

Security Review: Solaris 8 Setuid/Setgid Files

Information Systems and Technology

University of Waterloo

Synopsis

This paper is a brief update to the review we did on Solaris 7 Setuid/Setgid Files (21-Apr-1999). Solaris 8 (also known as SunOS 5.8) is very similar to Solaris 7 (also known as SunOS 5.7) with a few minor exceptions. We'll skip any discussion of the files which are common to the two systems (you should read the Solaris 7 paper) and describe only the differences. Our previous recommendations still stand for the setuid/setgid files common to Solaris 7 and 8.

Caution: the list of setuid/setgid files we found on our system may not correspond to what you find on your system -- it's only a point in time sample on one machine. The recommendations we've made are suitable for *medium grade security* requirements. It is possible to lock a system down very tightly -- see for example Warren Belfer (11-Aug-2000).

A Bourne Shell script to implement the recommendations made here is available (suitable for systems at UW and perhaps elsewhere) -- it can be edited to implement your choices.

(by) Reg Quinton, Information Systems and Technology
2000/08/17 - 2003/09/30

Security Review: Solaris 8 Setuid/Setgid Files

Information Systems and Technology

University of Waterloo

Baseline

The Solaris 8 system we reviewed and the list of setuid/setgid files we found where as follows:

```
Script started on Thu Aug 17 11:34:02 2000
[11:34am sun580] uname -a
SunOS sun580 5.8 Generic sun4u sparc SUNW,Ultra-5_10
[11:34am sun580] awk '/ f none [246]/ {print}' /var/sadm/install/contents
/etc/lp/alerts/printer f none 4555 lp lp 203 15969 945382884 SUNWlpmsg
/opt/SUNWspr/contrib/XEmacs20.4/lib/xemacs-20.4/sparc-sun-solaris2.5.1/movemail f none 2755 bin mail 13512 23933 913761148 SPROxmbin
/usr/bin/admintool f none 4511 root sys 341204 29025 947882627 SUNWadmap
/usr/bin/at f none 4755 root sys 36320 13542 947116469 SUNWcsu
/usr/bin/atq f none 4755 root sys 13796 39936 947116470 SUNWcsu
/usr/bin/atrm f none 4755 root sys 12756 31695 947116470 SUNWcsu
/usr/bin/cancel f none 4511 root lp 9736 23058 947116877 SUNWpcu
/usr/bin/chkey f none 4555 root sys 41708 46859 947116686 SUNWnisu
/usr/bin/crontab f none 4555 root bin 17136 40921 947116470 SUNWcsu
/usr/bin/ct f none 4111 root uucp 69784 37186 947116659 SUNWbnuu
/usr/bin/cu f none 4111 uucp uucp 83740 24096 947116673 SUNWbnuu
/usr/bin/eject f none 4555 root bin 13808 15887 947118400 SUNWcsu
/usr/bin/fdformat f none 4555 root bin 26372 49041 947116452 SUNWcsu
/usr/bin/login f none 4555 root bin 29292 59075 947116643 SUNWcsu
/usr/bin/lp f none 4511 root lp 22500 25594 955117207 SUNWpcu
/usr/bin/lpset f none 4511 root lp 7116 54809 947116827 SUNWpcu
/usr/bin/lpstat f none 4511 root lp 21592 1317 947116867 SUNWpcu
/usr/bin/mail f none 2511 root mail 61288 50965 947116674 SUNWcsu
/usr/bin/mailx f none 2511 root mail 126808 30865 947116848 SUNWcsu
/usr/bin/netstat f none 2555 root sys 55168 21029 947116860 SUNWcsu
/usr/bin/newgrp f none 4755 root sys 7328 37117 947116725 SUNWcsu
