UnixWorld Online: Tutorial Article No. 003

How to Improve Security on a Newly Installed SunOS 4.1.3 System

By Thomas M. Kroeger and Braden W. Carter

Questions regarding this article should be directed to the authors at tmk@cse.ucsc.edu or bwcarter@cse.ucsc.edu

We'd like this document to remain current and evolve to become even more useful to the Unix community. Please send Solaris 1.1 and 1.1.1 security tips not covered here, along with any necessary pointers or references to beccat@wcmh.com. We will include those we judge suitable along with a credit for the contributor.

Abstract

Our goal is to provide some of the more basic steps that you can do to improve security on a newly installed SunOS 4.1.3 (Solaris 1.1 or 1.1.1) system. *Disclaimer:* This is by no means an all-inclusive list of actions, just some of the simple and more common measures. These recommendations come with no guarantees!

The intended audience is anyone responsible for the system administration duties of a machine running SunOS 4.1.3. These recommendations are applicable to a stand-alone workstation, which may be connected to a larger network. It is assumed that the reader has some familiarity with basic Unix system administration. (You should be able to do a basic system installation by yourself, install patches, and use an editor).

Please note that this list limits its coverage to measures that can be done for a stand-alone workstation. In addition to the steps listed here, there are many measures that can be taken to improve the security of an environment. For example, filtering traffic to port `2049/udp` at the routers will prevent NFS calls from outside your domain. Such measures, while extremely helpful, can be quite specific to individual system needs and can become quite involved. A proper coverage of these issues would warrant a book, not a short write up. More detailed coverage of these measures can be found in Reference 2.

The truly paranoid may wish to implement these recommendations while in single user mode, as an extra measure of security to avoid possible subversive shenanigans by a wily cracker.

Steps to Improve Security

Patches to Install

4.1.3 Security listing

100103 SunOS 4.1;4.1.1;4.1.2;4.1.3: script to change file permissions
100173 SunOS 4.1.1/4.1.2/4.1.3 : NFS Jumbo Patch
100224 SunOS 4.1.1,4.1.2,4.1.3: /bin/mail jumbo patch *
100257 SunOS 4.1.1;4.1.2;4.1.3: jumbo patch for ld.so, ldd, and ldconf
100272 SunOS 4.1.3: Security update for in.comsat.
100296 SunOS 4.1.1, 4.1.2, 4.1.3: netgroup exports to world
100305 SunOS 4.1.1, 4.1.2, 4.1.3: lpr Jumbo Patch
100372 SunOS 4.1.1;4.1.2;4.1.3: tfs and c2 do not work together
100377 SunOS 4.1.1, 4.1.2, 4.1.3: sendmail jumbo patch
100383 SunOS 4.0.3;4.1;4.1.1;4.1.2;4.1.3: rdist security and hard link *
100448 OpenWindows 3.0: loadmodule is a security hole.
100452 OpenWindows 3.0: XView 3.0 Jumbo Patch
100478 OpenWindows 3.0: xlock crashes leaving system open
100482 SunOS 4.1;4.1.1;4.1.2;4.1.3: ypserv and ypxfrd fix, plus DNS fix *
100507 SunOS 4.1.1, 4.1.2, 4.1.3: tmpfs jumbo patch
100513 SunOS 4.1.1;4.1.2;4.1.3: Jumbo tty patch
100564 SunOS 4.1.2, 4.1.3: C2 Jumbo patch
100593 SunOS 4.1.3: Security update for dump. *
100623 SunOS 4.1.2;4.1.3: UFS jumbo patch
100630 SunOS 4.1.1, 4.1.2, 4.1.3: SECURITY: methods to exploit login/su
100631 SunOS 4.1.x: env variables can be used to exploit login(US only)
100632 SunSHIELD 1.0: ARM jumbo patch release *
100890 SunOS 4.1.3: domestic libc jumbo patch
100891 SunOS 4.1.3: international libc jumbo patch
100909 SunOS 4.1.1;4.1.2;4.1.3: Security update for syslogd.
101072 SunOS 4.1.1;4.1.2;4.1.3: Non-related data filled the last block
101080 SunOS 4.1.1 4.1.2 4.1.3: security problem with expreserve
101200 SunOS 4.1.1, 4.1.2, 4.1.3: Breach of security using modload
101206 ODS 1.0; NFS/fsirand security fix.
101480 SunOS 4.1.1;4.1.2;4.1.3: Security update for in.talkd. *
101482 SunOS 4.1.3, 4.1.2, 4.1.1: Security update for write. *

