Global Information Assurance Certification Paper

Mapping the Technical Security Requirements of the DCID 6/3 to the NSA's "Guide to the Secure Configuration of Solaris" for Solaris 2.5.1 and Solaris 9.

By Joel I. Kirch, GSEC, GCIH

For SysAdmin, Audit, Network, Security (SANS) Global Information Assurance Certification (GIAC) GIAC Certified Unix Security Administrator (GCUX) Certification, Version 2.1
Option 3 – Topics in UNIX Security

27 September 2004

Abstract

Director of Central Intelligence Directive 6/3 (DCID 6/3), “Protecting Sensitive Compartmented Information Within Information Systems” is the overarching security manual used to protect highly classified intelligence information systems. It contains a wide variety of security controls both technical and non-technical in nature. A few examples of some non-technical controls include, labeling procedures, configuration management, and maintenance.

From the perspective of hardening an operating system, the security controls are intertwined throughout the DCID 6/3 manual. This document attempts to distill just the technical security controls from DCID 6/3 as they apply to a specific instance of a fictional information system using Solaris 2.5.1 (and a comparison of a base-installation of Solaris 9), and map the security controls to the National Security Administration’s (NSA) “Guide to the Secure Configuration of Solaris”, which is based on the Center for Internet Security’s (CIS) “Solaris Benchmark.”

Table of Contents

Executive Summary

The security requirements of the system fall under the purview of the Director Of Central Intelligence Directive 6/3. The technical requirements for this particular system were extracted and included in this document. While the requirements are described in DCID 6/3, a specific technical solution is not provided.

The technical security controls from the DCID 6/3 have been paraphrased with just the relevant technical parts of each section included. The technical security controls include: Access Control, Account Management, Auditing, Identification & Authentication, Least Privilege, Resource Control, Screen Lock, Session Controls, Documentation, System Assurance, Test, Backup Integrity, and Malcode. However, they have been slightly modified for readability. These specific controls were extracted from the many controls in the DCID 6/3. They satisfy the technical controls for a PL2, basic, basic system.

The DCID 6/3 technical security controls were mapped to the NSA guide in an effort to provide a Rosetta stone in this document. The NSA Guide is based on the Center for Internet Security (CIS) Benchmark guide, with some additional steps. All of the sections shown in the “Mapping of DCID 6/3 Security Requirements to NSA Guide to Securing Solaris Table” include a discussion section to map the hardening step to the DCID 6/3 technical security control.

Background

The system described throughout this document utilizes a client-server architecture with a high performance UNIX-based workstation that utilizes an X-Windows / Motif graphical user interface (GUI) with Common Desktop Environment (CDE).

The user utilizes a dedicated workstation connected via an isolated Local Area Network (LAN) to specialized pieces of equipment. The system resides in a restricted space and is operated by personnel that have previously undergone background investigations. The system is NOT on the Internet or any network, other that its own LAN.

The security requirements of the system fall under the purview of the Director Of Central Intelligence Directive 6/3, (which will be discussed shortly). The technical requirements for this particular system were extracted and included in this document. While the requirements are described in DCID 6/3, a specific technical solution is not provided.

The Center for Internet Security (CIS) develops a benchmark guide to harden various operating systems. The guides are available for many operating systems. Volunteers comprising of academia, industry, and government make up the teams that develop the guides. The National Security Agency bases its guide on the CIS guide, with some additional requirements. Since the NSA is a government organization and their guide was based on the CIS guide it was chosen to satisfy DCID 6/3 security requirements.

This document attempts to map the technical security requirements from DCID 6/3 to the NSA guide to secure Solaris. Although this document applies to a specific system, the methodology performed here should apply to any system that uses the DCID 6/3. After the security level was ascertained, the technical security requirements were distilled from the DCID 6/3. Then these requirements were mapped to specific security steps to ensure compliance. The NSA Guide, based on the CIS Benchmark, does not meet all of these controls, but it does meet many of them (depending on your security level) and would be considered “Industry Best Practices” and should be performed on any production system.

System Specifications

This server fulfills the role as the primary interface for specialized intelligence-based equipment.

Solaris 2.5.1

The fictitious system described throughout this document used the Solaris 2.5.1 operating system. It was not a new system like the Solaris 9 system described below, but was an existing system running multiple custom legacy software applications for which the source code was not always available. In addition, this software had a dependency on the Legacy DataCube Video Board.

The following ports and services are used for the system:

- *ssh (22/tcp)*
- *ftp (21/tcp)*
- *tftp (69/udp)*
- *rpcbind (111/tcp)*
- *sometimes-rpc7 (32772/tcp)*
- sometimes-rpc5 (32771/tcp)

Hardware

VME based system
Force CPU-50/T Single Board Computer with 128 MB RAM
DataCube Xi Turbo-24 + 8 Display System Video Board
Seagate Barracuda ST318418N 18.5 GB HD - SCSI

Using two hard drives (new hard drive and the backup hard drive), boot the original OS.

Solaris 9

The Solaris 9 system was specifically setup to test the NSA Guide, and contained no additional software.

Hardware

VME-based system
Force CPU-50/T Single Board Computer with 128 MB RAM
Peritek Display System Video Board
Seagate Barracuda ST318418N 18.5 GB Hard Drive

Hardening of the System

There are two kinds of users that use the system, operators and maintainers. The operators are considered normal users, and the maintainers are considered system administrators and have root privileges. The general operations of the system are such that if there are any major problems, a whole new hard drive with a complete backup of the system is swapped with the problem drive using removable hard drives. The users do not store any data to the system, but do require the ability to load data from CD-ROMs and Floppy disks.

The software development team is responsible for keeping the system updated with the latest operating system and software application patches and periodically release new software builds. The system uses removable hard drives, and they are swapped with the older drives as needed.

Operationally the audit logs are available for review by the system maintainers, and the software development team and other appropriate groups review the logs from the old drives periodically. There are special procedures for handling non-routine situations in which the logs may be needed.

Due to the fact that the system is deployed in a very restricted area, on a stand-alone network (not on the Internet), with specially cleared personnel, the likelihood of an unexpected change in the state of the system (e.g. listening to a new port or new daemon running) is extremely small. Security managers are available to the users and maintainers should a situation occur. The primary defense against any security problems is a combination of great training for the operators and maintainers, an outstanding software development team, and the implementation of the NSA Guide.

Assumptions

It is assumed that the reader is not familiar with the system discussed or any particular set of security or information assurance regulations. No specific details about the system or its operations are needed to understand how the NSA guide satisfies the technical requirements for the DCID 6/3.

The reader should be familiar with Unix system administration and the fundamentals of information assurance and security. Attempts were made to document any changes that deviated from the technical guidance provided by the NSA guide. Many of the scripts provided in the NSA Guide will not work perfectly. It is assumed that someone qualified to work on the Solaris operating system, and trusted with root privileges, is available to modify these scripts as needed. Many System Administrators may feel more comfortable manually entering the changes and modifications done by the scripts rather than run the scripts provided in the NSA Guide.

Also, the system described does not require many of the components that the DCID 6/3 addresses (i.e. web, mail servers, etc.) and are considered outside the scope of this document.

DCID 6/3

The Director Of Central Intelligence Directive 6/3 titled, ”Protecting Sensitive Compartmented Information Within Information Systems” is a manual that provides guidance and recommendations for protecting Sensitive Compartmented Information and special access programs for intelligence information systems.

It is a comprehensive security document that is based on the tenets of providing Confidentiality, Integrity, and Availability to an information system. The term “Levels-of-Concern” relate to Integrity and Availability and Protection Levels (PL) relate to Confidentiality.

With regard to Integrity, the Level-of-Concern rating is defined in the DCID 6/3 as, “the degree of resistance to unauthorized modification of the information maintained, processed, and transmitted by the IS [Information System] that is necessary for accomplishing the mission of its users.” The system discussed in this document requires Basic Integrity, which is defined as, “Reasonable degree of resistance required against unauthorized modification, or loss of integrity will have an adverse effect.”

To deal with the topic of Availability, the Level-of-Concern rating is defined in the DCID 6/3 as, “the degree of ready availability required for the information maintained, processed, and transmitted by the IS in order to accomplish the mission of its users.” The system discussed here requires Basic Availability, which is defined as, “Information must be available with flexible tolerance for delay, or loss of availability will have an adverse effect.” It is further noted that, “In this context, "flexible tolerance for delay" means that routine system outages do not endanger mission accomplishment; however, extended system outages (days to weeks) may endanger the mission.”

Since any system using the DCID 6/3 is highly classified, the data on the system must be protected with the highest measures for Confidentiality. These are broken into five categories, which are called Protection Levels or PL. They range from PL1 to PL5.

Lowest Clearance	Formal Access Approval	Need To Know	PL
At Least Equal to Highest Data	All Users Have ALL	All Users Have ALL	1
At Least Equal to Highest Data	All Users Have ALL	NOT ALL Users Have ALL	2
At Least Equal to Highest Data	NOT ALL users have ALL	Not Contributing to Decision	3
Secret	Not Contributing to Decision	Not Contributing to Decision	4
Uncleared	Not Contributing to Decision	Not Contributing to Decision	5

In a PL1 system, all of the system users would be cleared, with formal access and have a need to know. This is the ideal environment. For a PL2 system, all users would be cleared, with formal access, however at least one user would not have a need to know all information contained on the system. Most systems should try for one of these two protection levels. A PL3 system would have all users cleared, but at least one user would not have formal access, which makes need to know irrelevant. A PL3 system would need some extensive security controls in place to ensure the CIA of the system was maintained.

A PL4 or PL5 system would have users that are not cleared to the level of the system. There may be such a system, but most likely PL4 and PL5 were included for completeness or as an academic exercise. In either case, such a system would be so cost prohibitive that (if one exists) it would never be employed with real data.

