GIAC CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

© SANS Institute 2000 - 2005, Author retains full rights.

Securing an IRIX 6.5.26 Workstation

Balancing Usability and Security in a Research Environment

Michael Schmidt

Submitted March 17, 2005

GSEC Practical Assignment v1.4c, Option 1

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Contents

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

1 Introduction

In a corporate environment, a central IT department manages the computer systems, the network and installed applications. Add a research department with non-standard lab and research computer systems that users want access to from their corporate computers and we have a more difficult mix, especially given that researchers generally want more local control of their computer systems. As the primary system administrator for over fifty Unix research computers, I have to secure these systems enough to continue their access to the corporate network. Hardening a system for security can greatly improve its chances against vulnerabilities, but can also leave the system and third party applications broken, or of limited productivity to the intended users. This is where the balancing act comes in: I need to keep the machines secure on the network for corporate IT, easy to manage for the research system administrators, and keep researchers' applications running in a usable manner. My goal with this paper is to present a "how-to" for securing IRIX in such an environment – secure enough for being on the corporate network, but usable for research without overburdening the users.

2 Background

Securing computers in a corporate research environment is a balancing act between the need for a secure system for network access and one open enough to handle applications that were likely developed without security in mind. These applications typically are written to communicate directly with instrumentation or to provide modeling and analysis tools to the researchers. Much of this software has its origins in university research labs where the driving force is not security, but providing a tool leading toward unique breakthroughs in science. Commercial organizations purchase software rights to these tools and repackage the software under their application umbrella. No matter where the software comes from, installing research software becomes a security risk for the system manager in corporate research environments. In a corporate environment, researchers want ease of use of the research computer and open connections to their business computers. This creates a balancing act for the system administrator who works to bridge the gaps between researcher requests, demands for secure systems on the corporate network and unknown security coding for third party applications.

IRIX is a Unix operating system used on Silicon Graphics computer systems which target scientific and manufacturing arenas. Default installations of IRIX need a fair amount of security hardening before placing the machine on the network. In the process of hardening the system, we must take care not to break the usability of the third party software. Careful management of the system and its network services is possible by understanding the requirements of the users, the third party applications and corporate IT security.

For the purposes of this paper, the target environment is an IRIX workstation intended for use by one or more users in a research environment. Requirements for this system include:

© SANS Institute 2000 - 2005 Author retains full rights.

- Controlling user passwords and logins
- Allowing remote job submission (typically through rsh or rexec)
- The potential need for remote X Windows
- File sharing and transfer capabilities
- Securing of network services

Sources driving these requirements include:

- Ease of access and use by the researchers
- Security policies from corporate IT and the local system administrators
- Management of the system by the local administrators
- Installation and support of third party applications and their prerequisites

IRIX Changes

Every release of IRIX is full of new features and bug fixes. For our purposes, we are interested in any major security enhancement made available in IRIX.

Summary of Recent IRIX Security Enhancements by Release

Version (Release Date)	**Brief Summary of Security Enhancements (taken from Key New Features and Changes document)**
IRIX 6.5.17 August 2002	• An update to rshd to check for expired passwords
IRIX 6.5.18 November 2002	• Adding /etc/shells to list appropriate user shells (checked by NIS and sendmail)
IRIX 6.5.19 February 2003	• OpenSSH 3.4p1 included in OS release (http://www.openssh.org/) rather than only as a freeware application • IPv6 support • Sendmail 8.12.5 – no longer SUID root, now SUID sgismmsp; split MTA and MSP programs; added sgismmsp account and group.
IRIX 6.5.20 May 2003	• Kerberos 1.2.7 bundled into IRIX (http://web.mit.edu/kerberos/www) • OpenLDAP 2.1.12 bundled into IRIX (http://www.openldap.org/)
IRIX 6.5.21 July 2003	• Tcp_wrappers built into inetd by default • OpenLDAP upgrade to 2.1.17 • OpenSSH upgrade to 3.6.1p2 • OpenSSL upgrade to 0.9.7b • NFS access enhancements
IRIX 6.5.22 November 2003	• PAM support added, but left off by default • NFS improvements • NTP support bundled into IRIX • BIND updated to version 9.2.2
IRIX 6.5.23 February 2004	• IPv6 support for the rtmon command added • ESP (Embedded Support Partner) updated to version 3.0
IRIX 6.5.24 May 2004	• *No security changes for this release were listed in the reference documents.*
IRIX 6.5.25 August 2004	• Support for Secure RPC (see ONC3/NFS Administrator's Guide)
IRIX 6.5.26 November 2004	• Change – rpc.mountd is no longer run from inetd • Banners – telnetd can display /etc/issue.net before login prompt
IRIX 6.5.27 Feb 2005 (released during this research)	• NFS over IPv6 • OpenSSH updated to version 3.9p1 • PAM support for SUNOS C2 security NIS master server; pam_tally module applicable to login, telnet, rlogin, and rsh

© SANS Institute 2000 - 2005 Author retains full rights.

In the preceding table, you will find a summary of recent IRIX changes taken from their listings of “Key New Features and Changes.”[1] Many of these changes, like OpenLDAP and OpenSSH, were previously only available by compiling these tools from source or acquiring the compiled packages from SGI’s freeware repository. The addition of these tools into the base IRIX release has made securing some insecure services an easy matter, such as installing OpenSSH and removing or limiting access to telnet and ftp.

3 Standard System Configuration and Security Changes for IRIX

This guide is assumes a fresh installation of IRIX 6.5.26, the same as would arrive on a newly shipped system.[2] Many points covered here can be implemented after an upgrade from earlier IRIX versions by using the examples as verification of correct usage. My primary goal in this section is getting IRIX running with a reasonable start for security before connecting to the corporate network and the additional security options recently provided in IRIX. This “how-to” contains information from over ten years of system administration on SGI computers combined with information from several publications on securing IRIX.[3]

To differentiate between Unix commands and code samples, the Unix commands are in bold, proportional font and begin with “IRIS #”. Text from files, system responses and code samples are proportionally spaced but not emphasized with bold print. The symbols “<” and “>” designate text that needs replacing with local settings, including the symbols.

3.1 Password and Login Configuration

Before configuring the SGI password management, you should review the corporate policy at your site for their password requirements. Your local settings should agree closely with the corporate policy. Take into consideration the habits of your users. Be sure to document where your settings differ from the corporate policy.

Add root password and lock the rest

IRIX by default is installed with several accounts with no password. You can view what accounts have no password (NP), are locked (LK), or password protected (PS) with the command:

```
IRIS # passwd -as
```

Your first step should be adding a password to the root user followed by locking the accounts that have no password. As the root user run these commands:

[1] This information was pulled from SGI’s Supportfolio Online at https://support.sgi.com/browse_request/irix_os and selecting “6.5.N Start Here: Installing IRIX” under IRIX Release Documents. Supportfolio requires a free login account. This information is duplicated on the Base Documentation CD-ROM for each release of IRIX, e.g., SGI part number 812-0779-026 for IRIX 6.5.26.

[2] Seven CD-ROMs were used in this installation – Installation Tools and Overlays [1 of 3], Overlays [2 of 3], Overlays [3 of 3], ONC3/NFS Version 3, Foundation 1, Foundation 2, and Applications November 2004.

[3] Castevens; Gaeng 9-15; Haprain; IRIX Admin: Backup, Security, and Accounting; Stern 13-41; UNIX.

