Oracle® Solaris 11.4 Security and Hardening Guidelines

Part No: E61019
May 2021

ORACLE

Oracle Solaris 11.4 Security and Hardening Guidelines

Part No: E61019

Référence: E61019

Accessibilité de la documentation

Pour plus d'informations sur l'engagement d'Oracle pour l'accessibilité de la documentation, visitez le site Web Oracle Accessibility Program, à l'adresse : http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Accès aux services de support Oracle

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info ou le site http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs si vous êtes malentendant.

Contents

Using This Documentation

- **Overview** – Provides an overview of Oracle Solaris security features and the guidelines for using those features to harden and protect an installed system and its applications.
- **Audience** – System administrators, security administrators, application developers, and auditors who develop, deploy, or assess security on Oracle Solaris 11.4 systems.
- **Required knowledge** – Site security requirements.

Product Documentation Library

Documentation and resources for this product and related products are available at http://www.oracle.com/pls/topic/lookup?ctx=E37838-01.

Feedback

Provide feedback about this documentation at http://www.oracle.com/goto/docfeedback.

♦ ♦ ♦ CHAPTER 1

About Oracle Solaris Security

Oracle Solaris is a robust, premier enterprise operating system that offers proven security features. With a sophisticated network-wide security system that controls the way users access files, protect system databases, and use system resources, Oracle Solaris 11.4 addresses security requirements at every layer. While traditional operating systems can contain inherent security weaknesses, the flexibility of Oracle Solaris 11.4 enables it to satisfy a variety of security objectives from enterprise servers to desktop clients. Oracle Solaris is fully tested and supported on a variety of SPARC and x86-based systems from Oracle and on other hardware platforms from third-party vendors.

This chapter covers the following topics:

What's New in Security Features in Oracle Solaris 11.4

This section highlights information for existing customers about important new security features in this release.

Compliance Security Features

Compliance enables you to define a security policy for a system and run regular assessments to verify the continued compliance of the system.

- You can run assessments remotely over authenticated RAD connections. To run remote assessments, you must configure Secure Shell so that it does not prompt the user for authentication. See "Configuring Administrators to Run Remote Compliance Commands" in *Oracle Solaris 11.4 Compliance Guide*.
- You can store assessments immediately in a remote common store or move them to the common store later. See "Using a Common Store for Compliance Assessments" in *Oracle Solaris 11.4 Compliance Guide*.
- Tags on assessments enable you to locate and manage reports based on the tags. Oracle Solaris provides tags and you can create your own tags. See "Using Metadata to Manage Assessments" in *Oracle Solaris 11.4 Compliance Guide*.
- Assessments that you start from a script called a *roster* run asynchronously on multiple systems from a local system. See "How to Run Asynchronous Remote Assessments" in *Oracle Solaris 11.4 Compliance Guide* and the `compliance`(8) and `compliance-roster`(8) man pages.
- The `compliance explain` command lists the rules of the current or specified benchmark or profile. See the `compliance`(8) man page.

Cryptography Security Features

Oracle Solaris provides the Cryptographic Framework, a central store for cryptographic functions. It closely conforms to recent U.S. government cryptographic requirements. Cryptography is available from other sources that are bundled with Oracle Solaris, such as SASL and OpenSSL.

- The Cryptographic Framework is based on the latest PKCS #11 Cryptographic Token Interface Standard, PKCS #11 v2.40. Several new cryptographic algorithms and security standards are included in this upgrade. See Chapter 1, "About Cryptographic Providers in Oracle Solaris" in *Managing Encryption and Certificates in Oracle Solaris 11.4*.
- PKCS #11 token labels are configurable. You can simultaneously create a new token, set its PIN, and assign it a label with the `pktool inittoken` command. You can also use this command to change the labels of existing tokens. However, to change the PINs of existing tokens, you continue to use the `pktool setpin` command. See "How to Create a PKCS #11 Keystore" in *Managing Encryption and Certificates in Oracle Solaris 11.4*.
- Administrators can use the `ucrypto` provider to directly access user-level cryptographic primitives. This faster access can significantly improve the performance of applications.

For more information, see "Simple and Fast ucrypto Provider" in *Managing Encryption and Certificates in Oracle Solaris 11.4* and the `libucrypto*`(3LIB) man pages.

- To prevent POODLE (Padding Oracle On Downgraded Legacy Encryption) attacks, the `libcrypto.so` and `libssl.so` OpenSSL libraries do not support the SSLv2 and SSLv3 protocols.
- Weak ciphers in OpenSSL are either removed or deprecated. MD2 is removed. MD4, MD5, RC2, RC4, and DES are deprecated.
- Enhancements to `elfsign` functionality add more protection of data from attackers. Also, `elfsign` separates the signature cryptographic algorithm calculation from the data range algorithm which simplifies adding and maintaining new algorithms. See "Elfsign Enhancements" in *Managing Encryption and Certificates in Oracle Solaris 11.4*.

Kernel and System Security Features

Security extensions, verified boot, and file labeling are added and upgraded.

- Enforced verified boot on some SPARC platforms requires a firmware upgrade. For details, see "Firmware Upgrade for Verified Boot" in *Securing Systems and Attached Devices in Oracle Solaris 11.4*.
- Verified Boot on x86 systems conforms with the UEFI v2.3.1 Errata B specification. Oracle Solaris uses a first-stage boot loader called "shim" to validate the GRUB2 boot loader. GRUB2 Verified Boot then validates the elfsign signature on the initial Oracle Solaris kernel module "`unix`". After Oracle Solaris starts executing from GRUB2, Oracle Solaris validates all other kernel modules.
- The `-P` and `-H` options to the recursive `chmod -R` command limit file permission changes across symbolic links. See "How to Change File Permissions Across Symbolic Links" in *Securing Files and Verifying File Integrity in Oracle Solaris 11.4* and the `chmod`(1) man page.
- Security extensions have several additions.
  - You can enable or disable the inheritance of a security extension's configuration by using the `-i` option with the `sxadm exec` command. For more information, see "Preventing Intentional Misuse of System Resources" in *Securing Systems and Attached Devices in Oracle Solaris 11.4* and the `sxadm`(8) man page.
  - You can add security extensions per object. See "Specifying Per-Object Security Extensions" in *Securing Systems and Attached Devices in Oracle Solaris 11.4*.
  - The `adiheap` security extension enables the `malloc()` family of functions in the `libumem` and `libc` libraries to support ADI, so provides a reliable defense against linear buffer overflows and mitigates against use-after-free issues. `adiheap` can uncover subtle bugs that are triggered by an otherwise innocuous code change. See "Preventing Process

Heap Corruption Using adiheap" in *Securing Systems and Attached Devices in Oracle Solaris 11.4*.

- The `adistack` security extension is available on SPARC platforms that support Application Data Integrity (ADI). `adistack` reports stack buffer overflows detected by ADI. For more information, see "ADI-Based Stack Protection Using adistack" in *Securing Systems and Attached Devices in Oracle Solaris 11.4*.

File and File System Security Features

ZFS adds the following security features to its existing security.

- Labeling sensitive data and access to the data to prevent data loss enables you to comply with isolation requirements from corporate security, legislation, and standards bodies. In Oracle Solaris you can identify sensitive files and file systems by applying labels to them. For more information, see Chapter 3, "Labeling Files for Data Loss Protection" in *Securing Files and Verifying File Integrity in Oracle Solaris 11.4*
- Only users who have the clearance to handle those sensitive files can view or modify them. Even privileged users and roles can be prevented from accessing the contents of labeled files. For more information, see Chapter 6, "Labeling Processes for Data Loss Protection" in *Securing Users and Processes in Oracle Solaris 11.4*.

User and Process Rights Features

For process labeling, see "Kernel and System Security Features" on page 13.

Note - Rights protect new features, such as the analytics dashboard for viewing the Oracle Solaris StatsStore. For the new authorizations and rights profiles that protect the StatsStore, see "Statistics Store Authorizations and Administrative Profiles" in *Using Oracle Solaris 11.4 StatsStore and System Web Interface*.

Additional security attributes are available for users and systems.

- The Service Management Facility (SMF) is the repository for system-wide security settings which were previously in the following files:

```
/etc/security/policy.conf
/etc/default/login
/etc/default/passwd
```

```
/etc/default/su
```

The values are set in an SMF stencil when the `svc:/system/account-policy:default` service is enabled. The service is disabled by default, so as not to interrupt your legacy practices. When the service is enabled, the following modification to the Oracle Solaris 11.3 `policy.conf` file is replaced by a `setprop` command in Oracle Solaris 11.4:

```
example-11u3$ ## /etc/security/policy.conf file
PRIV_DEFAULT=basic,!file_link_any

example-11u4-sys$ pfbash svccfg -s account-policy \
 setprop config/etc_security_policyconf/disabled = boolean: false
example-11u4-sys$ pfbash svccfg -s account-policy \
 setprop rbac/default_privileges astring: = "basic,!file_link_any"
```

Similar modifications to the properties of the `account-policy` service can affect logins and the security settings of the `su` command. For more information, see `account-policy(8S)`.

- The `unlock_after` user attribute has been added to the `user_attr` database. Administrators can use this new attribute to specify the time after which a successful authentication automatically unlocks a locked account. The time may be specified as a number of minutes, hours, days, or weeks. For further information, see "What's New in Rights in Oracle Solaris 11.4" in *Securing Users and Processes in Oracle Solaris 11.4* and the `user_attr(5)` man page.
- The `annotation` user attribute has been added to the `user_attr` database. Administrators can use this new attribute to require users to annotate their logins. For further information, see "What's New in Rights in Oracle Solaris 11.4" in *Securing Users and Processes in Oracle Solaris 11.4* and the `user_attr(5)` man page.
- In Oracle Solaris you can limit labeled file access to processes and users who have the clearance to handle those labeled files. Even privileged users and roles can be prevented from accessing the contents of labeled files. For more information, see Chapter 6, "Labeling Processes for Data Loss Protection" in *Securing Users and Processes in Oracle Solaris 11.4*.

