



## **NISCC Technical Note 11/03 Issued 10 December 2003**

### **Secure Configuration of Solaris**

#### **Key Points**

- Start with a clean install
- Plan the installation and configuration carefully
- Apply the latest patch cluster
- Lock the system down
- Create a backup
- Subscribe to appropriate alert services
- Perform regular maintenance

**National Infrastructure  
Security Co-Ordination Centre**  
PO Box 832  
London, SW1P 1BG

Tel: 020 7821 1330 Ext 4511  
Fax: 020 7821 1686  
Email: [enquiries@niscc.gov.uk](mailto:enquiries@niscc.gov.uk)  
Web: [www.niscc.gov.uk](http://www.niscc.gov.uk)

## Introduction

1. This Briefing details the steps and processes required to build and maintain a Solaris system in a secure configuration. It is aimed at Solaris 8, but the process is applicable for all versions of the Solaris 2 series (aka SunOS 5.x) including Solaris 9 and the pending Solaris 10.
2. Please remember that there is no such thing as a 100% secure system. The best you can achieve is to improve the security in the hope that any potential attacker will be discouraged, or detected before they succeed.
3. References to specific tools, web sites and documents should not be taken as an endorsement by NISCC. These are merely used as examples of what is available.

## Assumptions

4. It is assumed that the hardware is hosted in a physically secure environment. If this is not the case then further steps will have to be taken to ensure the security of the system – details can be found in paragraph 31.
5. Anybody using this document to build a system is assumed to be a technically competent Solaris administrator. There is no attempt to hold the reader's hand through any of the processes detailed.

## Other Reading

6. Sun provides various security related documents and links. This includes:
  - a. The Sun Security pages at <http://www.sun.com/software/security>
  - b. Sun BigAdmin at <http://www.sun.com/bigadmin/>
  - c. Sun BluePrints at <http://www.sun.com/solutions/blueprints/>
7. In particular the documents by Lance Spitzner in the BigAdmin section, and the security related documents in the BluePrints section are worth reading.

## Starting from Scratch

8. It is recommended that you begin with a clean build. While it is possible to work from an existing system, there will always be the risk that the system has already been compromised.
9. Start with known good, trusted, installation media. Ideally this should be original media from Sun, however it is acceptable to download the relevant ISO images from Sun, assuming that the checksums have been confirmed. There may be a charge from Sun for downloading ISO images and for licenses.
10. Ideally you should use a version certified to an appropriate level, under a known security standard (such as the Common Criteria). The most recent CC certified version at this time is Solaris 8 HW 2/02. If you are unable to use the certified version for operational reasons then you should use the most current release available to you.
11. Where possible avoid the use of NIS for password sharing. NIS has some significant security flaws that make it relatively trivial for an attacker with network access to the NIS server to gain

access to the encrypted passwords. An attacker using modern hardware should be able to break a number of those passwords within 24 hours to obtain usable username and password pairs.

## Priorities

12. If you are short of time and want to secure a system quickly then the following areas are ones that you should undertake first. Keep in mind that the system will not be as secure as if you had built it from scratch.

- a. Patches
- b. Lockdown

## The Install

13. Pull the network cable. Keep the system disconnected from any networks until you have completed this document. That reduces the risk that the system may be compromised during the install or configuration.

14. Read the Install documentation for the version of Solaris you are installing to ensure your hardware meets the requirements, and to ensure that you allocate sufficient swap and disk space to each partition.

15. Plan the disk layout carefully. As a minimum you should have separate partitions for / (root), the user home directories (traditionally /export/home) and /var. Where the system is going to be storing significant amounts of data (such as a departmental mail server) it is recommended you create a separate partition for that directory. The suggested sizes below assume a sufficiently large disk (if you have more than one disk, you may wish to put /export on another disk).

- a. / - the root partition. This should be sized to ensure it does not fill up, a minimum 500 MB
- b. /usr - holds the majority of the system binaries. A minimum 2 GB.
- c. /usr/local - locally installed software. The required size will vary according to expected use, but 2 GB is probably a good starting point. You may wish to simply allocate some extra space to /usr instead of having a separate partition.
- d. /opt - Sun's alternative to /usr/local. The space required will depend on what software you will be installing, but 4 GB is a good minimum. You may want to consider consolidating /opt with /usr or /usr/local (or all 3) to minimise wasted space.
- e. /var - system logs, spool directories etc. At least 200 MB, more for mail or log servers. If you have enabled the auditing feature of Solaris you will want to increase this, and possibly create a separate /var/audit partition. You may wish to mount this partition with the "nosuid" option to disable SUID files.
- f. /export - home directories etc. As large as is likely to be required. You should consider mounting this partition with the "nosuid" option to disabled SUID files.