© SANS Institute 2000 - 2005 Author retains full rights.

```
IRIS # passwd
Changing password for root
New password:  <enter password here>
Re-enter new password:   <repeat password here>

IRIS # foreach account (lp EZsetup nuucp demos guest OutOfBox)
? passwd -l $account
? end
```

To protect the passwords, be sure to turn on shadow passwords. Verify if the file /etc/shadow exists. If it does not exist, run the command pwconv.

```
IRIS # pwconv
```

Configure default rules for passwords and logins

To set up starting rules for passwords, create the file /etc/default/passwd, if it does not exist, and add the following settings as single lines (a fairly restrictive set):

```
PASSLENGTH=8
MINWEEKS=1
MAXWEEKS=6
HISTORYCNT=25
HISTORYDAYS=730
WARNWEEKS=1
```

Edit the file /etc/default/login to control login behavior. The following are some suggested options. You will need to remove the comment symbol (#) from some lines during editing. (This will vary depending on the guidelines from your corporate and local password policies.)

```
CONSOLE=/dev/console
PASSREQ=YES
ALTSHELL=YES
MANDPASS=YES
UMASK=027
TIMEOUT=60
DISABLETIME=300
MAXTRYS=3
LOGFAILURES=4
IDLEWEEKS=2
PATH=/usr/sbin:/usr/bsd:/sbin:/usr/bin:/usr/bin/X11:
SUPATH=/usr/sbin:/usr/bsd:/sbin:/usr/bin:/etc:/usr/etc:/usr/bin/X11
SYSLOG=ALL
INITGROUPS=YES
LANG=C
SVR4_SIGNALS=NO
LOCKOUT=4
LOCKOUTEXEMPT=root
```

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

It is important to note that PASSREQ, MANDPASS, and IDLEWEEKS are not supported if PAM is enabled. In addition, the LOCKOUTEXEMPT setting for the root account has conflicting recommendations from my research;[4] I chose to exempt the root account from lock out, but this potentially leaves this account open for attack. Customize the CONSOLE setting based on your default connection. For example, I maintain several SGIs with no graphics head using a serial port connection for the console. These machines have the setting CONSOLE=/dev/ttyd1, referencing the first serial port. The file /etc/default/login should only be readable by root, so run the following command:

```
IRIS # chmod 400 /etc/default/login
```

The same is true for /etc/default/passwd:

```
IRIS # chmod 400 /etc/default/passwd
```

Disable icon login on graphical logins by the following commands:[5]

```
IRIS # chkconfig noiconlogin on
IRIS # chkconfig visuallogin off
IRIS # chkconfig xdm off
```

Add a user account

You can easily add user accounts when logged into the GUI using the Toolchest. Under the Toolchest, select System, followed by System Manager. Click on “Security and Access Control,” then click “Add a User Account.” Just follow the steps in the next window to complete adding an account and be sure to add a password. For those who know exactly what they want in configuring a new user, use the command line program addUserAccount. An example follows here:

```
IRIS # /usr/sysadm/privbin/addUserAccount –l schmidt –u 3003 \
–g 20 –S /bin/tcsh –H /usr/people/schmidt –C \
–G “Michael Schmidt” –R
IRIS # passwd schmidt
New password:  <enter password here>
Re-enter new password:   <repeat password here>

IRIS # passwd –f schmidt
```

The above line forces the password to be changed at next login by user “schmidt.” Finer control of password aging can be done at the command line as well using the passwd command options of –n (minimum days before changing password again), -w (warning days before password expires), and –x (maximum days before password expires). These options override any settings from the /etc/default/login file. Consult “man passwd” for more options.

[4] The login man page recommended not including root in the LOCKOUTEXEMPT list so that the root account would not be open to repeated attacks. This is in contradiction to the information from IRIX Admin: Backup, Security and Accounting which says to include root in the LOCKOUTEXEMPT list to prevent denial of service attacks. Support of the latter was found (SANS 213).

[5] IRIX Admin: Backup, Security, and Accounting, chapter 4, section “System Login Options.”

© SANS Institute 2000 - 2005 Author retains full rights.

3.2 Network Configuration

Configuring your SGI for network connection is a key area to coordinate with your corporate IT department. I prefer to use static IP addresses and register them with the corporate DNS. Having the hostname registered in the DNS makes administering network backups and other services much easier. It also will later enable your users to contact the machine over the LAN.

When using a static IP address, be sure to make the following change:

```
IRIS # chkconfig autoconfig_ipaddress off
```

Edit /etc/sys_id to include your Fully Qualified Domain Name (FQDN) on a single line, no extra spaces on the end.

```
IRIS.testnetwork.com
```

Edit /etc/hosts to include your static IP address, FQDN, and alias name. Do not delete the entry for localhost!

```
192.168.1.80	IRIS.testnetwork.com IRIS
```

Following the examples in the file, edit /etc/config/static-route.options to include the IP address of your gateway. For the default route to the gateway on this network, add the following line to the bottom of the file:

```
$CAP_NET "$ROUTE $QUIET add -net default 192.168.1.1"
```

Edit /etc/resolv.conf to configure the connection to the DNS. It should look like the sample below:

```
domain testnetwork.com
nameserver <IP address of primary corporate DNS>
nameserver <IP address of secondary corporate DNS>
```

Sometimes it is necessary to edit /etc/nsswitch.conf to change the order that the name service looks for maps. For example, since NIS is not being used, change the “hosts” entry in /etc/nsswitch.conf to:

```
hosts: files dns nis
```

The nis entry could be left out, but leaving it in will not hurt anything since NIS is not running.

Find the name of the primary network interface by listing all the interfaces with:

```
IRIS # ifconfig –a
ec0:
flags=8410c43<UP,BROADCAST,RUNNING,FILTMULTI,MULTICAST,LINK0,IPALIAS,I
PV6>
        inet 192.168.1.80 netmask 0xffffff00 broadcast 192.168.1.255
lo0: flags=8001849<UP,LOOPBACK,RUNNING,MULTICAST,CKSUM,IPV6>
        inet 127.0.0.1 netmask 0xff000000
```

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Change the netmask for ec0 using the following command if necessary (the default netmask is 255.255.255.0 or 0xffffff00 in hex).

```
IRIS # ifconfig ec0 netmask 255.255.255.0
```

The netmask should also be set in /etc/config/ifconfig-1.options using hexadecimal notation. This sets the netmask for the first NIC (Network Interface Card); additional NICs would be controlled separately (e.g., the second NIC would use the settings in /etc/config/ifconfig-2.options). These files work closely with the settings in /etc/config/netif.options. For this configuration the setting in /etc/config/ifconfig-1.options would be:

```
netmask 0xffffff00
```

3.3 Disabling, Configuring and Tightening Vulnerable Network Services

Many services can be turned off, removed or reconfigured under IRIX to tighten security. The basic rule reiterated from the SANS: Security Essentials course is, “If you don’t need it, turn it off!” (SANS 132).

Turn off (or remove) unneeded services

SGI enables two web services by default on your system. The sgi_apache server provides an interface to an attached camera, system information, and user information that are not needed. Disable these web services with:

```
IRIS # chkconfig webface_apache off
IRIS # chkconfig sgi_apache off
```

Disable internet services by adding a comment character (#) or deleting the following services. You may want to make a backup of this file before you delete services.

```
IRIS # cp –p /etc/inetd.conf /etc/inetd.conf.ORIG
```

Then begin editing /etc/inetd.conf. For this example, I will show the commented lines, but remember that you should delete them for added security. (Long lines below were edited to include “\” for line continuation for readability.)

```
#finger  stream  tcp     nowait  guest   /usr/etc/fingerd  fingerd -L
#finger  stream  tcp6    nowait  guest   /usr/etc/fingerd  fingerd -L
#bootp   dgram   udp     wait    root    /usr/etc/dhcp_bootp dhcp_bootp –o \
/etc/config/dhcp_bootp.options
#tftp    dgram   udp     wait    guest   /usr/etc/tftpd    tftpd -s /usr/local/boot \ /usr/etc/boot
#ntalk   dgram   udp     wait    root    /usr/etc/talkd              talkd
#tftp    dgram   udp6    wait    guest   /usr/etc/tftpd    tftpd -s /usr/local/boot \ /usr/etc/boot
#echo    stream  tcp     nowait  root    internal
#discard         stream  tcp     nowait  root    internal
#chargen         stream  tcp     nowait  root    internal
#daytime         stream  tcp     nowait  root    internal
#time    stream  tcp     nowait  root    internal
#echo    stream  tcp6    nowait  root    internal
#discard         stream  tcp6    nowait  root    internal
#chargen         stream  tcp6    nowait  root    internal
#daytime         stream  tcp6    nowait  root    internal
```