Passwords and Authentication Security Features

Password defaults are strengthened, Simple Authentication and Security Layer (SASL) is based on Cyrus SASL, and OpenSSH is the basis for Secure Shell. For information about features that interact with authentication, see "Cryptography Security Features" on page 12 and "Auditing Security Features" on page 17.

- Password constraints are stronger. Passwords must have at least `PASSLENGTH` characters as defined in the `/etc/default/passwd` file. The default length is eight characters. Three

additional variables can constrain password duration: `MAXDAYS`, `MINDAYS`, and `WARNDAYS`. For more information, see "Password Parameters" in *Securing Systems and Attached Devices in Oracle Solaris 11.4* and the `passwd`(1) man page.

- The Simple Authentication and Security Layer (SASL) in Oracle Solaris is based on the open source Cyrus SASL with a few changes. For details of the implementation, see Chapter 2, "Using Simple Authentication and Security Layer" in *Managing Authentication in Oracle Solaris 11.4* and the SASL man pages, such as `saslauthd`(8).
- The sole Secure Shell implementation in Oracle Solaris is OpenSSH. For the release number, type `pkg info ssh` in a terminal window. OpenSSH replaces SunSSH. See "OpenSSH Implementation of Secure Shell" in *Managing Secure Shell Access in Oracle Solaris 11.4*.

  For keywords that enable OpenSSH and legacy Oracle Solaris 11 SunSSH systems to interoperate, see "Ignore Keywords in Secure Shell" in *Managing Secure Shell Access in Oracle Solaris 11.4*.
- Secure Shell can store and retrieve Secure Shell public keys from an LDAP directory server. See "Secure Shell and Remote Public Keys" in *Managing Secure Shell Access in Oracle Solaris 11.4* and the `ssh-ldap-pubkey`(8) man page.

Networking Security Features

Security is added to ports, IKEv2 optimizes the handling of large encrypted messages, and the Packet Filter firewall has additional features.

- Oracle Solaris Packet Filter (PF) adds the `ftp-proxy` service and firewall interface groups to PF. For more information, see Chapter 4, "Oracle Solaris Firewall" in *Securing the Network in Oracle Solaris 11.4* and the `ftp-proxy`(8) man page.
- IKEv2 can prevent most IP layer fragmentation of its messages by replacing large encrypted messages with a series of smaller encrypted messages. See "What's New in Network Security in Oracle Solaris 11.4" in *Securing the Network in Oracle Solaris 11.4* and "IKEv2 Service" in *Securing the Network in Oracle Solaris 11.4*.
- To enhance the security of ports, see Chapter 3, "Protecting Networks With IEEE 802.1X Certificates" in *Securing the Network in Oracle Solaris 11.4*.

Auditing Security Features

Auditing adds many new features, including per-object auditing, annotated login records, and analytics. Interfaces such as the `admhist` command and the Oracle Solaris StatsStore can present audit records and information in an easy-to-understand format.

- The `sstore` meta-class replaces the `lo` class as the default set of audit flags. In addition `lo`, the `sstore` meta-class includes the `ss`, `as`, `xa`, and `pe` audit classes. See "Viewing Audit Data in the Statistics Store" in *Managing Auditing in Oracle Solaris 11.4*.
- Audit information is available to the Oracle Solaris StatsStore and the Oracle Solaris Analytics BUI. For more information about how audit information is captured in the StatsStore and can be viewed in the Analytics BUI, see "Analytics' Auditing Sheet" in *Managing Auditing in Oracle Solaris 11.4* and *Using Oracle Solaris 11.4 StatsStore and System Web Interface*.
- The audit service supports per-object auditing. Administrators with the appropriate privileges can set ACL entries to audit access attempts for specific files or specific directories. For more information, see "New Feature – Per-Object Logging of Audit Events" in *Managing Auditing in Oracle Solaris 11.4*.
- Oracle Solaris enables administrators to require users to annotate their sessions at login. The annotation is written to the audit record. See "New Feature – Annotating Reason for Access in the Audit Record" in *Managing Auditing in Oracle Solaris 11.4* and several man pages, including `profiles`(1), `auditrecord`(8), and `pam_unix_cred`(7).
- The `admhist` command provides a summary of privileged execution audit records in a helpful, easy-to-understand format. This command extracts only audit events that successfully used privilege from the audit trail, so the output more accurately displays events that were likely to have modified the system. For more information, see "New Feature – Viewing a Summary of Audit Records" in *Managing Auditing in Oracle Solaris 11.4* and the `admhist`(8) man page.
- The `auditstat` command replaces the `-getstat` and `-setstat` options to the `auditconfig` command. See the `auditstat`(8) man page.
- The `pe` audit class enables the audit service to automatically track the use of privileges that allowed a process to change the system's configuration. For more information, see "New Feature – Per-Privilege Logging of Audit Events" in *Managing Auditing in Oracle Solaris 11.4*.
- Auditing tracks whether Verified Boot is enabled and working on your system. See "New Feature – Auditing Verified Boot" in *Managing Auditing in Oracle Solaris 11.4*.
- You must refresh the audit service after changing an audit configuration file. See "New Feature – Refreshing the auditset SMF Service After Changing Event-Class Mappings" in *Managing Auditing in Oracle Solaris 11.4*.
- You can filter audit records by functional areas such as `cpu` and `net` with the `auditreduce -t` command. The `audit_tags` database stores these functional areas as audit tags. For more

information, see "New Feature – Filtering Audit Records by Functional Area" in *Managing Auditing in Oracle Solaris 11.4* and the `audit_tags`(5) and `auditreduce`(8) man pages.

- Administrators can now view configured audit classes by using the `-lsclass` option to the `auditconfig` command. For more information, see the `auditconfig`(8) man page.
- Administrators can display audit event information per audit class by using the `auditconfig -lsevent` *audit_flags* command. See "New Feature – Listing Audit Events by Audit Class" in *Managing Auditing in Oracle Solaris 11.4* and the `auditconfig`(8) and `audit_flags`(7) man pages.
- All audit plugins can now specify which audit classes from the classes that are configured system-wide are to be written to their plugin. In addition, the Audit Remote Server (ARS) now supports specifying a set of audit flags on a per-connection group basis. For more information, see "New Feature – Flexible Per-Plugin Configuration of Audit Classes" in *Managing Auditing in Oracle Solaris 11.4* and the `auditconfig`(8) man page.

Oracle Solaris 11.4 Security After Installation

Oracle Solaris is installed "secure by default" (SBD). This security posture protects the system from intrusion and monitors login attempts, among other security features.

System Access Is Limited and Monitored

Initial user and `root` role accounts – The initial user account can log in from the console. This account is assigned the `root` role. The password for the initial user and the `root` accounts is identical at installation.

- After logging in, the initial user can assume the `root` role to further configure the system. Upon assuming the role, the user is prompted to change the `root` password. Note that no role can log in directly, including the `root` role.
- The initial user is assigned defaults from the `/etc/security/policy.conf` file. The defaults include the Basic Solaris User rights profile and the Console User rights profile. These rights profiles enable users to read and write to a CD or DVD, run any command on the system without privilege, and stop and restart their system when sitting at the console.
- The initial user account is also assigned the System Administrator rights profile. Therefore, without assuming the `root` role, the initial user has some administrative rights, such as the right to install software and manage the naming service.

Password requirements – User passwords must be at least eight characters long, and have at least two alphabetic characters and one non-alphabetic character. Passwords are hashed by using the `SHA256` algorithm.

Limited network access – After installation, the system is protected from intrusion over the network. Remote login by the initial user is allowed over an authenticated, encrypted connection with the Secure Shell protocol. This is the only network protocol that accepts incoming packets. The Secure Shell key is wrapped by the `AES128` algorithm. With encryption and authentication in place, the user can reach the remote system without interception, modification, or spoofing.

Recorded login attempts – The audit service is enabled for all `login/logout` events (login, logout, switching user, starting and stopping a Secure Shell session, and screen locking) and for all non-attributable (failed) logins. Because the `root` role cannot log in, the name of the user who is acting as `root` is recorded in the audit trail. The initial user can review the audit logs by a right granted through the System Administrator rights profile.

Kernel and File Protections Are in Place

After the initial user is logged in, the kernel, file systems, and system files are protected by file permissions, privileges, and user rights. User rights are also known as *role-based access control* (RBAC).

Kernel protections – Many daemons and administrative commands are assigned just the privileges that enable them to succeed. Many daemons are run from special administrative accounts that do not have `root` (`UID=0`) privileges, so they cannot be hijacked to perform other tasks. These special administrative accounts cannot log in. Security extensions protect kernel processes. Devices are protected by privileges.

File systems – By default, all file systems are ZFS file systems. The user's `umask` is `022`, so when a user creates a new file or directory, only the user is allowed to modify it. Members of the user's group are allowed to read and search the directory, and read the file. Logins that are outside the user's group can list the directory and read the file. The default directory permissions are `drwxr-xr-x` (`755`). The file permissions are `-rw-r--r--` (`644`).

System files – System configuration files are protected by file permissions. Only the `root` role or a user who is assigned the right to edit a specific system file can modify a system file. The audit service calls system files *public objects*.

Oracle Hardware Management Package

The Oracle Hardware Management Package provides a set of utilities for configuring, managing, and monitoring Oracle servers. This value-add set of tools for Oracle hardware is always available. It can automatically deliver certain hardware-related information to ILOM to complete the view that it has of system hardware. For information about the utilities and security, see Systems Management and Diagnostics Documentation Library (`https://docs.oracle.com/cd/F24624_01/index.html#hwmgmt`).

