

Solaris as a Server Security Best Practices

**JH Network Security
September 6, 2001**

Installing Solaris as a Server

Basic Steps to follow

1. Install Operating System
 - a. Configure Partitions
 - b. Create strong root password
2. Patch Operating System
 - a. Stop all possible services before connecting to network
3. Strip the Operating System
 - a. Disable startup scripts.
 - b. Remove unnecessary user accounts
 - c. Set /dev/null shells for unused accounts
4. Harden Operating System
 - a. Configure global login settings
 - b. Set global umask
 - c. Ip random sequence generation
5. Configure Networking
 - a. Ensure routing settings are appropriate for environment
 - b. Disable dhcp and multicast if not in use
 - c. Configure dns and routing
 - d. Configure syslog to log authentication information
 - e. Disable Ip Forwarding
6. Install Security Tools
 - a. Tcpwrappers
 - b. Secure Shell
7. Monitor Activity and Patches

Things you may need to know ahead of time:

- If installing on Sparc hardware, there may be some issues with the hardware release of the software you are installing. Verify this information ahead of time if possible.
 - For instance for some UltraSparc 5 and 10 you need at least the 3/98 revision of Solaris 2.6 to even boot the install CDROM.
 - Also, the hardware may have come with software that needs to be installed to get certain devices to work with certain software.
- If running on PC hardware you may have to know some things about your hardware
 - How many hard drives do you have?
 - What size is each hard drive (e.g., 3.2GB)?
 - If you have more than one hard drive, which is the primary one?
 - What kind of hard drive do you have (e.g., IDE, SCSI)?
 - How much RAM do you have (e.g., 256MB RAM)?
 - Do you have a SCSI adapter? If so, who made it and what model is it?
 - Do you have a RAID system? If so, who made it and what model is it?
 - What type of mouse do you have (e.g., PS/2, Microsoft, Logitech)?
 - How many buttons does your mouse have (2/3)?
 - If you have a serial mouse, what COM port is it connected to (e.g., COM1)?
 - What is the make and model of your video card? How much video RAM do you have?
 - What kind of monitor do you have (make and model)?
- Will you be connected to a network? If so, what will be the following:
 - Your IP address?

- Your netmask?
- Your gateway address?
- Your domain name servers IP addresses?
- Your domain name?
- Your hostname?
- Your number and types of network(s) card(s) (make and model)?

1. Installing the operating system.

- a. Install from original source media. This may be a tape or CDROM. DO NOT attach the system to the network until directed below. Default installation of Solaris starts up many services that are vulnerable to attack immediately. Physically isolate the machine if possible, this prevents someone else from accidentally connecting to the network or changing configurations.
- b. Consider system requirements, depends on amount of disk space, amount of users, and function of machine.
- c. An example of a workgroup server with one internal and one external 9GB disk :
 - / - 150MB
 1. The top of the hierarchical file tree.
 2. Contains the directories and files critical for system operation, such as the kernel (/kernel/unix), the device drivers, and the programs used to start (boot) the system.
 3. It also contains the mount point directories where local and remote file systems can be attached to the file tree.
 - Swap - 256 MB -2x Installed memory (max. 1GB swap)
 - /var - 2056MB
 1. Contains system files and directories that are likely to change or grow over the life of the local system.
 2. These include system logs, vi and ex backup files, and uucp files.
 3. For syslog/web/news/proxy servers, consider using a larger partition and/or a separate disk.
 - /usr - 1024MB
 1. Contains system files and directories that can be shared with other users.
 2. Files that run only on certain types of systems are in the /usr directory (for example SPARC® executables).
 3. Files (such as manual pages) that can be used on all types of systems are in /usr/share.
 - /opt - 1024MB
 1. Mount point for optional, third-party software.
 2. Many Packages will install here by default.
 3. Patch cluster stores information about patches here.
 - /export/home - 9GB
 1. The mount point for users' home directories, which store users' work files.
 - a. Size according to type & number of users on system.
 - b. If possible put on a separate disk.
 - /usr/local - 3072MB
 1. Most common location for custom applications. Many system administrators compile applications here. If possible place on a separate disk with /export/home for upgrades.

