Solaris 9 8/03

Security Release Notes

Common Criteria Certification

Document Number:	s9.0_125
Date:	January 11, 2005
Version:	0.2a

Abstract

This document provides security related release notes for a Common Criteria certified system, and in particular discusses the physical and procedural countermeasures that are required in order to ensure that Solaris 9 8/03 is operated in a secure manner. It is intended to complement the existing user and administration documentation.

Please
Recycle

Revision History

Version	Date	Author	Comments
0.1	December 2004	Vanessa Kong	First issue for Solaris 9 8/03 Sparc platform CC evaluation.
0.2	January 2005	Vanessa Kong	Changes made per evaluators' comments.
0.2a	January 2005	Jane Medefesser	Fixed a typo

Contents

Introduction 1

1.1 Purpose

This document provides the security release notes for a Solaris 9 8/03 Common Criteria certified system. Within this document are instructions to both users and administrators regarding procedural measures that are required to complement the security functionality of Solaris 9 8/03. These measures are mandatory if the product is to be operated in a secure manner.

This document is to be read in conjunction with the user and administrative documentation listed within Section 1.4, “References”.

1.2 Structure

This chapter provides an introduction.

Chapter 2 provides instructions to normal users.

Chapter 3 provides instructions to system administrators.

Annex A contains an addendum describing new audit records introduced to Solaris 9 8/03; these are not documented in [BSM].

1.3 Terminology

The terminology used in this document is consistent with Solaris 9 8/03 documentation. This document is intended for an audience familiar with Solaris 9 8/03, hence a glossary is not included.

1.4 References

Unless otherwise attributed, the documents referenced here are sourced from Sun Microsystems and associated companies (such as Sun Microsystems Federal Inc.)

[ADMCOMS] Solaris System Administration Commands; Sun Microsystems, Inc.; 817-0675-10; August 2003

[ADMGUIDE] Solaris System Administration Guide; Sun Microsystems, Inc.; 2003

Advanced Administration
817-1758-10
Basic Administration
817-1658-10
IP Services
806-4075-11
Naming and Directory Services (DNS, NIS, and LDAP)
817-0962-10
Resource Management and Network Services
817-0204-10
Security Services
817-0365-10

[BSM] Solaris System Administration Guide - Security Services (formerly known as 'SunSHIELD Basic Security Module Guide'); Sun Microsystems, Inc.; 2003; 817-0365-10

[CC] Common Criteria for Information Technology Security Evaluation, CCIMB-99-031, Version 2.1, August 1999

[FILEFORM] Solaris File Formats; Sun Microsystems, Inc.; 2003; 817-3945-10

[FSA] Solaris Administration Guide - Devices and File Systems; Sun Microsystems, Inc.; 2003; 817-6960-11

[HD] Solaris 9 8/03 High Level Design, Chapter 2, Issue 0.51, Sun Microsystems, s9.0_102

[NSAG] System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP); Sun Microsystems, Inc.; 2003; 817-2655-10

[OPENBOOT] OpenBoot 2.x Command Reference Manual; 2000, Sun Microsystems, Inc.; 806-2906-10

[SBCG] Binary Compatibility Guide; 2000, Sun Microsystems, Inc.; 806-1047-10

[SINST] Solaris 9 (SPARC Platform Edition) Installation Guide; Sun Microsystems, Inc.; 2002; 806-5205-10

[SPAA] Security, Performance and Accounting Administration, SunSoft; 1994

[ST] Solaris 9 8/03 Security Target, Issue 1.0, Sun Microsystems, s9.0_101

[UPMA] User Accounts, Printers, and Mail Administration; SunSoft, 1994

[USERCOMS] Solaris User Commands; Sun Microsystems, Inc.; 2003; 817-0674-10

User Security Notes 2

2.1 Overview

This section provides security instructions for both users and administrators of Solaris 9 8/03. The information detailed in this document must be followed by all the users of the system to maintain security.

2.2 Logging in

When your account is created, the administrator must securely inform you of your username and the password for the account. It is important that you log in immediately and change the password for the account. For guidance on passwords see Section 2.3, “Passwords”.

During logon to the system a valid username must be entered at the login prompt and a valid password entered at the password prompt. After the username has been entered and return pressed, you must wait until the password prompt appears on the screen before attempting to enter the password.

Warning – If you fail to wait, and the password is entered too quickly after the username, some of the password characters will be echoed onto the screen, which could compromise the confidentiality your password.

When logging in, details of the last successful login to your account are displayed on the screen. You should compare this with when you last logged in. If a discrepancy is noticed the administrator should be informed.

You must log out of the system completely before the terminal or workstation that you are using can be left unattended. If logging in to a terminal that does not appear to have completely logged out the previous user, you should ensure previous sessions are closed or contact the administrator.

2.3 Passwords

In order to prevent others logging in to your account the following rules must be adhered to:

- You must not tell anyone else your password, encrypted or unencrypted.
- You must not write the password down.

- You must change your password regularly.
- You must change your password immediately if you suspect that someone else has knowledge of it.
- If you experience a problem when attempting to change your password then contact the system administrator.
- You must choose passwords that are not easy to guess. For guidance on this see [SPAA].
- You should ensure that you are not overlooked when entering your password.

2.4 Groups

The group of any of your files on the system can be a locally defined or network defined group. All types of users, local and network, can belong to local or network groups

2.5 Protecting Data

It is your responsibility to protect your data. The system will protect your files and directories based on the permissions you have set.

It is possible to protect your data from unauthorised access by other users of the system, by assigning access rights to your files and directories. See [USERCOMS] under `chmod(1)` for details of how Access Control works on the product.

The command '`ls -l`' can be used to view the access rights on a file or directory. See [USERCOMS] under `ls(1)` and also the references above.

It may be necessary to restrict other users' access to your files and directories to read only. This can be done by setting the permissions to `r--` for group, and `r--` for others. See the man page for the `chmod(1)` command for further details.

Warning – If you give another user read access to one of your files then it should be understood that this gives that user the ability to take a copy of your file. This copy is under the control of the other user and you have no control over what happens to it. In particular that user is able modify the protection of the copy, which could be modified to allow all users access.

It is possible to completely deny all other users (with the exception of the administrator) access to your files and directories, by setting no permission for group and others (i.e. `---` for group and `---` for others). See the man page for the `chmod(1)` command for further details.

It is only possible for the owner of a file or directory, or the administrator to change the access permissions on that file or directory.

You may wish to give access to your file(s) to just one user, apart from yourself, on the system. If so then contact the administrator who will create a new group such that only you and the other user belong to that group. You can then assign the newly created group to the file(s) for which only the other user can have the required access. The other user gets the required access through the 'group' permission on the file(s).

When files and directories are created by a user, they are given a default protection. The system is set up in such a way that newly created files will have read access for Group and Others, and newly created directories will have read and execute access for Group and Others. This means that you will be the only user with write access to any file or directory you create. An entry can be made in your '`.profile`' file if you are using `sh` and `ksh` shells or in '`.cshrc`' file if you are using `csh` shell to set this default to whatever you wish. The entry should be of the form '`umask <xxx>`' where `<xxx>` are three OCTAL digits that refer to read/write/execute permissions for the owner, group and other, respectively. Each octal digit when subtracted from '7' will provide the default file protection. See [USERCOMS] under `umask(1)` for more details.