101640 SunOS 4.1.3: in.ftpd logs password info when -d option is used.
102023 SunOS 4.1.3: Root access possible via forced passwd race condition
101710 ONLINE DISKSUITE (ODS) 1.0: Security update for dump.

4.1.3_UI Security listing

101434 SunOS 4.1.3_U1: lpr Jumbo Patch
101435 SunOS 4.1.3_U1: ypserv fix *
101436 SunOS 4.1.3_U1: bin/mail jumbo patch *
101440 SunOS 4.1.3_U1: security problem: methods to exploit login/su
101558 SunOS 4.1.3_U1: international libc jumbo patch
101579 SunOS 4.1.3_U1: Security problem with expreserve for Solaris 1. *
101587 SunOS 4.1.3_U1: security patch for mfree and icmp redirect
101590 ONLINE DISKSUITE (ODS) 1.0, NFS/fsirand security fix
101621 SunOS 4.1.3_U1: Jumbo tty patch
101665 SunOS 4.1.3_U1: sendmail jumbo patch *
101679 SunOS 4.1.3_U1: Breach of security using modload
101759 SunOS 4.1.3_U1: domestic libc jumbo patch

* Some patches may not be required if you are disabling this feature. If this is the case, ensure that all relevant files have had their mode changed to remove the set-user-ID bit with `chmod u-s <file>`.

Please also note that some patches may not necessarily apply, based on packages installed (US Encryption...) or your configuration. Carefully check the `README` file for each patch.

Patches are available via anonymous FTP from ftp://ftp.uu.net/systems/sun/sun-dist/.

Back to the Index of Steps.

Network Changes

- **Disable source routing**
  Why
  Source routing enables the originating host to dictate the route the packet will take. This can be used to spoof a system into believing that the packets are coming from a trusted source.
  How
  Install source routing patch found in Reference 19.
  More Info
  Reference 2 Chap 2, Reference 19
- **Comment out all unnecessary services in `/etc/inetd.conf`**
  Why
  RPC services can be used to gain access as well as information about a system. These are very site specific adjustments and will have to be tailored to your needs. Additionally, TCP wrappers can be used to improve logging, prevent IP spoofing (one host pretending to be another in order to gain access to a target node), and limit access to a service as well as totally removing it. Reference 4

How

Edit the `/etc/inetd.conf` file and put a pound sign (`#`) in front of services that are not needed.

Note

Services possibly not needed, but probably desired include

- *ftp* - possibly needed for file transfer, however if all you want is outgoing ftp then this is can be commented out
- *telnet* - obvious (recommend restricting with TCP wrappers, Reference 4)
- *finger* - probably better to get a modified version that doesn't give up much information
- *talk* - nice to have but how much will you miss it?

Services that are probably unnecessary (see man pages for details)

- *name* - for name services, `tnamed`(8)
- *comsat* - for mail, not necessary
- *login* - for rlogin, please see discussion of ruserok
- *uucp* - if you're not sure you're using this then you probably are not
- *exec* - services for rexecd, best to do without

Services recommended against using. (*Find a way to live without these.*)

- *shell* - for rsh, major source for security problems
- *tftp* - only needed for support of an X terminal or diskless clients; doubtfully needed on a desktop machine

More Info

Reference 4, Reference 15, Reference 22 Chap 11

- **Enable NFS port monitoring (This is of value only if you are exporting file systems over NFS)**

Why

Port monitoring ensures that calls to NFS to mount a file system come from a port number less than 1024 (in other words, a port that requires root access to use).