- 2.If you know you will be storing large amounts of data, it does not hurt to put it on a separate disk if possible. That way if the system crashes it is possible to recover data easily.
- d.Different types of software groups to install. Depends on use of the system.
 - Entire Distribution Plus OEM
 - Entire Distribution
 - 1.The entire Solaris release (everything on the CD). Compilers and debuggers are not included.
 - Developer System Support -- Recommended software group.
 - 1.The end user software plus software for developing software including libraries, include files, man pages, and programming tools. Compilers and debuggers are not included.
 - 2.If planning on developing software, this is the group to install.
 - End User System Support
 - 1.The core group plus the recommended software for an end user including OpenWindows and the DeskSet software.
 - Core System Support
 - 1.The minimum software required to boot and run Solaris software.
 - 2.If no GUI user interface is required this is the group to install.
- e.After the first reboot, you will be asked to set a root password.
 - The password should not be based on any personal information such as: names, addresses, phone number, birthday, etc.
 - The password should be a minimum of 6 characters long.
 - The password should be a combination of uppercase and lowercase letters.
 - The password should include letters, digits, and special characters
 - 1.Including: ['~!@#\$%^&*()-_+=+{[]}\ |";,;<.>/?]
 - The password should not be any word found in any language. Substituting numbers for letters does not help here, because password-cracking utilities take this into account. For example, using r1dg3 instead of ridge is still a bad idea.

2.Patch the system

- a.Stop all network services.
 - Scripts are located in /etc/init.d
 - You stop the services by typing (for example) **./sendmail stop**.
 - Also, you will need to kill the inetd process.


```
ps -ef | grep inetd
kill -9 (whatever the pid number is)
```
- b.It is very important that you stop these services or your box could be compromised before you even start to protect it. It is not that uncommon for boxes to be attacked within the first few hours of it being attached to the network.
- c.Obtain Recommended patches from sunsolve.sun.com/pub/patches It can take twice as long to install patches as to install the core OS.
 - Name will depend on version and hardware.
 - For Intel Solaris 7, it would be 7_x86_Recommended.zip
- d.Read through CLUSTER_README file.
 - Save a log of what patches are installed already:


```
showrev -p > patches.before
```
- e.To install all the patches in one go, change to the subdirectory and run the installation, either install with either of the following methods:

- Installation on a new system, or where de-installtion is unlikely to be necessary, or a system reinstall is OK if the patch cluster messes things up
 - 1.This will save lots of disk space
 - 2..**install_cluster -nosave**
 - Installation on an existing system, or where de-installtion of the patches must be possible if the patch cluser messes things up.
 - 1.This will take more disk space as copies are saved in /var/sadm/patch.
 - 2..**install_cluster**
 - 3.Patches can only be individually de-installed, there is no "deinstall_cluster".
- f.Check to see what patches were actually installed:
- showrev -p > patches.after**
 - diff patches.after patches.before**
 - Check the installation log:
 - more /var/sadm/install_data/Solaris_<version>_Recommended_log**
- g.The patch cluster does not always contain all the patches, you will need to go to <http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access> and ensure you have the latest patches. **showrev -p** will show you the current patches installed. Keep in mind that you do not need to patch a service that you do not have installed.

3.Strip the operating system

- a.Having unnecessary services running opens you to more vulnerabilities, as well as potentially adversely affecting performance. Services are started from scripts with filenames beginning with S and a number. The number represents the order in which the scripts are executed. There are also "Kill" scripts, which begin with a K.
- b.For every startup script in /etc/rc0.d, /etc/rc1.d, and /etc/rc3.d rename to .no<filename>.
- c.It is recommended to disable the following services if you are not going to be using them. In /etc/rc2.d and rcS.d disable the following services by renaming them to something like .no<filename>. It is best to not delete these scripts, as you may discover you need to run a service later on:
 - autofs
 - 1.Disabling this will prevent the system from autoloading devices, like CDROMs or floppies.
 - autoinstall
 - 1.Used for "JumpStart"
 - devfsadm
 - 1.Manages special device files in /dev and /devices.
 - Dtlogin
 - 1.If you want to be able to graphical login, you will need this to run.
 - 2.**For servers it is recommended that the GUI is NOT used.**
 - nfs.client and nfs.server
 - 1.Both services are required to function as a nfs client.
 - nscd - name service cache daemon
 - 1.Provides caching for passwd, group, and hosts databases.
 - 2.May cause problems if using dns.
 - 3.Necessary to run any version of Netscape greater than 4.5.
 - powerd
 - 1.Running power management may require this to be running.
 - 2.It is a good idea to run this for a workstation, unless you need remote access.
 - PCMCIA