You must ensure that the permissions on your files and directories are correct. The permissions can be ascertained by using the command `ls -l` - see [USERCOMS] under `ls(1)`. Ensure that you understand what permissions are on all your files and directories.

Note – an owner will not be permitted access rights to his object, if Owner rights denies him access, even if Group access rights give him access. The owner is still permitted to change the OGO permissions.

Where a file system accessible to users is read-only, write access will not be granted to its constituent files, even if permitted by the OGO permissions. The user can enter the mount command, [USERCOMS] under `mount(1)`, to obtain a list of local and shared mounted file systems.

Access Control Lists (ACLs) can provide greater control over file permissions, see [USERCOMS] under `setfacl(1)` and `getfacl(1)`. When the `setfacl(1)` command is used, it may result in changes to the OGO permissions for that file. An ACL may also contain specific access modes for individually named users and groups, and default settings, which will override the normal permission bits (and by inference the user and group ACL entries) on the file.

2.6 Mail

It is possible to generate a mail message and make it appear that it comes from another user, even `root`. Because of this if you receive a mail message requesting some action, always verify that message before taking the requested action. In particular verify any message requesting action which purports to be from `root` with the administrator.

Care should also be taken when using the mail system to send information to other users. This is because when mail messages are sent to another user the mail message contents are then owned by that user, and the information within the mail message can be disseminated by that user.

The mail system should not be used to send information that is protected. In order to give other users access to your files use the Discretionary Access Controls that the product contains - see Section 2.5, "Protecting Data".

If you receive mail from another user make sure that if the contents need protecting then the access rights on the file containing the mail message are correct.

2.7 Allocating Devices

It is possible to gain exclusive use of a tape, CD-ROM or floppy disk drive that is attached to a workstation the user is logged in at using the command allocate - see [ADMINCOMS] under `allocate(1M)`. Once allocated you have sole use of the device until either you deallocate it, the administrator deallocates it or the permissions are changed on the device. All users of the system must use this mechanism for accessing the devices as it is the secure way of transferring data between the devices and the disk.

By allocating a device other users can be prevented from accessing the contents of a tape, CD-ROM or floppy disk you wish to place in the drive.

In order to make the tape, CD-ROM or floppy disk drive usable by another user the device must be either deallocated, see [ADMINCOMS] under `deallocate(1M)`, or the permissions must be changed on the device to allow other users access to it. See Section 2.5, “Protecting Data” for details concerning access rights.

If you deallocate a device the media must be removed from the device immediately after deallocation, or its contents could be accessed by another user.

Normal users do not have physical access to bootable removable media drives on machines. If you want to access such a device then you must consult the System Administrator.

2.8 Removable Media

When exporting data from the system, users must only use clean removable media (i.e. tapes, floppy disks, or CD-roms which are brand new and have never previously been used). This measure is to prevent the potential vulnerability of exporting information which has been ‘deleted’ but not yet treated for reuse.

2.9 Serial Login Devices

If serial login devices are used e.g. VT100 terminals directly connected to a workstation, users should ensure that the screen is cleared of all information after logging off, or when leaving the terminal unattended.

Administrator Security Notes 3

3.1 Purpose

This section is intended to provide information pertinent to administrators of the product in an operational environment. It is assumed that the System Administrator has attended an administrators training course as approved or recommended by Sun and is familiar with the administration of Solaris 9 8/03. The information provided in this document must be followed in order that the system is administered securely. The administrator should also read Chapter 2, “User Security Notes” before starting to administer the system. The information contained within this document and the referenced documentation is sufficient to administer the system in a secure manner.

The section discusses the following topics:

- Secure Installation of the Product
- Secure Configuration of the Product
- Secure Start-up of the product
- Secure Operation of the product

3.2 Secure Installation

The administrator shall perform the tasks described in this chapter in order to perform a secure installation of a Solaris 9 8/03 Common Criteria certified system, and before it is made available for general use. The administrator must keep a written record of when the operating system, patches and security enhanced features were installed.

Distribution media must be received in shrink-wrapped packages. If the packages appear to have been tampered with, or the shrink wrapping is damaged then do not proceed with the installation, and contact your supplier.

3.2.1 Installation Media Verification

The following installation media are required. Note that the installation may be done via CD in which case the installer will need the *Solaris 9 8/03 Binary CD Set* and the *Solaris 9 8/03 Documentation CD*, or the installation may be from DVD and the installer will need only the *Solaris 9 8/03 DVD Set*. The version numbers should be verified in order to ensure installation of the correct product.

Solaris 9 8/03 Binary CD Set; Sparc Platform Edition: consisting of the following cd-rom components:

- Solaris 9 8/03 Installation CD, Part No. 705-0578-10, August 2003, Revision A
- Solaris 9 8/03 Software 1 of 2 CD,Part No.705-0579-10, August 2003, Revision A
- Solaris 9 8/03 Software 2 of 2 CD, Part No 705-0580-10, August 2003, Revision A

Solaris 9 8/03 Documentation CD:

- Part No 705-0719-10, August 2003, Revision A

Solaris 9 8/03 DVD Set; Sparc Platform Edition:

- Part No 708-0045-10, August 2003, Revision A

Solaris 9 8/03 AMT Package:

- solaris9_803_AMT_<sol9_803_AMT_revision_number>.tar.Z file

Solaris 9 Security Release Notes Document:

- SRN_<SRN_revision_number>.pdf

Note – The Solaris 9 8/03 AMT (Abstract Machine Tests) package and the Security Release Notes can be downloaded from the SUN security certification website. This can be found at: www.sun.com/security. Select ‘Security Certification’.

3.2.2 Installing SPARC Solaris 9 8/03

The administrator must firstly ensure that the machine is shutdown and then commence installation from the ‘`ok`’ prompt. The installation of the base operating system is an automated process which can be started by inserting the Solaris 9 8/03 Installation CD (Part No. 705-0578-10), and typing `boot cdrom`. The administrator can then follow the on-screen instructions to install Solaris 9 8/03 as required.

Note – If the machine has previously been in use, then the disk should be reformatted at this stage. From the openwindows screen, start a command tool and use the `format` command. Installation will continue after this procedure.

The product should be installed by following the standard installation instructions. The final step of installation is to install the patches (if required) required for the certified configuration which are available from the sun.com web site.