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

```
#time    stream  tcp6     nowait  root     internal
#echo    dgram   udp      wait    root     internal
#discard         dgram    udp     wait     root     internal
#chargen         dgram    udp     wait     root     internal
#daytime         dgram    udp     wait     root     internal
#time    dgram   udp      wait    root     internal
#echo    dgram   udp6     wait    root     internal
#discard         dgram    udp6    wait     root     internal
#chargen         dgram    udp6    wait     root     internal
#daytime         dgram    udp6    wait     root     internal
#time    dgram   udp6     wait    root     internal
#rstatd/1-3  dgram   rpc/udp wait    root    /usr/etc/rpc.rstatd     rstatd
#walld/1     dgram   rpc/udp wait    root    /usr/etc/rpc.rwalld     rwalld
#rusersd/1   dgram   rpc/udp wait    root    /usr/etc/rpc.rusersd    rusersd
#rquotad/1   dgram   rpc/udp wait    root    /usr/etc/rpc.rquotad    rquotad
#sprayd/1    dgram   rpc/udp wait    root    /usr/etc/rpc.sprayd     sprayd
#ttdbserverd/1   stream  rpc/tcp wait root ?/usr/etc/rpc.ttdbserverd \ rpc.ttdbserverd
```

Other services were turned off by using chkconfig, such as:

```
IRIS # chkconfig routed off
IRIS # chkconfig privileges off
```

I recommend the following setting to monitor daemons during the boot sequence:

```
IRIS # chkconfig verbose on
```

Here is a good example of an extra application that was installed. You can disable Teleffect with:

```
IRIS # chkconfig tfxd off
```

Optionally, you can remove Teleffect with:

```
IRIS # versions remove Teleffect
```

Configuring time services

Make the following changes to slave this IRIX workstation to the local time master.

```
IRIS # chkconfig timed off
IRIS # chkconfig timeslave on
```

Edit /etc/config/timeslave.options to have the following setting, where 192.168.1.99 is acquiring time from a corporate time master and serving as master for this subnet:

```
-H 192.168.1.99
```

Edit /etc/TIMEZONE for the local time zone setting. Details on this setting can be found in the man pages for timezone and environ.

```
TZ=EST5EDT
```

The new time settings take effect after a system reboot.

Using NTP rather than timeslave

Timeslave works well when the time master is another SGI. If you get frequent error

© SANS Institute 2000 - 2005 Author retains full rights.

messages in SYSLOG from timeslave, configure NTP, turn timeslave off and enable NTP. NTP documentation is not contained in the man pages, but local to IRIX in HTML format at file:/usr/share/doc/ntp/index.htm. Originally, /etc/ntp.conf was modified for just setting the time master server, but a scan later by Nessus (http://www.nessus.org/) revealed that NTP was giving away information about the system. Research on NTP (http://www.ntp.org/) resulted in a more restrictive /etc/ntp.conf than provided in IRIX:

```
restrict default ignore
restrict 192.168.1.99 mask 255.255.255.255 nomodify notrap noquery
restrict 127.0.0.1
# Define servers and fallback in case time server can't be contacted
server 192.168.1.99
fudge 127.127.1.0 stratum 10
driftfile /etc/ntp.drift
broadcastdelay 0.008
```

Changes were also need with /etc/config/ntp.options, the new version of this contained only:

```
# This is the /etc/config/ntp.options file containing
# startup parameters for ntp daemon
#
# All non-commented lines are assembled on a single line

# Configuration file
-c /etc/ntp.conf
```

Disable timeslave and enable NTP:

```
IRIS # chkconfig timeslave off
IRIS # chkconfig ntp on
```

Localizing or disabling sendmail

As mentioned in the earlier table, IRIX started separating the MTA and MSP processes of sendmail in IRIX 6.5.19. The MTA runs as root while the MSP runs as sgismmsp.

On an end user workstation, sendmail does not need to relay beyond localhost. The default sendmail installation is open relay, but there are instructions in the sendmail.mc file and at the SGI Knowledgebase (http://support.sgi.com/kb/) on changing this to local. Find the line in /etc/mail/sendmail.mc beginning with:

```
DAEMON_OPTIONS(`Name=MTA-v4,Family=inet')dnl
```

Change this to:

```
DAEMON_OPTIONS(`Name=MTA-v4,Family=inet,Addr=127.0.0.1')dnl
```

Run configmail to update the sendmail.cf file:

```
IRIS # configmail mc2cf
```

Restart sendmail by running:

```
IRIS # /etc/init.d/mail stop
IRIS # /etc/init.d/mail start
```

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

As recommended by SANS (SANS 77), another option would be to disable sendmail completely and run the MSP program through cron. This would be accomplished with the following:

```
IRIS # chkconfig sendmail off
IRIS # /etc/init.d/mail stop
```

Edit root's cron entries to add running the MSP using:

```
IRIS # crontab –e
```

Append to the end of the file the following lines (SANS 77):

```
# Run the sendmail MSP process at the top of each hour
0 * * * * /usr/lib/sendmail –Ac –q
```

3.4 Permissions

File permissions control much of what can be executed and viewed by users of the system. It is very important to keep permissions appropriate to the service. With respect to user data, default to closed and let the user run commands to open permissions on files as necessary. This is the reason for the UMASK=027 in /etc/default/login, to give users permission with their own files, readable by those in the same group (assuming some strict control of groups), and no permission for others.

Here is an important permission change for any IRIX system. By default, system logs go into /var/adm/SYSLOG and this file has world read permission. Only root and system privileged accounts should really have access to this file. Change the permissions on SYSLOG with the following:

```
IRIS # chmod 640 /var/adm/SYSLOG
```

Make sure this setting remains during log rotations by editing root's cron entry. Edit the cron entry by typing:

```
IRIS # crontab –e
```

(The "-e" option launches the editor defined by the environment variables VISUAL or EDITOR, but will launch "vi" if the editor is not specified.) Find the line with SYSLOG and change the umask from 033 to 037. Here is the entry as changed (this is all one line in the file):

```
1	1	*	*	0	umask 037;export SYSLOGFILE=`grep "\*.crit" /etc/syslog.conf | awk '$1 !=
"#" && done == 0 {done =1; print $NF}'`; /sbin/suattr -M dbadmin -C
CAP_DAC_WRITE,CAP_MAC_WRITE=eip -c 'if test -f $SYSLOGFILE ; then :; else
SYSLOGFILE=/var/adm/SYSLOG; fi; OSYSLOGFILE=`dirname $SYSLOGFILE`/o`basename
$SYSLOGFILE`;if test -s $SYSLOGFILE && test `/sbin/stat -qs $SYSLOGFILE` -ge 10240; then mv -f
$SYSLOGFILE $OSYSLOGFILE;touch $SYSLOGFILE; killall 1 syslogd; fi'
```

Verify the contents of /etc/ftpusers and check the permissions on the file. IRIX installs this file by default with all the non-user accounts, but the permissions have world read. Change the permissions with:

```
IRIS # chmod 600 /etc/ftpusers
```

3.5 Banner Messages

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Appropriate banner messages are an important legal defense when monitoring your systems. Check corporate policy for a warning banner and use it in all locations where logins occur. If you cannot find a corporate warning banner, get approval from management for some protective banner.

