



Interested in learning more about security?

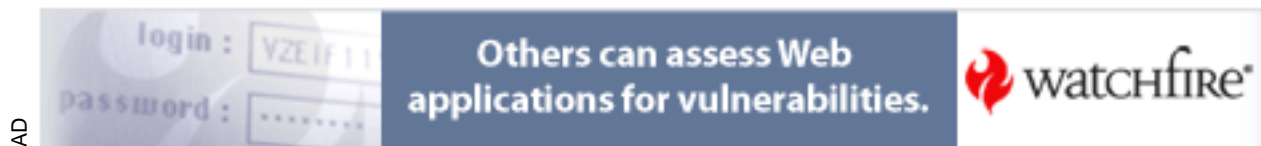
SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Securing IRIX 6.5

There are many people in my organization who use SGI workstations on a daily basis yet do not enjoy the luxury of having a dedicated system administrator. It is my hope this document will be of some guidance to those people who require a secure IRIX system yet don't have either the time or the desire to become IRIX security wizards.

Copyright SANS Institute
Author Retains Full Rights



Securing IRIX 6.5 v1.0

John C. Haprian

Introduction

There are many people in my organization who use SGI workstations on a daily basis yet do not enjoy the luxury of having a dedicated system administrator. It is my hope this document will be of some guidance to those people who require a secure IRIX system yet don't have either the time or the desire to become IRIX security wizards.

A Word to the Wise

System security is an often difficult balance between ensuring a system is completely secure (i.e. pulling the plug and burying it in a hole in the ground) and satisfying user needs. While reading this document please keep in mind that, in matters of computer security, I prefer to err on the side of caution. As such, the settings that I recommend are rather aggressive and, depending on your needs, may prove to be a little too aggressive.

Assumptions

This document assumes the following:

- You have a SGI system running IRIX 6.5 or higher.
- Your computer is configured for your network.
- You are logged in to your system as user "root".

Ready? OK, let's begin!

1. Set Root Password

The "root" account, which is included on your system by default, is a special account that has access to all of the files on your computer. Since anyone logged in as "root" has complete control over virtually every aspect of your computer it is very important that this account be protected with as secure a password as possible.

Care should be taken when selecting a root password. An easy and relatively secure method of generating passwords is to create a password using the first letters of a phrase or rhyme. For example, by using the first letters of the following famous sentence:

That's one small step for a man

You could generate the following password:

Tlssfam

Once you have chosen a good password use the following command to assign your password to the root account:

```
# passwd root
```

Be sure not to forget your root password! Only the root user can change the root password, so if you forget the root password you have effectively locked yourself out of your system.

2. Install the Latest Maintenance Release:

Operating system updates for IRIX 6.5 are called Maintenance Releases. Besides containing the latest updates and patches for your system each release is cumulative and contains all of the updates and patches of the previous releases. As such, SGI maintenance releases are huge. In fact, the latest available release (6.5.12) clocks in at over 940mb compressed! Please make sure you have enough room on your hard drive before downloading.

First, download the latest Maintenance Release:

<http://support.sgi.com/colls/patches/tools/relstream/index.html>

Then, gunzip and untar the release:

```
# gunzip IRIX6.5.12m.tar.gz
# untar IRIX6.5.12m.tar
```

Begin the installation:

```
# inst -f .
```

Once the inst program has started, check for conflicts:

```
Inst> conf
```

Assuming there are no conflicts, begin the installation:

```
Inst> go
```

After the installation has completed exit out of inst and reboot the system.

3. Lock Local Accounts

There are many default accounts on an IRIX system that can be safely disabled. This is a highly recommended practice because every open account on your computer is yet another potential avenue of attack.

Because I'm a bit paranoid I personally recommend disabling every account except for actual user accounts and, of course, the root account.

For example, to disable the default *OutOfBox* user you would use the following simple

command:

```
# passwd -l OutOfBox
```

If disabling every account besides active users and root proves to be too restrictive for your environment I suggest disabling, at a minimum, the following default users:

```
sysadm  
cmwlogin  
diag  
uucp  
sys  
adm  
nuucp  
auditor  
dbadmin  
sgiweb  
rfindd  
EZsetup  
demos  
OutOfBox  
4Dgifts
```

4. Enable Shadow Passwords

By default the file where passwords are stored, */etc/passwd*, is readable by any user on the system. This is a problem because a world-readable password file can be easily copied by a malicious user who could then run a password-cracking program at their leisure.

Enabling a feature called Shadow Passwords very neatly solves this problem. Shadow Passwords moves the encrypted password field to a file called */etc/shadow* that is readable only by root.

Use the following command to initialize shadow passwords:

```
# /sbin/pwconv
```

5. Secure */etc/inetd.conf*

The *inetd* daemon is the master daemon that controls many other daemons. By default there are many daemons that you can safely disable without compromising your systems' performance.