The Designated Accreditation Authority (DAA) made the decision that the fictional system described throughout this document would be operated at a PL2 mode. The DCID 6/3 has hundreds of Security and Information Assurance controls that must be met for to certify a system at a PL2 / Basic / Basic level. What follows in the next section are just the technical controls for one particular information system.

The thrust of this document is to match as many DCID 6/3 technical controls as possible with the NSA Guide to the Secure Configuration of Solaris 8, which is based on the Center for Internet Security Benchmark guide, thus, allowing for a step-by-step approach to meet the DCID 6/3 technical security controls. It is recognized that these technical controls will not satisfy all of the security controls from the DCID 6/3 or the other relevant security laws, regulations, and policies that a DoD Information System must comply with. However, dealing with that falls outside the scope of this document.

The next section describes the technical security controls from the DCID 6/3. These controls include: Access Control, Account Management, Auditing, Identification & Authentication, Least Privilege, Resource Control, Screen Lock, Session Controls, Documentation, System Assurance, Test, Backup Integrity, and Malcode.

The comprehensive list of controls has been paraphrased from DCID 6/3 with just the relevant parts of each section included below, but has been slightly modified for readability. While there is no discussion after each control in this section, the controls are discussed in the NSA guide section. These specific controls were extracted from the many controls in the DCID 6/3. They satisfy the technical controls for a PL2, basic, basic system. A table that maps the DCID 6/3 technical security control to the NSA guide follows this section.

Access Control

> *Access control including:*
>
> *A Discretionary Access Control (DAC) Policy. A system has implemented DAC when the Security Support Structure defines and controls access between named users and named objects (e.g., files and programs) in the system.*
>
> *The DAC policy includes administrative procedures to support the policy and its mechanisms. The enforcement mechanisms (e.g., self / group / public controls, access control lists, communities of interest [COIs], encryption) shall allow users to specify and control sharing of those objects by named individuals, or by defined groups of individuals, or by both, and shall provide controls to limit propagation of access rights.*
>
> *The DAC mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.*

Account Management

> *Account Management procedures that include:*
>
> - *Identifying types of accounts (individual and group, conditions for group membership, associated privileges).*
> - *Establishing an account (i.e., required paperwork and processes).*
> - *Activating an account.*
> - *Modifying an account (e.g., disabling an account, changing privilege level, group memberships, authenticators).*
> - *Terminating an account (i.e., processes and assurances).*

Auditing

Auditing procedures, including:

- *Providing the capability to ensure that all audit records include enough information to allow the ISSO [Information System Security Officer] to determine the date and time of action (e.g., common network time), the system locale of the action, the system entity that initiated or completed the action, the resources involved, and the action involved.*
- *Protecting the contents of audit trails against unauthorized access, modification, or deletion.*
- *The system's creating and maintaining an audit trail that includes selected records of:*
  - *Successful and unsuccessful logons and logoffs*
  - *Accesses to security-relevant objects and directories, including opens, closes, modifications, and deletions.*
  - *Activities at the system console (either physical or logical consoles), and other system-level accesses by privileged users.*
- *Individual accountability (i.e., unique identification of each user and association of that identity with all auditable actions taken by that individual).*
- *Periodic testing by the ISSO or ISSM [Information System Security Manager] of the security posture of the IS by employing various intrusion / attack detection and monitoring tools. The ISSO/M shall not invoke such attack software without approval from the appropriate authorities and concurrence of legal counsel. The output of such tools shall be protected against unauthorized access, modification, or deletion.*

Identification & Authentication

Identification and Authentication, including:

- *An Identification and Authentication (I&A) management mechanism that ensures a unique identifier for each user and that associates that identifier with all auditable actions taken by the user.*

  {NOTE: [Alternative controls, such as biometrics or smart cards, may be used at the discretion of the DAA. These alternative methods may have similar requirements. For example, the electronically stored version of biometric authentication patterns needs to be protected, as do password authenticators.]}

- *Individual and Group Authenticators must be specified. (Group authenticators may only be used in conjunction with the use of an individual / unique authenticator, that is, individuals must be authenticated with an individual authenticator prior to use of a group authenticator).*
- *Length, composition, and generation of authenticators must be specified.*
- *Aging of static authenticators (i.e., not one-time passwords or biometric patterns) must be specified.*

- *History of static authenticator changes, with assurance of non-replication of individual authenticators, per direction in approved SSAA [System Security Authorization Agreement] must be specified.*

- *Protection of authenticators to preserve confidentiality and integrity must be specified.*

- *Identification and Authentication: In those instances where the means of authentication is user-specified passwords, the ISSO or ISSM may employ (under the auspices of the DAA) automated tools to validate that the passwords are sufficiently strong to resist cracking and other attacks intended to discover the users' password.*

Least Privilege

Least Privilege procedures, including:

The assurance that each user or process is granted the most restrictive set of privileges or accesses needed for the performance of authorized tasks shall be employed.

Resource Control

All authorizations to the information contained within an object shall be revoked prior to initial assignment, allocation, or reallocation to a subject from the Security Support Structure's pool of unused objects. No information, including encrypted representations of information, produced by a prior subject's actions is to be available to any subject that obtains access to an object that has been released back to the system. There must be no residual data from the former object.

Screen Lock

Unless there is an overriding technical or operational problem, a terminal / desktop / laptop screen-lock functionality shall be associated with each terminal / desktop / laptop computer. When activated, a screen-lock function shall place an unclassified pattern onto the entire screen of the terminal / desktop / laptop, totally hiding what was previously visible on the screen.

Screen Lock shall:

- *Be enabled either by explicit user action or if the desktop / terminal / laptop is left idle for a specified period of time (e.g., 15 minutes or more).*
- *Ensure that once the terminal / desktop / laptop security / screen-lock software is activated, access to the terminal / desktop / laptop requires knowledge of a unique authenticator.*

- *Not be considered a substitute for logging out (unless a mechanism actually logs out the user when the user idle time is exceeded).*

Session Controls

Session controls including:

- *Notification to all users prior to gaining access to a system that system usage may be monitored, recorded, and subject to audit. Electronic means shall be employed where technically feasible.*
- *Notification to all users that use of the system indicates (1) the consent of the user to such monitoring and recording and (2) that unauthorized use is prohibited and subject to criminal and civil penalties. Electronic means shall be employed where technically feasible.*

Enforcement of Session Controls, including:

- *Procedures for controlling and auditing concurrent logons from different workstations.*
- *Station or session time-outs, as applicable.*
- *Limited retry on logon as technically feasible.*
- *System actions on unsuccessful logons (e.g., blacklisting of the terminal or user identifier).*

Documentation

Documentation shall include guide(s) or manual(s) for the system's privileged users.

The manual(s) shall at a minimum provide information on:

- *Configuring, installing, and operating the system;*
- *Making optimum use of the system's security features; and*
- *Identifying known security vulnerabilities regarding the configuration and use of administrative functions.*
- *The documentation shall be updated as new vulnerabilities are identified.*

System Assurance

System Assurance shall include:

- *Features and procedures to validate the integrity and the expected operation of the security-relevant software, hardware, and firmware.*
- *Features or procedures for protection of the operating system from improper changes.*
- *Control of access to the Security Support Structure (i.e., the hardware, software, and firmware that perform operating system or security functions).*

- *Assurance of the integrity of the Security Support Structure.*

Test

The ISSM shall provide written verification to the DAA that the system operates in accordance with the approved SSAA, and that the security features, including access controls, configuration management, and discretionary access controls, are implemented and operational.

Backup

Backup procedures, including good engineering practice with regard to backup policies and procedures.

Integrity

Good engineering practice with regard to COTS [Commercial Off The Shelf] integrity mechanisms, such as parity checks and Cyclical Redundancy Checks (CRCs).

Malcode

Procedures to prevent the introduction of malicious code into the system, including the timely updating of those mechanisms intended to prevent the introduction of malicious code (e.g., updating anti-viral software).

Mapping of DCID 6/3 Security Requirements to NSA Guide to Securing Solaris Table

NSA Guide to the Secure Configuration of Solaris									
DCID 6 / 3 Technical Security Requirements		**1.0 Patches and Additional Software**	**2.0 Minimize inetd Network Services**	**3.0 Minimize Boot Services**	**4.0 Kernel Tuning**	**5.0 Logging**	**6.0 File / Directory Permissions / Access**	**7.0 System Access, Authentication, and Authorization**	**8.0 User Accounts and Environment**
	Access Control				4.7	5.7			8.6, 8.8
	Account Management					5.7			
	Auditing	1.6				5.6, 5.7, 5.8		7.11	
	Identification & Authentication					5.7	6.5	7.12	8.3, 8.5
	Least Privilege			3.2		5.7	6.9	7.9, 7.11	8.4, 8.6, 8.8
	Resource Control			3.23	4.1	5.8			
	Screen Lock							7.7	
	Session Controls	1.5		3.17		5.3		7.12	
	Documentation								
	System Assurance						6.7, 6.9		
	Test						6.7, 6.9		
	Backup								
	Integrity								
	Malcode			3.16			6.2, 6.6		8.8

The table shows the correlation between technical security control from the DCID 6/3 and the corresponding step from the NSA Guide that helps to satisfy that requirement. For example, the Screen Lock security controls are met with NSA Guide step 7.7. Some security controls only have one step like Account Management, while others are met with several steps from different sections of the NSA Guide. For example, steps 1.6, 5.6 – 5.8, and 7.11, meet the Auditing controls. In each step listed above, a description will be provided in that relevant step from the NSA Guide.