Configuration of warning banners depends on the application serving the banner. For most Unix logins, /etc/issue will be the primary location of a warning banner. Be sure this file exists on your system with the corporate warning banner in place. Some services will also use the /etc/issue.net file, but I found that even though IRIX now supports this for telnet that it created a double warning; one came from /etc/issue and another from /etc/issue.net. Therefore, I removed /etc/issue.net from the system.

Contents of the sample /etc/issue file below contain a clear, concise banner message taken from the SANS: Security Essentials course (SANS 175). Replace this with your corporately approved banner message.

```
*********************************************
*           Authorized uses only.           *
* All activity may be monitored and reported. *
*********************************************
```

Update X Windows with this warning banner as well. Under IRIX, edit the "xlogin*greeting" line in /var/X11/xdm/Xresources. (The "\n" causes a new line to start and the "\" indicates the line of code continues on the next line in the file.)

```
xlogin*greeting:        Authorized uses only.\n\
All activity may be monitored and reported.
```

(Did you notice that the default greeting welcomed you to the system, displayed the machine name and the version of IRIX?)

3.6 X Windows

X Windows should be secured to only allow authorized access for remote display. The default use of "xhost" to allow remote connections is a bit too open. As described in IRIX Admin: Backup, Security and Accounting, chapter 5, "X Authority":

> For even better security than the default X server configuration [. . .], you can enable X authority. To do this, change the DisplayManager*authorize entry in /var/X11/xdm/xdm-config to:
>
> DisplayManager*authorize: on
>
> This makes xdm generate "magic cookies" (put in each user's $HOME/.Xauthority file), which are then required for any X client to connect to the X server. This provides a good means of X server access control.

These cookies are managed with the xauth command. For a good overview of X Windows and using xauth, read Arturo Guillen's "X Windows Security: How to Protect your Display" at http://www.sans.org/rr/whitepapers/unix/328.php.

Disable XDCMP

Change lines in /var/X11/xdm/Xaccess that begin with an asterisk "*" to begin with "!*"[6] to disable XDCMP broadcasting. Below are the changed lines:

```
!*                          #any host can get a login window
!*     CHOOSER BROADCAST    #any indirect host can get a chooser
```

3.7 Kernel Tuning

SGI's documentation mentions disabling IP forwarding for single NIC machines, which is the case for our workstation. Verify the IP forwarding setting with:

```
IRIS # netstat -s -p ip | grep forwarding
```

If IP forwarding is enabled, you can disable it by typing:

```
IRIS # systune ipforwarding 0
 ipforwarding = 0 (0x0)
 Do you really want to change ipforwarding to 0 (0x0)? (y/n)  y
```

This creates a new kernel at /unix.install that will install at the next reboot. If you have any IPv6 addresses being used, IPv6 will be enabled and you will have to run similar commands:

```
IRIS # netstat -s -p ipv6 | grep forwarding
```

and

```
IRIS # echo y | systune ip6forwarding 0
```

(The above command uses echo to make the "y" response to systune rather than waiting for the prompt.)

Additional network kernel tuning settings (Thomas) ignore ICMP redirects, set the TCP TIME _WAIT, disable accepting broadcast addresses as source addresses and randomize the low order bits of initial sequence number for TCP source addresses. Address these changes with systune as well:

```
IRIS # echo y | systune icmp_dropredirects 1
IRIS # echo y | systune tcp_2msl 60
IRIS # echo y | systune allow_brdaddr_srcaddr 0
IRIS # echo y | systune tcpiss_md5 1
```

(The tcp_2msl and allow_brdaddr_srcaddr settings are default under IRIX, but are repeated here for clarity.)

Disable users from giving away file ownership (Stern 15):

```
IRIS # echo y | systune restricted_chown 1
```

You should have a new kernel waiting for installation called /unix.install. Verify this with:

[6] Two different versions of changing Xaccess to disable XDCMP were found. Gaeng, p.14, indicated simply commenting these lines out. SANS Institute, pp.85-86, used "!*" to define "do not match any host". The latter seems like a safer approach.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

```
IRIS # ls –lt /uni*
```

If /unix.install does not exist, issue this command:[7]

```
IRIS # autoconfig –vf
```

Check for /unix.install again and if it exists, reboot the system:

```
IRIS # reboot
```

Verify after rebooting that /unix.install does not exist and has replaced the previous /unix.

3.8 File Sharing – NFS & Samba

Our primary security when running NFS or Samba is the strength of the corporate firewall (SANS 65). Proper configuration and up-to-date patching will mitigate many other security issues for these services.

NFS – Network File System

Providing NFS is a major time and space saver in a research computer network. Large file systems can be remotely mounted to provide access to common data and programs across the network. This research workstation will mount remote program and data directories using autofs for mapping of remote NFS trees. Local home directories will also be exported for common use on remote servers and clients in our Unix network.

The default configuration of autofs mounts remote directories under /hosts and always mounts them nosuid and nodev, both good security choices for NFS. Check this by viewing /etc/auto_master.

Another control is how local file systems are exported by NFS. This is defined in the file /etc/exports. You should always export file systems explicitly to the NFS clients and export read only where possible (SANS 65-66). Be sure to use a FQDN rather than an alias when specifying clients by name. For this base SGI workstation, there is only one directory to worry about exporting, /usr/people, the directory containing all the user directories. Optimally, do not put home directories on the system disk; install a second hard drive as an option disk and put home directories there, usually as /people (or /home). The sample /etc/exports file below will show exporting /usr/people. Options would be the same for other master home directories.

Contents of /etc/exports:

```
#
# NFS exported filesystem database (see exports(4) for more information).
#
# Entries in this file consist of lines containing the following fields:
#
```

[7] The "-v" option produces verbose output about the kernel building; "-f" forces a new kernel to build even if there would be no differences between /unix and /unix.install.

© SANS Institute 2000 - 2005 Author retains full rights.

```
# filesystem    [ options ]     [ netgroup ] [ hostname ] ...
#
# Filesystem must be left-justified and may name any directory within a
# local filesystem.  A backslash (\) at the end of a line permits splitting
# long lines into shorter ones.  Netgroup(4) and hostname refer
# to machines or collections of machines to which filesystem is exported.
#
/usr/people     server.testnetwork.com
```

The above provides read-write (rw) access to hostname server.testnetwork.com. Read-write is a default setting.

NFS is started by the /etc/init.d/network script. Verify with chkconfig that autofs, nfs, and nfsd are “on” before exporting or mounting NFS directories with:

```
IRIS # chkconfig | egrep “nfs|autofs”
        autofs              on
        nfs                 on
        nfsd                on
```

After changing /etc/exports, update NFS exporting by running:

```
IRIS # exportfs -a
```

NOTE: “Starting with the IRIX 6.5.24 release, TCP is used as the default protocol for NFS.”[8] This will cause issues with connections to systems that have not implemented NFS over TCP.

NOTE: From the ONC3/NFS Administrator’s Guide, chapter 4, section “Setting Up Secure RPC”:

> The IRIX 6.5.25 release has support for user authentication and optional integrity protection and encryption of NFS traffic using the RPCSEC_GSS authentication mechanism with a Kerberos V5 backend. It describes how to add an NFS client and NFS server to an existing Kerberos realm. As such, the NFS server and client are acting as clients of the Kerberos Domain Controller. SGI does not support the use of an IRIX system as the Domain Controller of a Kerberos realm.

Samba

If your users need file sharing connections between your SGI system(s) and their corporate computers running Microsoft Windows, install Samba (http://www.samba.org/) from SGI’s freeware packages (http://freeware.sgi.com/). I recommend working with someone from corporate IT to make sure you are not introducing any network insecurities by setting up Samba, especially if you are authenticating against an existing Windows domain. Choose options for Samba that require authentication, limit browsing and enable read-write only when needed.