Oracle Solaris Configurable Security

In addition to the solid foundation that Oracle Solaris security defaults provide, the security posture of a Oracle Solaris system is highly configurable to satisfy a range of security requirements.

The following sections provide a short introduction to the security features of Oracle Solaris. The descriptions include references to more detailed explanations and to procedures that show how to configure these features.

Protecting Data

Oracle Solaris protects data from booting through installation, use, and archiving. This section covers files, file systems, and cryptographic protections. Additional data protection features are described in “Protecting and Isolating Applications” on page 25 and “Labeled Security” on page 31.

File Permissions and Access Control Entries

The first line of defense for protecting objects in a file system are the default UNIX permissions that are assigned to every file system object. UNIX permissions support assigning unique access rights to the owner of the object, to a group assigned to the object, as well as to anyone else. Additionally, the default file system, ZFS, supports access control lists (ACLs), which more finely control access to individual or groups of file system objects.

For more information, see the following:

- For a description of security-relevant ZFS file attributes, see "Using File Attributes to Add Security to ZFS Files" in *Securing Files and Verifying File Integrity in Oracle Solaris 11.4* and the man pages.
- For an overview of file permissions, see "Using UNIX Permissions to Protect Files" in *Securing Files and Verifying File Integrity in Oracle Solaris 11.4*.
- For an overview and examples of protecting ZFS files, see "Setting ACLs on ZFS Files" in *Securing Files and Verifying File Integrity in Oracle Solaris 11.4* and the ZFS and `chmod(1)` man pages.

Cryptographic Services

The Cryptographic Framework feature of Oracle Solaris and the Key Management Framework (KMF) feature of Oracle Solaris provide central repositories for cryptographic services and key management. Hardware, software, and end users have seamless access to optimized algorithms. KMF provides a unified interface for otherwise different storage mechanisms, administrative utilities, and programming interfaces for various public key infrastructures (PKIs).

The Cryptographic Framework provides a common store of algorithms and PKCS #11 libraries to handle cryptographic requirements. The PKCS #11 libraries are implemented according to the RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki) standard. Cryptographic services, such as encryption and decryption for files, are available to regular users. The Cryptographic Framework is evaluated to run in FIPS 140-2 mode. See "How to Create a Boot Environment With FIPS 140-2 Enabled" in *Managing Encryption and Certificates in Oracle Solaris 11.4*.

KMF provides tools and programming interfaces for centrally managing public key objects, such as X.509 certificates and public/private key pairs. The formats for storing these objects can vary. KMF also provides a tool for managing policies that define the use of X.509 certificates by applications. KMF supports third-party plugins.

For more information, see the following:

- Selected man pages include `cryptoadm(8)`, `digest(1)`, `encrypt(1)`, `mac(1)`, `pktool(1)`, and `kmfcfg(1)`.
- *Managing Encryption and Certificates in Oracle Solaris 11.4*

Identity Service

The `svc:/system/identity` SMF service configures the basic network identity (names) of the Oracle Solaris instance. The identity includes its node name, RPC domain name, and the default set of X.509 certificates to use for the Remote Administration Daemon (RAD) and WebUI.

The service is composed of the following instances:

- `svc:/system/identity:node` – Specifies the host name or node name
- `svc:/system/identity:domain` – Specifies the RPC domain name
- `svc:/system/identity:cert` – Deploys or creates the X.509 certificates for WebUI and RAD connections that use the TLS transport
- `svc:/system/identity:cert-expiry` – Certificate expiry check
- `svc:/system/identity:version` – Updates the value that is used in `uname -v` output

The `identity:cert-expiry` instance periodically checks the expiry status of a `identity:cert`-created certificate. When it finds an expired certificate, the `identity:cert-expiry` instance has the `identity:cert` instance re-issue the certificate, if possible.

In addition, the `identity:cert-expiry` instance monitors the certificates in `/etc/certs/CA` that are distributed by the `ca-certificate` package. If any of those certificates are expired, the `identity:cert-expiry` instance enters degraded mode. When in degraded mode, `identity:cert-expiry` appears in `svcs -x` output and an FMA alert is posted. This situation generally occurs if you are not updating the system on a regular basis.

Oracle Solaris ZFS File System

ZFS is the default file system for Oracle Solaris. ZFS is robust, scalable, and easy to administer. Because file system creation in ZFS is lightweight, you can easily establish quotas and reserved space. UNIX permissions and ACLs protect files, and you can encrypt the entire dataset at creation. Oracle Solaris rights management supports the delegated administration of ZFS datasets, that is, users who are assigned a limited set of privileges can administer ZFS datasets.

For more information, see the following:

- *Managing ZFS File Systems in Oracle Solaris 11.4*
- Chapter 3, “Labeling Files for Data Loss Protection” in *Securing Files and Verifying File Integrity in Oracle Solaris 11.4*
- “How to Remotely Administer ZFS With Secure Shell” in *Managing Secure Shell Access in Oracle Solaris 11.4*

- "User Rights Management" in *Securing Users and Processes in Oracle Solaris 11.4*
- Selected man pages include `zfs`(8) and `zfs`(4FS).

Protecting Users and Assigning Additional Rights

Users are assigned a basic set of privileges, rights profiles, and authorizations from the `/etc/security/policy.conf` file, similar to the initial user as described in "System Access Is Limited and Monitored" on page 18. These rights are configurable. You can deny basic rights and increase the rights for a user.

Oracle Solaris protects users with flexible complexity requirements for passwords, authentication that is configurable for different site requirements, and user rights management. User rights management limits and distributes administrative rights by assigning privileges, authorizations, and rights profiles to trusted users. Additionally, special shared accounts called *roles* assign the user just those administrative rights when the user assumes the role. The ARMOR package provides predefined roles. For more information, see "Using ARMOR Roles" in *Securing Users and Processes in Oracle Solaris 11.4*.

Passwords and Password Policy

Your password change policy should follow industry standards. System administration logins, such as `root`, must be carefully controlled. Administration should be through roles, users with rights profiles, or `sudo`. These administrative methods use least privilege and write administrative events to the audit trail.

Note - The passwords for users who can assume roles must not be subject to any password aging constraints.

For more information, see the following:

- "Controlling Logins" in *Securing Systems and Attached Devices in Oracle Solaris 11.4*
- "Troubleshooting Passwords" in *Securing Users and Processes in Oracle Solaris 11.4*
- "Securing Logins and Passwords" in *Securing Systems and Attached Devices in Oracle Solaris 11.4*
- Selected man pages include `account-policy`(8S), `passwd`(1), and `crypt.conf`(5).

Pluggable Authentication Modules

The Pluggable Authentication Module (PAM) framework enables administrators to coordinate and configure user authentication requirements for accounts, credentials, sessions, and passwords without modifying the services that require authentication.

The PAM framework enables organizations to customize the user authentication experience as well as account, session, and password management functionality. System entry services such as `login` and `ssh` use the PAM framework to secure all entry points for the freshly installed system. PAM enables the replacement or modification of authentication modules in the field to secure the system against any newly found weaknesses without requiring changes to any system services that use the PAM framework.

Oracle Solaris delivers a broad set of PAM modules and configurations to meet most site policies. For more information, see the following:

- Chapter 1, "Using Pluggable Authentication Modules" in *Managing Authentication in Oracle Solaris 11.4*
- "Writing Applications That Use PAM Services" in *Developer's Guide to Oracle Solaris 11.4 Security*
- `pam.conf`(5) man page

User Rights Management

User rights in Oracle Solaris are governed by the security principle of least privilege. Organizations can selectively grant administrative rights to users or roles according to the unique needs and requirements of the organization. They can also deny rights to users when required. Rights are implemented as privileges on processes and authorizations on users or SMF methods. Rights profiles provide a convenient way to collect privileges and authorizations into a bundle of related rights.

For more information, see the following:

- *Securing Users and Processes in Oracle Solaris 11.4*
- Selected man pages include `auths`(1), `privileges`(7). `profiles`(1), `rbac`(7), `roleadd`(8), `roles`(1), and `user_attr`(5).

Protecting and Isolating Applications

Applications can be entry points for malware and malicious users. In Oracle Solaris, these threats are mitigated by the use of privileges and the containment of applications within zones. Applications can run with just the privileges that the application needs, so a malicious user does not have root privileges to access the rest of the system. Zones can limit the extent of an attack. Attacks on applications in a non-global zone can affect processes in that zone only, not the zone's host system. For more information, see “Oracle Solaris Zones” on page 26.

Security extensions, such as address space layout randomization (ASLR), `nxheap`, `nxstack`, `adiheap`, and `adistack` make it difficult for intruders to benefit from a stack overflow or to compromise an executable or the heap. For more information, see “Kernel and System Security Features” on page 13.

The Service Management Facility (SMF) also protects applications by enabling administrators to restrict starting, stopping, and using an application. For more information, see “Service Management Facility” on page 27.

Privileges in Oracle Solaris

Privileges are fine-grained, discrete rights on processes that are enforced in the kernel. Oracle Solaris defines over 80 privileges, ranging from basic privileges like `file_read` to more specialized privileges like `proc_clock_highres`. Privileges can be granted to a process, a user, or a role. Many Oracle Solaris commands and daemons run with just the privileges that are required to perform their task. Privilege-aware programs can prevent intruders from gaining more privileges than the program itself uses.

The use of privileges is also called *process rights management*. Privileges enable organizations to specify, hence limit, which privileges are granted to services and processes that run on their systems.