How

The default `/etc/rc.local` file sets up port monitoring only if the file `/etc/security/passwd.adjunct` exists. Otherwise, if you will be implementing shadowing then you can skip over this step. If you will not be implementing shadowing and you will be exporting files then you should modify `/etc/rc.local` to do the following two lines, regardless of whether or not the `passwd.adjunct` file exists.

```
echo "nfs_portmon/W1" | adb -w /vmunix /dev/kmem > /dev/null 2>&1
rpc.mountd
```

Note

One possible side effect is that non-Sun NFS client might not be able to mount exported files. Shadowing is covered under the ID Management Changes section.

More Info

Reference 3, pg. 177, and `mountd`(8C)

- **Ensure that `ypbind` is invoked with the `-s` option**

Why

Users could easily start their own ypbind services and activate a phony NIS database giving them access as any user.

How

As with port monitoring the default `/etc/rc.local` sets up `ypbind` in the secure mode, using the `-s` option, only if the file `/etc/security/passwd.adjunct` exists. If you will be implementing shadowing then you can skip over this step, otherwise you should modify `/etc/rc.local` to start `ypbind` with the `-s` option regardless of whether the `passwd.adjunct` file exists.

More Info

`ypbind`(8)

Return to the Index of Steps.

Kernel Changes

- **Disable IP forwarding**

  Why

  This could be used to spoof an IP address on a machine with two network interfaces.

  How

  Install the following line in the kernel configuration file:

  ```
  options "IPFORWARDING=-1"
  ```

  More Info

  For info on how to custom configure a kernel, see the file `/usr/sys/`arch`/conf/README`

- **Modify ruserok(3)** in /usr/lib/libc.so.1.8 (libc.so.1.9 on 4.1.3_U1) to disable
  - root `.rhosts` authentication,
  - wildcards in `.rhosts`, or
  - `.rhosts` entirely, depending on desired security level.

  Why

  `ruserok`(3) is a library routine that does the checking of both the `.rhosts` and `/etc/hosts.equiv` files for all the ‘‘r’’ commands.

  - `ruserok(3)` uses the source IP address in the rpc request for authentication. There are no guarantees that this address is correct. This address can easily be spoofed, yielding illegitimate access to a system.
  - Crackers will often insert plus signs (+) into users’ `.rhosts` file to allow them to gain access at a latter date. Most users don’t look at their `.rhosts` file too often.

  While using `.rhosts` prevents crackers from sniffing your users’ passwords, it also make them vulnerable to IP spoofing (claiming to be a host that you’re not).

  How

  To modify the source code requires a source code license. For those who wish to create their own modified version of `ruserok`(3) please see the technical note section at the end that describes some of the details for creating a custom libc.so.

  Additionally the logdaemon package Reference 15 has a modified version of libc.so that helps with this.

  Finally TCP wrappers can also be used to restrict access to each individual ‘‘r’’ command. Reference 4

  More Info

  `ruserok`(3), `hosts.equiv`(5), source code file /lib/libc/net/rcmd.c, Reference 4, Reference 15

- **Uncomment security options in frame buffer table file `/etc/fbtab`**

  Why

  Without these entries, ownership of console devices will not be properly set.

More Info

`fbtab`(5)

- **Remove `/dev/nit`**

Why

The `/dev/nit` device file is Sun's network interface, which can be used by crackers that have already broken into a machine to examine network packets for password information.

How

Remove the device from the kernel's configuration and rebuild the kernel. (The following steps are taken from Reference 21)

```
# cd /usr/kvm/sys/sun[3,3x,4,4c]/conf
# cp CONFIG_FILE SYS_NAME
```

Note that at this point, you should replace the `CONFIG_FILE` with your system specific configuration file, if one exists.

```
# chmod +w SYS_NAME
# vi SYS_NAME

   #
   # The following are for streams NIT support.  NIT is used by
   # etherfind, traffic, rarpd, and ndbootd.  As a rule of thumb,
   # NIT is almost always needed on a server and almost never
   # needed on a diskless client.
   #
   pseudo-device   snit            # streams NIT
   pseudo-device   pf              # packet filter
   pseudo-device   nbuf            # NIT buffering module
```

Comment out the preceding three lines, then save and exit the editor before proceeding.

```
# config SYS_NAME
# cd ../SYS_NAME
# make

# mv /vmunix /vmunix.old
# cp vmunix /vmunix

# /etc/halt
> b
```

This step will reboot the system with the new kernel.