Samba configuration is beyond the scope of this paper, but there are plenty of

[8] ONC3/NFS Administrator’s Guide, chapter 1, section “NFS Protocol.”

© SANS Institute 2000 - 2005, Author retains full rights.

resources about it on the internet, starting at http://www.samba.org/samba/docs/. SGI even has a publication entitled “Samba for IRIX Installation and Administration Guide,” located at http://docs.sgi.com/library/tpl/cgi-bin/browse.cgi?coll=0650&db=bks&cmd=toc&pth=/SGI_Admin/Samba_IAG.

4 Using (New) IRIX Features to Maintain Usability

Features have been added to IRIX in recent years that were historically released as part of SGI’s freeware distributions, such as tcp_wrappers, PAM, OpenSSL and OpenSSH. The following are important considerations in our reseach workstation environment as they can tighten the security of what was presented above without causing major new hassles for the researchers. I have marked some of these as optional due to implementation issues or the value of the security features gained.

4.1 IRIX Implementation of TCP_Wrappers

As noted in earlier, IRIX has implemented tcp_wrappers into inetd. This configuration is different enough from the typical use of tcp_wrappers that it is worth covering the IRIX implementation. Man pages applicable to understanding this implementation include inetd, tcp_wrappers and hosts_access(5), along with reading the comments in the /etc/inetd.conf file.

Enable tcp_wrappers in inetd.conf by editing or creating the /etc/config/inetd.options file to include the following:

```
-t on
```

Edit /etc/hosts.deny. This is an easy denial configuration and can be customized for greater control):

```
ALL: ALL
```

Edit /etc/hosts.allow to allow services from internal addresses. This is an example version and should be customized. Notice that the service name in line one is just telnetd, not in.telnetd as in most implementations of tcp_wrappers. This is true for all wrapped services in IRIX. Also, notice the special cases for the tcpmux services by comparing /etc/inetd.conf with /etc/hosts.allow.

```
telnetd: .testnetwork.com
ftpd:  192.168.1.99
rshd:  192.168.1.0/255.255.255.100
rlogind:       192.168.1.0/255.255.255.100
rexecd:        192.168.1.0/255.255.255.100
sgi_scanner:   192.168.1.0/255.255.255.100
sgi_printer:   192.168.1.0/255.255.255.100
sgi_sysadm:    192.168.1.0/255.255.255.100
sgi_dmusrcmd:  192.168.1.0/255.255.255.100
```

If all these wrapped services cover the same networks, a simple version of /etc/hosts.allow would be:

```
ALL:    .testnetwork.com
```

© SANS Institute 2000 - 2005 Author retains full rights.

Edit /etc/inetd.conf and add an “!” to the path of any service we want covered by tcp_wrappers. Read the comments and man pages to understand what services can be wrapped. Below are the edited versions from my /etc/inetd.conf file. Long lines have a “\” added to indicate continuation.

```
ftp       stream  tcp     nowait  root      !/usr/etc/ftpd      ftpd -l
telnet    stream  tcp     nowait  root      !/usr/etc/telnetd telnetd
shell     stream  tcp     nowait  root      !/usr/etc/rshd                rshd -L
login     stream  tcp     nowait  root      !/usr/etc/rlogind rlogind
exec      stream  tcp     nowait  root      !/usr/etc/rexecd              rexecd
sgi-dgl stream    tcp     nowait  root/rcv !/usr/etc/dgld \
          dgld -IM -tDGLTSOCKET
ftp       stream  tcp6    nowait  root      !/usr/etc/ftpd      ftpd -l
telnet    stream  tcp6    nowait  root      !/usr/etc/telnetd telnetd
shell     stream  tcp6    nowait  root      !/usr/etc/rshd                rshd -L
login     stream  tcp6    nowait  root      !/usr/etc/rlogind rlogind
tcpmux/sgi_scanner stream tcp nowait root   !?/usr/lib/scan/net/scannerd \
          scannerd
tcpmux/sgi_printer stream tcp nowait root   !?/usr/lib/print/printerd \
          printerd
tcpmux/sgi_sysadm stream tcp nowait root   !?/usr/sysadm/bin/sysadmd sysadmd
tcpmux/sgi_dmusrcmd stream tcp nowait root !?/usr/etc/dmusrcmd \
          /usr/etc/dmusrcmd
```

A reboot of the system is the easiest way to insure this starts cleanly. Optionally if you are on the console, you can stop and start all the network services:

```
IRIS # /etc/init.d/network stop
IRIS # /etc/init.d/network start
```

4.2 OpenSSH

Previously, the quickest method to get SSH available on IRIX was to install the SGI freeware distribution of OpenSSH (fw_openssh). With IRIX 6.5.19, OpenSSH is installed as an IRIX product (openssh) not as the freeware version. The major difference between these distributions is location of files, but the configuration of SSH remains pretty much the same. If you are upgrading IRIX and previously had the fw_openssh package installed, be mindful of the changes by backing up your fw_openssh installation before starting the upgrade.

The default IRIX installation does not install the openssh.sw.server package, only the client and related documentation. Follow SGI’s instructions for installing packages to install openssh.sw.server from the IRIX 6.5.26 Overlays [3 of 3] CD-ROM and then configure OpenSSH as follows.

Edit /etc/openssh/sshd_config by changing or removing comments (# character at beginning of line) from these settings:

```
Protocol 2
PermitRootLogin no
```

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

```
X11Forwarding yes
PrintMotd yes
UsePrivilegeSeparation yes
Banner /etc/issue
IgnoreRhosts yes
RhostsRSAAuthentication no
```

Change the permissions on sshd_config with:

```
IRIS # chmod 600 /etc/openssh/sshd_config
```

Enable sshd with chkconfig and start the service:

```
IRIS # chkconfig sshd on
IRIS # /etc/init.d/sshd start
```

With OpenSSH installed, the choice to remove telnetd and ftpd from the inetd services can be made. The limitation on removal of these services will be based on third party applications. If no third party applications require telnetd or ftpd services running, then remove the appropriate lines from /etc/inetd.conf (removal is safer than leaving it commented in the file). All you have left is training your user base on using ssh and sftp. Be sure to let them know that their passwords are not visible as plain text on the network now.

This also handles the security issues around remote X Windows. If users launch ssh with the –X option and sshd is configured for X11forwarding as above, authentication of remote X Windows is handled in an encrypted fashion.

CAUTION: Graphically intensive programs running X Windows through ssh will be sluggish due to encryption. Therefore, ssh cannot completely replace all functions needed when running remote X Windows.

NOTE: There is a known bug (SGI BUG 919370[9]) in the IRIX 6.5.26 implementation of OpenSSH in which the time zone is not set correctly and log files show the GMT timestamps instead of the local time zone. To eliminate this bug, either upgrade to OpenSSH from the 6.5.27 IRIX release or uninstall openssh and install the fw_openssh package from SGI's freeware distribution.

4.3 PAM (optional)

IRIX added support of Pluggable Authentication Modules (PAM) in IRIX 6.5.22. PAM , subsystem eoe.sw.pam, can be installed from the IRIX 6.5.26 Installation Tools and Overlay [1 of 3] CDROM. The current implementation is not overly complex and covers just a few services using authentication. The IRIX PAM installation uses the /etc/pam.d directory to enumerate services covered rather than having a single /etc/pam.conf. The /etc/security directory will also contain files used by PAM services.

[9] This bug information was found by searching the "SGI Knowledgebase" in Supportfolio, http://support.sgi.com/, which requires a free login account. Use "sshd SYSLOG GMT" keywords in your search for quickest results.

© SANS Institute 2000 - 2005 Author retains full rights.