/usr/bin/passwd f none 6555 root sys 101744 17766 947116784 SUNWcsu
/usr/bin/pfexec f none 4555 root bin 6508 15149 947116796 SUNWcsu
/usr/bin/rcp f none 4555 root bin 21008 46516 947116847 SUNWcsu
/usr/bin/rdist f none 4555 root bin 55480 2951 947116862 SUNWcsu
/usr/bin/rlogin f none 4555 root bin 16012 22907 947116848 SUNWcsu
/usr/bin/rsh f none 4555 root bin 8964 44609 947116849 SUNWcsu
/usr/bin/sparcv7/ipcs f none 2555 root sys 10740 24101 947116577 SUNWipc
/usr/bin/sparcv7/ps f none 4555 root sys 27752 13090 947116855 SUNWcsu
/usr/bin/sparcv7/uptime f none 4555 root bin 11368 18254 947118347 SUNWcsu
/usr/bin/sparcv9/ipcs f none 2555 root sys 15280 38703 947116613 SUNWipcx
/usr/bin/sparcv9/ps f none 4555 root sys 36520 46480 947116883 SUNWcsxu
/usr/bin/sparcv9/uptime f none 4555 root bin 15392 12481 947118363 SUNWcsxu
/usr/bin/su f none 4555 root sys 17156 18585 947116989 SUNWcsu
/usr/bin/tip f none 4511 uucp bin 55228 34692 947117116 SUNWcsu
/usr/bin/uucp f none 4111 uucp uucp 66940 19365 947116529 SUNWbnuu
/usr/bin/uuglist f none 4111 uucp uucp 22500 1281 947116540 SUNWbnuu
/usr/bin/uuname f none 4111 uucp uucp 19568 48864 947116551 SUNWbnuu
/usr/bin/uustat f none 4111 uucp uucp 61832 47952 947116576 SUNWbnuu
/usr/bin/uux f none 4111 uucp uucp 70852 38527 947116599 SUNWbnuu
/usr/bin/volcheck f none 4555 root bin 5980 54244 947118400 SUNWvolu
/usr/bin/volrmmount f none 4555 root bin 10780 34826 947118400 SUNWvolu
/usr/bin/write f none 2555 root tty 11344 52327 947118343 SUNWcsu
/usr/dt/bin/dtaction f none 6555 root sys 22808 25926 944116689 SUNWdtbas
/usr/dt/bin/dtappgather f none 4555 root bin 34036 23313 944119013 SUNWdtbde
/usr/dt/bin/dtmail f none 2555 bin mail 1492864 46045 944121774 SUNWdtbde
/usr/dt/bin/dtmailpr f none 2555 bin mail 458004 62889 944121786 SUNWdtbde
/usr/dt/bin/dtprintinfo f none 4555 root bin 357228 13850 944120546 SUNWdtbde
/usr/dt/bin/dtsession f none 4555 root bin 164224 2740 944156363 SUNWdtwmm
/usr/dt/bin/sdtcm_convert f none 6555 root daemon 304176 60120 944118943 SUNWdtmnm
/usr/lib/acct/accton f none 4755 root adm 5040 60848 947116317 SUNWaccu
/usr/lib/fbconfig/SUNWifb_config f none 4555 root bin 99740 25218 944854900 SUNWifbcf
/usr/lib/fs/ufs/quota f none 4555 root bin 13840 12392 947116826 SUNWcsu
/usr/lib/fs/ufs/ufsdump f none 4555 root bin 82484 36819 947116540 SUNWcsu
/usr/lib/fs/ufs/ufserstore f none 4555 root bin 901204 45373 947116661 SUNWcsu
/usr/lib/lp/bin/netpr f none 4511 root bin 19620 15476 955117226 SUNWpsu
/usr/lib/pt_chmod f none 4111 root bin 4104 3778 947116854 SUNWcsu
/usr/lib/sendmail f none 4555 root bin 658616 55541 947116988 SUNWsdmdu
/usr/lib/utmp_update f none 4555 root bin 7068 60409 947117172 SUNWcsu
/usr/lib/uucp/remotex.unknown f none 4111 uucp uucp 5964 49215 947116732 SUNWbnuu
/usr/lib/uucp/uucico f none 4111 uucp uucp 166268 6445 947116855 SUNWbnuu
/usr/lib/uucp/uusched f none 4111 uucp uucp 33436 60100 947116758 SUNWbnuu
/usr/lib/uucp/uuxqt f none 4111 uucp uucp 82760 20856 947116876 SUNWbnuu