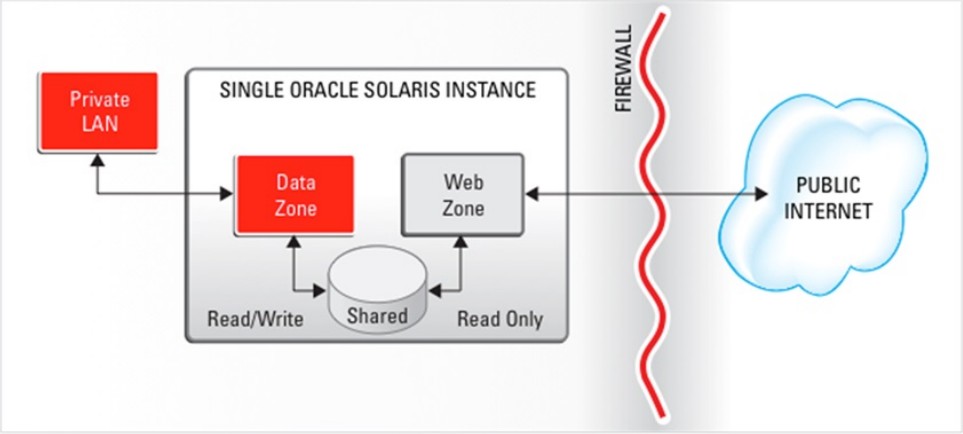
For more information, see the following:

- “Process Rights Management” in *Securing Users and Processes in Oracle Solaris 11.4*
- Chapter 2, “Developing Privileged Applications” in *Developer’s Guide to Oracle Solaris 11.4 Security*
- Selected man pages include `ppriv`(1) and `privileges`(7).

Oracle Solaris Zones

The Oracle Solaris Zones software partitioning technology enables you to maintain the one-application-per-server deployment model while simultaneously sharing hardware resources. Figure 1, “Zones Sharing Hardware,” on page 26 illustrates two zones sharing the same hardware. The Data Zone connection to the private LAN is read-write, while the Web Zone connection to the Internet is read-only.

FIGURE 1 Zones Sharing Hardware



Zones are virtualized operating environments that enable multiple applications to run in isolation from each other on the same physical hardware. This isolation prevents processes that run within a zone from monitoring or affecting processes that run in other zones, viewing each other's data, or manipulating the underlying hardware. Zones also provide an abstraction layer that separates applications from physical attributes of the system on which they are deployed, such as physical device paths and network interface names.

For added protection, physical global zones, called Immutable Global Zones, and virtual global zones, called Oracle Solaris Kernel Zones, can be read-only. Immutable global zones are slightly more powerful than Kernel Zones, but neither can permanently change the hardware or configuration of the system. Read-only zones boot faster and are more secure than zones that allow writes.

For maintenance, immutable global zones define a special set of processes, called the Trusted Path Domain (TPD) that can be configured to limit administrative logins. For more information, see Chapter 10, "Configuring and Administering Immutable Zones" in *Creating and Using Oracle Solaris Zones* and the `tpd`(7) man page. For information about zone configuration resources, see *Introduction to Oracle Solaris Zones*. See also the `mwac`(7) and `tpd`(7) man pages.

Oracle Solaris Kernel Zones are useful for deploying a compliant system. For example, you can configure a compliant system, create a Unified Archive, then deploy the image as a kernel zone. For more information, see the `solaris-kz`(7) man page, *Creating and Using Oracle Solaris Kernel Zones*, "Oracle Solaris Zones Overview" in *Introduction to Oracle Solaris 11.4 Virtual Environments*, and *Using Unified Archives for System Recovery and Cloning in Oracle Solaris 11.4*.

For more information, see the following:

- "Configuring Immutable Zones" in *Creating and Using Oracle Solaris Zones*
- *Introduction to Oracle Solaris Zones*
- Selected man pages include `brands`(7), `zoneadm`(8), and `zonecfg`(8).

Security Extensions

Oracle Solaris security extensions are flags at the kernel level that protect applications from compromise. For more information, see the following:

- For administrator information, see "Preventing Intentional Misuse of System Resources" in *Securing Systems and Attached Devices in Oracle Solaris 11.4*
- For developer information, follow the links in "Writing Applications That Run Securely" on page 33
- Selected man pages include `ld`(1) and `sxadm`(8).

Service Management Facility

Services are persistently running applications. A service can represent a running application, the software state of a device, or a set of other services. The Service Management Facility (SMF) feature of the Oracle Solaris is used to add, remove, configure, and manage services. SMF uses rights management to control access to service management functions on the system. In particular, authorizations determine who can manage a service and what functions that person can perform.

SMF enables organizations to control access to services, as well as to control how those services are started, stopped, and refreshed.

For more information, see the following:

- *Managing System Services in Oracle Solaris 11.4*
- "How to Assign Specific Privileges to the Apache HTTP Server" in *Securing Users and Processes in Oracle Solaris 11.4*
- Selected man pages include `svcadm`(8), `svcs`(1), and `smf`(7).

Java Cryptography Extension

Java provides the Java Cryptography Extension (JCE) for developers of Java applications. JCE provides a framework for implementing encryption, key generation and key agreement, and message authentication code (MAC) algorithms. For more information, see Java SE Security (`https://www.oracle.com/java/technologies/javase/javase-tech-security.html`).

Securing Network Communications

Network communications can be protected by features such as firewalls, TCP wrappers on networked applications, and encrypted and authenticated remote connections.

Packet Filtering

Packet filtering provides basic protection against network-based attacks. Oracle Solaris includes the OpenBSD Packet Filter firewall and TCP wrappers.

OpenBSD Packet Filter Firewall

The OpenBSD Packet Filter (PF) replaces the IP Filter feature in Oracle Solaris. PF is a network firewall that captures inbound packets and evaluates them for entry to and exit from the system. PF provides stateful packet inspection. It can match packets by IP address and port number as well as by the receiving network interface.

PF is based on OpenBSD Packet Filter version 5.6, which is enhanced to work with Oracle Solaris components, such as zones with exclusive IP instances.

For more information, see the following:

- For an overview, see Chapter 4, "Oracle Solaris Firewall" in *Securing the Network in Oracle Solaris 11.4*.
- For examples of using PF, see Chapter 5, "Configuring the Firewall in Oracle Solaris" in *Securing the Network in Oracle Solaris 11.4* and the man pages.
- Selected man pages include `pf.conf`(7), `pfctl`(8), and `pf.os`(7).

TCP Wrappers

TCP wrappers provide access control for internet services. When various internet (`inetd`) services are enabled, the `tcpd` daemon checks the address of a host requesting a particular network service against an ACL. Requests are granted or denied accordingly. TCP wrappers also log host requests for network services in `syslog`, which is a useful monitoring function.

The `sendmail` feature of Oracle Solaris is configured to use TCP wrappers. Network services that have a one-to-one mapping to executable files, such as `proftpd` and `rpcbind`, are candidates for TCP wrappers.

TCP wrappers support a rich configuration policy language that enables organizations to specify security policy not only globally but on a per-service basis. Further access to services can be permitted or restricted based upon host name, IPv4 or IPv6 address, netgroup name, network, and even DNS domain.

For information about TCP wrappers, see the following:

- "Using TCP Wrappers in Oracle Solaris" in *Administering TCP/IP Networks, IPMP, and IP Tunnels in Oracle Solaris 11.4*
- For information and examples of the syntax of the access control language for TCP wrappers, see the `hosts_access`(4) man page.
- Selected man pages include `tcpd`(8) and `inetd`(8).

Remote Access

Remote access attacks can damage a system and a network. Oracle Solaris provides defense in depth for network transmissions. Defense features include encryption and authentication checks for data transmission, login authentication, and the disabling of unnecessary remote services.

IPsec and IKE

IP security (IPsec) protects network transmissions by authenticating the IP packets, by encrypting them, or by doing both. Because IPsec is implemented well below the application layer, Internet applications can take advantage of IPsec without requiring modifications to their code.

IPsec and its automatic key exchange protocol, IKE, use algorithms from the Cryptographic Framework. Additionally, the Cryptographic Framework provides a central keystore. When IKE is configured to use the metaslot, organizations have the option of storing the keys on disk or in a software keystore called *softtoken*. Oracle Solaris supports both the IKE Version 2 (IKEv2) protocol and the IKEv1 protocol.

IPsec and IKE require configuration, so are installed but not enabled by default. When properly administered, IPsec is an effective tool in securing network traffic.

For more information, see the following:

- Chapter 6, "About IP Security Architecture" in *Securing the Network in Oracle Solaris 11.4*
- Chapter 7, "Configuring IPsec" in *Securing the Network in Oracle Solaris 11.4*
- "IPsec and FIPS 140-2" in *Securing the Network in Oracle Solaris 11.4*
- Chapter 8, "About Internet Key Exchange" in *Securing the Network in Oracle Solaris 11.4*
- Chapter 9, "Configuring IKEv2" in *Securing the Network in Oracle Solaris 11.4*
- Selected man pages include `ipsecconf`(8) and `in.iked`(8).

OpenSSH Secure Shell

By default, OpenSSH (Secure Shell) is the only active remote access mechanism on a newly installed system. All other network services are either disabled or in listen-only mode.

Secure Shell creates an encrypted communications channel between systems. Secure Shell can also be used as an on-demand virtual private network (VPN) that can forward X Window system traffic or can connect individual port numbers between a local system and remote systems over an authenticated and encrypted network link.

Thus, Secure Shell prevents a would-be intruder from being able to read an intercepted communication and prevents an adversary from spoofing the system.

The `openssh` implementation of Secure Shell can run in FIPS 140-2 mode. OpenSSH sets FIPS 140-2 mode dynamically.

For more information, see the following:

- Chapter 1, "Using Secure Shell" in *Managing Secure Shell Access in Oracle Solaris 11.4*
- "Secure Shell and FIPS 140-2" in *Managing Secure Shell Access in Oracle Solaris 11.4*
- Selected man pages are available on the command line and include `ssh`(1), `sshd`(8), `sshd_config`(5), and `ssh_config`(5).

Kerberos Service

The Kerberos feature of the Oracle Solaris enables single sign-on and secure transactions, even over heterogeneous networks where systems run different operating systems and run the Kerberos service. You can install Kerberos clients by using AI, so that the client is a Kerberized system at first boot.