This document is not intended to be a tutorial on PAM, but it will show how to configure some PAM enabled applications to mimic many of the changes we did for UNIX passwords above. At the time of this writing the pam_tally module has just been added in IRIX 6.5.27, so the /etc/default/login settings of LOCKOUT and LOCKOUTEXEMPT will not be mirrored in these PAM settings. In addition, the login man page states that the following settings in /etc/default/login are ignored when PAM is enabled – PASSREQ, MANDPASS, and IDLEWEEKS.

Enabling PAM

Before enabling PAM, change a few settings for stronger security. This will only involve changing a few lines in login and passwd, both located in /etc/pam.d. These changes correspond with PASSLENGTH and HISTORYCNT from /etc/default/passwd. Here are the new versions of these files with remember=25 as an argument on the pam_unix module and minlen=8 as a pam_cracklib argument.

Listing of modified /etc/pam.d/passwd:

```
#PAM-1.0
#[For version 1.0 syntax, the above header is optional]
#
# The PAM configuration file for the `passwd' service
#
password   requisite  pam_cracklib.so retry=3 minlen=8
# to remember old passwords, uncomment the following line and
# create /etc/security/opasswd file
password   required   pam_unix.so remember=25 use_authtok nullok
#password   required   pam_unix.so use_authtok nullok
```

Listing of modified /etc/pam.d/login:

```
#PAM-1.0
#[For version 1.0 syntax, the above header is optional]
#
# The PAM configuration file for the `login' service
#
# Uncomment the following line to let rlogind/rshd to
# use .rhosts and /etc/hosts.equiv file
# auth       sufficient   pam_rhosts_auth.so promiscuous
#
# comment the following two lines if CAP/MAC is not supported in your system
auth       required   pam_mac.so noprompt
auth       required   pam_cap.so noprompt
auth       required   pam_unix.so nullok
account    required   pam_unix.so
password   requisite  pam_cracklib.so retry=3 minlen=8
# to remember old passwords, uncomment the following line and
# create /etc/security/opasswd file
password   required   pam_unix.so remember=25 use_authtok nullok
```

© SANS Institute 2000 - 2005 Author retains full rights.

```
#password   required   pam_unix.so use_authtok nullok
session    required   pam_unix.so
```

Create /etc/security/opasswd if it does not exist, so the password history can be stored (remember=25). (Do not confuse this file with the /etc/opasswd file created by pwconv.)

```
IRIS # touch /etc/security/opasswd
IRIS # chmod 600 /etc/security/opasswd
```

Enable PAM with:

```
IRIS # chkconfig pam on
```

Enabling PAM ignores any settings in /etc/default/passwd. To set password aging settings with PAM enabled, you will need to use the options to the passwd command to set warning days, minimum days, and maximum days. Here is a sample to achieve these settings with value equivalent to those in the /etc/default/passwd described previously.

```
IRIS # passwd –w 7 –n 7 –x 42 schmidt
```

Why is this optional?
The major reason for installing PAM at the current stage of IRIX implementation would be improving password strength. If your users are well versed in creating strong passwords, the configurations from /etc/default/login and /etc/default/passwd cover the major areas of good password security features (SANS Institute 212) except dictionary checking passwords. If you choose not to use PAM, you should implement a scheduled password scanning policy so you can educate the users of weak passwords.

4.4 Kerberos (optional)

From the Kerberos home page (Kerberos section "What is Kerberos?"):

> Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography [. . .].
>
> The Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server has used Kerberos to prove their identity, they can also encrypt all of their communications to assure privacy and data integrity as they go about their business.

Kerberos 1.3.1a is the version installed under IRIX 6.5.26, with earlier versions dating back to IRIX 6.5.20, released in May 2003. The IRIX Kerberos man page informs us of support for "rlogin, rsh, rcp, telnet, ftp, krdist (a Kerberized version of rdist), ksu (a Kerberized version of su), login, and Xdm." Other implementations of Kerberos are found in PAM,[10] ssh,[11] Samba[12] and NFS.[13]

© SANS Institute 2000 - 2005 Author retains full rights.

Proper planning for Kerberos must be completed before installation, notably preparation of a Key Distribution Center (KDC). IRIX only supports being a Kerberos client at this time,[14] so a primary KDC should be established on another system. Secondary KDCs improve the stability of the authentication system. You should check for implementations of Kerberos and a KDC within your site before proceeding with your own configuration.

Detailed coverage of Kerberos is beyond the scope of this paper. Overviews of the Kerberos protocol and installation guides are available from the internet (Rome; Todaro; Tung) and the Kerberos home page, http://web.mit.edu/kerberos/www/, is great place to start.

4.5 IPFilter (optional)

Kernel changes were made earlier to protect the system from certain network vulnerabilities, but that does not cover them all. Installation of IP filtering software provides a means to protect the system from additional known IP vulnerabilities.

While not a part of the base installation described here, SGI IPFilter (http://www.sgi.com/products/software/ipfilter.html) can be used as a local firewall solution. You can easily install the free download of SGI IPFilter, but the configuration requires a good understanding of IPFilter commands. Many good sources exist for explaining and configuring IPFilter.[15] Using IPFilter may require you to undo the earlier kernel changes, e.g., allowing IP forwarding.

Protection by a strong corporate firewall may make use of IPFilter seem like overkill, but addition of a local firewall will add defense from potential internal attacks. It can provide a means of monitoring the inbound and outbound packets to your workstation by logging packet activity.

5 Optional Tools for Security and Auditing

The following tools are extras that you can install to maintain auditing for your system. Read the documentation about these carefully before you decide to implement them, since some will affect system performance. You have to judge whether these services add value to your security configuration without affecting usability.

5.1 Tripwire

Tripwire (http://www.tripwire.org/) will monitor key files on your system and alert you to changes in file attributes including size, time stamps, etc. An SGI freeware distribution is available from http://freeware.sgi.com/.

[10] IRIX 6.5 Product Release Notes / Information kerberos.
[11] IRIX 6.5 Man Pages SSHD_CONFIG(5).
[12] IRIX 6.5 Man Pages SMB.CONF(5).
[13] ONC3/NFS Administrator's Guide, chapter 4, section “Setting Up Secure RPC.”
[14] ONC3/NFS Administrator's Guide, chapter 4, section “Setting Up Secure RPC.”
[15] IPFilter and PF resources; IPFilter Firewall User's Guide; Rauch; Reed.

© SANS Institute 2000 - 2005 Author retains full rights.

5.2 Auditing and Accounting

Enable sar (system activity reporting) to monitor system activity and performance.

```
IRIS # chkconfig sar on
```

IRIX by default does not install or enable auditing. Auditing your system is an encouraged security management tool. Full details for enabling auditing (eoe.sw.audit) on your SGI are given in chapter 6 of IRIX Admin: Backup, Security and Accounting.

Likewise, chapter 7 of the same SGI publication covers installing and configuring system accounting (eoe.sw.acct).

5.3 Quotas

File system quotas are used to limit the space used per account. You can also enable them without imposing limits in order to provide a quick response for how much space a given user is taking. IRIX does not install quotas by default. You will have to install eoe.sw.quotas from the distribution CD-ROMs and then enable quotas on your filesystems in /etc/fstab. On a workstation, this may be overkill, but on a server, running quotas is a must on mount points containing user files. The quotas option is controlled by chkconfig and will need a reboot to enable monitoring of the disks. Consult the man pages for quotas and fstab for configuration options.

6 Maintaining the Balance

Now that you have installed all these tools and hardened the system, how do you maintain the balance of usability and security?

6.1 Keep Up with Corporate Policy

Consult your company's internal Web site for on-line documentation of corporate computer security policies. Keeping abreast of changes to this site enables you to be proactive in maintaining your systems on the corporate network. Form a good relationship with your corporate network team and security response team; you never know when you will need them to assist with a security incident.