NSA Security Guide

Do not continue reading without having a copy of the NSA Security Guide open and available for reference at the same time you are viewing this document. If you do not have the NSA Security Guide, download it immediately from http://www.nsa.gov/snac/os/sunsol/Solaris8.pdf before proceeding.

For this section to make sense, the reader should download the NSA Security Guide, which is available from: http://www.nsa.gov/snac/os/sunsol/Solaris8.pdf. The following sections directly mirror the NSA Guide and should be viewed while looking at this document. The NSA Guide is based on the Center for Internet Security (CIS) Benchmark guide, with some additional steps. It should be noted that the CIS scoring tool, which is a script that checks to see if the recommended steps from the guide were followed and provide a score, will not check the additional steps listed in the NSA Guide.

The additional steps in the NSA Guide, but not in the CIS Benchmark guide are:

1.1 Partition hard drive to compartmentalize data
1.4 Install random number generator
1.6 Install NTP**
2.12 Disable multicasting and routing discovery
2.13 Disable IPv6
2.14 Enable encrypted remote administration if necessary
3.21 Disable BIND
3.22 Disable nscd
3.23 Use RMTMPFILES to clear /var/tmp**
4.7 Setup host based firewalls**
4.8 Set routing policies / configuration
5.7 Setup Role-Based Access Control**
6.3 Configure vold.conf to allow users access to CDs only**
8.2 Assign noshell for system accounts
8.10 Change user's .forward file to mode 600
8.14 Change root's home directory
8.15 Setup user file quotas

**Steps 1.6, 3.23, 4.7, 5.7, and 6.3 are used to help satisfy the technical security requirements from DCID 6/3.

The phrase, "this step should help to satisfy some of the [type of security control] requirements," is seen throughout this section of the document in the discussion area. Because each system is evaluated individually, what may satisfy requirements for one system may not satisfy the security requirements for another system. All of the sections shown in the "Mapping of DCID 6/3 Security Requirements to NSA Guide to Securing Solaris Table" include a discussion section to map the hardening step to the DCID 6/3 technical security control.

0 Initial Setup

0.0 Backup Key Files

Solaris 2.5.1

> Due to the difficulties in attempting to rebuild the system from scratch, a backup of the system was created and that backup was modified for testing of the NSA Guide. No individual files were backed up because the entire drive was backed up and saved as backup_image.tar.

Solaris 9

> Done per the directions.

Discussion:

Using a separate developmental system that includes a four-bay DataSilo with removable hard drives the backup was done as described below.

```
This was performed according to the following procedure:

1. Insert the disk in slot 0 of the DataSilo array.
2. Logout of the system.
3. Login to the system as "root".
4. Type the following commands:

   mount /dev/dsk/c1t0d0s0 /source_drive
   mount /dev/dsk/c1t0d0s5 /source_drive/opt
   /opt/tools/shell_scripts/make_backup_image

5. Verify that the backup image file exists. The file should be:

   /source_drive/opt/backup_image.tar

Once the backup image was made, the following operations were performed on two (2) hard
disks that were inserted in slots 1 and 2 of the DataSilo:

1. Verify that the hard disks were partitioned as follows:

   Partition "/" contained 3 GB of space.
   Partition "swap" contained 1 GB of space.
   Partition "5" contained the reset of the hard disk.

2. Once both drives had been verified as being appropriately partitioned, the following
commands were performed:

   newfs /dev/rdsk/c1t1d0s0
   newfs /dev/rdsk/c1t1d0s5
   newfs /dev/rdsk/c1t2d0s0
   newfs /dev/rdsk/c1t2d0s5
   mount /dev/dsk/c1t1d0s0 /clone_1
   mkdir /clone_1/opt
   mount /dev/dsk/c1t1d0s5 /clone_1/opt
   cd /clone_1
   tar -xvf /source_drive/opt/backup_image.tar
   mount /dev/dsk/c1t2d0s0 /clone_2
   mkdir /clone_1/opt
```

```
mount /dev/dsk/c1t2d0s5 /clone_2/opt
cd /clone_2
tar -xvf /source_drive/opt/backup_image.tar
installboot /usr/platform/sun4u/lib/fs/ufs/bootblk /dev/rdsk/c1t1d0s0
installboot /usr/platform/sun4u/lib/fs/ufs/bootblk /dev/rdsk/c1t2d0s0
cd /clone_1/opt
cp /source_drive/opt/backup_image.tar .
cd /clone_1/opt
cp /source_drive/opt/backup_image.tar .
cd /opt
cp /source_drive/opt/backup_image.tar ./CurrentVersion.tar
gzip CurrentVersion.tar
cd /
umount /clone_2/opt
umount /clone_1
umount /clone_1/opt
umount /clone_1
umount /source_drive/opt
umount /source_drive
```

The make_backup_image script described above follows:

```
#! /bin/sh
#
# FILE    : make_backup_image
#
# VERSION : 07/02/2002
#
# PURPOSE : The purpose of this shell script is to back up all the UFS file
#           systems.
#
# NOTE(S) :
#
#   1. The "tar" command can't handle 30K file names on a single command
#      line. But, it can handle them if they are passed to it in an
#      "include file".
#
#   2. All files in the "/dev" and "/devices" directories are filtered out
#      of the backup process. Also, all files in "./clipboard.clp" directories
#      are filtered out. These files have caused problems with the backup
#      process in the past.
#
#   3. The Solaris 2.5.1 tar command has been superseded by the GNU tar
#      command.
#

clear
echo Moving to the root directory
cd /source_drive

echo Running the GNU tar command.
echo Excluding the lost+found directories.
echo Excluding all core files.
echo Excluding the proc directory.

/usr/bin/tar \
 --create\
 --file=./opt/backup_image.tar\
 --exclude=./opt/backup_image.tar\
 --exclude=./cdrom/*\
 --exclude=./*/core\
```

```
 --exclude=./floppy/*\
 --exclude=./*/lost+found/*\
 --exclude=./proc/*\
 --exclude=./tmp/*\
 --exclude=./usr/tmp/*\
 --exclude=./var/mail/*\
 --verbose ./*

/bin/mt -f /dev/rmt/0 offline
echo All done!
```

The reason that tar was used instead of using ufsdump was because there was a known issues with ufsdump being limited to a 2GB partition under Solaris 2.5.1. A search of the internet with the search terms of "ufsdump to file 2gb limit" revealed the following message thread, which seems to confirm this: http://www.netsys.com/sunmgr/1997-10/msg00146.html *Another, message from Sun's site also seems to confirm this problem with a more recent date of August 2000:* http://forum.sun.com/thread.jsp?forum=10&thread=1746

1 Patches and Additional Software

1.1 Partition hard drive to compartmentalize data

Using a separate developmental system that includes a four-bay DataSilo with removable hard drives the procedures were completed as described below. This could also have been done using an Installation CD to boot from in Single User Mode. The instructions for how to do this can be found in the following manual from Sun. The manual is "SPARC: Installing Solaris Software," it can be downloaded from http://docs-pdf.sun.com/802-1959/802-1959.pdf

Solaris 2.5.1

Partition	Size
/	1 GB
/swap	1 GB – due to application requirements
backup	Invisible overlay of the whole drive
/opt	9.5 GB
/opt/users	2 GB (substitutes for /export/home)
/usr	3 GB (includes /usr/local)
/var	2 GB

Using the format command, the drive was partitioned.

"format" - initial program called
"partition" - moves you into the partition menu
"print" - to display the current partition table

There are 8 partitions available for Solaris and backup is on partition 2 by default.

Partition permission flags [wm] is default, which stands for Writeable and Mountable, respectively. The backup partition is [wu], which stands for Writeable and Unmountable. Since partition 7 was unused it had the flags [ru], which stands for Readable and Unmountable.

Cylinders and block size are calculated for you.

The finished partition table is presented below:

Part	Tag	Flag	Cylinders	Size
0	root	wm	0 – 1424	1.00 GB
1	swap	wu	1425 – 2849	1.00 GB
2	backup	wu	0 – 26431	18.55 GB
3	unassigned	wm	12424 – 26431	9.83 GB
4	unassigned	wm	2449 – 5298	2.00 GB
5	usr	wm	5299 - 9573	3.00 GB
6	var	wm	9574 – 12423	2.00 GB
7	unassigned	*ru*	0	0

Partitions 0,3,4,5 and 6 had newfs run on them to add the UFS filesystem to the partitions. The command was run by using “newfs /dev/rdsk/c0t2d0sX” where X corresponds with the Part (partition number.) For example, “newfs /dev/rdsk/c0t2d0s0” operates on the root partition.

- Mount all the file systems from the new drive so that the backup images could be restored to the new drive.

```
mount /dev/dsk/c0t2d0s0 /mnt

mkdir /mnt/opt
mkdir /mnt/usr
mkdir /mnt/var

mount /dev/dsk/c0t2d0s3 /mnt/opt
mount /dev/dsk/c0t2d0s5 /mnt/usr
mount /dev/dsk/c0t2d0s6 /mnt/var

mkdir /mnt/opt/users
mount /dev/dsk/c0t2d0s4 /mnt/opt/users
```

- restore the backup image

```
cd /mnt
tar -xvf /opt/backup_image.tar
```

- make sure the boot block is on the new drives

```
installboot /usr/platform/sun4u/lib/fs/ufs/bootblk /dev/rdsk/c0t2d0s0
```

modify the /etc/vsftab file as follows:

Device to mount	Device to fsck	Mount point	FS type	Fsck pass	Mount at boot	Mount options
fd	-	/dev/fd	fd	-	no	-

Device to mount	Device to fsck	Mount point	FS type	Fsck pass	Mount at boot	Mount options
/proc	-	/proc	proc	-	no	-
/dev/dsk/c0t3d0s1	-	swap	-	no	no	-
/dev/dsk/c0t3d0s0	/dev/rdsk/c0t3d0s0	/	ufs	1	yes	-
/dev/dsk/c0t3d0s3	/dev/rdsk/c0t3d0s3	/opt	ufs	1	yes	-
/dev/dsk/c0t3d0s4	/dev/rdsk/c0t3d0s4	/opt/users	ufs	1	yes	-
/dev/dsk/c0t3d0s5	/dev/rdsk/c0t3d0s5	/usr	ufs	1	yes	-
/dev/dsk/c0t3d0s6	/dev/rdsk/c0t3d0s6	/var	ufs	1	yes	-
swap	-	/tmp	tmpfs	-	yes	-

Partitions 3, 4 and 6 had to be added, and partition 5 had to be modified as show above.