/usr/openwin/bin/Xsun f none 2755 root root 1941644 50450 945299632 SUNWxwplrt
/usr/openwin/bin/ff.core f none 6555 root bin 18144 34372 944701225 SUNWoldst
/usr/openwin/bin/kcms_calibrate f none 6755 root bin 89792 30381 942279681 SUNWkcspsg
/usr/openwin/bin/kcms_configure f none 6755 root bin 24292 42591 942279643 SUNWkcsst
/usr/openwin/bin/mailtool f none 2555 root mail 637516 56657 944701580 SUNWoldst
/usr/openwin/bin/sparcv9/kcms_configure f none 6755 root bin 31952 45773 942273275 SUNWkcsrx
/usr/openwin/bin/sys_suspend f none 4755 root bin 44452 6322 942282798 SUNWpmowu
/usr/openwin/bin/xlock f none 4775 root bin 68860 43780 945300248 SUNWxwplrt
/usr/openwin/lib/mkcookie f none 4755 root bin 27620 24111 945299729 SUNWxwplrt
/usr/platform/sun4u/sbin/EEPROM f none 2555 root sys 11376 38891 947116438 SUNWkvm
/usr/platform/sun4u/sbin/prtdiag f none 2755 root sys 4512 22503 947118367 SUNWkvm
/usr/sbin/afbcfg f none 4555 root bin 61508 19299 944695277 SUNWafbcf
/usr/sbin/allocate f none 4755 root bin 17616 53173 947118389 SUNWcsu
/usr/sbin/aspppls f none 4555 root bin 5584 20920 947116576 SUNWapppu
/usr/sbin/ffbcfg f none 4555 root bin 58980 12585 944695292 SUNWffbcf
/usr/sbin/igsconfig f none 4555 root bin 37260 36326 941496138 SUNWigsu
/usr/sbin/lpmove f none 4511 root lp 6868 16863 947116882 SUNWpcu
/usr/sbin/m64config f none 4555 root bin 28388 54466 944595359 SUNWm64cf
/usr/sbin/mkdevalloc f none 4755 root bin 9800 55620 947118389 SUNWcsu
/usr/sbin/mkdevmaps f none 4755 root bin 9948 50881 947118389 SUNWcsu
```

```
/usr/sbin/pgxconfig f none 4555 root bin 102904 64555 929538945 TSIPgxw
/usr/sbin/ping f none 4555 root bin 48028 22774 947116432 SUNWcsu
/usr/sbin/pmconfig f none 4555 root bin 28956 51944 947116837 SUNWpmu
/usr/sbin/sacadm f none 4755 root sys 22640 34467 947116901 SUNWcsu
/usr/sbin/sparcv7/prtconf f none 2555 root sys 19544 58600 947116840 SUNWcsu
/usr/sbin/sparcv7/swap f none 2555 root sys 10316 41822 947116998 SUNWcsu
/usr/sbin/sparcv7/sysdef f none 2555 root sys 22656 30408 947117013 SUNWcsu
/usr/sbin/sparcv7/whodo f none 4555 root bin 12916 13815 947118347 SUNWcsu
/usr/sbin/sparcv9/prtconf f none 2555 root sys 24488 18373 947116858 SUNWcsxu
/usr/sbin/sparcv9/swap f none 2555 root sys 13528 20913 947117006 SUNWcsxu
/usr/sbin/sparcv9/sysdef f none 2555 root sys 31520 30875 947117034 SUNWcsxu
/usr/sbin/sparcv9/whodo f none 4555 root bin 17408 20324 947118363 SUNWcsxu
/usr/sbin/static/rcp f none 4555 root bin 762688 41154 947116852 SUNWsut1
/usr/sbin/traceroute f none 4555 root bin 35652 19177 947116415 SUNWcsu
/usr/sbin/wall f none 2555 root tty 9872 39608 947118341 SUNWcsu
/usr/ucb/sparcv7/ps f none 4555 root sys 22988 61065 947118751 SUNWscpu
/usr/ucb/sparcv9/ps f none 4555 root sys 31544 33406 947118759 SUNWscpx
/usr/vmssys/bin/chkperm f none 6555 bin bin 9836 4379 947383480 SUNWfac
/usr/xpg4/bin/sparcv7/lpc f none 2555 root sys 10780 31054 947116578 SUNWxcu4
/usr/xpg4/bin/sparcv9/lpc f none 2555 root sys 15344 31816 947116613 SUNWxcu4x
[11:34am sun580] exit
script done on Thu Aug 17 11:34:20 2000
```