3.3 Installing the Solaris 9 8/03 Common Criteria Package

The Solaris 9 8/03 Common Criteria Package consists of a tar file: solaris9_cert_sparc_<sol9_CC_revision_number>.tar.Z where:

- <sol9_CC_revision_number> refers to the Solaris 9 Common Criteria release number

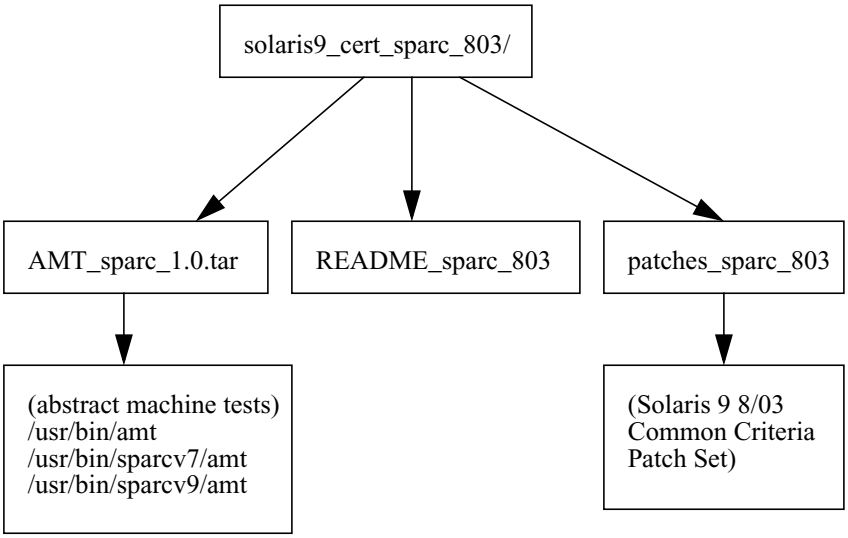
Each Package contains:

- AMT_sparc_<AMT_revision_number>.tar contains abstract machine tests used to verify that the low level functions necessary to enforce the object reuse requirements of the Controlled Access Protection Profile on a Common Criteria security certified system are working properly.
- README_sparc_<sol9_CC_revision_number> file contains a list of patches and revision-specific installation instructions.
- patches_sparc_<sol9_CC_revision_number> directory contains the Solaris 9 Common Criteria patch set.

The contents may be extracted from the tar file into a directory called /tmp/patches by typing:

```
# mkdir /tmp/sol9CC
# cd /tmp/sol9CC
# uncompress \
  solaris9_cert_sparc_<sol9_CC_revision_number>.tar.Z
# tar xvf \
  solaris9_cert_sparc_<sol9_CC_revision_number>.tar
```

An example of the directory structure for a sparc version of the Solaris 9 Common Criteria 8/03 release is shown below:



3.4 Installing Solaris 9 8/03 Common Criteria Patch Set

3.4.1 Standard Solaris Patches

Once Solaris 9 8/03 has been installed, the required patch set should be installed via the `patchadd(1M)` command. All patches must be installed so that your system is in the *evaluated configuration*..

Each patch is contained in its own directory where the name of the containing directory is the patch_id_number. The patches can then be installed by typing:

```
# cd
  /tmp/sol9CC/\
  solaris9_cert_<sol9_CC_revision_number>/\
  patches_<sol9_CC_revision_number>
# patchadd <patch_id_number>
```

Refer to the `README_<sol9_CC_revision_number>` file for any revision-specific installation instructions.

The system must be rebooted before progressing to the configuration steps.

Warning – In order to maintain a system in the evaluated configuration, *only* those patches which comprise the Solaris 9 8/03 Common Criteria patch set may be applied to the system.

3.4.2 praudit

Included in the Common Criteria patch set is an updated version of `praudit(1M)`. To install this program, do the following:

```
# cd
  /tmp/sol9CC/\
  solaris9_cert_<sol9_CC_revision_number>/\
  patches_<sol9_CC_revision_number>
# cd praudit
# mv /usr/sbin/praudit /usr/sbin/praudit.orig
# cp -p ./praudit /usr/sbin/praudit
# chmod 555 /usr/sbin/praudit
# chown root /usr/sbin/praudit
# chgrp bin /usr/sbin/praudit
```

3.5 Secure Configuration

The procedures detailed below must be performed by the administrator before the ToE becomes operational in order to ensure that the system is secure. If followed correctly the procedures detailed below do not require the administrator to make any choices. So therefore only one configuration of the ToE is possible for each installation. The administrator shall not alter the functionality of any commands or change the file protections on files not specified in this document. The procedures must be performed in the order that they are given below.

3.5.1 Setting `root` Password

A '`root`' account is automatically created without a password during installation of Solaris 9 8/03. This account must be given a password immediately after installation.

3.5.2 Setting PROM Password - SPARC

The full security mode PROM password shall be set on all the machines in the network configuration. The administrator shall set the PROM password by logging on as '`root`' and entering the following:

```
eeprom security-mode=full security-password=
```

Enter the PROM password and verify it. Further details on setting the PROM password can be found in [ADMCOMS] under `eeprom(1M)`.

3.5.3 Setting `umask`

The administrator shall set the file creation mode mask by inserting '`umask=022`' entry in the '`/etc/default/login`' file.

3.5.4 Boot Device

3.5.4.1 SPARC Configuration

The Boot device for the server is the disk, and this is set by entering '`eeprom boot-device=disk`'.
The Boot device for diskless clients is the Ethernet Server, and this is set by entering '`eeprom boot-device=net disk`'. In the first instance it will attempt to boot from the Ethernet Server and if that fails then it will attempt to boot from the local disk.

For dataless and standalone clients the boot device is the disk and this is set by entering '`eeprom boot-device=disk`'.

3.5.5 32- and 64-bit Modes

Solaris 9 8/03 for Sparc can be run in either 32 or 64 bit mode. A system in the evaluated configuration may only be run in 64-bit mode.

3.5.6 Enable BSM

To enable BSM, the administrator shall follow the instructions specified below. This must be performed on all the machines in the system.

1. Logon as '`root`'.
2. Bring the system into single user mode by entering '`/etc/telinit 1`'.
3. Change the directory to '`/etc/security`' and execute the '`bsmconv`' script by entering '`./bsmconv`'.
4. Reboot the system by entering '`/etc/telinit 0`'.

3.5.7 Device Allocation

The administrator must make the following devices, if available, allocatable (assignable) on the machine they are connected to:

- CD-ROM
- tape-drive
- floppy-drive

Each of the above allocatable devices must have an entry in the file '`/etc/security/device_allocate`', which specifies the device name, the device type and the device clean pathname. Also the file '`/etc/security/device_maps`' must have an entry for each of the above allocatable devices, which specifies the device name, device type and a list of the device special files associated with the device. The administrator shall ensure that the device clean script ejects the media and informs the user. If the media has to be ejected manually then the device clean script shall display such a message to the screen. See [BSM], Chapter 5, for further information.

3.5.8 Password Policy

When creating users on the system the administrator must construct the passwords to meet the requirements detailed in the `passwd(1)` manual page, which in brief says:

- Each password must have at least six, but no more than eight characters. In the file '`/etc/default/passwd`', '`PASSLENGTH=6`' is set by default and the password length must be set to at least this value.
- Each password must contain at least two alphabetic characters and at least one non-alphabetic character (which is enforced by the default product configuration).
- Each password must differ from the user's login name and any reverse or circular shift of that login name.
- New passwords must differ from the old by at least three characters.

Warning – When using the `passwd(1)` command, the user whose password is being modified *must* be specified: `passwd <target username>`. Because Solaris allows for multiple identity changes, this policy is required to ensure that the user issuing the command does not unintentionally change the password of a user.