- shutdown and remove old drive and boot from new drive

Solaris 9

Total disk cylinders available: 26432 + 2 (reserved cylinders)

Part	Tag	Flag	Cylinders	Size
0	root	wm	1426 - 2849	1023.50 MB
1	swap	wu	0 – 1424	1.00 GB
2	backup	wm	0 – 26431	18.55 GB
3	unassigned	wm	12822 – 26431	9.55 GB
4	unassigned	wm	5699 – 8547	2.00 GB
5	usr	wm	8548 – 12821	3.00 GB
6	var	wm	2850 - 5698	2.00 GB
7	unassigned	wm	0	0

1.2 Apply latest OS patches

Solaris 2.5.1

The 104489-15 OpenWindows 3.5.1: ToolTalk patch had previously caused problems with our video card, and had been omitted. Therefore, the ToolTalk patch was skipped and then

installed last, and the system worked as expected.

Solaris 9

Done per the directions.

1.3 Install TCP Wrappers

Solaris 2.5.1

Because the target system does not have a compiler environment, all compilation was done on a separate development machine.

Whenever possible the actual source code, and not pre-compiled binaries were used. The source code for tcp_wrappers_7.6.tar.bz2 was used. The gzip utility had to be added to the Solaris 2.5.1 and was used to gunzip tcp_wrappers.

After unzipping and untaring, “configure”, “make” was done to compile the source. The compiled program was manually installed by putting a copy of the 5 executables to /usr/local/sbin. The 5 executables are: safe_finger, tcpd, tcpdchk, tcpdmatch, and try-from.

The only deviation from step 6 was that:

{ $7 = $6; $6 = “/usr/local/bin/tcpd” }; \

to

{ $7 = $6; $6 = “/usr/local/sbin/tcpd” }; \

Solaris 9

Done per the directions.

1.4 Install Random Number Generator

Solaris 2.5.1

After step 1, the package was uncompressed using gunzip.
In step 2, the

```
pkgadd –d packagefile
```

command put the prngd file in /usr/local/sbin and not in /usr/local/bin where step 3 is expecting it. So, the following command had to be done:

```
mv /usr/local/sbin/prngd /usr/local/bin
```

Steps 3 and 4 were done per the directions, but replacing Solaris-7 with Solaris-2.5.1.

Solaris 9

No action needed.

1.5 Install SSH

Done per the directions for both Solaris 2.5.1 and Solaris 9.

Discussion:

This step should help to satisfy some of the session control and enforcement of session control requirements. SSH provides for session time-outs and limited retries for logging on to the system.

1.6 Install NTP

Done per the directions for both Solaris 2.5.1 and Solaris 9.

Discussion:

This step should help to satisfy some of the auditing requirements. Having a synchronized timeserver is one of the fundamental tenets of keeping good logs. The last thing an experienced or professional malicious cracker will do after compromising a system is to either, destroy or modify the log files in an attempt to cover his tracks. By using NTP, the date and time portion of auditing requirement should be met.

2 Minimize inetd Network Services

2.1 Disable standard services

Solaris 2.5.1

Manually edited /etc/inet/inetd.conf to comment out the following services:

Service	Endpoint type	Protocol	Wait status	UID	Server Program	Server arguments
time	stream	Tcp	nowait	root	internal	
time	dgram	Udp	wait	root	internal	
echo	stream	Tcp	nowait	root	internal	
echo	dgram	Udp	wait	root	internal	
discard	stream	Tcp	nowait	root	internal	
discard	dgram	Udp	wait	root	internal	
daytime	stream	Tcp	nowait	root	internal	
daytime	dgram	Udp	wait	root	internal	
chargen	stream	Tcp	nowait	root	internal	
chargen	dgram	Udp	wait	root	internal	
fs	stream	Tcp	wait	nobody	/usr/local/sbin/tcpd	/usr/openwin/lib/fs.auto
dtspc	stream	Tcp	nowait	root	/usr/local/sbin/tcpd	/usr/dt/bin/dtspcd
exec	stream	Tcp	nowait	root	/usr/local/sbin/tcpd	/usr/sbin/in.rexecd
comsat	dgram	Udp	wait	root	/usr/local/sbin/tcpd	/usr/sbin/in.comsat
talk	dgram	Udp	wait	root	/usr/local/sbin/tcpd	/usr/sbin/in.talkd
finger	steam	Tcp	nowait	nobody	/usr/local/sbin/tcpd	/usr/sbin/in.fingerd
uucpd	stream	Tcp	nowait	root	/usr/local/sbin/tcpd	/usr/sbin/in.uucpd
name	dgram	Udp	wait	root	/usr/local/sbin/tcpd	/usr/sbin/in.tnamed
100068/2-5	dgram	rpc/udp	wait	root	/usr/dt/bin/rpc.cmsd	rpc.cmsd
100221/1	tli	rpc/tcp	wait	root	/usr/openwin/bin/kems_server	kems_server
100232/10	tli	rpc/udp	wait	root	/usr/sbin/sadmind	sadmind
rstatd/2-4	tli	rpc /datagram_v	wait	root	/usr/lib/netsvc/rstat/rpc.rstatd	rpc.rstatd
ruserd/2-3	tli	rpc /datagram_v, circuit_v	wait	root	/usr/lib/netsvc/rusers/rpc.rusersd	rpc.rusersd
sprayd/1	tli	rpc / datagram_v	wait	root	/usr/lib/netsvc/spray/rpc.sprayd	rpc.sprayd
walld/1	tli	rpc / datagram_v	wait	root	/usr/lib/netsvc/rwall/rpc.rwalld	rpc.rwalld
shell	steam	Tcp	nowait	root	/usr/local/sbin/tcpd	/usr/sbin/in.rshd
login	stream	Tcp	nowait	root	/usr/local/sbin/tcpd	/usr/sbin/in.rlogind
telnet	stream	Tcp	nowait	root	/usr/local/sbin/tcpd	/usr/sbin/in.telnetd
ftp	stream	Tcp	nowait	root	/usr/local/sbin/tcpd	/usr/sbin/in.ftpd

Service	Endpoint type	Protocol	Wait status	UID	Server Program	Server arguments
tftp	dgram	Udp	wait	root	/usr/local/sbin/tcpd	/usr/sbin/in.tftpd -s /tfpboot
100083/1	stream	rpc/tcp	wait	root	/usr/dt/bin/rpc.ttdbserverd	rpc.ttdbserverd

The following services were not found in the file so were not commented out:

```
xaudio
100146
100147
100150
100155
100235
printer
100229
100230
100242
100234
100134
```

Solaris 9

The script did not seem to work correctly. The four scripts (for loops) had to be manually done by reading the script and then "commenting out" those services mentioned. The file permissions were then set manually.

Only 3 services remained:

```
(2) sun-dr tcpd
(1) 100153 sunvts
```

2.2 Only enable telnet if absolutely necessary

Disabled for both Solaris 2.5.1 and Solaris 9.

2.3 Only enable ftp if absolutely necessary

Disabled for both Solaris 2.5.1 and Solaris 9.

2.4 Only enable rlogin / rsh / rcp if absolutely necessary

Disabled for both Solaris 2.5.1 and Solaris 9.

2.5 Only enable TFTP if absolutely necessary

Disabled for both Solaris 2.5.1 and Solaris 9.

2.6 Only enable printer service if absolutely necessary

Disabled for both Solaris 2.5.1 and Solaris 9.

2.7 Only enable rquotad if absolutely necessary

Disabled for both Solaris 2.5.1 and Solaris 9.

2.8 Only enable CDE-related daemons if absolutely necessary

For both Solaris 2.5.1 and Solaris 9 there is a mission critical need for the GUI to be on the system, so the CDE-related daemons were left enabled.

2.9 Only enable Solaris Volume Manager Daemons if absolutely necessary

Disabled for both Solaris 2.5.1 and Solaris 9.

2.10 Only enable Kerberos-related daemons if absolutely necessary

Disabled for both Solaris 2.5.1 and Solaris 9.

2.11 Minimize inetd.conf file

Done per the directions for both Solaris 2.5.1 and Solaris 9.

2.12 Disable multicasting and routing discovery

This section was skipped due to the fact that ipfilters will be used for both Solaris 2.5.1 and Solaris 9.

2.13 Disable IPv6

Solaris 2.5.1

IPv6 is not available for Solaris 2.5.1, so this section was skipped.

Solaris 9

Done per the directions.

2.14 Enable encrypted remote administration if necessary

Skipped for both Solaris 2.5.1 and Solaris 9 because no remote administration is used.

3 Minimize Boot Services

3.1 Disable login: prompts on serial ports

Done per the directions for both Solaris 2.5.1 and Solaris 9.

