of the TOE. Any reference to these items in the documentation listed in Table 1 should be ignored:

- Network Information Service (NIS) (note that the NIS server software is not installed by default)
- FTP
- Telnet
- TCP/IP forwarding for SSH
- InfiniBand Sockets Direct Protocol 20 and Reliable Datagram Sockets v321
- Remote XDMCP access
- Host-based authentication for SSH
- Host-based access control
- Direct X11 connections from other machines by using the TCP protocol
- OpenSSL Version 1.0.0
- DES and ARCFOUR encryption algorithms for Kerberos
- IPsec rules that use Blowfish, RC4, or MD5
- WebNFS
- SSH for TCP/IP Forwarding
- DHCP[38] when Kerberos is used for authentication
- DES and ARCFOUR encryption algorithms for Kerberos

[37] LDAP – Lightweight Directory Access Protocol
[38] DHCP – Dynamic Host Configuration Protocol

- Common Internet File System Server in Workgroup Mode
- Time out over TOE Shells
- Transport Layer Security
- User-space client programs such as Java Runtime Engine (JRE), Apache Web Server, Perl, and Python amongst others. As mentioned above all services disabled in TOE by default are not part of the evaluated configuration unless explicitly required to be enabled by authorized administrator as specified in this document.

CHAPTER

4 Acronyms

This section defines the acronyms.

Acronym	Definition
3DES	Triple Data Encryption Standard
ACK	Acknowledge
AES	Advanced Encryption Standard
AH	Authentication Header
API	Application Programming Interface
ARP	Address Resolution Protocol
CBC	Cipher Block Chaining
CC	Common Criteria
CCM	CBC Counter Mode
CFB	Ciphertext Feedback
CIFS	Common Internet File System
CTR	Counter-mode Encryption
CTS	Ciphertext Stealing
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DNSSEC	DNS Security Extensions
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
ECB	Electronic Code Book
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GB	Gigabyte
GCM	Galois Counter Mode

GMAC	Galois Message Authentication Code
GNOME	GNU Network Object Model Environment
GUI	Graphical User Interface
HMAC	Hashed Message Authentication Code
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
IPS	Image Packaging System
IT	Information Technology
JRE	Java Runtime Engine
KDC	Key Distribution Center
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MB	Megabyte
MD5	Message Digest 5
NFSv4	Network File System version 4
NIS	Network Information Service
PKCS	Public-key Cryptography Standards
RC4	ARCFOUR
RDMA	Remote Directory Memory Access
RSA	Rivest, Shamir and Adleman
rsh	Remote Shell
SBD	Secure By Default
SCTP	Stream Control Transmission Protocol
SHA	Secure Hash Algorithm
SMF	Service Management Facility
SPARC	Scalable Processor Architecture
SSH	Solaris Secure Shell
SYN	Synchronize
TCP	Transmission Control Protocol
TGT	Ticket Granting Ticket
TLS	Transport Layer Security

TOE	Target of Evaluation
TSF	TOE Security Functionality
TX	Trusted Extensions
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VNC	Virtual Network Computing
WAN	Wide Area Network
XDMCP	X Display Manager Control Protocol