3.5.9 Disable `xhost` Command

The '`xhost`' command shall be made '`root`' only accessible command by the administrator changing the access permission on the files, by typing:

```
chmod 744 /usr/openwin/bin/xhost
chmod 744 /usr/X/bin/xhost
```

3.5.10 Configuration File for Name Service - nsswitch.conf

The configuration file, `/etc/nsswitch.conf`, for the name services switch shall contain the following entries:

```
passwd:     files ldap
group:      files ldap
hosts:      ldap [NOTFOUND=return] files
services:   files ldap
```

```
networks:   ldap [NOTFOUND=return] files
protocols:  ldap [NOTFOUND=return] files
rpc:        ldap [NOTFOUND=return] files
ethers:     ldap [NOTFOUND=return] files
netmasks:   ldap [NOTFOUND=return] files
bootparams: ldap [NOTFOUND=return] files
publickey:  ldap [NOTFOUND=return] files
netgroup:   ldap
automount:  files ldap
aliases:    files ldap
sendmailvars:   files
```

The `/etc/nsswitch.conf` file on all machines in the system must contain the above entries.

3.5.11 Configuration of Files and Tables

The administrator must ensure that the following files and tables have the specified permissions:

- `/etc/default/passwd` `r-- r-- r--` (On all machines in system)
- `/etc/passwd` `rw- r-- r--` (On all machines in system)
- `/etc/security/audit_user` `rw- r-- ---` (On all machines in system)
- `/etc/shadow` `r-- --- ---` (On all machines in system)

3.5.12 Default User and Group IDs

When the ToE is installed a number of default user accounts and groups are created. These accounts and groups shall only be used by the administrator in order to administer the ToE. The User Accounts created do not have passwords and only `root` user can `su` to them. The default accounts and groups are detailed below:

- The following local user accounts are created:

```
daemon
bin
sys
adm
lp
smtp
uucp
nuucp
listen
nobody
noaccess
```

- The following local groups are created:

```
root
other
bin
sys
```

```
adm
uucp
mail
tty
lp
nuucp
staff
daemon
sysadmin
nobody
noaccess
```

- No network user accounts or network groups are created.

3.5.13 Solaris Management Console (SMC)

Solaris Management Console 2.1 must be used to administer user accounts.

3.5.14 NFS-Mounted Audit Directories

For NFS mounted directories, you must set the option '`noac`' in the `/etc/vfstab` file in order to obtain the correct behavior when an audit partition fills. If this option is not set, audit records may be lost when moving to a new partition.

Below is an example of how the '`noac`' option is set:

```
<remote_machine>:/audit1    -      /var4   nfs    -      yes    noac
```

3.5.15 Hardware-Specific Configuration Tasks

3.5.15.1 SunFire System Controller Cards

The SunFire servers provides for both direct and remote connection of a system hardware console via the System Controller (SC) card, which is a hardware component within the interconnect cabinet. To maintain a system in an evaluated configuration, the system controller *must* only be connected directly to a dedicated administration network (to which only administrators have access) or directly to a console to which only administrators have physical access. The password length must be commensurate with the level of security required, at least 6 characters but 8 is recommended. The SC is capable of much stronger password usage if the administrator should choose to use that level of protection.

3.5.16 Abstract Machine Tests

The abstract machine tests are used to verify that the low level functions necessary to enforce the object reuse requirements of the Controlled Access Protection Profile on a Common Criteria security certified system are working properly.

If required by your installation, the tests should be run periodically by doing the following:

```
# su
# cd
```

```
  /tmp/sol9CC/\
  solaris9_cert<sparc|i86>_<sol9_CC_revision_number>
# tar xf AMT_<sparc|i86>_<AMT_revision_number>.tar
# exit
$ rehash
$ /usr/bin/amt
```

Test results will be listed with a “pass” or “fail” for each test it performs. An exit status of 0 is returned when all tests pass. Refer to the `amt(1)` manual page for additional details.

3.5.17 Disable IPv6 Re-numbering

IPv6 re-numbering must be disabled. To do this, as `root` user edit the file: `/etc/rc2.d/S69inet`. Search for the following lines:

```
if [ -f /usr/lib/inet/in.ndpd ]; then
     /usr/lib/inet/in.ndpd
fi
```

There are two occurrences of these lines. Add the `-a` option to disable the autoconfiguration of addresses and re-numbering:

```
if [ -f /usr/lib/inet/in.ndpd ]; then
     /usr/lib/inet/in.ndpd -a
fi
```

Restart the daemon by:

```
# /etc/rc2.d/S69inet stop
# /etc/rc2.d/S69inet start
```

3.6 Secure Startup

3.6.1 Secure Start-up - SPARC Workstations

When the SPARC workstation is switched on the firmware on the hardware is immediately executed. The PROM password is prompted and on specifying the correct password the boot process continues. If the PROM password is incorrect there is delay of about 10 seconds before the Restricted Monitor Mode prompt appears. There are only three available options at this prompt; ‘`b`’ to boot, ‘`c`’ to continue and ‘`n`’ for new command. On specifying the ‘`b`’ or the ‘`n`’ option the PROM password is prompted and the ‘`c`’ option remains in the Restricted Monitor mode.

After specifying the correct PROM password and immediately pressing STOP-A key sequence from the keyboard, gets the system into Restricted Monitor Mode. The Restricted Monitor Mode prompt is ‘`>`‘ and in this mode the following screen is displayed:

```
Type b (boot), c (continue), or n (new command mode)
>
```

On pressing ‘b’ it prompts for the PROM password. On pressing ‘c’ it resumes (continues) the booting process. On pressing ‘n’ it first prompts for the PROM password. On specifying the correct PROM password it enters the Forth Monitor Mode and the prompt for this mode is ‘ok’. On entering this mode the following screen is displayed:

```
Type help for more information
ok
```

In this mode the system administrator can use functions detailed in [OPENBOOT].

An uninterrupted boot process gets into the normal multi-user mode.

3.6.2 Secure Start-up - SPARC Servers

The applicable guidelines for the use of the system controllers must be followed as defined in the following manuals:

“Securing the SunFire Midframe System Controller, Part No. 816-4940-10

“System Controller Command Reference Manual”, Part No. 805-7372-13

3.6.3 Operational Modes

The two types of mode of operation for Solaris 9 8/03 are multi-user mode and single user-mode.

3.6.3.1 Multi-user Mode

This is the normal operating mode of the ToE. The transition into this mode is from:

- An uninterrupted boot process from power on.
- Single-user mode by entering ‘`/etc/telinit 3`’.

The transitions from this mode are:

- For SPARC system, pressing `STOP-A` key sequence from the keyboard to transition to Restricted Monitor Mode.
- Single-user mode by entering ‘`/etc/telinit 1`’.
- Shutdown of the machine by entering ‘`shutdown -i5`’.

3.6.3.2 Single-user Mode

This is the operating mode for the maintenance of the ToE by the administrator. The transition into this mode is from:

- Multi-user mode by first shutting down the system and then entering ‘`/etc/telinit 1`’.
- Forth Monitor Mode by entering ‘`boot -s`’ at the ‘`ok`’ prompt.