(by) Reg Quinton, Information Systems and Technology
2000/08/17 - 2003/09/30

Security Review: Solaris 8 Setuid/Setgid Files

Information Systems and Technology

University of Waterloo

Setuid/Setgid files missing in Solaris 8

There are a couple of Setuid/Setgid files we find in (current up to patch) Solaris 7 that we don't find in Solaris 8:

```
/usr/platform/sun4m/sbin/eeprom
/usr/sbin/arp
```

The **eeprom** is just an architecture difference -- the Solaris 8 system we used was an Ultra-sparc and the same program is found under the **sun4u** platform. The **arp** is nice to see -- Sun seems to have recognized that there's no need for this to be setgid (as per our previous recommendations).

There was one Solaris 7 setgid we had found a year ago that (on current up to patch) Solaris 7 is no longer setgid:

```
/usr/sbin/dmesg
```

Apparently some patch in the interim has prudently dropped the setgid. Actually it's a much better fix than that! The command used to be setgid so it could do kernel prods. Now it's a simple shell script that just displays information from the syslog files:

```
[3:39pm sun580] more /usr/bin/dmesg
#!/usr/bin/sh
#
# Copyright (c) 1998 by Sun Microsystems, Inc.
# All rights reserved.
#
#ident  "@(#)dmesg.sh  1.1      98/09/30 SMI"

/usr/bin/echo
/usr/bin/date
/usr/bin/cat -s ` /usr/bin/ls -tr1 /var/adm/messages.? 2>/dev/null` \
    /var/adm/messages | /usr/bin/tail -200
```

That's an elegant solution to the problem -- you no longer need to do any kernel prodding! I'm not sure which patch set gave us that version of the tool but I'm certainly happy to see it.

(by) Reg Quinton, Information Systems and Technology
2000/08/17 - 2003/09/30

Security Review: Solaris 8 Setuid/Setgid Files

Information Systems and Technology

University of Waterloo

Setuid/Setgid files new in Solaris 8

There are a few Setuid/Setgid files we found in Solaris 8 that we didn't find in Solaris 7:

```
/usr/bin/pfexec
/usr/bin/sparcv9/ipcs
/usr/bin/sparcv9/ps
/usr/bin/sparcv9/uptime
/usr/lib/fbconfig/SUNwifb_config
/usr/openwin/bin/sparcv9/kcms_configure
/usr/platform/sun4u/sbin/eeprom
/usr/platform/sun4u/sbin/prtdiag
/usr/sbin/afbconfig
/usr/sbin/aspppls
/usr/sbin/ffbconfig
/usr/sbin/igsconfig
/usr/sbin/m64config
/usr/sbin/pgxconfig
/usr/sbin/sparcv9/prtconf
/usr/sbin/sparcv9/swap
/usr/sbin/sparcv9/sysdef
/usr/sbin/sparcv9/whodo
/usr/ucb/sparcv9/ps
/usr/xpg4/bin/sparcv7/ipcs
/usr/xpg4/bin/sparcv9/ipcs
```

Most of the **sparcv9** programs under **/usr/bin**, **/usr/sbin** and **/usr/ucb** match with the **sparcv7** versions we found in Solaris 7 and most of the **sun4u** platform specific programs match Solaris 7 versions. Again they're mostly just an architectural difference between the Sparc (32bit) and Ultra-Sparc (64bit) kernels. There are a couple of surprises though -- **kcms_configure** under the Open-Windows **sparcv9** and **prtdiag** under the **sun4u** platform are new!