- 1. Only disable if you have don't have PCMCIA devices
- PRESERVE
- rpc
 - 1.If you intend to run CDE, you will need to allow this to run.
 - 2.Required for autofs
 - 3.Required for nfs
- sendmail
 - 1.If not properly configure can be exploited for relaying
 - 2.Many vulnerabilities in older versions.
 - 3.Best to disable this service initially even if planning to run it.
 - 4.Always install the latest supported version.
- sysid.net
- sysid.sys
- tsquantum
 - 1.Has something to do with time steps.
- d.Remove the line "sc:234:respawn:/usr/lib/saf/sac -t 300" from /etc/inittab. This is a process to listen on serial ports. If you are planning to connect a modem to one of the serial ports, do not disable this process. Disabling this prevents someone from locally connecting to the serial port.
- e.Remove unnecessary user accounts & set /dev/null shells


```
# for user in uucp nuucp adm lp smtp listen
> do
> /usr/sbin/passmgmt -d $user
> done
```
- f.Accounts like nobody and noaccess should have their shells set to /dev/null to prevent people from logging into them.
 - Do not set the shell to /dev/null for root or any users that will be actively logging into the system! If you do, you will not be able to access these accounts, from anywhere!
 - edit /etc/passwd and change shell to /dev/null change


```
nobody:x:60001:60001:Nobody:/:
to
nobody:x:60001:60001:Nobody:/:/dev/null
```
- g.NEVER have root equivalent accounts!! There should be no reason to be root equivalent.
 - In terms of auditing, it may be easier to determine what happened if only one account as root privileges.
 - If you like to use a different shell, simply su then evoking the shell.

4.Harden the OS

- a.Edit su and login files in /etc/default to set default path. You may want to add /usr/local/bin to the default path, since this is where most software installs binaries.
 - Placement of /usr/local/bin in the path is important.
 - 1.If there are multiples of the same binary the one found in path first will be used.
 - A good practice to protect you server would be to restrict write access of /usr/local/bin to only root.
 - This means only root can install new software everyone has access to.
 - This can prevent binaries from be altered.
- b.It is also a good idea to set a timeout. If someone forgets to log out and walks away from the machine, they will be automatically logged out after a set amount of time.

- Uncomment the timeout line in the /etc/default/login file.
- c.Add all users in /etc/passwd to /etc/ftpusers.
- This file lists users that CANNOT ftp. Even if ftp server is not presently running, it is best to add all accounts to this file to protect against future changes.
 - Be sure to change ownership and mode of file. This prevents other users from making changes to this file.
 - Be sure to add any new users to this file also.
 - 1.touch /etc/ftpusers
 - 2.chown root:root /etc/ftpusers
 - 3.chmod 600 /etc/ftpusers
 - # for user in root daemon bin sys nobody noaccess nobody4
 - > do
 - > echo \$user >> /etc/ftpusers
 - > done
- d.Fix IP random sequence generation. This will help prevent people from using spoofing to attack your machine. There may be performance issues in changing this option. If you are going to have very high traffic volumes, you may want to leave this option default.
- Edit the last line of /etc/default/inetinit to say:
 - TCP_STRONG_ISS=2
 - If machines main purpose it to be a webserver, you may want to set this to 0.
- e.You can create a message that appears whenever someone accesses or logs in to your machine. This may be required on some systems, to alert people they are accessing a sensitive system and that they are being monitored.
- /etc/issue is banner that comes up when system is accessed. It is a good idea not to reveal too much information as to the contents and use of the box in issue. Any user who attempts to connect to your box will see this information and can use it to find vulnerabilities.
 - /etc/motd is shown after a successful login. Here you can give more specific information if you desire, because the user has already authenticated to the box. Issue is not shown when using ssh, however motd can be if selected in ssh config.
 - Sample motd or issue:


```
*****
Use of this system is restricted to
authorized personnel only.

All use of and activity on this system is
monitored and logged. Use of this system
constitutes consent to such monitoring.

Contact security@jhmi.edu for more information.

*****
```
- f.Configure logging so any login attempts are logged.
- To log to file add line "auth.info /var/log/authlog"
 - White spaces must be tabs. This can be set to log to file, remote host, or printer
 - If using log file, be sure to create and chown and chmod file
 - chmod 600 /var/log/authlog
 - chown root:sys /var/log/authlog

- Be sure to restart the syslogd process
 - ps -ef | grep syslogd**
 - kill -HUP "pid"**
- g. Comment out rhosts_auth from pam.conf. This prevents the use of rlogin, rsh and other remote commands. So if you require the use of these commands do not remove it from pam.conf. Any line containing rhosts, put a # in front of it.
- h. Create startup script to set umask.

```

•echo 'umask 022' >/etc/init.d/umask.sh
•chmod 744 /etc/init.d/umask.sh
  # for dir in /etc/rc?.d
  > do
  > ln -s ../init.d/umask $dir/S00umask.sh
  > done