The transitions from this mode are:

- For SPARC system, pressing `STOP-A` key sequence from the keyboard to transition to Restricted Monitor Mode.
- Multi-user mode by entering '`/etc/telinit 3`'.
- Shutdown of the machine by entering '`shutdown -i5`'.

Further details on the command /etc/telinit and shutdown can be found in [ADMCOMS] under `init(1M)` and `shutdown(1M)` respectively.

3.6.4 Security

There is no possible deactivation or modification of the Security Enforcing Functions during Secure Start-up of the ToE.

3.6.5 Administrative Components

The components (functions) that are relevant to the administrator are those that have been identified and mentioned in this document. The security parameters that are under the administrators control are the parameters that are identified in the manual pages of those components. The only component relevant to the administrator that obtains information is the auditreduce command. All the other components are classified as controlling components and some of them can also be used to obtain information as well.

3.7 Secure Operation

Where the word 'system' is used this refers to a complete installation of the ToE, i.e. all machines in all domains and sub-domains.

3.7.1 Setting Up An LDAP Server

Once the ToE is installed following the guidelines provided in Chapter 3.2, "Administrator Security Notes", one LDAP naming server instance and one or more LDAP client(s) must be created.

For more information on this process, refer to the *Solaris 9 8/03 System Administration Guide: Naming and Directory Services (DNS, NIS and LDAP)*. In particular, see *Part V: LDAP Naming Services Setup and Administration*.

3.7.2 The `root` Account

A password policy, see Section 3.5.8, "Password Policy", exists on the system which applies to all users with the exception of the administrator. The administrator must ensure that the `root` password also conforms to this policy by choosing passwords that conform to the policy, and by changing the `root` password conforming to this policy.

The administrator can also change any other users password using the `passwd(1)` command. When changing user's passwords the administrator must ensure that the new password is chosen at random. When choosing a users password use the guidance given in Chapter 2, "User Security Notes".

3.7.3 Users and Groups

3.7.3.1 Creating Local Groups

Local groups can be created using the SMC Group Manager. All local groups created on all machines must have a different gid. Furthermore the administrator must ensure that all groups whether local or network defined on the system have a unique name and gid. This must be manually checked by the administrator. Local groups can contain both local and network users.

3.7.3.2 Deleting Local Groups

Local groups can be deleted by using the SMC Group Manager. When a local group is deleted from the system the administrator must ensure that all objects with this gid are also deleted from the system, or alternatively reassigned to another group. Also the administrator must ensure that all users who have the deleted group as their primary group are reassigned another primary group.

3.7.3.3 Creating Local Users

Local users should be created using the SMC User Manager. The administrator shall select a unique user name and user id when creating a new local user. Before creating the new user the administrator must check the user name and user id's of all the users on the network by entering the command logins, see [ADMCOMS] under login(1M), on all the machines on the network.

Once a user has been created, a password must be provided for to enable the user to log on. This is achieved via the `passwd(1)` command. Once created the user must be given his password securely and told to log in straight away and change his password.

Warning – Administrators should be aware that Expiration Date of user accounts does not cause accounts to be locked. No reliance should be placed upon this feature when configuring user accounts.

3.7.3.4 Suspending Local Users

See [USERCOMS] under `passwd(1)` for details on how to suspend a local user, i.e. this means locking a password entry.

When using `passwd(1)` to force a user to change his/her password upon the next login, administrators must use the `-n` and `-x` options with the `-f` option. For later changes, just the `-f` option would be sufficient.

Warning – Administrators should be aware that Expiration Date of user accounts does not cause accounts to be locked. Administrators should not use this feature to disable accounts.

3.7.3.5 Deleting Local Users

Local users can be deleted using the SMC User Manager. When a local user is deleted from the system the administrator must ensure that the users home directory and any objects owned by that user are also deleted. As an alternative to deleting objects owned by the user, the administrator may wish to change the ownership of these objects to another user who is defined on the system. The administrator must also ensure that all batch jobs still to run associated with the deleted user are also deleted. The administrator must ensure that there are no objects or processes belonging to a deleted user that remain on the system.

3.7.3.6 Creating a Network User

In order to create a Network User the following steps must be followed:

- The administrator shall select a unique user name and user id when creating a new network user. Before creating the new network user the administrator must check the user name and user id's of all the users on the network by entering the command `logins`, see [ADMCOMS] under `logins(1M)`, on all the machines on the network.
- Decide which domain to make the network user part of
- Logon to the master server for that domain

Use the command line Administration User Management commands to add a user entry.

- Once an entry has been created, give the network user a password using the `passwd(1)` command. Once created the user must be given his password securely and told to log in straight away and change his password.

Warning – Administrators should be aware that Expiration Date of user accounts does not cause accounts to be locked. No reliance should be placed upon this feature when configuring user accounts.

3.7.3.7 Suspending a Network User

See [USERCOMS] under `passwd(1)` for details on how to suspend a network user.

Warning – Administrators should be aware that Expiration Date of user accounts does not cause accounts to be locked. Administrators should not use this feature to disable accounts.

3.7.3.8 Deleting Network Users

Network users may be deleted using the SMC User Manager.

When a network user is deleted from the system the administrator must ensure that the users home directory and any objects owned by that network user are also deleted. As an alternative to deleting objects owned by the network user, the administrator may

wish to change the ownership of these objects to another user who is defined on the system. The administrator must also ensure that all batch jobs still to run associated with the deleted network user are also deleted.

The administrator must ensure that there are no objects or processes belonging to a deleted user that remain on the system.

3.7.3.9 Further Information on Local and Network Users

- The initial password chosen by the administrator for the user must conform to the password policy detailed in Section 3.5.8, “Password Policy”. The initial password for a user must also be chosen at random, so that the next initial password cannot be guessed.
- Once a user has been created and a password provided, the user must be informed immediately to log on and change their password. It is necessary to inform the user of their username and initial password in a secure manner.
- When creating users the administrator must ensure that all usernames and all UIDs of these new users are unique on the system. This also includes uniqueness between local and network users, and between local users on different machines.
- Only the methods detailed above shall be used to Create, Suspend and Delete users. The administrator must not attempt to modify the password file and table in any other way.
- Chapters 1 and 2 of [UPMA] provide further details on User Accounts. These are to be used as guidance, but the creation and deletion of users must be by the methods specified above.
- Upon successful login, the real and audit user ids are set to the uid specified by the authentication data. The real group id is set to the gid from the authentication data. The uid and gids for each user should be assigned and maintained by the administrator using User Manager and Group Manager. These applications should be used in accordance with the measures outlined in this document to ensure secure operation.

3.7.4 Sharing Filesystems

It is possible to make filesystems read-only or read-write. If a filesystem is mounted read-only then write access will not be granted to any files within that filesystem regardless of the OGO permissions on those files. This restriction also applies to the `root` user. When sharing NFS file systems the default unix authentication mechanism shall be used.