Kerberos is based on the Kerberos V5 network authentication protocol from MIT. The Kerberos service offers strong user authentication, as well as integrity and privacy. Using the Kerberos service, you can log in once and access other systems, execute commands, exchange data, and transfer files securely. Additionally, the service enables administrators to restrict access to services and systems.

For more information, see the following:

- "How to Configure Kerberos Clients Using AI" in *Automatically Installing Oracle Solaris 11.4 Systems*
- *Managing Kerberos in Oracle Solaris 11.4*
- "Kerberos and FIPS 140-2 Mode;" in *Managing Kerberos in Oracle Solaris 11.4*
- Selected man pages include `kadmin`(8), `kdcmgr`(8), `kerberos`(5), `kinit`(1), and `krb5.conf`(5).

Labeled Security

Oracle Solaris now supports file and process labeling using the same labeling APIs and CLIs as Trusted Extensions. The label syntax described in the *Compartmented Mode Workstation Labeling: Encodings Format* applies to both environments. Similarly, the new `labelcfg` command can configure labels in both environments.

The labeling scenario for the Oracle Solaris environment is distinct from the Trusted Extensions environment.

- Labeling for privacy – In this scenario, labels are applied to files, directories and System V IPC objects that contain sensitive data. Access to labeled data is restricted to the few users

who are assigned the clearance to access it. Hosts and zones are not labeled. Users who have access to labeled data can share the data at their discretion. Users also can choose to lower the clearance of processes that they execute by running them in sandboxes. This is the default behavior for Oracle Solaris.

- Mandatory Access Control – In this scenario, zones and hosts are assigned a label and all the data that can be modified within a zone is automatically labeled with the zone's label. Users are assigned a clearance which determines which zones they can see or log in to. When executing in a labeled zone, users are only permitted to share data with processes and network endpoints at the same label. Administrative users can be given permission to share read-only data with higher level zones or hosts. This scenario is handled by Trusted Extensions.

Labeling for Privacy

In Oracle Solaris, you can protect data from unwarranted access by applying labels to datasets, user processes, and SMF processes at administrative discretion. Most users and processes are not visibly labeled. File systems can contain multiple labels below the declared upper bound of the file system.

In this labeled environment, trusted users can also be assigned or create sandboxes, that is, protected areas for work at a specified label and for processes at that label.

For more information, see the following:

- Chapter 3, "Labeling Files for Data Loss Protection" in *Securing Files and Verifying File Integrity in Oracle Solaris 11.4*
- Chapter 6, "Labeling Processes for Data Loss Protection" in *Securing Users and Processes in Oracle Solaris 11.4*
- "Configuring Sandboxes for Project Isolation" in *Securing Users and Processes in Oracle Solaris 11.4*
- Selected man pages include `sandboxing`(7), `sandboxadm`(8), and `sandbox`(1).

Mandatory Access Control

The Trusted Extensions feature of Oracle Solaris is an optionally enabled layer of secure labeling technology that enables data security policies to be separated from data ownership on disk and over the wire. Trusted Extensions supports both traditional discretionary access control (DAC) policies based on ownership, as well as label-based mandatory access control (MAC)

policies. When the Trusted Extensions layer is enabled, all data flows are restricted based on a comparison of the labels associated with the processes (subjects) requesting access and the objects containing the data.

Trusted Extensions features include:

- All file systems are labeled – By default, Trusted Extensions file systems are assigned a single label in a zone at that same label. You can create a multilevel ZFS dataset, mount it on a Trusted Extensions system, and with appropriate permissions, upgrade and downgrade the files in that dataset. For more information, see "Multilevel Datasets for Relabeling Files" in *Trusted Extensions Configuration and Administration*.
- All network communications are labeled – Trusted Extensions labels network communications. Data flows are restricted based on a comparison of the labels associated with the originating network endpoint and the receiving network endpoint. Gateways and in-between hops must also be labeled to allow the passage of information at the label of the communication. NFS and multilevel ZFS datasets provide additional features on a network.

The Trusted Extensions implementation is unique in its ability to provide high assurance, while maximizing compatibility and minimizing overhead.

For more information, see the following:

- *Trusted Extensions Configuration and Administration*.
- Selected man pages include `trusted_extensions`(7), `labeladm`(8), and `labeld`(8).

Writing Applications That Run Securely

Developers should write and compile applications to run securely on Oracle Solaris. For general information, see the following:

- *Developer's Guide to Oracle Solaris 11.4 Security*
- *Oracle Solaris 11.4 Linkers and Libraries Guide*

For specific suggestions, see the following:

- `ld`(1) man page – Security extension flags as arguments to the `-z sx=` option
- Appendix A, "Secure Coding Guidelines for Developers," in *Developer's Guide to Oracle Solaris 11.4 Security*
- Appendix E, "Security Considerations When Using C Functions," in *Developer's Guide to Oracle Solaris 11.4 Security*
- "Runtime Security" in *Oracle Solaris 11.4 Linkers and Libraries Guide*

Site Security Policy and Practice

For a secure system or network of systems, your site must have a security policy in place with security practices that support the policy. If you are developing programs or installing third-party programs, you must develop and install those programs securely. For more information, see Appendix A, “Site Security Policy and Enforcement”.

♦ ♦ ♦ CHAPTER 2

Configuring Oracle Solaris Security

This chapter describes the actions to take to configure security on your system. The chapter covers installing packages, configuring the system itself, then configuring various subsystems and additional applications that you might need, such as IPsec.

Installing the Oracle Solaris OS

The Oracle Solaris OS is installed by selecting a set of packages called a *group* from a package repository. Different groups supply packages for different uses, such as multipurpose servers, minimally installed or *hardened* systems, and desktop systems. Packages are signed and their secure transfer can be verified.

When you install the Oracle Solaris OS, choose the media that installs the appropriate *group* package, as follows:

- **Oracle Solaris Large Server –** Both the default manifest in an Automated Installer (AI) installation and the text installer install the `group/system/solaris-large-server` group, which provides an Oracle Solaris large server environment.
- **Oracle Solaris Small Server –** The Automated Installer (AI) installation and the text installer optionally install the `group/system/solaris-small-server` group, which provides a useful command-line environment to which you can add packages.

- **Oracle Solaris Minimal Server –** The Automated Installer (AI) installation and the text installer optionally install the `group/system/solaris-minimal-server` group, which provides a minimal command-line environment to which you can add just the packages that you want. This group can provide the base for a hardened system.
- **Oracle Solaris Desktop –** The AI can install the `group/system/solaris-desktop` group. Alternatively, after using the text installer, add the `solaris-desktop` package to provide an Oracle Solaris 11.4 desktop environment.

To automate installation with the Automated Installer (AI), see *Automatically Installing Oracle Solaris 11.4 Systems*. You can secure AI installations with certificates and keys for the install server, for specified client systems, for all clients of a specified install service, and for any other AI clients.

To guide your media choice, see the following installation and package content guides:

- *Automatically Installing Oracle Solaris 11.4 Systems*
- *Manually Installing an Oracle Solaris 11.4 System*
- *Creating a Custom Oracle Solaris 11.4 Image*
- *Updating Systems and Adding Software in Oracle Solaris 11.4*

Initially Securing the System

The following tasks are best performed in order. At this point, the Oracle Solaris OS is installed and only the initial user who can assume the `root` role has access to the system.

1. Check that packages and their signatures are valid – "Verifying Packages and Fixing Verification Errors" in *Updating Systems and Adding Software in Oracle Solaris 11.4*
2. Ensure that security extensions protect executables – "Preventing Intentional Misuse of System Resources" in *Securing Systems and Attached Devices in Oracle Solaris 11.4*
3. Safeguard the hardware settings on the system – "Controlling Access to System Hardware" in *Securing Systems and Attached Devices in Oracle Solaris 11.4*
4. Disable unneeded services – "Stopping a Service" in *Managing System Services in Oracle Solaris 11.4*
5. Prevent the workstation owner from powering down the system – "How to Remove Power Management Capability From Users" in *Securing Users and Processes in Oracle Solaris 11.4*
6. Notify users before and after authentication that the system is monitored – "How to Place a Security Message in Banner Files" in *Securing Systems and Attached Devices in Oracle Solaris 11.4*

Securing Users

At this point, only the initial user who can assume the `root` role can access the system. The following tasks are best performed in order before regular users can log in.

1. (Optional) Configure restrictive file permissions for regular users – "How to Set a More Restrictive umask Value for Regular Users" in *Securing Users and Processes in Oracle Solaris 11.4*
2. Set account locking for regular users – "How to Set Account Locking for Regular Users" in *Securing Users and Processes in Oracle Solaris 11.4*
3. Monitor and record all administrative events – "Viewing Audit Data in the Statistics Store" in *Managing Auditing in Oracle Solaris 11.4*
4. Distribute discrete administrative tasks to roles – "Assigning Rights to Users" in *Securing Users and Processes in Oracle Solaris 11.4*

   For ease of role creation, use predefined ARMOR roles – "Creating a Role" in *Securing Users and Processes in Oracle Solaris 11.4*
5. (Optional) Limit a user's basic privileges – "Removing Privileges From Users" in *Securing Users and Processes in Oracle Solaris 11.4*

Protecting the Network

At this point, you might have created users who can assume roles, and have created the roles.

In your assigned role as network security administrator, perform tasks from the following list that site security requires. These network tasks strengthen the IP, ARP, and TCP protocols.