Notes

Please note that even after the new kernel is installed, you need to take care to ensure that the previous kernel (for example, vmunix.old) is not used to reboot the system.

More Info

Reference 21

Return to the Index of Steps.

File system Changes

- **Editing Files**
  - **Create the file *ftpd-root*`/etc/ftpusers`**

    Why

    This file is a list of users that will not be allowed to access the system via ftp. This prevents Joe Cracker from using ftp to modify a file (such as `/etc/passwd`). If he is able to determine your root password, a shell provided via ftp could be used as a springboard for a superuser shell.

    How

    Create the file *ftpd-root*`/etc/ftpusers` with the following entries (one per line), including any other existing accounts for which you don't want to allow ftp access.

    ```
    root          daemon        sys        bin
    nobody        uucp          news       ingres
    AUpwdauthd    AUyppasswdd   sysdiag    sundiag
    ```

    More Info

    `ftpusers`(5)
  - **Remove the plus sign (`+`) in `/etc/hosts.equiv`**

    Why

    Well..... Everyone gains access with this.

    Note

    `/etc/hosts.equiv` should not have any comment lines.

    More Info

    `hosts.equiv`(5)
  - **Edit `/etc/exports` and remove all entries you don't want exported. Ensure whatever entries remain have restricted access.**

    Why

    NFS leaves the normal file system protection up to the client instead of the server. A cracker with root access on a client can work around many of these protections. As a result file systems exported to the world are particularly vulnerable.

    How

    Edit the `/etc/exports` file to:

    1. Only export what you need to export. If you aren't certain that it needs to be exported, then it probably doesn't.
    2. Never export to the world. Use the `-access=host.foo.bar.edu` option.
    3. Export the file systems read-only whenever possible, using the `ro` option.

    You can use `showmount -e` to see what you currently have exported.

    More Info

    `exports`(5), `exportfs`(8), `showmount`(8)
  - **Use `nosuid` in mounts**

    Why

    Use the nosuid option when adding entries to `/etc/fstab` to mount a file system exported by another host. Anyone gaining access to the other host can create or modify an existing program which could compromise your system. *This doesn't work on tmpfs file systems.*

    How

    Include the nosuid when you add an entry to `/etc/fstab` to import a file system.

    More Info

Reference 3, pg. 175, `fstab`(5)

- **Edit `/etc/ttytab` to remove the secure option from all entries**

  Why

  The secure entry in `/etc/ttytab` allows logins directly to root on that tty. If you feel that your machine is not in a physically secure location, you may choose to remove the secure option from the console as well. As a result you will first login as a user in the wheel group and then su to root.

  More Info

  `ttytab`(5)

- **Edit syslog.conf to uncomment `auth` and `mail` lines**

  Why

  This enables improved logging of system access and su's, but be prepared for voluminous reports.

  More Info

  `syslog.conf`(5)

Return to the Index of Steps.

- **EEPROM Configuration**
  - **Set eeprom secure field to ''command'' or ''full''**

    Why

    If you feel that your machine is not in a secure location, then the eeprom secure field can be used to prevent unauthorized root access by crashing your machine.

    Note

    With the full option the system will not auto-reboot and will wait for the root password to be entered.

    More Info

    `eeprom`(5)

  - **Remove openprom support if you do not intend to use the eeprom secure field**

    Why

    A cracker who gains root access could install an eeprom password and make your life a bit harder.

    How

    Remove the device driver from the kernel by commenting out the following.