See [FSA], and [ADMCOMS] under `share(1M)`, `shareall(1M)` and `share_nfs(1M)`

3.7.5 Discretionary Access Control

There are a number of administration issues concerned with DAC, that the administrator must be aware of:

- DAC only applies to objects that are subject to the administration of rights.
- The administrator should ensure that the following file permissions are always maintained so that authentication data is protected by DAC, and so that only owners may read encrypted passwords (i.e. via the trusted programs, `login`, `su`, `ftp`, `telnet` and `rlogin`):

File	Permissions
local `passwd` (each client)	`rw-r--r--`
local `shadow` (each client)	`r--------`
local `group` (each client)	`rw-r--r--`

  In addition, authentication information such as passwords, must not be stored on removable media.

- The operating system has a configuration option {`_POSIX_CHOWN_RESTRICTED`}, to restrict ownership changes. When this option is in effect the owner of the file is prevented from changing the owner ID of the file. Only the super-user can arbitrarily change owner IDs whether or not this option is in effect. By default this option is in effect, however to turn it off add the line `set rstchown=0` to the file `/etc/system`. To turn it on again, replace the `0` with `1`. Any changes require a `reboot`.

Note – When using the getconf command to determine the setting of {`_POSIX_CHOWN_RESTRICTED`}, the value of "`0`" is displayed as "`undefined`". The value "`1`" is displayed as "`1`".

- The command '`ls -l <object name>` can be used in order to check permissions on objects, to ensure that they are correctly protected. The administrator can also examine the audit trail to check whether there are any unauthorised access attempts to these objects. See [BSM].

3.7.6 Accounting and Audit

Details of the Accounting and Audit system can be found in [BSM]. The BSM provides instructions on how to set the system up to record the required events for the required users. The document also provides details on how to examine the audit trails after the events have been recorded. An addendum to [BSM] detailing additions and corrections is provided in this document as Annex A. See also [ADMCOMS] under `audit(1M)`, `audit_startup(1M)`, `auditconfig(1M)`, `auditd(1M)`, `auditreduce(1M)`, and `praudit(1M)`.

Each machine audits it own events locally, and the auditing system of each machine is managed by the local `root` user of that machine. This is true whether the machine is an LDAP server or a client.

The auditing system can be started in one of two ways. If the file `/etc/security/audit_startup` exists then auditing starts every time the system is rebooted. See [BSM] for details of this file. Alternatively the commands

'auditd' and 'audit -t' can be used by the administrator in order to start and stop auditing. See [ADMCOMS] under auditd(1M) and audit(1M) for details of these commands.

If auditing is required on the system, the administrator must ensure that auditing is started on reboot (i.e. the administrator must create an audit_startup file). This is also important for maintaining a secure and consistent audit configuration (especially with regard to the AUDIT_CNT flag - see below) as the audit_startup file provides a means of setting the audit policies every time the audit daemon is started.

The command 'audit -t' which stops recording on the system must be used with care. This command will mean that any auditable user actions will not be recorded until the administrator starts the accounting system again, or until the system is rebooted (if an audit_startup file exists).

The command 'ps -ef | grep audit' can be used to ascertain whether the auditd process is running or not. See [USERCOMS] under ps(1) for details of this command.

The audit trail files are stored in a directory which is specified in the file /etc/security/audit_control. See [ADMCOMS] for details of this file. The files in this directory are protected in such a way that only the administrator has access to them. The permissions on files within this directory must not be changed by the administrator. The administrator must also ensure that any files created by virtue of using the auditreduce(1M) command are also properly protected, so that normal users do not have access to them.

If the audit trail is to be stored on a partition which is NFS mounted, the 'noac' option must be used to ensure audit records are not lost no exhaustion of the available space.

Warning – To operate the system in a certified configuration, audit trails stored on NFS mounted partitions must use the a partition mounted with the noac flag, either explicitly or in the /etc/vfstab file. An entry in the /etc/vfstab file will look similar to:

```
<remote_machine>:/var/audit - /var/audit2 nfs - yes noac
```

This line ensures that local caching is turned off, a write error will result on a full partition and audit records will not be lost.

The audit trail must not be stored on media which is physically removable from a machine by unauthorised users.

Whenever the audit daemon encounters an unusual condition while writing audit records, it invokes the /etc/security/audit_warn script. This script is used to warn the administrator if the audit directory is becoming full. ([BSM] and the audit_warn(1M) manual page provide further details.) The administrator must ensure that audit_warn is adequately set up for the particular installation of the ToE.

The command ‘`df -k`’ can be used in order to check on available space on the disk. See [USERCOMS] under `df(1)` for details of this command.

The ToE must be set up so that if the audit trail files fill up, then all auditable processes are suspended until some storage space is freed. `audit_warn` notifies the administrator when this happens, and the administrator must either archive the audit trails, or provide further storage space. See [BSM] for further details.

Warning – To operate the system in a certified configuration, there must exist an audit_startup file containing the following lines:

```
auditconfig -setpolicy -cnt
```

This line ensures that the `AUDIT_CNT` flag is not set, thus preventing loss of audit data upon kernel audit buffer overflow. In addition, administrators must ensure that this file never contains a line saying ‘`auditconfig -setpolicy +cnt`’, which may override the required policy.
Administrators should be aware that the system sets the `AUDIT_CNT` flag by default, and they should therefore set up the `audit_startup` file immediately after installation, then `reboot`. The line should also never be removed to ensure that the required policy is restored following subsequent system reboots.

The administrator needs to ensure that the audit trail captures and is examined for the auditing of user account management commands.

Warning – If CLI commands are used to administer accounts, to ensure the creation, deletion and modification of user accounts is audited, the following line must be added to the `audit_startup` file.

```
auditconfig -setpolicy +argv
```

This line ensures that the `ex` flag captures the full path of the `useradd, userdel, usermod, groupadd, groupdel and groupmod` commands when executed so that their use is audited thus preventing loss of audit data.

System procedures must exist which deal with the analysing and archiving of audit data. These procedures must be adequate so that in normal operation the audit trail files do not completely fill up.

The administrator must regularly examine the audit trail for attempts to breach the security of the system. If repeated attempts at breaching the security of the system are detected appropriate action must be taken.

There must be procedures in place for each system which define what events are to be audited. The administrator must follow these procedures when setting up the `/etc/security/audit_control` file.

If it is required to audit events which constitute [CC] functionality, then the following flags must be set in the `/etc/security/audit_control` file. See [BSM] for details of how to set these flags.

```
flags:fr,fw,fm,fc,fd,ad,lo,ex
naflags:lo
```

The file /etc/security/audit_control can be viewed by the administrator at any time to check what events the system is set up to record.

Warning – The administrator should be aware that administration of user accounts using the useradd(1M, usermod(1M)) and userdel(1M) commands will not generate any user-level audit events directly. The administrator must adopt a policy of searching for the exec record with the full path of these commands. This can be done by auditing the actions of these commands by setting the 'ex' flag and examining the audit trail for AUE_EXEC and AUE_EXECVE kernel-level events. The 'ex' flag will record every executed command along with any specified attributes.

3.7.7 Devices

It is possible for all users of the system to allocate themselves exclusive use of the devices attached to the machine at which they are logged in. By using the -F flag the administrator can reassign the device to another user, or alternatively the administrator can use the deallocate command to deallocate the device. See [ADMCOMS] under allocate(1M) and deallocate (1M) for further details.