- g. swap – traditionally 2 times the installed RAM, however a minimum size of 512 MB is recommended by Sun. The maximum size will vary according to the expected use of the server and installed memory. A file server will require less memory than a busy database server.

16. Install only the packages required for that particular system. Installing a larger set may be convenient, however it is likely to introduce vulnerabilities. Where possible do not install any compilers. If you need to compile code do it on a dedicated system and copy the compiled executables across.

17. When prompted for a root password – pick a strong password. With Solaris (at least up until Solaris 9) only the first 8 characters are significant – anything beyond that is ignored. The password should contain a mix of upper and lower case letters, numbers and symbols. It should not be a word (in any language) or based upon one. An example of a suitable password is T!d#20tS. Any written record of the password must be kept secure.

## Post install – time to patch

18. Download and install the latest patch cluster from the Sun web site (<http://sunsolve.sun.com>). This will install all of the universally applicable patches released up to the point that the patch cluster was created. A more complete patch install can be completed later, once the system has been secured.

19. To identify all required patches you should investigate Sun's PatchPro. This is designed to be run on systems with either direct Internet access, or access through an HTTP proxy. You can find it, and other patch management tools, under the patches section of Sun's BigAdmin site (<http://www.sun.com/bigadmin/patches/index.html>).

## Secure the System

20. Now the system has been built and brought up to date with patches, it is time to lock it down. There are a number of steps to take, and tools that may help.

21. Sun have a tool called the Solaris Security Toolkit (also known as JASS) that is designed to automate the process of securing a Solaris system. It is suggested that you download this tool and investigate its suitability for your environment. Do not run it on a production system without first testing it. (If you do, you may find that required functionality has been disabled and the system no longer meets your business needs). You can find it at <http://www.sun.com/solutions/blueprints/tools/>.

22. Secure the file systems.

- a. Remove unrequired write access from a large number of directories and files, for example by using the unsupported `fix-modes` tool by Casper Dik (one of Sun's engineers). Applying patches may require this tool to be re-run.
- b. Mount file systems read only where possible (such as `/usr`, `/usr/local` and `/opt`).
- c. Where file systems do not hold system binaries (or other files that must be SetUID) mount them `nosuid` to disable SetUID programs. The filesystems that this should not be used on include `/`, `/usr` and possibly `/opt`.

23. Secure login accounts

- a. Remove any accounts that are not required, using `userdel` or the Sun Management Console. This does not just refer to user accounts, but to some of the pre-installed accounts such as `listen` and `uucp`. Which accounts can be safely removed will depend on the purpose of the system.
- b. For accounts that are required, but should not normally be used, disable them by locking their password (`passwd -l <account>`). Set the account's shell to an invalid shell such as `/usr/bin/false`. Where the Solaris Security Toolkit has been installed there is a `/sbin/noshell`, which has the advantage of logging attempted access.

24. Restrict access to job scheduling (`at`, `cron` and `batch`)

- a. Only accounts that require access to job scheduling should be given access. This can be controlled by listing these accounts in the relevant files, `/etc/cron.allow` and `/etc/at.allow`. By listing accounts in these files you automatically deny other accounts access to job scheduling.
- b. At a minimum you must provide `root`, `adm` and `lp` with the ability to schedule jobs.

25. Set the kernel level security

- a. You can tighten security by adding the following to `/etc/system` and then performing a configuration reboot (`reboot -- -r`)

```
set nfssrv:nfs_portmon = 1
set noexec_user_stack = 1
set noexec_user_stack_log = 1
set sys:coredumpsize = 0
```
- b. These configure the NFS server (if used) to only accept requests from privileged ports, disable support for executing code on the system stack and disable core dumps.