- Limit access to systems by would-be network sniffers – "How to Enable Dynamic Routing on a Single-Interface System" in *Configuring an Oracle Solaris 11.4 System as a Router or a Load Balancer*
- Prevent the dissemination of information about the network topology – "How to Disable Broadcast Packet Forwarding" in *Securing the Network in Oracle Solaris 11.4* and "How to Disable Responses to Echo Requests" in *Securing the Network in Oracle Solaris 11.4*
- Prevent packets that do not have the address of the gateway in their header from moving beyond the gateway – "How to Set Strict Multihoming" in *Securing the Network in Oracle Solaris 11.4*
- Prevent Denial of Service (DoS) attacks by controlling the number of incomplete system connections – "How to Set Maximum Number of Incomplete TCP Connections" in *Securing the Network in Oracle Solaris 11.4*

- Prevent DoS attacks by controlling the number of permitted incoming connections – "How to Set Maximum Number of Pending TCP Connections" in *Securing the Network in Oracle Solaris 11.4*
- Increase security that administrative actions reduced – "How to Reset Network Parameters to Secure Values" in *Securing the Network in Oracle Solaris 11.4*
- Add TCP wrappers to network services to limit applications to legitimate users – "Using TCP Wrappers in Oracle Solaris" in *Administering TCP/IP Networks, IPMP, and IP Tunnels in Oracle Solaris 11.4*
- Configure a firewall – Chapter 5, "Configuring the Firewall in Oracle Solaris" in *Securing the Network in Oracle Solaris 11.4*
- Configure encrypted and authenticated network connections – Chapter 7, "Configuring IPsec" in *Securing the Network in Oracle Solaris 11.4* and Chapter 9, "Configuring IKEv2" in *Securing the Network in Oracle Solaris 11.4*
- Configure Kerberos – *Managing Kerberos in Oracle Solaris 11.4*

Protecting File Systems

ZFS file systems are lightweight and can be encrypted, compressed, and configured with reserved space and disk space quotas. The `tmpfs` file system can grow without bound.

The following tasks configure ZFS and `tmpfs` so provide a glimpse of the protections that are available in ZFS.

- Prevent DoS attacks by managing and reserving disk space – "Setting ZFS Quotas" in *Managing ZFS File Systems in Oracle Solaris 11.4*, "Setting Reservations on ZFS File Systems" in *Managing ZFS File Systems in Oracle Solaris 11.4*, and the `zfs`(8) man page
- Encrypt data on a file system – "Encrypting ZFS File Systems" in *Managing ZFS File Systems in Oracle Solaris 11.4* and "Examples of Encrypting ZFS File Systems" in *Managing ZFS File Systems in Oracle Solaris 11.4*
- Prevent malicious users from creating large files in `/tmp` – "Preventing tmpfs File Systems From Filling Up the System" in *Securing Files and Verifying File Integrity in Oracle Solaris 11.4*
- Prevent unauthorized access to sensitive file systems – Chapter 3, "Labeling Files for Data Loss Protection" in *Securing Files and Verifying File Integrity in Oracle Solaris 11.4*

Protecting and Modifying Files

By default, only the `root` role can modify system file permissions. Roles and users who are assigned the `solaris.admin.edit/`*path-to-system-file* authorization can modify that *system-file*. Only the `root` role can search for all files.

The following tasks illustrate several strategies for protecting the files in your system.

- Configure restrictive file permissions for regular users – "How to Set a More Restrictive umask Value for Regular Users" in *Securing Users and Processes in Oracle Solaris 11.4*
- Use extended security attributes to protect files – "Using File Attributes to Add Security to ZFS Files" in *Securing Files and Verifying File Integrity in Oracle Solaris 11.4*
- Prevent accidental deletion of critical files, such as Oracle database logs – "Preventing Accidental Deletions With the nounlink Attribute" in *Securing Files and Verifying File Integrity in Oracle Solaris 11.4*
- Maintain system file integrity – "How to Find Files With Special File Permissions" in *Securing Files and Verifying File Integrity in Oracle Solaris 11.4*

Securing System Access and Use

You can configure Oracle Solaris security features to protect your system use, including applications and services on the system and on the network.

- Prevent buffer overflows – "Preventing Process Heap Corruption Using adiheap" in *Securing Systems and Attached Devices in Oracle Solaris 11.4*
- Prevent programs from heap or executable stack corruption – "Protecting the Process Heap and Executable Stacks From Compromise" in *Securing Systems and Attached Devices in Oracle Solaris 11.4*
- Customize auditing according to site security requirements – *Managing Auditing in Oracle Solaris 11.4*
- Protect core files that might contain sensitive information – "Enabling File Paths" in *Troubleshooting System Administration Issues in Oracle Solaris 11.4* and "Administering Your Core File Specifications" in *Troubleshooting System Administration Issues in Oracle Solaris 11.4*
- Create zones to contain and isolate applications – *Introduction to Oracle Solaris Zones*
- Create read-only zones that cannot be modified – Chapter 10, "Configuring and Administering Immutable Zones" in *Creating and Using Oracle Solaris Zones*

  Administer read-only zones – "Administering Immutable Non-Global Zones" in *Creating and Using Oracle Solaris Zones*

- Manage resources in zones – *Administering Resource Management in Oracle Solaris 11.4*
- Create a labeled environment with limited access – Chapter 3, "Labeling Files for Data Loss Protection" in *Securing Files and Verifying File Integrity in Oracle Solaris 11.4* and Chapter 6, "Labeling Processes for Data Loss Protection" in *Securing Users and Processes in Oracle Solaris 11.4*
- Configure Kerberos – *Managing Kerberos in Oracle Solaris 11.4*
- Protect legacy services by assigning limited rights to the application – "Protecting SMF Services" on page 40

Protecting SMF Services

You can limit application configuration to trusted users or roles by adding the application to the Service Management Facility (SMF) feature of Oracle Solaris, then requiring rights to start, refresh, and stop the service.

For services that are run by `inetd`, you should control the number of concurrent processes to prevent a security breach. For more information, see the following:

- "Recommendations for Systems That Run inetd Based Services" in *Administering TCP/IP Networks, IPMP, and IP Tunnels in Oracle Solaris 11.4*
- "Modifying Services that are Controlled by inetd" in *Managing System Services in Oracle Solaris 11.4*

For information and procedures about SMF, see the following:

- "Securing Service Tasks" in *Developing System Services in Oracle Solaris 11.4*
- `smf`(7) and `smf_security`(7)
- `svcadm`(8), `svcbundle`(8), and `svccfg`(8)

Adding Labeled Security

Labeled security in Oracle Solaris is provided by two features, file and process labeling in Oracle Solaris, and the Trusted Extensions feature that is provided in an optional set of packages.

- File and process labeling enables administrators to apply labels to selected datasets and give clearances to selected users. Data that is not privileged is not explicitly labeled, and regular users cannot access labeled data. For more information, see:

- Chapter 3, “Labeling Files for Data Loss Protection” in *Securing Files and Verifying File Integrity in Oracle Solaris 11.4*
- Chapter 6, “Labeling Processes for Data Loss Protection” in *Securing Users and Processes in Oracle Solaris 11.4*

- Trusted Extensions labels all users, processes, and network communications.

  You must install the Trusted Extensions packages, then configure the system. The `system/trusted` and `system/trusted/trusted-global-zone` packages are sufficient for a headless system or server. Network configuration is required to communicate with other systems.

  For information and procedures, see the following:

  - Part 1, “Initial Configuration of Trusted Extensions,” in *Trusted Extensions Configuration and Administration*
  - Part 2, “Administration of Trusted Extensions,” in *Trusted Extensions Configuration and Administration*

♦ ♦ ♦ CHAPTER 3

Maintaining and Monitoring Oracle Solaris Security

This chapter describes the actions to take to maintain and monitor security on your system, beginning with booting.

Verifying System Integrity Before Regular Users Log In

Oracle Solaris provides ways to ensure that the booting process is secure and the packages on your system are valid.

- Verified boot – Secures the boot process. Verified boot is disabled by default.

  This feature protects the system from threats such as the installation of unauthorized kernel modules and trojan applications.

  For more information, review the following:

  - Chapter 2, "Protecting Oracle Solaris System Integrity" in *Securing Systems and Attached Devices in Oracle Solaris 11.4*
  - "Using Verified Boot" in *Securing Systems and Attached Devices in Oracle Solaris 11.4*
- Repository verification – Verifies that your local IPS repository files are valid.

  Maintaining a valid and secured IPS repository is essential for package installation. If you are using a local IPS repository, you can run the `pkgrepo verify` command to verify that the repository is not corrupted. With any signature policy other than `ignore`, the command verifies that signed packages are correctly signed.

  For more information, review the following:

  - *Creating Package Repositories in Oracle Solaris 11.4*.

    - "Best Practices for Creating and Using Local IPS Package Repositories" in *Creating Package Repositories in Oracle Solaris 11.4*.
- Package verification – Verifies that the installed packages are valid.

  After installing or updating packages, you can run the `pkg verify` command to ensure that the packages on your system did not install files with incorrect ownership or hashes, for example. With any signature policy other than `ignore`, the command verifies that signed packages are correctly signed.

  For more information, see the following:

    - "Properties for Signing Packages" in *Updating Systems and Adding Software in Oracle Solaris 11.4*
    - "Verifying Packages and Fixing Verification Errors" in *Updating Systems and Adding Software in Oracle Solaris 11.4*
    - `pkg`(1) man page

Monitoring System Security

Perform the following tasks to monitor access and use of your system and data, and adherence to your site's security requirements.

- Verify that you are running the latest version of the OS – "Administering CVE Updates in Oracle Solaris" in *Oracle Solaris 11.4 Compliance Guide*
- Assess the system's compliance to security benchmarks regularly

  The `compliance assess` command provides a snapshot of your system's security posture. The reports from the assessments suggest specific changes to your system to satisfy its default security policy. For more information, see *Oracle Solaris 11.4 Compliance Guide* and the `compliance`(8) man page.
- Verify file integrity regularly

  BART is a rule-based file integrity scanning and reporting tool that uses cryptographic-strength hashes and file system metadata to report changes. BART enables you to comprehensively validate systems by performing file-level checks of a system over time.