Disabling a service in */etc/inetd.conf* involves placing a pound sign (#) at the beginning of each daemon that you wish to disable.

For example, the default entry in */etc/inetd.conf* for the *finger* service looks like this:

```
finger stream tcp nowait guest /usr/etc/tcpd fingerd -L
```

Placing a pound sign at the beginning of the line disables the service from starting:

```
#finger stream tcp nowait guest /usr/etc/tcpd fingerd -L
```

I suggest disabling the following services:

```
telnet  
ftp  
shell  
login  
exec  
finger  
http  
wn-http  
bootp  
tftp  
ntalk  
echo  
discard  
chargen  
daytime  
time  
uucp  
mouted/1,3  
sgi_mouted/1  
rstatd/1-3  
wall/1  
rusersd/1  
rquotad/1  
sprayd/1  
bootparam/1  
ypupdated/1  
rex/1  
sgi_videod/1  
sgi_toolkitbus/1  
sgi_snoopd/1  
sgi_pcsd/1  
sgi_pod/1  
sgi_xfsmd/1  
sgi_espd/1  
sgi-esphttp  
ttdbserverd/1  
tcpmux/sgi_scanner
```

Please note that in my opinion both telnet and ftp should be turned off. Both services represent clear security risks since they transmit passwords in plain text. For this reason and many others

you should be using OpenSSH instead. (Please see #8 for more details.)

6. Chkconfig

The `chkconfig` command is a very handy way to disable services that are running by default but which are either a security risk or not required by your system (or both!). Using `chkconfig` is simple. For example, to get a listing of your current system configuration, simply type:

```
# chkconfig
```

To disable a service, such as `gated`, you would type the following:

```
# chkconfig gated off
```

Likewise, to enable the service `gated` you would type the following:

```
# chkconfig gated on
```

Use the following as suggested guide for the various services configured by `chkconfig`. Please keep in mind that we've attempted to make this list as comprehensive as possible but your system may have one or more services installed that aren't included in our list. If this is the case we suggest not disabling any extra services unless you are certain they are not required.

Enable:

```
desktop  
esp  
lockd  
lp  
mediad  
network  
noiconlogin  
nsd  
rtmond  
savecore  
verbose  
visuallogin  
windowssystem  
xdm
```

Disable:

```
appletalk  
array  
autoconfig_ipaddress  
autofs  
automount  
fcagent  
fontserver  
gated
```

ipaliases
mrouted
named
nds
netwr_client
nfs
nostickytmp
ns_admin
nss_fasttrack
pmcd
pmie
privileges
proclaim_relayagent
proclaim_server
proxymngr
quickpage
rarpd
routed
rsvdpd
rwhod
sar
sdpd
sendmail
sendmail_cf
snetd
timed
timeslave
ts
vswap
webface
yp
ypmaster
ypserv

7. Install Additional Applications

SGI provides a large library of freely available, pre-compiled programs that can be obtained from <http://freeware.sgi.com>. While this resource does provide a convenient, centralized location for obtaining many popular programs, for some reason SGI choose to make `/usr/freeware/bin` the default installation directory. Besides the confusion that can be caused by putting binaries in a non-standard location, the `/usr/freeware/bin` directory is not part of the default SGI command path. Luckily, SGI supplies a script called `fixpath` that, when run, will automatically append `/usr/freeware/bin` to your command path. Please run the following command after you install your first freeware app:

```
# /usr/freeware/bin/fixpath
```

TCP Wrappers

This program allows you to very precisely and selectively control which systems can access the various TCP/IP services running on your computer.

First, download and install the TCP Wrappers program from <http://freeware.sgi.com>

Then, copy the `/usr/freeware/bin/tcpd` to `/usr/etc`:

```
# cp /usr/freeware/bin/tcpd /usr/etc/tcpd
```

Create the `/usr/etc/...` (yes, the name of the directory is three dots!)

```
# mkdir /usr/etc/...
```

Move the daemons that you wish to wrap to the `/usr/etc/...` directory:

```
# cd /usr/etc
# mv telnetd ftpd rshd rlogind rexecd fingerd /usr/etc/...
```

Add `tcpd` to the appropriate lines in `/etc/inetd.conf`. When you are done they should look something like this:

```
ftp stream tcp nowait root /usr/etc/tcpd ftpd -l
telnet stream tcp nowait root /usr/etc/tcpd telnetd
shell stream tcp nowait root /usr/etc/tcpd rshd -L
login stream tcp nowait root /usr/etc/tcpd rlogind
exec stream tcp nowait root /usr/etc/tcpd rexecd
finger stream tcp nowait guest /usr/etc/tcpd fingerd -L
```

Create a file called `/var/adm/tcpd.log`:

```
# touch /var/adm/tcpd.log
```

The access rules for TCP Wrappers are defined in two files - `/etc/hosts.allow` and `/etc/hosts.deny`. As their names suggest, the `/etc/hosts.allow` file is where you define who can access the system while the `/etc/hosts.deny` file applies to anyone who isn't defined in `/etc/hosts.allow`.