The two versions of **ipcs** under **/usr/xpg4** are yet another version of the **ipcs** program we found on Solaris 7 and the same recommendations apply. Apparently **XPG4** is one of the POSIX standards that Solaris implements (see the man page).

Nevertheless there are a few new tools we need to evaluate.

Security Review: Solaris 8 Setuid/Setgid Files

Information Systems and Technology

University of Waterloo

Recommendations

These recommendations are restricted to just those new files we find in Solaris 8:

1. `/usr/bin/pfexec f none 4555 root bin 6508 15149 947116796`
`SUNWcsu`

This setuid **root** tool is new to Solaris 8. It's part of the "*Core Solaris, (Usrc)*" (SUNWcsu) package. The manual page says:

The pfexec program is used to execute commands with the attributes specified by the user's profiles in the exec_attr(4) database. It is invoked by the profile shells, pfsh, pfesh, and pfksh which are linked to the Bourne shell, C shell, and Korn shell, respectively.

Profiles are searched in the order specified in the user's entry in the user_attr(4) database. If the same command appears in more than one profile, the profile shell uses the first matching entry.

This seems to be a facility for granting fine grained access controls to users. Running **pfsh** or **pfesh** seem to give me a useless shell -- probably because the two databases mentioned are trivial. I don't see any usage in any of the startup scripts in `/etc/init.d`. I did find a reference at SecurityFocus Inc. where the author recommends that you don't need it.

Recommendation: Drop the setuid -- wait until you discover an application that requires this.

2. `/usr/lib/fbconfig/SUNWifb_config f none 4555 root bin 99740`
`25218 944854900 SUNWifbcf`

Another setuid **root** tool. This is part of the "*Sun Expert3D (IFB) Graphics Configuration Software*" (SUNWifbcf) package. The Manual page says:

SUNWifb_config configures the Sun Expert3D Graphics Accelerator and some of the X11 window system defaults for the graphics accelerator.

On systems that don't have a glass console of the sort supported by this tool there's obviously no need for this. On systems that do have the graphics hardware I have a hard time believing that this tool needs to be run very often (if at all) by anyone other than the root user. Given the history of security problems with similar tools (there have been advisories wrt. the Kodak Color Management System) I can't see leaving this setuid **root**.

Recommendation: Drop the setuid -- if you need to configure the graphics hardware **su** first.

3. `/usr/openwin/bin/sparcv9/kcms_configure f none 6755 root bin 31952 45773 942273275 SUNWkcsrx`

This one is quite a surprise. There's already a `/usr/openwin/bin/kcms_configure` that's setuid so this can't be one of those ISA versions (unless they've inadvertently made an `isaexec` copy and needlessly marked it setuid). Package information explains things:

```
[3:45pm sun580] pkginfo SUNWkcsrt
application SUNWkcsrt      KCMS Runtime Environment
[3:46pm sun580] pkginfo SUNWkcsrx
application SUNWkcsrx      KCMS 64 bit Runtime Environment
```

I suppose both might be required but would make the same observations -- you don't need this very often and when you do need it you should be **root**. You don't want arbitrary users mucking with this. Gosh, I seem to recall that you need special diagnostic devices to use this tool anyway.

Recommendation: As before, drop the setuid -- if you need to configure the graphics hardware **su** first.

4. `/usr/platform/sun4u/sbin/prtdiag f none 2755 root sys 4512 22503 947118367 SUNWkvm`

A setgid **sys** surprise. The manual page says "**prtdiag** displays system configuration and diagnostic information on sun4u and sun4d systems." That explains why we didn't see it on Solaris 7 -- we were reviewing a different hardware platform.

Recommendation: Drop the setgid -- if you need to use this then **su** first.