3.7.7.1 SPARC

On SPARC machines the user is permitted access to bootable removable media drives. The user must be instructed to remove his media when he has finished using it. It may be necessary for the administrator to load media into drives for a user, in which case the user must inform the administrator immediately he has finished using it so that it is removed. This prevents its use by other, potentially unauthorized users. The secure use by users of assignable devices is covered in [USER].

3.7.8 Trusted Clients

All clients to the server must be identified and authenticated by the server.

The file /etc/hosts or the hosts table contain details of the trusted clients. After installation only the administrator can change data in these files/tables. The administrator must not change the permissions on these files/tables that would enable normal users to change them. The command 'ls -l /etc/hosts' can be used to ascertain the permissions on the file.

Details of the /etc/hosts file can be found in [FILEFORM] under hosts(4).

The file /etc/nsswitch.conf allows the administrator to specify whether the file /etc/hosts will be searched before the corresponding LDAP directory or vice-versa. Details of this file can be found in [FILEFORM] under nsswitch.conf.

3.7.9 Unauthorised Software

Only the administrator shall be allowed to introduce new software onto the system. This include compilers and similar tools. The java compiler, which is installed by default, should be modified by changing the permissions on /usr/java1.2/bin/.javawrapper to allow access to only authorised users.

The remaining measures are provided by physical methods which need to provided at each installation of the ToE. The Physical Methods to protect the system, which need to be defined for each individual installation are:

- Access to the system as a whole shall be protected
- Removable media shall be protected
- Backup media shall be protected
- Any network machines, servers, and peripheral cabling shall be protected from unauthorised access

3.7.10 Checking the Configuration

The `pkgchk` command shall be used any time the system administrator suspects the integrity of the system may have been compromised, see [ADMCOMS] under `pkgchk(1M)` for further details.

Additionally, the Abstract Machine Tests should be executed periodically to ensure that domain separation is being enforced.

3.7.11 Mail

The administrator must not use the Mail System of the product to send messages of an Instructional nature to other users on the system. There is a possibility that another user of the system can spoof a message, and make it appear that it came from `root`. See [USER] for more details on this.

If a user of the system receives mail purporting to be from the administrator, the user is instructed to confirm with the administrator to ensure that the mail is genuine. If confirmation is sought by a user, and no mail was sent by the administrator then the administrator must endeavor to detect the source of the mail and take appropriate action. The type of appropriate action will depend on the specific installation of the system.

3.7.12 Binary Compatibility Mode (on SPARC)

The ToE contains Binary compatibility packages `SUNWbcp` and `SUNWowbcp` which allows existing SunOS 4.x applications to run on the Solaris 9 8/03 release without modification or recompilation. The binary compatibility packages are invoked automatically and transparently when running a SunOS 4.x application. The administrator shall ensure that the path `/usr/ucb` must not precede the path `/usr/bin` in the system wide default `PATH` variable. For further details the administrator shall consult [SBCG].

3.7.13 Secure Operating Procedures

If the Secure Operating procedures are followed, then there is no possible deactivation or modification of security enforcing functions during secure operation.

3.7.14 Administration Documentation

It is recommended that administrators refer to the set of book-form documentation for Solaris 9 8/03 when operating the ToE.

3.7.15 `login -f` Option

The `login` command has an undocumented option "`-f`". The use of this option, especially when combined with the `-r` option can cause unexpected effects. There are no known security implications when using this undocumented feature, but it is advised that this feature not be used by administrators.

3.7.16 Buffer Overflow in `ufsrestore`

A buffer overrun exists in the 'netpr' program, part of the `SUNWpcu` (LP) package included with Solaris 9 8/03. The overflow is present in the `-p` option, normally used to specify a printer. By specifying a long buffer containing machine executable code, it is possible to execute arbitrary commands as `root`. On SPARC, the exploits provided will spawn a `root` shell.

The suggested fix is to disable `ufsdump(1M)` and `ufsrestore(1M)` and use `cpio` command instead

The following should be lines executed during the configuration of the system and after any re-boots if needed:

```
# chmod u-s /usr/lib/fs/ufs/ufsrestore
# chmod u-s /usr/lib/fs/ufs/ufsdump
```

3.7.17 Buffer Overflow in `uucp(1C)` and `uustat(1C)`

The buffer overflows in `uucp(1C)` and `uustat(1C)` can allow `uucp` uid access. The `uucp(1C)` and `uustat(1C)` commands contain insecure code which may allow an ordinary user access to the privileged `uucp` uid. There is a reasonable fix: Remove the setuid bit from `uucp(1C)` and `uustat(1C)`:

```
# chmod u-s /usr/bin/uucp
# chmod u-s /usr/bin/uustat
```

3.7.18 Buffer Overflow in `snmpdx`

This buffer overflow would allow remote `root` access through the `snmpdx` daemon which allows ordinary users to gain unauthorized remote access. There is a faulty boundary check in encoding PDUs which causes the `root` compromise. Hence the system must be configured such that `snmpdx` is disabled with:

```
# mv /etc/rc3.d/S76snmpdx /etc/rc3.d/snmpdxS76
# /etc/init.d/init.snmpdx stop
```

3.7.19 Buffer Overflow in `snmpdXmi`

This buffer overflow would allow the `snmpXdmi` daemon which allows ordinary users to gain unauthorized remote `root` access. Hence the system must be configured such that `snmpdx` is disabled with:

```
# mv /etc/rc3.d/S77dmi /etc/rc3.d/dmiS77
# /etc/init.d/dmi stop
```

3.7.20 Entry Into Debugger Mode

In Solaris 9 8/03, audit records are generated when a user enters and exits debugger mode. However, this feature only works if the `STOP-A` is done from a console. Entry into debugger mode via a tip line is not audited and therefore this feature must be disabled. To do so, edit the file `/etc/system`. At the end of the file, add the line:

```
set abort_enable = 0
```

3.7.21 Truncated Password

Users can change to passwords such as “abcdefghijk12” and then log in with just “abcdefgh”. Only the first eight characters of the typed password are significant, whether you are setting it or authenticating. Anything longer is truncated after the eighth character.

When you try to set the password to “abcdefgh”, the `passwd` command complains:

```
passwd: The first 6 characters of the password must
contain at least two alphabetic characters and at least
one numeric or special character.
```

This was expected, however, when you set the password to “abcdefgh123”, it does not complain and the effective password is set to “abcdefgh”. Conversely, using numerals, you can set your password to “12345678” by typing “12345678&abc” as the new password, but not by typing “12345678”.

In order to maintain the Strength of Function claim, the site must require that users input a password of no more than eight characters and that at least one character must be a numeric or special character. See Section *3.5.8 Password Policy* of this document for a complete list of password policy rules.

3.7.22 `/bin/login` is `setuid`

The program `/bin/login` is `setuid root` largely for historical reasons. It is executed by a number of programs that run as `root` anyway. These programs are the most common users of `login`:

- `ttymon`
- `telnetd`
- `rlogind`

/bin/login is not required to be setuid. Only when executed from the shell, which will directly exec /bin/login, does login need to be setuid. However, that 'feature' is unnecessary in current operating environments.