  After you verify that files are installed correctly, BART reports can easily and reliably track file changes. The reports might indicate that a system has not been patched, an intruder has installed unapproved files, or an intruder has changed the permissions or contents of system files, such as `root`-owned files.

  For more information, see the following:

    - Chapter 4, "Verifying File Integrity by Using BART" in *Securing Files and Verifying File Integrity in Oracle Solaris 11.4*

    - `bart`(8), `bart_rules`(5), and `bart_manifest`(5) man pages
- Find and remove suspicious files – "How to Find Files With Special File Permissions" in *Securing Files and Verifying File Integrity in Oracle Solaris 11.4*
- Review log files
    - SMF provides log files for every service. To locate the log file for a service, run the `svcs -L` *service* command.
    - The `rsyslog` daemon writes a centralized log that can inform and warn administrators of critical conditions in many services. See the `rsyslogd`(8) man page.
    - Other features create their own logs. For example, you can display package summary information with the `pkg history` command.
- Locate unusual access and use of the system by reviewing audit logs regularly

  Auditing keeps a record of how the system is being used. The audit service includes tools to assist with the analysis of the auditing data. For tools new in this release, see "What's New in Security Features in Oracle Solaris 11.4" on page 11.

  The audit service is described in *Managing Auditing in Oracle Solaris 11.4*. For a list of the man pages and links to them, see "Audit Service Man Pages" in *Managing Auditing in Oracle Solaris 11.4*.

♦ ♦ ♦ APPENDIX A

Site Security Policy and Enforcement

This appendix discusses site security policy issues. It covers the following topics:

For additional references, see Appendix B, "Bibliography for Oracle Solaris Security".

Creating and Managing a Security Policy

Each Oracle Solaris site is unique and must determine its own security policy. Perform the following tasks when creating and managing a security policy.

- Establish a security team. The security team needs to have representation from top-level management, personnel management, computer system management and administrators, and facilities management. The team must review administrators' policies and procedures, and recommend general security policies that apply to all system users.
- Educate management and administration personnel about the site security policy. All personnel involved in the management and administration of the site must be educated about the security policy. Security policies must not be made available to regular users because this policy information has direct bearing on the security of the computer systems.
- Educate users about Oracle Solaris software and the security policy. Because the users are usually the first to know when a system is not functioning normally, the user must become acquainted with the system and report any problems to a system administrator. A secure environment needs the users to notify the system administrators immediately if they notice any of the following:

    - A discrepancy in the last login time that is reported at the beginning of each session
    - An unusual change to file data
    - The inability to operate a user function
    - A lost or stolen printout
    - A lost or stolen mobile device
    - Reported login from unusual sites
    - Emails that request the user to log in to an unusual website or that request sensitive information
- Enforce the security policy. If the security policy is not followed and enforced, the data on your computers is not secure. Establish procedures to record any problems and the measures you took to resolve the incidents.
- Periodically review the security policy. The security team must perform a periodic review of the security policy and all incidents that occurred since the last review. Adjustments to the policy can then lead to increased security.

Site Security Policy and Oracle Solaris

The security administrator must design the network based on the site's security policy. The security policy for Oracle Solaris systems dictates configuration decisions, such as the following:

- How much auditing is done for all users and for which classes of events
- How much auditing is done for users in roles and for which classes of events
- How audit data is managed, archived, and reviewed

  See *Managing Auditing in Oracle Solaris 11.4*.
- Which systems are labeled and which users and processes run at a higher clearance

  See Chapter 3, “Labeling Files for Data Loss Protection” in *Securing Files and Verifying File Integrity in Oracle Solaris 11.4*.
- Which individuals or roles are assigned which clearances

  See Chapter 6, “Labeling Processes for Data Loss Protection” in *Securing Users and Processes in Oracle Solaris 11.4*.

Computer Security Recommendations

Consider the following list of guidelines when you develop a security policy for your site.

- Update your Oracle Solaris systems to the latest SRU in a timely manner.
- Perform package verification and compliance checks regularly.

  See *Oracle Solaris 11.4 Compliance Guide*.
- Perform file verification regularly.

  See Chapter 4, "Verifying File Integrity by Using BART" in *Securing Files and Verifying File Integrity in Oracle Solaris 11.4*.
- Minimize the number of administration IDs.
- Eliminate third-party setuid and setgid programs. Use rights profiles and roles to execute programs and to prevent misuse.
- Encrypt sensitive data on disk and archive media to avoid breaches if hardware or media is lost or stolen.

  See *Managing ZFS File Systems in Oracle Solaris 11.4*.
- Encrypt network traffic with Kerberos, TLS, or IPsec.

  See *Managing Kerberos in Oracle Solaris 11.4* and *Securing the Network in Oracle Solaris 11.4*.
- Isolate appropriate services or applications in different zones or virtual machines.

  See *Introduction to Oracle Solaris Zones*.
- Protect encryption keys and certificates against exposure or loss.

  See *Managing Encryption and Certificates in Oracle Solaris 11.4*.
- Restrict access to shared file systems and network servers to known hosts, users, or network groups which require access.

  See *Managing Secure Shell Access in Oracle Solaris 11.4* and *Managing Network File Systems in Oracle Solaris 11.4*.
- For a system that is configured with labels, assign the maximum label to not be greater than the maximum security level of work being done at the site.

  Assign clearances and administrative rights only to users who need them and who can be trusted to use them properly.

  See Chapter 6, "Labeling Processes for Data Loss Protection" in *Securing Users and Processes in Oracle Solaris 11.4*,
- Assign privileges to programs only when they need the privileges to do their work, and only when the programs have been scrutinized and proven to be trustworthy in their use of privilege. Review the privileges on existing Oracle Solaris programs as a guide to setting privileges on new programs.

If possible, assign at least two individuals to administer Oracle Solaris systems. Assign one person security-related responsibilities, such as assigning passwords and clearances. Assign the other person the System Administrator rights profile for system management tasks.

See *Securing Users and Processes in Oracle Solaris 11.4*.

- Restrict operating manuals and administrator documentation to individuals with a valid need for access to that information.
- Document file system damage, and analyze all affected files for potential security policy violations.
- Report and document unusual or unexpected behavior of any Oracle Solaris software, and determine the cause.
- Review and analyze audit information regularly. Investigate any irregular events to determine the cause of the event.

  See *Managing Auditing in Oracle Solaris 11.4*.
- Manually record system reboots, power failures, and shutdowns in a site log.
- Establish a regular backup routine.

Physical Security Recommendations

Consider the following list of guidelines when you develop a security policy for your site.

- Restrict access to your systems. The most secure locations are generally interior rooms that are not on the ground floor.
- Monitor and document access to systems.
- Consider removable storage media for sensitive information. Lock up all removable media when the media are not in use.
- Store system backups and archives in a secure location that is separate from the location of the systems.
- Restrict physical access to the backup and archival media in the same manner as you restrict access to the systems.
- Install a high-temperature alarm in the computer facility to indicate when the temperature is outside the range of the manufacturer's specifications. A suggested range is 10°C to 32°C (50°F to 90°F).
- Install a water alarm in the computer facility to indicate water on the floor, in the subfloor cavity, and in the ceiling.
- Install a smoke alarm to indicate fire, and install a fire-suppression system.
- Install a humidity alarm to indicate too much or too little humidity.

- Consider emission security, shielding machines from leaking emanations, including unintentional radio or electrical signals, sounds, and vibrations. This shielding might be appropriate for facility walls, floors, and ceilings.
- Allow only certified technicians to open and close emission security equipment to ensure its ability to shield electromagnetic radiation.
- Check for physical gaps that allow entrance to the facility or to the rooms that contain computer or networking equipment. Look for openings under raised floors, in suspended ceilings, in roof ventilation equipment, and in adjoining walls between original and secondary additions.
- Prohibit eating, drinking, and smoking in computer facilities or near computer equipment. Establish areas where these activities can occur without threat to the computer equipment.
- Protect architectural drawings and diagrams of the computer facility.
- Restrict the use of building diagrams, floor maps, and photographs of the computer facility.

Personnel Security Recommendations

Consider the following list of guidelines when you develop a security policy for your site.

- Inspect packages, documents, and storage media when they arrive and before they leave a secure site.
- Require identification badges on all personnel and visitors at all times.
- Use identification badges that are difficult to copy or counterfeit.
- Establish areas that are prohibited for visitors, and clearly mark the areas.
- Escort visitors at all times.

Equipment Retirement Recommendations

Consider the following list of guidelines when you develop a security policy for your site. Also, refer to NIST 800-88r1.

- Do not re-purpose a system with sensitive data to a network that carries less sensitive data.
- Clear and purge hardware disks before destroying them.
  - For hardware disk purging methods, see *Managing Devices in Oracle Solaris 11.4*.
  - For scrubbing a USB, run the `dd` command several times. You have a couple of options:

```
# dd if=/dev/zero of=/dev/sdx iflag=nocache oflag=direct bs=4096

# dd if=/dev/urandom of=/dev/sdx iflag=nocache oflag=direct bs=4096
```

    - For scrubbing solid state devices (SSDs), obtain OS-specific secure erase utilities from the vendor of your SSDs. You can also use a third-party scrubbing application, such as the `sg_sanitize`(8) utility.
- Forbid the use of flash drives and USBs that could carry sensitive information off-site.