26. Disable services that are not required

- a. Set the value of `umask` in `/etc/default/init` to `027`. This ensures that files created by the system are not group writeable, or world accessible by default.
- b. Disable `sendmail` if the host is not a mail server. This will not stop your system sending email, however it will stop it listening to receive email. You may have to schedule a job to periodically process the mail queue, in case of delivery problems. You can do this by putting the following in `root`'s crontab:

```
0 * * * * /usr/lib/sendmail -q
```

- c. Disable standalone services started by `init`. These are found in the directories `/etc/rcX.d`, where `X` is either `S` or a number from `0` to `6`) that start with the letter `S` (ie `/etc/rc3.d/S98tcpchk`). Prefix any services that are not required with an underscore to disable them.

d. Services you may wish to disable on most servers include:

i. `/etc/rc2.d`

`pppd`            `uucp`            `slpd`            `sendmail`

ii. `/etc/rc3.d`

`apache`            `snmpdx`            `samba`

e. Disable (remove or prefix with a '#' symbol) services managed by `inetd`. These are listed in `/etc/inetd.conf`.

i. Replace `telnet`, `rlogin`, `rsh`, `rcp`, `rexec` and `ftp` with a more secure alternative such as `ssh` (which encrypts all network traffic). These services pass the username and password unencrypted across the network, meaning anybody with access to the network can capture usernames and passwords.

ii. You can disable the user of `/etc/hosts.equiv` and `$HOME/.rhosts` by commenting out the following lines of `/etc/pam.conf` and then rebooting:

```
rlogin        auth    sufficient   pam_rhosts_auth.so.1
```

```
rsh    auth    sufficient   pam_rhosts_auth.so.1
```

iii. Disable or remove the following, at a minimum:

```
tnamed
uucpd
fingerd
sysstat
netstat
time
echo
discard
chargen
tftp (leave on servers that support network boot clients)
lpd
```

f. You can also disable most RPC based services in `/etc/inetd.conf`. These can be identified by the protocol field starting "`rpc/`". For any that remain you should ensure that they use either `AUTH_DES` or `AUTH_KERB` instead of the default `AUTH_UNIX`, which is known to be weak and easily forged.

g. On systems that will not be receiving `syslog` messages from other hosts, disable the listening port of `syslog`. You can do this by editing `/etc/init.d/syslog` and appending "`-t`" to the startup for `syslog`. On Solaris 9 and later you can achieve this by putting the following in `/etc/default/syslog`:

```
LOG_FROM_REMOTE=NO
```

## 27. Install and Configure TCP Wrappers

a. On Solaris 8 and older you may wish to install TCP Wrappers (it is included with Solaris 9). These allow you to control access to TCP-based services on your host.

You can use TCP Wrappers with services launched from inetd, and with some other services that support it.

- b. While not a replacement for patching services, or running a firewall, it does help restrict the risk of running any services that can be protected.

## 28. Install and configure firewalling software.

- a. Any systems that connects, directly or indirectly, to networks outside of your control (eg other organisations or the Internet) should be protected by a firewall. As well as providing firewalls at the network boundary it is worth considering running firewall software on the host itself, for example:
  - i. SunScreen light is a product that is bundled with Solaris 8 and later. It can filter traffic on no more than 2 network interfaces.
  - ii. IP Filter is a freeware alternative that is available for Solaris 2.3 and later.
- b. Remember that a poorly configured firewall is often no better than not having one at all. The default action should always be to deny (drop or block). Access should be defined as tightly as possible.

## 29. Install checksum software

- a. Software such as Tripwire and Aide allow you to take checksums of your installed system and then compare the existing files against those checksums to alert you to any changes.
- b. Sun holds a database of fingerprints for Sun software. This is an effective check of the authenticity of any software provided by Sun, but it is not able to confirm the authenticity of non-Sun software or configuration files.
- c. Once any checksum software has been run and has produced a database, you must copy this database to a read only medium. This ensures that, if the system is compromised, the attacker cannot wipe or alter this database. Some checksum software cryptographically signs the database to detect attempts to alter it, but it cannot stop the database from being wiped.

## 30. Miscellaneous Security

- a. Create `/var/adm/loginlog` to enable logging of failed logins. This must have mode 0600 and be owned by root with a group of sys.
- b. Enable logging to a central host by uncommenting the line in `/etc/syslog.conf` that begins with `"#auth.notice ifdef..."`. This ensures that you will still have log entries if the host is compromised. You may need to change how the syslog server is started on the remote machine to enable it to accept remote clients.
- c. Set the `CONSOLE` entry in `/etc/default/login` to either `/dev/console` (for the local console) or `/dev/ttya` (for the serial console). If possible set it to `"-"` to force access to the root account to be only via the su command.
- d. For NFS exports ensure that the exports are to named hosts only and provide the minimum access required. Share only the directories that are required. Where

possible use strong authentication, such as AUTH\_DES or AUTH\_KERB, instead of the default unix security mechanisms (AUTH\_UNIX).