At a minimum, I suggest the following for `/etc/hosts.allow`:

```
ALL : .yourdomain.com
```

I suggest the following for `/etc/hosts.deny` (don't forget to substitute your hostname and email address!):

```
ALL:ALL:spawn echo "Attempt from %h %a to %d at `date`" \
| /usr/bin/tee -a /var/adm/tcpd.log | /usr/sbin/mailx \
-s "Security Alert - host.domain.com" root@host.domain.com
```

This script does several things. First, it tells your computer to deny access to anyone who isn't included in the `/etc/hosts.allow` file. Second, it generates a warning message that includes the attacking hostname, IP address, and date and which is appended to the `/var/adm/tcpd.log` file. Third, it emails the proper person a copy of the access attempt log entry.

OpenSSH

This is a free, secure replacement for ftp, telnet, rcp, and several other insecure programs which encrypts data transmitted between systems to help prevent information from being intercepted or modified by malicious individuals.

First, install the following packages in the following order from <http://freeware.sgi.com>:

```
zlib
openssl
openssh
```

Then, run the following command to ensure openssh starts when the system is booted:

```
# chkconfig sshd on
```

If you're curious, additional technical details about OpenSSH can be found at <http://www.openssh.org>.

8. Change Root Email Alias

Your system has several email addresses that are installed on your system by default. Two of the most important are postmaster and root. Many important system messages are automatically sent to one or sometimes both of these addresses and it is wise to monitor these messages closely. A convenient way of doing this is modifying your system so that any messages sent to either of these two addresses are automatically sent to your personal email address instead. Doing this is simple:

Edit the `/etc/aliases` file and modify the following line from this:

```
#root:
```

To this:

```
root:your@emailaddress.com
```

Then, reinitialize the alias file to make sure your changes take effect:

```
# newaliases
```

9. Subscribe to Mailing Lists

The world of computer security is very complex and changes rapidly. New bugs and the attacks

that exploit them are constantly being discovered; by subscribing and reading one or more of the following lists regularly you can help ensure that you remain as well informed as possible.

- SGI Wiretap Mailing List
- BuqTraq
- CERT Advisory Mailing List

Details on subscribing to these and other lists can be found here:

<http://www.sgi.com/support/security/posts.html>

References

Silicon Graphics, Inc. “SGI Security Homepage.”

<http://www.sgi.com/support/security/index.html>

Silicon Graphics, Inc. “SGI Maintenance Release Homepage.”

<http://support.sgi.com/colls/patches/tools/relstream/index.html>

Silicon Graphics, Inc. “SGI Freeware Homepage.”

<http://freeware.sgi.com>

Silicon Graphics, Inc. “SGI Newsgroups and Mailing Lists Homepage.”

<http://www.sgi.com/support/security/posts.html>

The OpenBSD Project. “OpenSSH Homepage.”

<http://www.openssh.org>

European Organization for Nuclear Research (CERN). “CERN Security Handbook.” v1.2. 12 December, 1996.

http://consult.cern.ch/writeups/security/security_3.html#SEC7



Upcoming SANS Training

[Click Here for a full list of all Upcoming SANS Events by Location](#)

SANS London 2009	London, United Kingdom	Nov 28, 2009 - Dec 06, 2009	Live Event
SANS WhatWorks in Incident Detection Summit 2009	Washington, DC	Dec 09, 2009 - Dec 10, 2009	Live Event
SANS CDI East 2009	Washington, DC	Dec 11, 2009 - Dec 18, 2009	Live Event
SANS WhatWorks in Data Leakage Prevention and Encryption Summit 2010	New Orleans, LA	Jan 07, 2010 - Jan 12, 2010	Live Event
SANS Security East 2010	New Orleans, LA	Jan 10, 2010 - Jan 18, 2010	Live Event
SANS AppSec 2010 and WhatWorks in AppSec Summit	San Francisco, CA	Jan 29, 2010 - Feb 05, 2010	Live Event
SANS Phoenix 2010	Phoenix, AZ	Feb 14, 2010 - Feb 20, 2010	Live Event
SANS Tokyo 2010 Spring	Tokyo, Japan	Feb 15, 2010 - Feb 20, 2010	Live Event
SANS Geneva CISSP at HEG 2009 Autumn	OnlineSwitzerland	Nov 23, 2009 - Nov 28, 2009	Live Event
SANS OnDemand	Books & MP3s Only	Anytime	Self Paced