3.2 Set daemon umask

Solaris 2.5.1

Two services were remaining in /etc/inetd.conf at this point: ftp and tftp. The umask.sh file was created in /etc/init.d/ and Symlinks were made by:

```
ls -s /etc/init.d/umask.sh /etc/rc0.d/s00umask.sh
ls -s /etc/init.d/umask.sh /etc/rc1.d/s00umask.sh
ls -s /etc/init.d/umask.sh /etc/rc2.d/s00umask.sh
ls -s /etc/init.d/umask.sh /etc/rc3.d/s00umask.sh
ls -s /etc/init.d/umask.sh /etc/rcS.d/s00umask.sh
```

Solaris 9

No action needed because 022 is the default setting.

Discussion:

This step should help to satisfy some of the least privilege requirements. By setting the umask to 022, daemon processes will now be created with the *NSA Guide's recommended* set of privileges.

3.3 Turn on inetd tracing, disable inetd if possible

Solaris 2.5.1

Edited /etc/init.d/inetsvc file and added "-t" to the last line as follows:

```
/usr/sbin/inetd -s -t
```

Rebooted the machine.

Solaris 9

Done per the directions.

Discussion:

Since other machines on the stand-alone network require ftp and tftp, inetd is required.

3.4 Prevent syslog from accepting messages from the network

Solaris 2.5.1

The "-t" flag was not implemented until Solaris 8, so some steps were not done. This is a breakdown of the steps followed:

(Skipped)
```
awk '$1 ~ /syslogd/ && !/-(t|T)/ { $1 = $1 " -t" }; \
        { print }' /etc/init.d/syslog >/etc/init.d/newsyslog
```

```
cp /etc/init.d/syslog /etc/init.d/syslog.old
```

(Skipped)
```
mv /etc/init.d/newsyslog /etc/init.d/syslog
```

```
chown root:sys /etc/init.d/syslog
chmod 744 /etc/init.d/syslog
rm -f /etc/rc2.d/S74syslog
ln -s /etc/init.d/syslog /etc/rc2.d/S74syslog
```

Solaris 9

Done per the directions.

Discussion:

The "-t" flag was not implemented until Solaris 8, so this step was not done. However as an alternative, blocking port UDP 514 in step 4.7 (Setup host based firewalls) should mitigate the risk of the system being flooded with irrelevant data.

3.5 Disable email server if possible

Solaris 2.5.1

The following steps were before starting the Action (Solaris 7 and earlier) section:
```
cd /etc/rc2.d
touch .NOS88sendmail
```

(the first line was modified from)
```
mv /etc/rc2.d/S88sendmail /etc/rc2.d/.NOS88sendmail
```

(to just)
```
mv /etc/rc2.d/.NOS88sendmail
```

Then the rest of the steps were followed.

Solaris 9

Done per the directions.

Discussion:

Sendmail was verified to be disabled by examining /etc/init.d.

3.6 Disable boot services if possible

Solaris 2.5.1

Edited /etc/init.d/nfs.server to comment out the line which start the tftp boot server and followed the rest of the instructions.

Solaris 9

Done per the directions.

3.7 Disable other standard boot services

Solaris 2.5.1

The notation NF means the file was “Not Found.” The tables follow the format found in the NSA Guide. The following table shows the files from /etc/rc2.d:

Filename	**/etc/rc2.d**
S72autoinstall	.NOS72autoinstall
S85power	NF
S89bdconfig	.NOS89bdconfig
S73cachefs.daemon	NF
S93cacheos.finish	.NOS93cacheos.finish
S40llc2	NF
S47pppd	NF
S47asppp	.NOS47asppp
S70uucp	.NOS70uucp
S72slpd	NF
S75flashprom	NF
S80PRESERVE	.NOS80PRESERVE
S89PRESERVE	NF
S90wbem	NF
S94ncalogd	NF
S95ncad	NF

The following table shows the files from /etc/rc3.d:

Filename	**/etc/rc3.d**
S77dmi	NF
S80mipagent	NF

The following table shows the files from /etc/rc2.d:

Filename	**/etc/rc2.d**
S73nfs.client	.NOS73nfs.client
S74autofs	.NOS74autofs
S71rpc	.NOS71rcp
S72directory	NF
S71ldap.client	NF
S80lp	.NOS80lp
S80spc	NF
S92volmgt	.NOS92volmgt
S91afbinit	NF
S91ifbinit	NF
S42ncakmod	NF

The “S99dtlogin” was left because it was needed to allow login to the CDE of the legacy device. A custom serial cable could be used to mitigate this.

The following table shows the files from /etc/rc3.d:

Filename	/etc/rc3.d
S90samba	NF
S15nfs.server	.NOS15nfs.server
S13kdc.master	NF
S14kdc	NF
S50apache	NF
S76snmpdx	NF
S34dhcp	NF

Solaris 9

Done per the directions with the following exceptions:

The “S71rpc” and “S99dtlogin” was left because it was needed to allow login to the CDE of the legacy device. “S92volmgt” which is needed to mount CD-ROMs and floppy disks was disabled, but will likely need to be turned on due to operational needs.

The following files were not found or differed from the NSA Guide:

```
S80PRESERVE
S95ncad
S47asppp
S92volmgt -> in /etc/rc3.d S81volmgt exists so this file was not changed.
```

3.8 Only enable Windows-compatibility servers if absolutely necessary

Not applicable for both Solaris 2.5.1 and Solaris 9.

3.9 Only enable NFS server processes if absolutely necessary

Currently not acting as a NFS fileserver. Believed not to be needed, so left disabled by default for both Solaris 2.5.1 and Solaris 9.

3.10 Only enable NFS client process if absolutely necessary

Currently not acting as a NFS fileserver. Believed not to be needed, so left disabled by default for both Solaris 2.5.1 and Solaris 9.

3.11 Only enable other RPC-based services if absolutely necessary

Not needed, so left disabled by default for both Solaris 2.5.1 and Solaris 9.

3.12 Only enable Kerberos server daemons if absolutely necessary

Not applicable, so left disabled by default for both Solaris 2.5.1 and Solaris 9.

3.13 Only enable directory server if absolutely necessary

Not applicable, so left disabled by default for both Solaris 2.5.1 and Solaris 9.

3.14 Only enable the LDAP cache manager if absolutely necessary

Not applicable, so left disabled by default for both Solaris 2.5.1 and Solaris 9.

3.15 Only enable the printer daemons if absolutely necessary

Not needed, so left disabled by default for both Solaris 2.5.1 and Solaris 9.

3.16 Only enable the volume manager if absolutely necessary

There is an operational requirement for users to mount CD-ROMs and floppy disks; however, this was left disabled by default for both Solaris 2.5.1 and Solaris 9. It will most likely be enabled during functional testing.

Discussion:

While it may provide a vector for an insider attacker to deliver malicious code to the system, this threat is countered by the fact that all the personnel are highly trained and have undergone extensive background checks. Additionally, the legacy software and operational environment requires the users to be able to mount CD-ROMs and floppy disks.

3.17 Only enable GUI login if absolutely necessary

The GUI login was enabled due to operational requirements of the system for both Solaris 2.5.1 and Solaris 9.

Discussion:

This step should help to satisfy some of the session control requirements. The X Windows-based CDE GUI weakness is countered because the system is on a stand-alone network. A warning banner is provided, in which the user must accept the terms of the banner BEFORE allowed access to the machine. This should provide the adequate "notification to all users prior to gaining access to a system that system usage may be monitored, recorded, and subject to audit. Electronic means shall be employed where technically feasible. Notification to all users that use of the system indicates (1) the consent of the user to such monitoring and recording and (2) that unauthorized use is prohibited and subject to criminal and civil penalties," as required by the DCID 6/3

3.18 Only enable Web server if absolutely necessary

Not applicable, so left disabled by default for both Solaris 2.5.1 and Solaris 9.

3.19 Only enable SNMP if absolutely necessary

Not applicable, so left disabled by default for both Solaris 2.5.1 and Solaris 9.

3.20 Only enable DHCP server if absolutely necessary

Not needed, so left disabled by default for both Solaris 2.5.1 and Solaris 9.

3.21 Disable BIND

Solaris 2.5.1

> Step 1) There is no /etc/init.d/named.script and DNS was not started. The following lines were commented out of /etc/init.d/inetsvc:

```
if [ -f /usr/sbin/in.named –a –f /etc/named.boot ]; then
      /usr/sbin/in.named;      echo “Starting internet domain name server.”
fi
```

Then the chown root:sys inetsvc and chown 744 inetsvc commands were run. Steps 2 and 3 were then followed.

Solaris 9

Done per the directions.

3.22 Disable nscd

Solaris 2.5.1

Done per the directions, however, S76nscd was changed to .NOS76nscd

Solaris 9

Done per the directions.

3.23 Use RMTMPFILES to clear /var/tmp

Solaris 2.5.1

Done per the directions, however, line 78 (EXIT) in /etc/init.d/RMTMPFILES was commented out.

Solaris 9

Done per the directions.

Discussion:

This step should help to satisfy some of the resource control requirements.

> *“All authorizations to the information contained within an object shall be revoked prior to initial assignment, allocation, or reallocation to a subject from the Security Support Structure’s pool of unused objects. No information, including encrypted representations of information, produced by a prior subject’s actions is to be available to any subject that obtains access to an object that has been released back to the system. There must be no residual data from the former object.” DCID 6/3.*

While this would not meet the entire security control, which would require a trusted operating system, it certainly helps to reduce the risk of leaving behind residual data. Any files put in the /var/tmp directory can potentially be viewed by other users on the system; this control helps to mitigate that risk.

4 Kernel Tuning

4.1 Disable core dumps

Done per the directions for both Solaris 2.5.1 and Solaris 9.

Discussion:

This step should help to satisfy some of the resource control requirements. Like 3.23 above, complete implementation of this control would require a trusted operating system. Core dumps can contain sensitive data, which would violate the tenant of confidentiality, by preventing core dumps on operational systems this much of this risk is mitigated.