6.2 Maintain the System and System Documentation

Upgrade, patch, document, test and repeat as necessary. If you have the luxury of having extra machines, take the time to test all your upgrades and patches on these "non-production" machines. Installing a new patch and breaking the usability of a workstation is not a way to make friends. Subscribe to appropriate mailing lists for your system along with bug and vulnerability reports. Good subscription selections include:

- BugTraq from SecurityFocus (http://www.securityfocus.com/subscribe?listname=1)
- SGI's Supportfolio (http://support.sgi.com/)
- National Cyber Alert System from US-CERT (http://www.us-cert.gov/cas/signup.html)

© SANS Institute 2000 - 2005 Author retains full rights.

- SANS Computer Security Newletters and Digests (http://www.sans.org/newsletters/)

Maintain documentation that proves useful for your system. Keep a file or binder documenting where your systems differ from corporate policy. You will want these handy if you are audited by corporate IT.

Run vulnerability scanners with permission (preferably off the network), to verify the security of your system and its outages. Be sure to keep your scanners' plug-ins current. Many free tools exist for vulnerability testing. To confirm the results of the configuration presented here, SARA and Nessus were used to probe the system from a laptop running Fedora Core 3. Nessus scanning was critical in finding the issues in the default configuration of NTP, as noted earlier in this paper. Print out the results of your scans and save them for future reference. If you are not comfortable running vulnerability scanners, the corporate IT group can usually provide this as a service.

6.3 Educate and Inform Your Users

Take the time to educate the users of your system. This can be accomplished a number of ways. User group meetings, newsletters, and e-mail notices are great ways to let your users know about issues on the system. Maintain a FAQ document for users' quick reference.

With the tasks accomplished by this document, you should instruct users to:

- Choose strong passwords[16] under the local password policy.
- Read corporate policy on what constitutes appropriate use.
- Use ssh for remote login and "ssh –X" for remote X Windows. Explain why this is better than rsh, rexec, rlogin, telnet, ftp, using "xhosts +" and .rhosts files.
- Properly format and set permissions on ~/.rhosts, since we still need rsh for remote job submittal.
- Use xauth rather than xhost.
- Change default file permissions and promote best practices for sharing files.
- Prepare for the potential use of Kerberos.

6.4 Communicating Security Issues with Application Vendors

It is easy to forget about this step, but you will find that actively communicating security concerns to your third party application vendors raises awareness. Often you will discover that other customers have expressed the same issues to the vendor. If you do not keep security at the top of your list with the vendor, it will not be at the top of their priorities for improving the software. Here are two recent examples from my own experience where conversations with vendors have made a difference:

Example 1: Recently a vendor sent me a script designed to synchronize data between a Linux server responsible for daily data download and an SGI Origin hosting a web interface into that data. The original instructions had the SGI mount the Linux system's

[16] Guidelines section "How To Select A Safe Password."

© SANS Institute 2000 - 2005 Author retains full rights.

data directory through NFS, while the Linux box used ssh to call scripts on the SGI to rsync the two data trees. They were using a secure method to initiate rsync (plain text) transfers on an insecure NFS connection. We discussed this and the scripts were modified to take advantage of the rsync ability to use ssh for its communication. The NFS connection became unnecessary.

Example 2: I have had multiple discussions with a vendor about their use of rsh as a means of submitting jobs to remote machines. Recently, when requesting that they look into supporting a queuing system for remote jobs, we revisited the rsh vs. ssh debate. More customers have since asked for ssh support and the vendor is investigating changes they would need to make to their batch system use ssh.

7 Conclusions

Major security changes were made on an IRIX system that still allow the services needed by third party applications without making major new headaches for the users. From the original requirements:

- Controlling user passwords and logins:
    - Stronger settings have been enabled by configuring /etc/default/login and /etc/default/passwd; optionally enable PAM.
    - Telnet has been restricted by tcp_wrappers; or telnet can be disabled and replaced with ssh.
- Allowing remote job submission – rsh and rexec are still permittted, but tcp_wrappers have limited their access.
- The potential need for remote X Windows – xauth and ssh can be used to provide a more secure X Window connection than using the xhost command.
- File sharing and transfer capabilities:
    - NFS configured with defined clients.
    - SAMBA can be configured for sharing Unix file systems with Windows.
    - FTP is limited by tcp_wrappers and /etc/ftpusers; or FTP is disabled in favor of sftp.
- Securing of network services:
    - Many network services were disabled (e.g., sendmail MTA).
    - Limit services with tcp_wrappers.
    - Replacing services with more secure options, like ssh, scp and sftp.

Computer security is a moving target. This paper covers a foundation of techniques to harden a base IRIX system, but there is always room for improvement. Kerberos implementation will provide a better security layer for rsh, rlogin, X Windows and NFS. Installing IPFilter adds an important network protection layer between the corporate network zone and the local research computer. Auditing tools, quotas, and tripwire warn us about changes to the managed computer system.

The balance between security and usability is maintainable. It requires diligence by the local system administrator(s) to keep up with new computer vulnerabilities, system patches, OS updates and the needs of the user community. Good interaction by the

© SANS Institute 2000 - 2005 Author retains full rights.

administrator with the users, third party software vendors, and corporate IT keeps research computers working smoothly and securely.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

References

Castevens, Charles. "Securing IRIX." 4 Apr. 2004. 6 Mar. 2005 <http://www.geocities.com/Athens/6270/securing.html>.

Computer Security Newletters and Digests. 2005. SANS Institute. 10 Mar. 2005 <http://www.sans.org/newsletters/>.

Gaeng, Thomas. "IT Security on SGI Systems running IRIX 6.5.x." GIAC practical repository. Oct. 2004. SANS Institute. 6 Mar. 2005 <http://www.giac.org/certified_professionals/practicals/gsec/4158.php>.

"Guidelines For Developing A Sensible Password Policy." Security Bulletins. 31 May 1993. AusCERT. 11 Mar. 2005 <http://www.auscert.org.au/render.html?it=1832>.

Guillen, Arturo. "X Windows Security: How to Protect your Display." Information Security Reading Room. 16 Nov. 2001. SANS Institute. 6 Mar. 2005 <http://www.sans.org/rr/whitepapers/unix/328.php>.

Haprain, John C. "Securing IRIX 6.5." Information Security Reading Room. 20 Aug. 2001. SANS Institute. 6 Mar. 2005 <http://www.sans.org/rr/whitepapers/unix/326.php>.

IPFilter and PF resources. 16 Mar. 2005 <http://www.obfuscation.org/ipf/>.

IPFilter Firewall User's Guide. 007-4599-002. 17 Jan. 2003. Silicon Graphics, Inc. 16 Mar. 2005 <http://techpubs.sgi.com/library/tpl/cgi-bin/browse.cgi?coll=0650&db=bks&cmd=toc&pth=/SGI_Admin/IPFilter_UG>.

IRIX 6.5 Applications November 2004. 812-0877-026. CD-ROM. Silicon Graphics, Inc.,

© SANS Institute 2000 - 2005, Author retains full rights.

Nov. 2004.

IRIX 6.5 Foundation 1. 812-0759-002. CD-ROM. Silicon Graphics, Inc., June 1998.

IRIX 6.5 Foundation 2. 812-0760-002. CD-ROM. Silicon Graphics, Inc., June 1998.

“IRIX 6.5 Man Pages chkconfig(1M).” SGI Techpubs Library. Silicon Graphics, Inc. 10 Mar. 2005 <http://docs.sgi.com/library/tpl/cgi-bin/getdoc.cgi?coll=0650&db=man&fname=/usr/share/catman/a_man/cat1/chkconfig.z>.