    ```
    # The "open EEPROM" pseudo-device is required to support the
    # eeprom command.
    #
    pseudo-device   openeepr        # onboard configuration NVRAM
    ```

    More Info

    `eeprom`(5)

Return to the Index of Steps.

- **File Permissions**
  - `chmod 600 /dev/eeprom`

    Why

Prevents users from reading the eeprom passwd.

More Info

`eeprom`(5)

- **Add `umask 022` to `/etc/rc` and `/.login`**

  Why

  Prevent key files created during startup and root operation from being created world writable.

  Note

  You may want to set umask in `/.login` to 077 instead of 022.

  More Info

  `umask`(1), `rc`(8)

- `chmod go-w /etc/*`
  `chmod go+w /etc/tmp`
  `chmod g+w /etc/dumpdates`

  Why

  None of the files in the `/etc` directory should require write access by world except for `dumpdate`, which requires group write access, and `tmp`, which requires group and other write access.

  More Info

  `chmod`(1), `aliases`(5), `state`(5), `utmp`(5), `remote`(5), `rmtab`(5)

- **Edit `/etc/rc.local` to comment line(s) that `chmod 666 motd`**

  Why

  `/etc/motd` is the standard message-of-the-day file. It won't allow people to gain root access, but it could be a nuisance if they can change this anonymously. Additionally, it is important to ensure that the line `"rm -f /tmp/t1"` is at the beginning of this portion of `/etc/rc.local`

- Disable set-user-ID (`chmod u-s file`) for the following program files, unless you specifically use them:

```
/usr/bin/cu              /usr/bin/tip             /usr/bin/fusage
/usr/bin/nsquery         /usr/bin/uucp            /usr/bin/uuname
/usr/bin/uustat          /usr/bin/uux             /usr/ucb/rcp
/usr/ucb/rdist           /usr/ucb/rlogin          /usr/lib/uucp/uusched
/usr/lib/uucp/uuxqt      /usr/ucb/rsh             /usr/lib/uucp/uucico
/usr/games/hack          /usr/games/chesstool     /usr/games/fortune
/usr/lib/exrecover       /usr/games/robots        /usr/lib/uucp/remote.unknow
/usr/games/hack          /usr/games/snake         /usr/bin/sunview1/sv_releas
/usr/etc/rfsetup         /usr/bin/allocate        /usr/ucb/quota
/usr/lib/expreserve
```

  Why

  Disabling set-user-ID modes for those programs you don't use helps prevent would be crackers from exploiting unknown security flaws that could be used to compromise your system.

  Note

  `/usr/bin/allocate` is used with C2 security.
  `/usr/ucb/quota` is used with disk quotas.
  `/usr/lib/expreserve` is used to recover a `vi` edit session that died.
  If the following programs are only run by root:

```
/usr/etc/shutdown        /usr/lib/acct/accton
```

they don't need to be set-user-ID.

More Info

Reference 22 Chap 4, lots of man pages ;-)

- Disable set-group-ID mode (`chmod g-s` *`program-file`*) for the following files unless you specifically use them:

```
/usr/bin/wall          /usr/etc/trpt          /usr/bin/sunview1/toolplace
/usr/bin/iostat        /usr/bin/ipcs          /usr/ucb/vmstat
/usr/ucb/netstat       /usr/etc/arp           /usr/etc/dmesg
/usr/etc/dkinfo        /usr/etc/chill         /usr/etc/dumpfs
/usr/etc/devinfo       /usr/etc/nfsstat       /usr/old/perfmon
/openwin/bin/xload     /usr/kvm/pstat         /usr/kvm/crash
/usr/kvm/getcons       /usr/etc/kgmon         /usr/etc/trpt
```

Why

Disabling set-group-ID modes for programs that you won't need helps prevent would be crackers from exploiting unknown security flaws.

More Info

Reference 22, chap 4, lots of man pages ;-)

- `chmod 640 /vmunix` and `chgrp kmem /vmunix`

Why

Prevent crackers from finding out more about your kernel configuration.

Return to the Index of Steps.