4.2 Enable stack protection

Done per the directions for both Solaris 2.5.1 and Solaris 9.

4.3 Restrict NFS client requests to privileged ports

Done per the directions for both Solaris 2.5.1 and Solaris 9.

4.4 Modify network parameters

Done per the directions for both Solaris 2.5.1 and Solaris 9.

4.5 Modify additional network parameters

Done per the directions for both Solaris 2.5.1 and Solaris 9.

4.6 Use better TCP sequence numbers

Solaris 2.5.1

> *The use of better TCP sequence numbers was not implemented by Sun for Solaris 2.5.1. The Solaris™ Operating Environment Network Settings for Security BluePrints (http://www.sun.com/blueprints/1299/network.pdf) on page 18 states, "Unfortunately, Solaris 2.5.1 software does not offer the RFC 1948 method and there are no plans to backport it." However, the "improved method with random increment value, TCP_STRING_ISS = 1, was used as the short-term risk mitigation strategy. The long-term strategy is to migrate to a more modern version of Solaris.*
>
> *The following steps in the BluePrint were followed to help mitigate network risks; these steps were not covered in section 4.4 Modify Network Parameters or section 4.5 Modify Additional Network Parameters:*
>
> ```
> ndd -set /dev/ip ip_respond_to_echo_broadcast 0
> ndd -set /dev/tcp tcp_conn_req_max_q 1024
> ndd -set /dev/tcp tcp_smallest_nonpriv_port 2050
> ```

Solaris 9

> Done per the directions.

4.7 Setup host based firewalls

Solaris 2.5.1

Installed ipfilters version 4.1.3, which was obtained from: http://coombs.anu.edu.au/~avalon/

Added the additional rule to block unwanted rcommands (from section 7.1):

```
block return-rst in log first level auth.warn quick on hme0 proto tcp from any to any \
port=512 #rexec

block return-icmp(port-unr) in log first level auth.warn quick on hme0 proto udp from \
any to any port=512 #comsat & biff

block return-rst in log first level auth.warn quick on hme0 proto tcp from any to any \
port=513 #rlogin

block return-icmp(port-unr) in log first level auth.warn quick on hme0 proto udp from \
any to any port=513 #who

block return-rst in log first level auth.warn quick on hme0 proto tcp from any to any \
port=514 #rsh
```

Added the additional rule to block unwanted syslog traffic (from section 3.4):

```
block return-icmp(port-unr) in log first level auth.warn quick on hme0 proto udp from \
any to any port=514 #syslog
```

Solaris 9

Installed ipfilters version 4.1.3.

Discussion:

This step should help to satisfy some of the discretionary access control requirements. Ipfilters provides an access control list, which would help to mitigate a malicious insider putting a rouge machine on the stand-alone network.

4.8 Set routing policies / configuration

Since the machine was not acting as a router this step was left disabled by default for both Solaris 2.5.1 and Solaris 9.

5 Logging

5.1 Capture messages sent to syslog AUTH facility

Done per the directions for both Solaris 2.5.1 and Solaris 9.

5.2 Capture FTP and inetd connection tracing info

Done per the directions for both Solaris 2.5.1 and Solaris 9.

5.3 Create /var/adm/loginlog

Done per the directions for both Solaris 2.5.1 and Solaris 9.

Discussion:

This step should help to satisfy some of the enforcement of session control requirements. This step will meet some of the control requirement, namely logging the unsuccessful logons. While this will not create the denial-of-service effect that blacklisting the terminal or user would provide, this should be argued (again due to the environment that this system is deployed) to be “good enough” when combined with periodic reviews of this log file.

5.4 Turn on cron logging

Solaris 2.5.1

> No changes required. The /etc/default/cron file already had "CRONLOG=YES" in it...

Solaris 9

> Done per the directions.

5.5 Enable system accounting

Done per the directions for both Solaris 2.5.1 and Solaris 9.

5.6 Enable kernel-level auditing

Done per the directions for both Solaris 2.5.1 and Solaris 9, however for Solaris 2.5.1 the line "/var/spool/cron/crontab/root" had to be manually added to the crontab from step 3.

Discussion:

This step should help to satisfy some of the auditing requirements. The Basic Security Module (BSM) will provide auditing data and it will allow the ISSO to determine when an event occurred, show logons, access to files, and individual and privileged users activities. It may be necessary to “tune down” the level and events that are actually audited as the data tends to get rather large very quickly. It would be a good idea to discuss this with whoever is able to make decisions about exactly how much data is needed (i.e. the DAA for the system.)

5.7 Setup Role-Based Access Control

Done per the directions for both Solaris 2.5.1 and Solaris 9.

Discussion:

This is an extremely important step because it helps to satisfy many different security control requirements including: auditing, access control, account management, identification and authentication, and least privilege. While this step just sets up the audit account for monitoring the audit logs, it facilitates many different security controls.

Since role-based access controls allow the systems administrator to configure the granularity of access to system resources down to the individual level, it is the primary tool for enforcing the principles of least privilege. This control allows a normal user to use the “su” command to change his role and increase his level of access to the system resources.

This step helps to ensure the audit trails are protected, and that a users activity is logged, including when they elevate their privileges. It also provides for the individual accountability that is required by the DCID 6/3 security controls. It also works toward satisfying the discretionary access control policy by enabling the enforcement mechanisms the ability to function in a granular enough mode to audit individuals on the system.

While it does not provide any procedural or process based functions, it does facilitates the controls that require them. It allows for identifying, establishing, activating, modifying, and terminating user accounts and group memberships. This step also ensures that a unique UserID is created for each user and user-role (like auditing.)

5.8 Confirm permissions on system log file

Both Solaris 2.5.1 and Solaris 9 had the following problems with the directions. The "/var/log/syslog" and "/var/adm/wtmpx" files were not on the system and had to be created. Also, the "/var/adm/sa" directory was not on the system and had to be created.

Discussion:

This step should help to satisfy some of the auditing and resource control requirements. This clearly meets the control for “protecting the contents of audit trails against unauthorized access, modification, or deletion.” In addition, and as discussed previously, it helps in meeting the resource control requirement. This may be an instance where the defense-in-depth can occur as a substitute for a trusted operating system. By layering many different steps together the system begins to take on some of the important characteristics of a trusted operating system. This combination of factors (seen as steps from the NSA Guide) works to make the system’s resource controls more secure, even though it is not a trusted operating system.

6 File / Directory Permissions / Access

6.1 Add 'logging' option to root file system

Done per the directions for both Solaris 2.5.1 and Solaris 9.

6.2 Add 'nosuid' option to /etc/rmmount.conf

Done per the directions for both Solaris 2.5.1 and Solaris 9.

Discussion:

This step should help to satisfy some of the malicious code requirements. Since there is a system requirement to allow users to be able to mount CD-ROMs and floppy disks, this should work to mitigate some of that risk. For example, if a user has root privileges on a machine (for example their own Linux or Solaris x86 machine) and copies a program such as “bash” (which is a shell) onto a CD-ROM and that program has its setuid bit set, that user could mount and execute that file with root privileges on a system in which that user only has normal user privileges. However, this step prevents users from doing that.

6.3 Configure vold.conf to allow users access to CD's only

Done per the directions for both Solaris 2.5.1 and Solaris 9.

Discussion:

However, this will most likely be changed when the system goes to functional testing because there is an operational requirement for users to be able to mount CD-ROMs and floppy disks for this system.

6.4 User full path names in /etc/dfs/dfstab file

Done per the directions for both Solaris 2.5.1 and Solaris 9.

6.5 Verify passwd, shadow, and group file permissions

Done per the directions for both Solaris 2.5.1 and Solaris 9.

Discussion:

This step should help to satisfy some of the identification and authentication requirements. Namely, it should satisfy the “protection of authenticators to preserve confidentiality and integrity,” security control.

6.6 Verify world-writable directories have their sticky bit set

Done per the directions for both Solaris 2.5.1 and Solaris 9.

Discussion:

This step should help to satisfy some of the malicious code requirements. By enforcing the sticky bit, the operating system will ensure that only the owner of a file can remove a file from a world-writable directory. This step helps to prevent the introduction of malicious code because only the file owner can delete a file, making it difficult for a malicious user to replace that file with a Trojan horse replacement.

6.7 Find unauthorized world-writable files

Done per the directions for both Solaris 2.5.1 and Solaris 9.

Discussion:

This step should help to satisfy some of test and system assurance requirements. This step helps to make sure the operating system is more resistant to changes (integrity) and potential inadvertent disclosure of data (confidentiality.) It also provides the ISSM a list of files that could be included in a report to the DAA.

6.8 Find unauthorized SUID / SGID system executables

Done per the directions for both Solaris 2.5.1 and Solaris 9.

Discussion:

The tool ADEOS does everything in sections 6.7 and 6.8 and is run as an unprivileged user. It is available from:

http://linux.wku.edu/~lamonml/software/adeos/ or
http://freshmeat.net/projects/adeos/

6.9 Run fix-modes

Done per the directions for both Solaris 2.5.1 and Solaris 9.

Discussion:

This is an extremely important step because it helps to satisfy many different security control requirements including least privilege, system assurance and testing. The fix-modes software ensures that programs used have the correct and therefore the least privileges they need. It also, validates the expected levels of permissions for the operating system software including the security software and provides the ISSM with output that can be reported to the DAA.

7 System Access, Authentication, and Authorization

7.1 Remove .rhosts support in /etc/pam.conf

Solaris 2.5.1

Since PAM was not implemented until Solaris 2.6 and .rhosts files are not used on the system, the following modified steps were done for this section:

```
cd /etc
touch pam.conf
chown root:sys pam.conf
chmod 644 pam.conf
```

In step 4.7 the rules to block unwanted ports 512 through 514 were implemented to mitigate the risks of not having PAM implemented in Solaris 2.5.1. This was recommended in the NSA guide as a way to control the use of .rhosts files.