```

5. Setting up networking

- a. The machine needs to know how to access the rest of the network. Do this by setting a default route.
- echo xxx.xxx.xxx.xxx > /etc/defaultrouter**
 - Where xxx.xxx.xxx.xxx is equal to whatever your default router should be. In most cases it will be the first 3 octets of your ip then .1. For example. IP of 128.220.56.223 defaultrouter of 128.220.56.1.
 - These number may not be correct for all networks. Contact your network administrator if you are unsure of these numbers.
- b. Create notrouter, this will disable ip forwarding.
- touch /etc/notrouter**
- c. Configure dns information. If you are using DHCP this is not necessary.
- Edit /etc/resolv.conf and add the following lines. List additional nameserver on separate lines.

domain name	<nts>.jhu.edu
nameserver	128.220.2.7
nameserver	128.220.2.82
 - Ensure the line "hosts: files dns" is in /etc/nsswitch.conf. If it not, then add it.
- d. Set correct network mask information, this is important in terms of routing. Your machine will route more efficiently if it is properly aware of its location on the network. Having this set correctly also reduces excess network traffic.
- Edit /etc/netmasks to set proper broadcast domain.
 - 128.220.72.0 255.255.255.0
 - These number may not be correct for all networks. Contact your network administrator if you are unsure of these numbers.
- e. Inetinit: Disable ip forwarding, source routing (if there is more than one network interface), and avoid echo broadcasts. Add the following to the end of /etc/init.d/inetinit:
- ndd -set /dev/ip ip_forward_directed_broadcasts 0**
 - ndd -set /dev/ip ip_forward_src_routed 0**
 - ndd -set /dev/ip ip_forwarding 0**
 - ndd -set /dev/ip ip_respond_to_echo_broadcast 0**
 - ndd -set /dev/ip ip_strict_dst_multihoming 1**
- f. If inetd, multicast and dhcp are not required, disable them.
- NDS for Solaris uses SLP, which requires Multicast be enabled.
 - This will also disable inetd.
 - 1./etc/inetd.conf fields explained

- a.service name
- b.socket type (stream or datagram)
- c.protocol type (TCP or UDP)
- d.wait/nowait - If wait server will subsequently process all connections, if nowait server will exec a new server process for each connection
- e.user
- f.command Name
- g.arguments (Optional)
- h.-- sample inetd.conf section --
- i.


```
#ftp stream tcp nowait root /usr/sbin/in.ftpd in.ftpd
#telnet stream tcp nowait root /usr/sbin/in.telnetd
in.telnetd
```

--sample inetd.conf section --

- 2.Inetd is a daemon whose purpose is to listen for TCP or UDP connections. When a connection is received, inetd passes that connection to the appropriate service.
- 3.Inetd uses the file /etc/inetd.conf. If you plan to use inetd, be sure to comment out any services you do not need to have running.
 - a.Type **grep -v "^#" /etc/inetd.conf** if any lines show that you do not want to run, edit /etc/inetd.conf and comment out the line.

•Edit the /etc/init.d/inetsvc

- 1.make backup first **cp /etc/init.d/inetsvc /etc/init.d/inetsvc.orig**
- 2.Comment out all lines relating to dhcp, inetd and multicast.
- 3.Comment out all lines after "Add a static route for multicast packets out our default interface. The default interface is the interface that corresponds to the node name"
- 4.Be sure to comment out last line!
 - a.#/usr/sbin/inetd -s &

g.Verify all services that can be stopped are.

•Type ps -ef. For a box, running a GUI this is the typical output

```
UID PID PPID C STIME TTY TIME CMD
root 0 0 0 15:54:08 ? 0:01 sched
root 1 0 0 15:54:08 ? 0:00 /etc/init -
root 2 0 0 15:54:08 ? 0:00 pageout
root 3 0 0 15:54:08 ? 0:42 fsflush
root 128 1 0 15:54:27 ? 0:00 /usr/sbin/cron
root 629 1 0 09:19:23 console 0:00 /usr/lib/saf/ttymon -g -h -p
jhns console login: -T sun -d /dev/console -l con
root 107 1 0 15:54:26 ? 0:00 /usr/local/sbin/sshd
root 635 505 0 09:27:15 pts/2 0:00 sh
root 124 1 0 15:54:27 ? 0:00 /usr/sbin/syslogd
root 139 1 0 15:54:28 ? 0:00 /usr/lib/utmpd
root 866 1 0 11:09:28 ? 0:00 /usr/sbin/rpcbind
root 868 1 0 11:09:28 ? 0:00 /usr/sbin/keyserv
root 856 635 0 11:03:41 pts/2 0:00 ps -ef
root 885 1 1 11:09:44 ? 0:00 /usr/dt/bin/dtlogin -daemon
```