“IRIX 6.5 Man Pages KERBEROS(1).” SGI Techpubs Library. Silicon Graphics, Inc. 10 Mar. 2005 <http://docs.sgi.com/library/tpl/cgi-bin/getdoc.cgi?coll=0650&db=man&fname=/usr/share/catman/u_man/cat1/kerberos.z>.

“IRIX 6.5 Man Pages login(1).” SGI Techpubs Library. Silicon Graphics, Inc. 10 Mar. 2005 <http://docs.sgi.com/library/tpl/cgi-bin/getdoc.cgi?coll=0650&db=man&fname=/usr/share/catman/u_man/cat1/login.z>.

“IRIX 6.5 Man Pages RPCSEC_GSS(7).” SGI Techpubs Library. Silicon Graphics, Inc. 10 Mar. 2005 <http://docs.sgi.com/library/tpl/cgi-bin/getdoc.cgi?coll=0650&db=man&fname=/usr/share/catman/a_man/cat7/rpcsec_gss.z>.

“IRIX 6.5 Man Pages SSHD_CONFIG(5).” SGI Techpubs Library. Silicon Graphics, Inc. 10 Mar. 2005 <http://docs.sgi.com/library/tpl/cgi-bin/getdoc.cgi?coll=0650&db=man&fname=/usr/share/catman/p_man/cat5/openssh/sshd_config.z>.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

"IRIX 6.5 Man Pages SMB.CONF(5)." SGI Techpubs Library. Silicon Graphics, Inc. 10 Mar. 2005 <http://docs.sgi.com/library/tpl/cgi-bin/getdoc.cgi?coll=0650&db=man&fname=/usr/share/catman/u_man/cat5/smb.conf.z>.

"IRIX 6.5 Product Release Notes / Information kerberos." SGI Techpubs Library. Silicon Graphics, Inc. 10 Mar. 2005 <http://docs.sgi.com/library/tpl/cgi-bin/getdoc.cgi?coll=0650&db=relnotes&fname=/usr/relnotes/kerberos&srch=kerberos>.

IRIX 6.5.26 Installation Tools and Overlays [1 of 3]. 812-0818-026. CD-ROM. Silicon Graphics, Inc., Nov. 2004.

IRIX 6.5.26 Overlays [2 of 3]. 812-0819-026. CD-ROM. Silicon Graphics, Inc., Nov. 2004.

IRIX 6.5.26 Overlays [3 of 3]. 812-0817-026. CD-ROM. Silicon Graphics, Inc., Nov. 2004.

IRIX Admin: Backup, Security, and Accounting. 007-2862-007. 2 Aug. 2004. Silicon Graphics, Inc. 7 Mar. 2005 <http://docs.sgi.com/library/tpl/cgi-bin/browse.cgi?coll=0650&db=bks&cmd=toc&pth=/SGI_Admin/IA_BakSecAcc>.

IRIX Network Programming Guide. 007-0810-110. 29 Jul. 2003. Silicon Graphics, Inc. 16 Mar. 2005 <http://techpubs.sgi.com/library/tpl/cgi-bin/browse.cgi?coll=0650&db=bks&cmd=toc&pth=/SGI_Developer/IRIX_NetPG>.

Kerberos: The Network Authentication Protocol. 27 Jan. 2005. Massachusetts Institute of Technology. 7 Mar. 2005 <http://web.mit.edu/kerberos/www/>.

Linux-PAM. 16 Sept. 2003. Kernel.Org Organization, Inc. 7 Mar. 2005

© SANS Institute 2000 - 2005

Author retains full rights.

<http://www.kernel.org/pub/linux/libs/pam/>.

National Cyber Alert System. 5 Mar. 2005. United States Computer Emergency Readiness Team (US-CERT). 10 Mar. 2005 <http://www.us-cert.gov/cas/signup.html>.

Nessus Open Source Vulnerability Scanner Project. 2004. Tenable Network Security. 7 Mar. 2005 <http://www.nessus.org/>.

NTP: The Network Time Protocol. 14 Dec. 2004. NTP Project. 7 Mar. 2005 <http://www.ntp.org/>.

ONC3/NFS Administrator's Guide. 007-0850-170. 6 Feb. 2005. Silicon Graphics, Inc. 7 Mar. 2005 <http://docs.sgi.com/library/tpl/cgi-bin/browse.cgi?coll=0650&db=bks&cmd=toc&pth=/SGI_Admin/ONC3NFS_AG>.

ONC3/NFS Version 3 for IRIX 6.2, 6.3, 6.4, and 6.5. 812-0774-002. CD-ROM. Silicon Graphics, Inc., May 1999.

OpenSSH. 2005. OpenBSD. 7 Mar. 2005 <http://www.openssh.org/>.

Rauch, Jeremy. “Introduction to IP Filter.” 17 July 2000. INFOCUS. SecurityFocus. 16 Mar. 2005 <http://www.securityfocus.com/infocus/1378>.

Reed, Darren. IP Filter. 16 Mar. 2005 <http://coombs.anu.edu.au/ipfilter/>.

Rome, Jim. How to Kerberize your site. 10 Mar. 2005 <http://www.ornl.gov/~jar/HowToKerb.html>.

Samba for IRIX Installation and Administration Guide. 007-3965-007. 21 Oct. 2004. Silicon Graphics, Inc. 7 Mar. 2005 <http://docs.sgi.com/library/tpl/cgi-bin/browse.cgi?coll=0650&db=bks&cmd=toc&pth=/SGI_Admin/Samba_IAG>.

© SANS Institute 2000 - 2005

Author retains full rights.

SANS Institute. Track 1 – SANS Security Essentials. Volume 1.6. SANS Press, January 2004.

SARA (Security Auditor's Research Assistant). 2005. The Advanced Research Corporation. 7 Mar. 2005 <http://www-arc.com/sara/>.

SecurityFocus BugTraq Mailing Lists Subscription. 2005. SecurityFocus. 10 Mar. 2005 <http://www.securityfocus.com/subscribe?listname=1>.

SGI IPFilter. 2005. Silicon Graphics, Inc. 15 Mar. 2005 <http://www.sgi.com/products/software/ipfilter.html>.

SGI IRIX Freeware. 2005. Silicon Graphics, Inc. 7 Mar. 2005 <http://freeware.sgi.com/>.

SGI Techpubs Library. 2005. Silicon Graphics, Inc. 7 Mar. 2005 <http://docs.sgi.com/>.

SGI Supportfolio Online. 2005. Silicon Graphics, Inc. 7 Mar. 2005 <http://support.sgi.com/>.

Stern, Steve. "Operating System Security Control for the SGI IRIX Environment." GIAC practical repository. 28 Mar. 2003. SANS Institute. 6 Mar. 2005 <http://www.giac.org/certified_professionals/practicals/gcux/0185.php>.

Thomas, Rob. "UNIX IP Stack Tuning Guide v2.7." 3 Dec. 2000. The Team Cymru Document Collection. Team Cymru Website. 12 Mar. 2005 <http://www.cymru.com/Documents/ip-stack-tuning.html>.

Todaro, Pam. "An Overview of the Kerberos Authentication Protocol." Information Security Reading Room. 14 Oct. 2003. SANS Institute. 6 Mar. 2005 <http://www.sans.org/rr/whitepapers/windows/1288.php>.

Tripwire.org – Home of the Tripwire Open Source Project. Tripwire, Inc. 10 Mar. 2005

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

<http://www.tripwire.org/>.

Tung, Brian. The Moron's Guide to Kerberos, Version 1.2.2. 19 Dec. 1996. 10 Mar. 2005 <http://www.isi.edu/gost/brian/security/kerberos.html>.

“UNIX Security Checklist v2.0.” 8 Oct. 2001. Checklists. AusCERT. 11 Mar. 2005 <http://www.auscert.org.au/render.html?it=1935>.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.