- Install Random Number I-node Generator on File systems fsirand

Why

Predictable root handles assists crackers in abusing NFS. After installing the patch for fsirand you'll need to run fsirand for all your file systems.

How

Ensure the file system is unmounted and run fsirand.

More Info

`fsirand`(8), SunOS patch 100173 (NFS Jumbo), Reference 22 pg. 268

Return to the Index of Steps.

ID Management Changes

- Disable set-user-ID mode for passwd program (if using NIS) or disable `-F` option in `/bin/passwd` program.

Why

Here two scenarios exist.

1. If you are using NIS for your user database, you don't need `/bin/passwd` to be set-user-ID root. The same applies to the two hard links pointing to `/bin/passwd`, namely `/bin/chfn` and `/bin/chsh`.
2. If you are using NIS and you want to support password modification in the your local `/etc/passwd` file, then please note that `/bin/passwd` has a race condition that can be

exploited to write to files as root, allowing a cracker to gain root access.

Because `rpc.yppasswdd` runs as user-ID root on the NIS server, neither `yppasswd`, `ypchfn`, nor `ypchsh` need to be set-user-ID root.

How

No matter which of the above scenarios you wish to implement, do

```
cd /bin; chmod u-s yppasswd ypchfn ypchsh
```

Then, choose one of these options.

1. To disable `/bin/passwd`, do

   ```
   cd /bin; chmod u-s passwd chfn chsh
   ```

2. Otherwise, to allow users to modify `/etc/passwd` via `passwd`, `chfn`, or `chsh`, either.
   - Replace `/bin/passwd` with a proactive `passwd` program that checks for bad passwords (Reference 7), or
   - do a binary edit of /bin/passwd (Sun's code) from the prompt, as shown below.

   ```
   # cd /bin
   # cp passwd passwd.old; chmod 700 passwd.old
   # adb -w - passwd
   not core file = passwd
   /l 'F:'
   0x68de
   0x68de/w 0
   0x68de:         0x463a  =       0x0
   <CTRL-D>
   # chmod 4711 /bin/passwd
   ```

   Note that the above address, `0x68de`, is required for the `0x68de/w 0` step.

Note

The following files should all contain the same code, and be set-user-ID root (unless disabled as discussed above). If you intend to use any of these, ensure they are a link to the modified file `/bin/passwd`.

```
yppasswd        ypchfn        ypchsh        chfn        chsh
```

More Info

Reference 6

- Remove `sync` entry from the password file

  Why

  This account is used to let administrators ‘‘sync’’ the file system before a system crash. By default, `sync` has no password, allowing it to be abused to gain access to the system. The simplest solution is to live without this feature and remove this account.

  More Info

  `passwd`(5)

- Implement password shadowing

  Why

  To restrict access to all users' encrypted passwords. Even though passwords are encrypted, Crack (a publicly available program) can be used to effectively guess users' passwords. Reference 20

  How

  This can be done one of two different ways.

  1. By implementing Sun's C2 security package, which provides additional auditing. I've

found that this auditing can be troublesome to maintain and I didn't have need for the extensive data.

2. The second option is to implement shadowing but not C2, this procedure is fully explained in detail in Reference 5. In summary,
   - Ensure patch 100564 is installed, (note this also implements securenets for NIS),
   - split `/etc/passwd` into `/etc/passwd` and `/etc/security/passwd.adjunct`,
   - divide `/etc/group` into `/etc/group` and `/etc/security/group.adjunct`,
   - add required Audit users (even if not implementing auditing),
   - comment out the part of `/etc/rc.local` that starts audit, and
   - reboot.

Note

The existence of the `/etc/security/passwd.adjunct` file has several other effects in `rc.local` that improves system security (`ypbind -s` and `rpc.mountd` without -n).

More Info Reference 5

- Ensure all accounts have passwords

  Why

  Any account without a password provides open access to your system. *Note that as delivered the `/etc/passwd` file has no password for the ''root'' account!*

  More Info

  `passwd`(5)

Back to the Index of Steps.