In addition, the following was done to link the .rhosts, .shosts, and hosts.equiv files to /dev/null to help reduce the residual risks further:

```
ln –s /dev/null /etc/hosts.equiv
ln –s /dev/null /.rhosts
ln –s /dev/null /.shosts

chown root:sys /etc/hosts.equiv
chown root:sys /.rhosts
chown root:sys /.shosts

chmod 644 /etc/hosts.equiv
chmod 644 /.rhosts
chmod 644 /.shosts
```

For each account with a "home" directory the following was done:

```
ln –s /dev/null <path to home directory>/.rhosts
ln –s /dev/null <path to home directory>/.shosts

chown root:sys <path to home directory>/.rhosts
chown root:sys <path to home directory>/.shosts

chmod 644 <path to home directory>/.rhosts
chmod 644 <path to home directory>/.shosts
```

Solaris 9

Done per the directions.

7.2 Create symlinks for dangerous files

Done per the directions.

7.3 Create /etc/[/ftpd]/ftpusers

Solaris 2.5.1

Manually edited the “/etc/ftpusers” file because it did not appear to exist on Solaris 2.5.1to block ftp access from the following users:

```
root
audit
daemon
bin
sys
adm
lp
smtp
uucp
nuucp
listen
nobody
noaccess
nobody4
shutdown
```

Solaris 9

Done per the directions.

7.4 Create /etc/shells

Done per the directions for both Solaris 2.5.1 and Solaris 9.

7.5 Prevent remote XDMCP access

Done per the directions for both Solaris 2.5.1 and Solaris 9.

7.6 Prevent X server from listening on port 6000/tcp

Solaris 2.5.1

Implementation of this step caused the system not to display the CDE login prompt. This section had to be undone; therefore this section is still not implemented.

However, to mitigate the risk, step 4.7 Setup Host Based Firewalls includes a rule to block Xserver (tcp ports 5999 through 6005).

Solaris 9

Done per the directions.

7.7 Set default locking screensaver timeout

Solaris 2.5.1

The "/usr/dt/config/C/sys.resources" file was modified by hand and the following lines were added:

```
dtsession*saverTimeout: 10
dtsession*lockTimeout: 10
```

Solaris 9

Done per the directions.

Discussion:

This step should help to satisfy the screen lock requirements. The DCID 6/3 states, “when activated, a screen-lock function shall place an unclassified pattern onto the entire screen of the terminal / desktop / laptop, totally hiding what was previously visible on the screen.” It is important to make sure the screen saver completely blanks out the screen, for example the “melting screen” still allows someone to view parts of the screen while active. A local policy defining what screen savers are permitted may be appropriate. This step should also satisfy the requirement of having a screen saver enabled after 15 minutes or more and requiring a password to gain access to the terminal again.

7.8 Restrict at /cron to authorized users

Done per the directions for both Solaris 2.5.1 and Solaris 9.

7.9 Remove empty crontab files and restrict file permissions

Done per the directions for both Solaris 2.5.1 and Solaris 9.

Discussion:

This step should help to satisfy the least privilege requirements because unprivileged users do not need to be able to view or modify system crontab files.

7.10 Create appropriate warning banners

Done per the directions for both Solaris 2.5.1 and Solaris 9. However, the custom warning banner that is displayed using a Tcl/Tk script that runs at boot time addresses this section.

Discussion:

This step should help to satisfy the session control requirements because the system provides a warning banner that gives the proper notice to users about monitoring, recording, and auditing of all actions the users takes on the system and that the user is consenting to this and acknowledges that any unauthorized use is prohibited.
As discussed in section 3.17, this step should help to satisfy the session control requirements. The source code for this script is included below:

#!/usr/local/bin/wish

```
# ************************************************************************
# *
# * FILE
# *
# * VERSION
# *
# * PURPOSE   : The purpose of this Tcl/Tk script is to implement the mandatory
# *             Navy AIS (Account Information Security) Warning Banner that is
# *             required to be displayed to all those logging into the system.
# *
# * INPUT(S)  : None...
# *
# * OUTPUT(S) : None...
# *
# * HISTORY
# *
# ************************************************************************
```

```
#
# Step 1 : Build the window and display it.
#

wm title . "Navy AIS Warning Banner"

label .aisTitle \
  -font lucidasans-bold-24 \
  -justify center \
  -padx 4 \
  -pady 4 \
  -text "Navy AIS Warning"

label .aisText \
  -font lucidasans-18 \
  -justify left \
  -padx 4 \
  -pady 4 \
  -text "\n\
This is a Department Of Defense computer system.\n\
This computer system, including all related equipment,\n\
networks and network devices (specifically  including\n\
internet access), are provided only for authorized\n\
U.S. Government use. DoD computer systems may be\n\
monitored for all lawful purposes, including to ensure\n\
that their use is authorized, for management of the\n\
system, to facilitate protection against unauthorized\n\
access, and to verify security procedures, survivability\n\
and operational security. Monitoring includes active\n\
attacks by authorized DoD entities to test or verify\n\
the security of this system. During monitoring,\n\
information may be examined, recorded, copied and used\n\
for authorized purposes. All information, including\n\
personal information, placed on or sent over this\n\
system may be monitored. Use of this DoD computer\n\
system, authorized or unauthorized, constitutes consent\n\
to monitoring of this system. Unauthorized use may\n\
subject you to criminal prosecution. Evidence of\n\
unauthorized use collected during monitoring may be\n\
used for administrative, criminal or adverse action.\n\
Use of this system constitutes consent to monitoring\n\
for these purposes.\n\
\n\
If you wish to continue using this system, please\n\
press the \"Continue\" button. If you wish to stop\n\
using this sytem, please press the \"Exit\" button.\n\
\n"

frame .buttonFrame

button .buttonFrame.okButton \
  -command exit \
  -font lucidasans-bold-18 \
  -padx 4 \
  -pady 4 \
  -text "Continue" \
  -underline 0 \
  -width 8

button .buttonFrame.notokButton \
  -command byebye \
  -font lucidasans-bold-18 \
```

```
  -padx 4 \
  -pady 4 \
  -text "Exit" \
  -underline 0 \
  -width 8

bind . <KeyPress-c> {exit}
bind . <KeyPress-C> {exit}
bind . <KeyPress-e> {byebye}
bind . <KeyPress-E> {byebye}

grid configure .buttonFrame.okButton -column 1 -row 1 -pady 4 -sticky "nws"
grid configure .buttonFrame.notokButton -column 2 -row 1 -pady 4 -sticky "nes"

pack .aisTitle
pack .aisText
pack .buttonFrame

# additional interface code
tkwait visibility .
set sHeight [winfo screenheight .]
set sWidth [winfo screenwidth .]
set wHeight [winfo height .]
set wWidth [winfo width .]
set xpos [expr $sHeight - $wHeight]
set xpos [expr $xpos / 2]
set ypos [expr $sWidth - $wWidth]
set ypos [expr $ypos / 2]
set times x
set myGeom [concat $wWidth$times$wHeight+$ypos+$xpos]
wm geometry . $myGeom
# end additional interface code

proc byebye { } {
  if { [ file exists /usr/local/bin/which ] == 1 } {
    set whichCommand "/usr/local/bin/which"
  } else {
    set whichCommand "/usr/bin/which"
  }
  set grepCommand [exec $whichCommand grep]
  set killCommand [exec $whichCommand kill]
  set psCommand [exec $whichCommand ps]
  set whoamiCommand [exec $whichCommand whoami]
  set username [exec $whoamiCommand]
  set processString [exec /usr/proc/bin/ptree $username]
  set processList [split $processString]
  set previousToken ""
  for {set index 0} {$index < [llength $processList]} {incr index 1} {
    set currentToken [lindex $processList $index]
    if { [string length $currentToken] != 0 } {
      if { [string first "Xsession" $currentToken] != -1} {
        set psResult [exec $psCommand -ef | $grepCommand "$previousToken"]
        set psSplit [split $psResult]
        for {set index2 0} {$index2 < [llength $psSplit]} {incr index2 1} {
          set dummyString [lindex $psSplit $index2]
          if { [string length $dummyString] != 0 } {
            if { [string compare $username $dummyString] == 0 } {
              set dummy [exec $killCommand -9 $previousToken]
            }
          }
        }
      } else {
```

```
        set isNumber "1"
        for {set index1 0} {$index1 < [string length $currentToken]} {incr index1 1} {
          if { [string index $currentToken $index1] >= "0" } {
            if { [string index $currentToken $index1] > "9" } {
              set isNumber "0"
            }
          } else {
            set isNumber "0"
          }
        }
        if { [string compare $isNumber "1"] == 0 } {
          set previousToken $currentToken
        }
      }
    }
  }
}
```

7.11 Restrict root logins to system console

Done per the directions for both Solaris 2.5.1 and Solaris 9.

Discussion:

This step should help to satisfy the auditing and least privilege requirements. By forcing root to first logon to the system as a normal user, individual accountability is achieved because the normal user must su or sudo to run with elevated privileges. This leaves a good audit trail for the ISSO. This also reinforces the concept of least privilege, because the most restrictive set of accesses are employed.

7.12 Limit number of failed login attempts

Done per the directions for both Solaris 2.5.1 and Solaris 9.

Discussion:

Done per the directions for both Solaris 2.5.1 and Solaris 9.

7.13 Set EEPROM security-mode and log failed access

Done per the directions for both Solaris 2.5.1 and Solaris 9.