Common Security Violations

Because no computer is completely secure, a computer facility is only as secure as the people who use it. Most actions that violate security are easily resolved by careful users or additional equipment. However, the following list gives examples of problems that can occur:

- Users give passwords to other individuals who should not have access to the system.
- Users write down passwords, and lose or leave the passwords in insecure locations.
- Users set their passwords to easily guessed words or easily guessed names.
- Users learn passwords by watching other users type a password.
- Users leave their systems unattended without locking the screen.
- Users change the permissions on a file to allow other users to read the file.
- On a labeled file system, users change the labels on a file to allow other users to read the file.
- Users discard sensitive hardcopy documents without shredding them, or users leave sensitive hardcopy documents in insecure locations.
- Users store sensitive data on unauthorized cloud services.
- Users forward email to unprotected mail servers.
- Users use insecure applications to transfer sensitive data.
- Users leave access doors unlocked.
- Users lose their keys.
- Users lose their laptops and mobile devices.
- Users do not lock up removable storage media.
- Computer screens are visible through exterior windows.
- Unauthorized users remove, replace, or physically tamper with hardware.
- Unauthorized users gain access by plugging their laptop into an ethernet port.
- Unauthorized users connect to wireless networks whose signal extends outside the building.
- Network cables are tapped.
- Wireless network signals are monitored.
- Electronic eavesdropping captures signals emitted from computer equipment.
- External electromagnetic radiation interference such as sun-spot activity scrambles files.
- Power outages, surges, and spikes destroy data.

- Earthquakes, floods, tornadoes, hurricanes, and lightning destroy data.

Security Requirements Enforcement

To ensure that the security of the system is not compromised, administrators need to protect passwords, files, and audit data. You must train users to do their part. To be consistent with the requirements for an evaluated configuration, follow the guidelines in this section.

Users and Security Requirements

Each site's security administrator ensures that users are trained in security procedures. The security administrator needs to communicate the following rules to new employees and remind existing employees of these rules on a regular basis:

- Do not tell anyone your password.

  Anyone who knows your password can access the same information that you can without being identified and therefore without being accountable.
- Do not write your password down or include it in an email message.
- Choose passwords that are hard to guess.
- Do not send your password to anyone by email.
- Do not leave your computer unattended without locking the screen or logging off.
- Do not leave your laptop or other mobile devices unattended in an insecure location.
- Remember that administrators do not rely on email to send instructions to users. Never follow emailed instructions from an administrator without first double-checking with the administrator.

  Be aware that sender information in email can be forged.
- Because you are responsible for the access permissions on files and directories that you create, make sure that the permissions on your files and directories are set appropriately. Do not allow unauthorized users to read a file, to change a file, to list the contents of a directory, or to add to a directory.

Your site might provide additional suggestions.

Email Usage Guidelines

It is an unsafe practice to use email to instruct users to take an action.

Warn users not to trust email with instructions that purport to come from an administrator. Doing so prevents the possibility that spoofed email messages could be used to fool users into changing a password to a certain value or divulging the password, which could subsequently be used to log in and compromise the system.

Password Enforcement

The System Administrator role must specify a unique user name and user ID when creating a new account. When choosing the name and ID for a new account, you must ensure that both the user name and associated ID are not duplicated anywhere on the network and have not been previously used. See also "Passwords and Password Policy" on page 23.

The Security Administrator role is responsible for specifying the original password for each account and for communicating the passwords to users of new accounts. You must consider the following information when administering passwords:

- Make sure that the accounts for users who are able to assume the Security Administrator role are configured so that the account cannot be locked. This practice ensures that at least one account can always log in and assume the Security Administrator role to reopen everyone's account if all other accounts are locked.
- Communicate the password to the user of a new account in such a way that the password cannot be eavesdropped by anyone else.
- Change an account's password if you have any suspicion that the password has been discovered by someone who should not know it.
- Never reuse user names or user IDs over the lifetime of the system.

  Ensuring that user names and user IDs are not reused prevents possible confusion about the following:

  - Which actions were performed by which user when audit records are analyzed
  - Which user owns which files when archived files are restored

Information Protection

You as an administrator are responsible for correctly setting up and maintaining discretionary access control (DAC) and mandatory access control (MAC) protections for security-critical files. Critical files include the following:

- `shadow` **file –** Contains encrypted passwords. See the `shadow`(5) man page.
- `auth_attr` **file –** Contains custom authorizations. See the `auth_attr`(5) man page.

- `prof_attr` **file –** Contains custom rights profiles. See the `prof_attr`(5) man page.
- `exec_attr` **file –** Contains commands with security attributes that the site has added to rights profiles. See the `exec_attr`(5) man page.
- **Audit trail –** Contains the audit records that the audit service has collected. See the `audit.log`(5) man page.

Password Protection

In local files, passwords are protected from viewing by DAC and from modifications by both DAC and MAC. Passwords for local accounts are maintained in the `/etc/shadow` file, which is readable only by `root`. For more information, see the `shadow`(5) man page.

Group Administration Practices

The System Administrator role needs to verify on the local system and on the network that all groups have a unique group ID (GID).

When a local group is deleted from the system, the System Administrator role must ensure the following:

- All objects with the GID of the deleted group must be deleted or assigned to another group.
- All users who have the deleted group as their primary group must be reassigned to another primary group.

User Deletion Practices

When an account is deleted from the system, the System Administrator role and the Security Administrator role must take the following actions:

- Delete the account's home directories in every zone.
- Delete any processes or jobs that are owned by the deleted account:
  - Delete any objects that are owned by the account, or assign the ownership to another user.
  - Delete any `at` or `batch` jobs that are scheduled on behalf of the user. For details, see the `at`(1) and `crontab`(1) man pages.
- Never reuse the user name or user ID.

♦ ♦ ♦ APPENDIX B

Bibliography for Oracle Solaris Security

The following references contain useful security information for Oracle Solaris systems. Security information from earlier releases of Oracle Solaris contain some useful and some outdated information.

Security References on the Oracle Technology Network

The following books and articles on the Oracle Solaris 11 Documentation web site contain descriptions of security on Oracle Solaris 11.4 systems:

- *Securing Systems and Attached Devices in Oracle Solaris 11.4*
- *Securing Files and Verifying File Integrity in Oracle Solaris 11.4*
- *Securing the Network in Oracle Solaris 11.4*
- *Securing Users and Processes in Oracle Solaris 11.4*
- *Managing Encryption and Certificates in Oracle Solaris 11.4*
- *Managing Auditing in Oracle Solaris 11.4*
- *Managing Authentication in Oracle Solaris 11.4*
- *Managing Kerberos in Oracle Solaris 11.4*
- *Managing Secure Shell Access in Oracle Solaris 11.4*
- *Oracle Solaris 11.4 Compliance Guide*
- *Trusted Extensions Configuration and Administration*
- *Using a FIPS 140-2 Enabled System in Oracle Solaris 11.4*
- *Developer's Guide to Oracle Solaris 11.4 Security*

For additional information from Oracle about security, review the following articles:

- Importance of Software Security Assurance (`https://www.oracle.com/support/assurance/index.html`)

- What Is Assurance and Why Does It Matter? (https://blogs.oracle.com/oraclesecurity/what-is-assurance-and-why-does-it-matter)

Additional Security References

Government publications describe in detail the standards, policies, methods, and terminology associated with computer security. Other security publications are useful in gaining a thorough understanding of UNIX security problems and solutions.

The web also provides resources. In particular, the CERT (https://www.sei.cmu.edu/about/divisions/cert/index.cfm) web site alerts companies and users to security holes in the software. The SANS Institute (https://www.sans.org/) offers training, an extensive glossary of terms, and an updated list of top threats from the Internet.

U.S. Government Publications

The U.S. government offers many of its publications on the web. The U.S. Department of Homeland Security (https://www.us-cert.gov/security-publications) publishes security information. Also, the National Institute of Standards and Technology (NIST) publishes articles on computer security. The following are a sample of the publications that can be accessed on the NIST Special Publications site (https://csrc.nist.gov/publications/sp).

- *An Introduction to Computer Security: The NIST Handbook*. SP 800-12, October 1995.
- *Computer Security Incident Handling Guide*. SP 800-61 Rev 2, August 2012.
- *(Draft) Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*. SP 800-52 Rev 2, November 2017.
- *Guidelines on Electronic Mail Security*. SP 800-45 Version 2, February 2007.
- *Guidelines on Securing Public Web Servers*. SP 800-44 Version 2, September 2007.
- *Guidelines on Firewalls and Firewall Policy*. SP 800-41 Rev 1, September 2009.
- *Building an Information Technology Security Awareness and Training Program*. SP 800-61, October 2003. Includes a useful glossary.
- *Guide to General Server Security*. SP 800-123, July 2008.
- *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*. SP 800-70 Rev 4, February 2018.
- *Usability and Security Considerations for Public Safety Mobile Authentication*. NISTIR 8080, July 2016.
- *Security of Interactive and Automated Access Management Using Secure Shell (SSH)*. NISTIR 7966, October 2015.

UNIX Publications

Garfinkel, Simson, Gene Spafford, and Alan Schwartz. *Practical UNIX and Internet Security, 3rd Edition*. O'Reilly & Associates, Inc, 2006.

Nemeth, Evi, Garth Snyder, Trent R. Hein, and Ben Whaley. *UNIX and Linux System Administration Handbook (4th Edition)* Pearson Education, Inc. 2010.

General Computer Security Publications

Brunette, Glenn M. *Toward Systemically Secure IT Architectures*. Oracle Technical Paper, June 2006.

Pfleeger, Charles P. and Shari L., and Jonathan Margulies. *Security in Computing (5th Edition)*. Prentice Hall, 2015.

Rhodes-Ousley, Mark. *Information Security: The Complete Reference, Second Edition* . McGraw-Hill/Osborne, 2013.

Stewart, J Michael. *Network Security, Firewalls, and VPNs 1st Edition*. Jones & Bartlett Publishers, 2010.

Kim, David. *Information Security Fundamentals*. Jones & Bartlett Publishers, 2016.

Easttom, Chuck. *System Forensics, Investigation And Response, 2nd Edition*. Jones & Bartlett Publishers, 2014.

McClure, Stuart, Joel Scambray, George Kurtz. *Hacking Exposed 7: Network Security Secrets & Solutions*. McGraw-Hill, 2012.

Index

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X

Z