5. `/usr/sbin/afbconfig f none 4555 root bin 61508 19299 944695277 SUNWafbcf`

Another setuid **root** tool for mucking with graphics hardware (the AFB Graphics Accelerator). This is part of the "*Elite3D Graphics Configuration Software*" (SUNWafbcf) package but I have the same recommendation.

Recommendation: Drop the setuid -- if you need to configure the graphics hardware **su** first.

6. `/usr/sbin/aspppls f none 4555 root bin 5584 20920 947116576 SUNWapppu`

This is part of the "*PPP/IP Asynchronous PPP daemon and PPP login service*" (SUNWapppu) package. And that allows for IP connections over serial lines -- typically modems and the telephone. Certainly not required for anyone on the campus network. This looks like an optional package that should not be installed on servers.

Recommendation: Drop the setuid unless you actually need a PPP connection.

7. `/usr/sbin/ffbconfig f none 4555 root bin 58980 12585 944695292 SUNWffbcf`

Another setuid **root** tool for mucking with graphics hardware (this time the FFB Graphics Accelerator). This is part of the "*Creator Graphics Configuration Software*" (SUNWffbcf) package. Same recommendation:

Recommendation: Drop the setuid -- if you need to configure the graphics hardware **su** first.

8. `/usr/sbin/igsconfig f none 4555 root bin 37260 36326 941496138 SUNWigsu`

Another setuid **root** tool for mucking with graphics hardware (this time the IGS Graphics Adaptor). This is part of the "*IGS CyberPro2010 DDX (OW) Driver and Utilities*" (SUNWigsu) package. Same recommendation:

Recommendation: Drop the setuid -- if you need to configure the graphics hardware **su** first.

9. `/usr/sbin/m64config f none 4555 root bin 28388 54466 944595359 SUNWm64cf`

Another setuid **root** tool for mucking with graphics hardware (this time the M64 Graphics Accelerator). This is part of the "*M64 Graphics Configuration Software*" (SUNWm64cf) package. Same recommendation:

Recommendation: Drop the setuid -- if you need to configure the graphics hardware **su** first.

10. `/usr/sbin/pgxconfig f none 4555 root bin 102904 64555 929538945 TSIPgxw`

Another setuid **root** tool for mucking with graphics hardware (this time the PGX32 (Raptor GFX) Graphics Accelerator). This is part of the "*PGX32 (Raptor GFX) X Window System Support*" (TSIPgxw) package. Same recommendation:

Recommendation: Drop the setuid -- if you need to configure the graphics hardware **su** first.

The **pfexec** tool may be great solution for managing fine grained access to services. It may, until it's had some time in the market, be a security problem. While it's nice to see support for lots of display accelerators it's very dangerous to see all the setuid **root** tools for mucking with them. The **prtdiag** program is another needless instance of allowing all users access to kernel information. The support for dialup PPP is nice was well -- for those who need it -- but a needless security exposure for everyone else.

The cautious system manager should restrict access to these new tools by dropping the setuid on all of them -- none are required for the casual user. These additions are, in my opinion, an unwarranted risk. You can reduce your risk by using the Bourne Shell script that implements the recommendations made here and in the companion paper on Solaris 7.

Security Review: Solaris 8 Setuid/Setgid Files

Information Systems and Technology

University of Waterloo

See Also

Some further reading for the brave or curious:

- YASSP: Yet Another Solaris Security Package Jean Chounard
- Solaris 2 FAQ Casper Dik
- SUNSOLVE ONLINE (vendor's site)
- Sun Product Documentation (vendor's site)
- The Solaris Security FAQ (sunworld -- Peter Baer Galvin)

We have companion papers for Solaris 2.6 and Solaris 7 on the same issue -- hardening by minimizing setuid/setgid files. We also have a paper on Solaris Network Hardening -- hardening a system by removing network services.

Any questions or concerns about this documentation should be addressed to the author.

(by) Reg Quinton, Information Systems and Technology
2000/08/17 - 2003/09/30