8 User Accounts and Environment

8.1 Block system accounts

Solaris 2.5.1

The "passmgmt" command was run manually to change the shell used by the following users:

```
bin
adm
lp
smtp
uucp
nuucp
listen
nobody
noaccess
nobody4
```

The command used was:

```
passmgmt -m -s /dev/null [username]
```

Solaris 9

Done per the directions with the following results:

```
Results: There was no smtp as seen below.
passwd: password information changed for adm
passwd: password information changed for bin
passwd: password information changed for lp
passwd: password information changed for smmsp
passwd: password information changed for nobody
passwd: password information changed for noaccess
passwd: password information changed for uucp
passwd: password information changed for nuucp
Permission denied
/usr/sbin/passmgmt: name does not exist
passwd: password information changed for listen
passwd: password information changed for nobody4
```

8.2 Assign noshell for system accounts

Done per the directions for both Solaris 2.5.1 and Solaris 9.

8.3 Set account expiration parameters on active accounts

Solaris 2.5.1

The "passwd" command was manually used to change the min, max and warning values for the following accounts:

```
bin
lp
smtp
uucp
nuucp
nobody
```

```
noaccess
nobody4
shutdown
```

The root, audit, daemon, sys and listen were left as is.

Solaris 9

Done per the directions.

Discussion:

As suggested in the NSA guide, and since there were a limited number of users they were individually setup with the following commands:

```
usermod -f 30 <login>
```

where <login> was replaced with the correct username. This expired idle accounts after 30 days of inactivity.

```
usermod -e <date> <login>
```

Where <date> was replaced with the date the account should expire on.

The passwd program for Solaris 2.5.1 has the following features:

> *Passwords must be constructed to meet the following require-ments:*
>
> - *Each password must have PASSLENGTH characters, where PASSLENGTH is defined in /etc/default/passwd and is set to 6. Only the first eight characters are signifi-cant.*
> - *Each password must contain at least two alphabetic characters and at least one numeric or special charac-ter. In this case, "alphabetic" refers to all upper or lower case letters.*
> - *Each password must differ from the user's login name and any reverse or circular shift of that login name. For comparison purposes, an upper case letter and its corresponding lower case letter are equivalent.*
> - *New passwords must differ from the old by at least three characters. For comparison purposes, an upper case letter and its corresponding lower case letter are equivalent.*

Quoted from Solaris 2.5.1 man page for the passwd program: http://www.cs.virginia.edu/cgi-bin/manpage?section=all&topic=passwd. The man pages for Solaris 2.5.1 are available online from: http://www.cs.virginia.edu/cgi-bin/manpage.

8.4 Verify no legacy '+' entries exist in passwd, shadow, and group files

Done per the directions for both Solaris 2.5.1 and Solaris 9.

8.5 Verify that there are no accounts with empty password fields

Done per the directions for both Solaris 2.5.1 and Solaris 9.

Discussion:

This step should help to satisfy the identification and authentication requirements by ensuring that all accounts have passwords. Without this step, any user would be able to log into an account without needing to provide a password.

8.6 Verify that no UID 0 accounts exist other than root and audit

Done per the directions for both Solaris 2.5.1 and Solaris 9.

Discussion:

This step should help to satisfy the access control and least privilege requirements. Because superuser accounts have a UID 0 and by forcing normal users to “su” to root, the principles of least privilege are enforced because users only have the absolute minimum amount of privileges they need to complete their work. This discretionary access control allows the system to have the granularity of controls to the user level, needed to meet the DCID 6/3 security requirements.

8.7 Disallow '.' or group / world-writable directory in root $PATH

Done per the directions for both Solaris 2.5.1 and Solaris 9.

8.8 Set user home directories to mode 750 or more restrictive

Done per the directions for both Solaris 2.5.1 and Solaris 9.

Discussion:

This step should help to satisfy the access control, least privilege, and malcode requirements. By setting the default permissions on user’s home directories to 750 the discretionary access controls are enabled to limit access to a specific users files within that directory. This helps to satisfy both the discretionary access and least privilege controls. Furthermore, it makes it more difficult for a malicious user to add or modify files that do not belong to that user.

8.9 Disallow group / world-writable user dot-files

Done per the directions for both Solaris 2.5.1 and Solaris 9.

8.10 Change user's .forward file to mode 600

Done per the directions for both Solaris 2.5.1 and Solaris 9, however a search of the whole hard disk for any files named ".forward" returned no results because there is no mail on this system.

8.11 Remove user .netrc files

Done per the directions for both Solaris 2.5.1 and Solaris 9.

8.12 Set default UMASK for users

Done per the directions for both Solaris 2.5.1 and Solaris 9.

8.13 Set “mesg n” as default for all users

Done per the directions for both Solaris 2.5.1 and Solaris 9.

8.14 Change root's home directories

Done per the directions for both Solaris 2.5.1 and Solaris 9.

8.15 Setup user file quotas

This step was not implemented. Several questions would need to be answered when the system is in functional testing before quotas could be established. These questions include:

- How much hard drive space should individual user accounts be allocated?
- Should we give individual users different directories / file systems for different functions?
- How do we make sure the user has the necessary disk space to store data?

Once the hardened system can be analyzed in functional testing these types of questions can be answered.

Conclusions

The DCID 6/3, “Protecting Sensitive Compartmented Information Within Information Systems” is the overarching security manual used to protect highly classified intelligence information systems. With regard to hardening an operating system, the security controls are tightly intertwined throughout the DCID 6/3 manual. This document focused on just the technical security controls from DCID 6/3 as they apply to a fictional information system using Solaris 2.5.1 and also compared with a base-installation of Solaris 9. A discussion was presented to show how each step tracks in the, “Mapping of DCID 6/3 Security Requirements to NSA Guide to Securing Solaris Table.” The security controls from the National Security Administration’s (NSA) “Guide to the Secure Configuration of Solaris”, are based on the Center for Internet Security’s (CIS) “Solaris Benchmark.”

A system administrator following the NSA Guide should satisfy many of the DCID 6/3 security requirements. However, the discussion area was phrased “should help to satisfy”, because each system is different and the final approval of the system is for the DAA to decide. Certainly the steps in the NSA Guide are good “best practices” and should be implemented whenever possible.

There are still some areas that were not covered even with the recommendations in the NSA Guide that may be needed for your particular system’s security implementation. For example, no real file integrity software is employed like tripwire or creating a MD5 sum of critical files. *A good tool that could be used to check for unexpected changes in the system configuration is called AFICK. AFICK stands for Another File Integrity Checking (tool) and can be found at: http://afick.sourceforge.net/.* Also, log rotation is discussed, but the length of time the logs need to be archived is outside the scope of the NSA Guide. *A good tool that could be used to help ensure the regular review of log files is called Swatch and can be found at http://swatch.sourceforge.net/.*

The system will still have to be fine-tuned and the security changes will have to be verified and validated. This testing, including regression testing, will take place during the functional testing. This is an important point, because just having a System Administrator implement the NSA Guide will not make your system secure without training, testing and verifying the changes have been implemented correctly. For example, some of the security controls may not function on an older operating system such as Solaris 2.5.1. For example section 4.2 from the NSA Guide was implemented per the directions, and it received a positive grade from the CIS scoring tool, but it seemed to have no effect on the system.

Some of the more modern security features of a newer operating system are not available for Solaris 2.5.1 and alternatives need to be used to mitigate the risk. For example, TCP sequence prediction is a residual risk for which there is no good solution other than upgrading the operating system. The risk of session hijacking is mitigated by a defense in depth approach, such as limited access to the system by highly cleared personnel, keeping the system in a stand-alone configuration (not on the internet), following the NSA Guide, and the physical security protecting the system. Also, using ipfilters to limit the access from mis-configured systems or a malicious user with a rogue machine on the stand-alone network mitigates other residual risks such as, unwanted syslog traffic, rcommands (rlogin, rexec, rshell, etc), and preventing the Xserver from accepting connections from the network.

Security is a multifaceted discipline, and hardening an operating system is just one facet. It is the critical piece that any secure information system is built upon. By combining the security requirements from the DCID 6/3 with the step-by-step approach in the NSA Guide, system administrators can layout the framework for building that secure information system.

References

Adeos File System Security Scanner, URL: http://linux.wku.edu/~lamonml/software/adeos/

Another File Integrity Checker (AFICK), URL: http://afick.sourceforge.net/

Center for Internet Security, URL: http://www.cisecurity.org/

"CIS Level-1 Benchmark and Scoring Tool for Solaris", URL: http://www.cisecurity.org/bench_solaris.html

"Director Of Central Intelligence Directive 6/3 - Protecting Sensitive Compartmented Information Within Information Systems", 05 June 1999 URL: http://www.fas.org/irp/offdocs/dcid.htm

ipfilters version 4.1.3, URL: http://coombs.anu.edu.au/~avalon/

"National Security Agency -- Security Recommendation Guides." URL: http://www.nsa.gov/snac/

National Security Agency – "Guide to the Secure Configuration of Solaris 8", URL: http://www.nsa.gov/snac/os/sunsol/Solaris8.pdf

Solaris Operating System, URL: http://wwws.sun.com/software/solaris/

Solaris Operating Environment Network Settings for Security, Alex Noordergraaf and Keith Watson, Sun BluePrints™ OnLine, December 1999, URL: http://www.sun.com/blueprints/1299/network.pdf

Solaris Manual "SPARC: Installing Solaris Software", URL: http://docs-pdf.sun.com/802-1959/802-1959.pdf

Solaris 2.5.1 man pages, URL: http://www.cs.virginia.edu/cgi-bin/manpage.

Simple Watcher for Log Files (Swatch), URL: http://swatch.sourceforge.net/