Mail System Modifications

Why

The sendmail program itself has been notorious for numerous bugs that can give crackers root access illegitimately. This is a huge topic and should be a paper or book in itself. We claim no expertise here. ;-) Even so, there are several different possible configurations and options that will be outlined before we point you to further references.

Host configuration:

1. If you intend to send and receive mail directly on your machine, your options are to:
   - live with sendmail by installing the newest version, following a few guidelines, or
     - Ensure a mail file is always in existence for all users. Reference 10 and Reference 11
     - `chmod u-s /bin/mail` and change sendmail to use "procmail" or mail.local. Reference 17
     - Change sendmail default user-ID in `sendmail.cf` to 65534.
     - Turn on security features of sendmail, including

       ```
       Opauthwarnings  needmailhelo  noexpn  novrfy  restrictmailq
       ```

       Reference 2 and Reference 9

   - install Zmailer. Reference 8

Note

Zmailer does not use the `/bin/mail` program so `chmod u-s /bin/mail`.

2. If your mail delivery is handled by another host then your system should only need to support outgoing mail. To prevent the sendmail daemon from being started, comment out the line(s) in `/etc/rc.local` that invoke sendmail. For outgoing mail,
   - install latest version of sendmail, or
     - see previous comments in this section for things to change in sendmail config,
     - `chmod u-s /bin/mail`, since mail delivery is being handled by main mail host there is no need for `/bin/mail` to be set-user-ID.
   - install Zmailer. Reference 8

     Zmailer does not use `/bin/mail` so `chmod u-s /bin/mail`.
3. No need for mail whatsoever on this machine--incoming, outgoing, or internal. This is certainly the most secure mode because e-mail will not be able to be sent from or to this machine. This basic restriction of outside access will prevent abuse of that service.

   How

   To disable mail totally,
   - `chmod u-s /usr/lib/sendmail /usr/lib/sendmail.mx /bin/mail`
   - comment out the line(s) in `/etc/rc.local` that invoke Sendmail.

Back to the Index of Steps.

Packages for Better Security and Monitoring

- **Tripwire**, Reference 13

  (Be sure to include all set-user- and set-group-ID files in your configuration.)
- **Tcp wrappers**, Reference 4
- **COPS**, Reference 14

  Set up to run each night. Be careful to check the bit bucket output to ensure that it is working properly.
- **Modified `portmapper, login, rshd, rlogind, pidentd`** from W. Venema, Reference 15
- **TAMU Tiger Scripts**, Reference 16
- **xinetd**, an improved version of inetd, Reference 23

Note: the Australian group SERT (Reference 18) has put together a package named **MegaPatch** that includes several of these packages as well as many of the patches to SunOS previously mentioned.

Back to the Index of Steps.

References

[1] Dan Farmer & Wietse Venema, "Improving the security of your Site by Breaking Into it", 1993. (ftp://ftp.win.tue.nl:/pub/security/admin-guide-to-cracking.Z)

[2] W. Cheswick & S. Bellovin, "Firewalls and Internet Security", Addison-Wesley, April 94.

[3] H. Stern, "Managing NFS & NIS", O'Reilly & Associates, April 92.

[4] Wietse Venema, "TCP WRAPPER: Network monitoring, access control and booby traps" (ftp://ftp.win.tue.nl/pub/security/tcp_wrapper.ps.Z), Proceedings of the Third Usenix Unix Security Symposium, pg. 85-92. (text version) (tcp wrapper package -- look for most recent version of tcp_wrappers_*.shar.Z)

[5] Eric Oliver, "How to shadow without C2 Auditing", June 94. (ftp://ftp.hawaii.edu/pub/security/docs/shadow.wo.audit.4.1.3)

[6] [8lgm]-Advisory-7.UNIX.passwd.11-May-1994.NEWFIX

[7] Proactive password changing programs (`passwd+`, `npasswd`) (There are several this is the only one who's URL I had available) anlpasswd (look for most recent version of anlpasswd-*.tar.Z), passwdd (look for the most recent version of passwdd-*.tar.Z)

[8] Zmailer package, and the README file (ftp://cs.toronto.edu/pub/zmailer/)

[9] Bryan Costales, Eric Allman, and Neil Rickert, "Sendmail", O'Reilly & Associates, June 93.