- e. If the system has multiple network interfaces but is not to act as a router, then you must create `/etc/notrouter`. If you do not, then Solaris will automatically act as a router, broadcasting routing information and potentially disrupting your network, as well as possibly providing an unexpected, and unprotected, route between networks.
- f. Configure `ntp` to ensure that all systems agree on the current time. Details can be found in the Blueprint section of the Sun web site - <http://www.sun.com/solutions/blueprints/>.
- g. Create `/etc/issue` with an appropriate message in it. What should go here will be defined by your security policy, and may include warnings about unauthorised use being unacceptable.
- h. Create empty banners (or one with no useful information for identifying the operating system, host platform etc) for telnet, ftp and other services that support it, to hide the OS information, making life slightly harder for would-be attackers. This can be done by adding the following line to the files `/etc/default/telnet` and `/etc/default/ftp`:  
  

```
BANNER=""
```
- i. On Solaris 8, and earlier, add `-t` to the `inetd` startup in `/etc/init.d/inetsvc`. In Solaris 9 you can achieve the same by setting `ENABLE_CONNECTION_LOGGING=YES` in `/etc/default/inetd`. This will log all incoming connections to the `inetd` daemon.
- j. Disable caching of passwords by the name service cache daemon (`ncsd`) by setting the time to live to zero for password and RBAC entries in `/etc/ncsd.conf`.

### 31. Securing from physical access

- a. For systems that you cannot secure physical access to, consider use of the EEPROM security mode command to stop people booting from unauthorised media. You can do this when logged in as root by typing the following:  
  

```
eeeprom boot-mode=command
```
- b. On those systems you may also want to disable the `<STOP><A>` sequence by adding the following line to `/etc/system`:  
  

```
set abort_enable=0
```
- c. On Solaris 8 and later you can achieve this by setting the following in `/etc/default/kbd`:  
  

```
KEYBOARD_ABORT=DISABLE
```

## Backup

32. Before you go any further it is important that you take the time to back the system up (creating what is known as a Day Zero backup) and check that the backup has worked.
33. This serves 2 purposes:
  - a. You can easily clone this system to create more like it. Once the backup has been restored you can use the `sysunconfig` command to remove settings such as the hostname, IP address etc. Then you simply reboot and answer a few questions.
  - b. If something goes wrong, you can recover the system easily and quickly.

## Time to go online

34. You can now connect your system to the network.
35. To keep your patches current, and make identifying what you need to apply easier, Sun provide a number of options. It is worth visiting <http://sunsolve.sun.com/> and examining the patch options to see what suits your environment the best.

## Watch the news

36. Subscribe to Solaris related mailing lists to ensure you receive timely notification of patches and new vulnerabilities.
37. Watch sites such as <http://www.uniras.gov.uk/>, <http://www.cert.org/> and <http://www.securityfocus.com/>. They, and other similar sites, provide useful information about new vulnerabilities.

## Ongoing maintenance

38. At regular intervals, ideally daily but at least weekly, perform the following checks as an absolute minimum:

- a. Disk space – are any of the partitions filling up rapidly? This could indicate an attempted or successful attack.
- b. Checksums – have any changed? If you are making changes to the system remember to check the checksums before and after the change, investigating any unexpected differences. Once you have completed the changes make sure you update the master database.
- c. SUID/SGID files – have you gained any new ones? You can find SUID files by using the following command:

```
find / -type f -perm -4000 -ls
```

To find SGID files use:

```
find / -type f -perm -2000 -ls
```

- d. Inappropriate writable access – do any system files or directories have group or world write when they shouldn't have?
- e. System logs – are there any unusual or suspicious entries? There are a number of tools to help with this process.
- f. Patches – are you current? Keep in mind that installing patches may undo some of your security changes. After installation ensure that nothing you have disabled has been re-enabled or that no configuration changes or permission changes have been reset.
- g. Services – are there any services running that should not be? You can use “netstat -an” to find out what ports have been bound to. A useful third party tool for this is “lsof” that lists open files, but can also list open ports with “lsof -i”.
- h. Accounts – are there any new accounts on the system?
- i. Backups – ensure you take backups at regular intervals. These should be tested periodically to ensure that they are working and providing valid data for recovery.

39. Tools such as Tripwire and Aide can provide some of the functionality above (particularly identifying changed, new and removed files) and may be worth investigating. Other checks are scriptable with only a little effort.