•There will also be processes under whichever username you log in as

6. Install tools

- a. If you have multiple similar machines, the best practice would be to compile on only one machine. Do not install compilers unless you need them, or uninstall them when not using them. Most likely going to need gzip and gcc <http://www.sunfreeware.com/>
Ensure that /usr/ccs/bin and wherever gcc installed to is in your path.
- b. **Install Tcpwrappers** <ftp://ftp.porcupine.org/>.
- Tcpwrappers allow you to control which ip addresses can connect to which services. It will create two files: /etc/hosts.allow and /etc/hosts.deny
- c. You can use ip addresses or domain name information. Do not put things like 128.220. or jhu.edu. This makes room for a greater chance of being hacked, since internal mischief can occur.
- d. Your /etc/hosts.allow should look like this to allow ssh in from specific hosts:
- **sshd: xxx.xxx.xxx.xxx**
 - Remember that services run as daemons. meaning if you want to control who can connect to telnet, you must put telnetd not just telnet.
- e. In order to install TcpWrappers you will need to edit the Makefile. Uncomment the proper REAL_DAEMON_DIR for your operating system In the section about your particular Os, you may need to tell it which compiler you are using. **CC=gcc**
- You must add /usr/ccs/bin and wherever you installed gcc to (by default it is usually /usr/local/bin) Make will not work if these are not in your path!
 - Then type:
 - **make sys-type** (i.e. sunos5)
 - tcpd.h and libwrap.a will be created. Copy them to /usr/lib.
 - If installing ssh-3.0.1 you will need to copy libwrap.a to /usr/lib and tcpd.h to /usr/include
- f. In order to use tcpwrappers in conjunction with inetd, you must edit the lines of the services you wish to use.
- To use tcpwrappers with ftp for example in /etc/inetd.conf:
 - 1.ftp stream tcp nowait root /usr/sbin/in.ftpd in.ftpd
 - 2.change to
 - 3.ftp stream tcp nowait root /usr/sbin/tcpd in.ftpd in.ftpd
 - Be sure to restart the inetd process after making changes.
 - Tcpd will be created during the make above, copy this to /usr/sbin for this work.
- g. Prevent access from anyone not specifically allowed.
- Configure /etc/hosts.deny
 1. Blanket deny ALL:ALL statement. /etc/hosts.allow overrides /etc/hosts.deny, so deny all and allow specifically. You can have email messages sent if access is attempted
 2. /etc/hosts.deny should look like this:
**ALL:ALL: /usr/bin/mailx **
**-s "%s: connection attempt from %c" **
user@domain.com
- h. To allow access using tcpwrappers, edit the /etc/hosts.allow file.
- For example to allow ftp access you would add the line:
in.ftpd : host.you.want.to.allow
 - You can use ip addresses or dns information here.
- i. **Install SSH** <ftp://ftp.ssh.org/>.
- Secure shell allows you to securely connect to a remote machine. It is highly recommended that you use ssh exclusively. It replaces, telnet, ftp and all r commands. See secure shell documentation on jhns for more information.

j. Configure Sendmail.

- Some Standard Mail User Agents invoke sendmail directly to deliver mail; therefore even if sendmail is not running as a service, it still needs to be configured.
 - You will need to add the fully-qualified domain name to /etc/hosts
 - 1.Be sure to add it after the short name
 - 2.128.220.xxx.xxx servername servername.jhu.edu
 - Configure the /etc/mail/sendmail.cf so sendmail uses a "Smart" relay
 - 1.Look for this line:
"Smart" relay host (may be null)
 - 2.Then add this below it
DSjhtml.hcf.jhu.edu
- k.Should do level 0 (complete) backup now.
- Attempt to keep backup secure.
 - Keep tape separate from other backup to prevent tape from being overwritten.
 - If you can avoid it, do not use a networked backup scheme.
 - 1.Usually requires additional software to be installed.
 - 2.Often these programs overrides system security
 - 3.Data most likely passed in clear text.
 - a.If someone is monitoring network traffic, they can see all your files.

7. Monitoring

- a. Monitor daily for changes to system files.
- b. Pay close attention to the processes running, and look for the reappearance of inetd.conf. Also for new users and permission changes.
- c. Monitor /var/log/authlog and /var/adm/loginlog for any unusual activity or attempts to connect.

Monitor the web for security updates and patches to your OS and programs you are running. If possible test patches before using them in a production environment.