8lgm advisories are available though the 8lgm file server at 8lgm-fileserver@bagpuss.demon.co.uk. Please note that you must include information about which advisory you want. To get instructions, include the word `help` in the message body.

[10] [8lgm]-Advisory-5.UNIX.mail.24-Jan-1992
[11] [8lgm]-Advisory-5.UNIX.mail.24-Jan-1992.PATCH
[12] [8lgm]-Advisory-6.UNIX.mail2.2-May-1994

[13] Gene Kim & Gene Spafford Tripwire, 1994. (ftp://coast.cs.purdue.edu/pub/Purdue/papers/spafford/Tripwire.ps.Z)

[14] Dan Farmer & Gene Spafford Cops, 1990. (ftp://ftp.cert.org/pub/tools/cops/)

[15] Wietse Venema `portmapper`, `login`, `rshd`, `rlogind` portmap, logdaemon (ftp://ftp.win.tue.nl/pub/security/)

[16] Safford et. al. TAMU tiger script, 1993. (ftp://net.tamu.edu/pub/security/TAMU/)

[17] Local mail delivery agents including procmail, mail.local (by Joerg Czeranski). (ftp://ftp.informatik.rwth-aachen.de/pub/packages/)

[18] SERT's MegaPatch (ftp://ftp.sert.edu.au/security/tools/)

[19] Source Routing Patch (ftp://ftp.greatcircle.com/pub/firewalls/digest/v03.n153.Z)

[20] Crack (ftp://ftp.uu.net/usenet/comp.sources.misc/volume28/crack)

[21] CERT Advisory CA-94:01
(ftp://ftp.cert.org/pub/cert_advisories/CA-94:01.ongoing.network.monitoring.attacks)

[22] Simson Garfinkel and Gene Spafford "Practical Unix Security", O'Reilly & Associates, June 1991.

[23] "xinetd-2.1.2" ("ftp://unix.hensa.ac.uk/pub/uunet/published/oreilly/nutshell/miis/xinetd-2.1.2.tar.gz)

Back to the Index of Steps.

Technical Note

We felt that this item was not really directed toward our targeted audience, yet still worth mention:

Customizing `ruserok`(3)

How

If you have source license to 4.1.3, modify the routine `ruserok`(3) to return -1 for the cases you wish to disallow. To disable `.rhosts` authentication entirely, simply have this routine return -1. Look at the `/usr/lib/shlib.etc/README` file for how to modify `libc.so`.
Note to also make the following changes:

- In the file `/usr/lib/shlib.etc/README` below the line:
  ```
  % mv rpc_commondata. rpc_commondata.o
  ```
  insert
  ```
  % mv xccs.multibyte. xccs.multibyte.o
  ```
- In the Makefile, change the lines below to read as they do here.
  ```
  OBJSORT=/usr/lib/shlib.etc/objsort
  AWKFILE=/usr/lib/shlib.etc/awkfile
  ```
- Add the `-ldl` option at the end of both ld command lines.

More Info

`ruserok`(3), `hosts.equiv`(5) source code file /lib/libc/net/rcmd.c Reference 4, Reference 15

Back to the Index of Steps.

Acknowledgments

Thanks to all the people in comp.security.unix who offered their suggestions, and thanks to the following people for their kind review:

spaf@cs.purdue.edu (Gene Spafford)
rgoodman@uhunix.uhcc.hawaii.edu (Becky Goodman)
andys@unipalm.co.uk (Andy Smith)

Back to the Index of Steps.

Thomas M. Kroeger (tmk@cse.ucsc.edu) / Braden W. Carter (bwcarter@cse.ucsc.edu)

Edited by Becca Thomas / Online Editor / UnixWorld Online / beccat@wcmh.com

Last Modified: Wednesday, 23-Aug-95 16:01:46 PDT