/bin/login can be used to remove the hostname from your utmp entry. To eliminate this potential vulnerability, disable the use of /bin/login

```
# chmod u-s /bin/login
```

3.7.23 mail(1), mailx(1) is setgid

The following files have their setgid bits set to mail:

```
/usr/bin/mail
/usr/bin/mailx
/usr/dt/bin/dtmail
/usr/dt/bin/dtmailpr
/usr/openwin/bin/mailtool
```

In order to remove this vulnerability, the administrator shall:

- remove the setgid mail from all of the above listed programs

```
# chmod g-s <program_name>
```

- make sure that all files in /var/mail are created with mode 600 and not 660.

3.7.24 Buffer Overflow in nawk(1)

There is a possible buffer overflow situation in nawk(1). This may lead to data corruption. Disable nawk(1)by doing the following:

```
# chmod a-x /usr/bin/nawk
```

3.7.25 /usr/ucb/ps -e

The command /usr/ucb/sparcv9/ps displays environment variables for all processes (including processes for other users) when the -e option is used. Only root should be able to see environment variables for all processes; non-root users should only see the environment variables of its own processes.

```
# chmod u-s /usr/ucb/sparcv9/ps
```

3.7.26 /usr/bin/eject

/usr/bin/eject is setuid root and can be used to find files which are not owned by the user who runs the /usr/bin/eject command. /usr/bin/eject will report a "/path/file: Permission denied" error if the file exists. It will report a "/path/file: No such file or directory" if a file does not exist.

This command should be disabled in the evaluated configuration by doing the following:

```
# chmod u-s /usr/bin/eject
```

3.7.27 Buffer Overflow in `rcp(1)` Command Line Argument

By executing `rcp(1)` on a local system with excessively ong command line arguments, a user may produce a segmentation fault which in turn may result in memory corruption. An attacker must execute `rcp(1)` with 10,000 bytes in each of the fields for the filename, destination hostname, and destination filename. As `rcp(1)` is a `setuid root` executable, it may be possible to gain elevated privileges.

The administrator must remove the setuid bit from `rcp(1)`.

```
# chmod u-s /usr/bin/rcp
```

3.7.28 `dtterm(1)` Window Title

The window title reporting feature of `dtterm(1)` may be used to execute arbitrary commands on the system running the terminal emulator. The terminal software supports escape sequences which can change the title of a terminal window and then report the title back to the command line. In this manner, an attacker can inject malicious escape equences which include arbitrary commands in the terminal window title and then cause the commands to be displayed on the command line. Note that exploitation of this vulnerability will still require the user to press '`Enter`' once the malicious commands are dumped from the window title to the command line.

All users should be wary of any suspicious activity that occus while using the terminal emulator. This may include changes in the terminal window title, suspicious command line input or any server responses that seem unusual. All of these behaviors may indicate attempts to exploit this issue.

3.7.29 `libXpm`

Multiple vulnerabilities have been reported in `libXpm` which potentially can be exploited by malicious users.

- When a specially crafted `XPM` file is processed, a boundary error within the `xpmParseColors()` function can be exploited to cause a stack based buffer overflow. Sucessful exploitation may potentially allow execution of arbitrary code.
- Again when a specially crafted `XPM` file is processed, various input validation errors can be exploited to cause integer overflows. Successful exploitation causes an affected application to crash and may potentially allow arbitrary code execution.

Users must be advised to not load `X PixMap` (`.xmp`) images from untrusted sources.

3.7.30 RBAC `exec_attr(4)` Search in LDAP

The RBAC backend for LDAP composes its search for a wildcard rule using an unfiltered '`*`'. This results in a pattern that matches any command in the named profile rather than matching just a '`*`' command.

This issues must be handled via administrative policy. Administrators are advised to limit user access to LDAP commands for unprivileged users.

3.7.31 `format(1M)` Shell Escape in RBAC

Using RBAC, and administrator can define rights profiles that allow non-`root` users access to certain `root` commands. This may be done without giving the user general `root` access. If someone defines a profile with `format(1)`, the user could use `format(1)`'s shell escape to gain general `root` access.

The file `/etc/security/exec_attr` gives the "File System Management" profile the right to execute `/usr/sbin/format` with user ID = 0. It should use "`euid=0`". To eliminate this vulnerability, edit `/etc/security/exec_attr`, find the entry for `/usr/sbin/format` and change "`uid=0`" to "`euid=0`".

3.7.32 Buffer Overflow in `libDtSvc`

`libDtSvc` contains a buffer overflow when dealing with the `DTDATABASESEARCHPATH` environment variable.

The workaround for this vulnerability is to `chmod 0555` any `setuid`/`setgid` application linking to `libDtSvc`. Applications may still dump core but will not raise user privileges. Note that functionality in these applications will be impacted. For example, `dtmail(1)` will no longer be able to read nfs mounted email folders.

Addendum for BSM Guide A

A.1 Purpose

This annex is intended to provide additional information and corrections that are relevant to the SunShield Basic Security Module for Solaris 9.

A.2 Audit Record Corrections

`mount`

system call	`mount`	see `mount(2)`
event ID	`62`	`AUE_MOUNT`
event class	`ad`	(0x00000800)
audit record		
<unix filesystem>		
header-token		
argument-token		(3,"flags",flags)
text-token		(filesystem type)
path-token		
[attr-token]		
subject-token		
return-token		
<nfs filesystem>		
header-token		
argument-token		(3,"flags",flags)
text-token		(filesystem type)
text-token		(host name)
argument-token		(3,"internal flags",flags)
path-token		
[attr-token]		
subject-token		
return-token		

A.3 Additional Audit Records

A.3.1 Kernel-Level Generated Audit Records

acl

system call	`acl`	see `acl(2)`
event ID	`251`	`AUE_ACLSET`
event class	`fm`	(0x00000008)
audit record		
header-token		
subject-token		
path-token		
return-token		

facl

system call	`facl`	see `facl(2)`
event ID	`252`	`AUE_FACLSET`
event class	`fm`	(0x00000008)
audit record		
header-token		
subject-token		
path-token		
return-token		

setreuid

system call	`setreuid`	see `setreuid(2)`
event ID	`40`	`AUE_SETREUID`
event class	`pc`	(0x00000080)
audit record		
header-token		
argument-token		(1,"real uid",ruid)
argument-token		(2,"effective uid",euid)
subject-token		
return-token		

setregid

system call	`setregid`	see `setregid(2)`
event ID	`41`	`AUE_SETREGID`
event class	`pc`	(0x00000080)
audit record		
header-token		
argument-token		(1,"real gid",rgid)
argument-token		(2,"effective gid",egid)
subject-token		
return-token		

A.3.2 User-Level Generated Audit Records

`init`

program	`/usr/sbin/init`	see `init(1M)`
event ID	`6166`	`AUE_init_solaris`
event class	`ad`	(0x40000800)
audit record		
header-token		
subject-token		
text-token		(level)
return-token		

`shutdown`

program	`/usr/ucb/shutdown`	see `shutdown(1B)`
event ID	`6168`	`AUE_shutdown_solaris`
event class	`ad`	(0x40000800)
audit record		
header-token		
subject-token		
return-token		