Recreating Pre-2007 (Pre-3.1.7)SETUID Permission Bit Behavior

Special Notices

Information in this document is correct to the best of our knowledge at the time of this writing. Please send feedback by fax to "AIXServ Information" at (512) 823-4009.

Please use this information with care. IBM will not be responsible for damages of any kind resulting from its use. The use of this information is the sole responsibility of the customer and depends on the customer's ability to evaluate and integrate this information into the customer's operational environment.

> **Note:** The information in this document has **not** been verified for AIX 4.1.

About This Document

This document contains the process for recreating SETUID and SETGID permission bits.

SETUID Behavior

A fix for a potential security risk dealing with the use of the SETUID and SETGID permission bits on shell scripts was included in AIX 3.1.7, (which corresponds to update level 2007). Prior to 3.1.7, when a shell script was executed whose permissions included the SETUID bit (set user-id), the shell script ran with the permissions of the shell script's owner. Similarly, if the SETGID bit (set group-id) was set, the shell script ran with the permissions of the shell script's group. Beginning with AIX 3.1.7, the SETUID and SETGID permission bits will no longer be supported for shell scripts. This change will NOT effect compiled programs.

Here is an example.

- Create a shell script named 'shell.sh' that contains the following 2 lines. These lines should begin in the leftmost column.

  ```
  #!/bin/ksh
  id
  ```

- Set the shell script's owner to root, and the permissions to rwsr-xr-x (SETUID bit on).

```
chown root shell.sh
chmod 4755 shell.sh
```

Prior to AIX 3.1.7, if an ordinary user named 'joeuser' ran shell.sh, the output would be:

```
uid=200(joeuser) gid=200(staff) euid=0(root)
```

The 'euid=0(root)' indicates that the user was 'effectively' root while the shell script executed.

For AIX 3.1.7 and later, the output is:

```
uid=200(joeuser) gid=200(staff)
```

The SETUID bit no longer has any meaning for shell scripts.

If your application requires the previous SETUID behavior, you can call the shell script from a small compiled program that has the SETUID bit set in its permissions.

- Create a C program similar to the following named execsh.c. Note the full path name in the execvp call. This is a good idea for security reasons.

```
main(int argc, char *argvfffl“)
{
execvp("/path/shell.sh", argv);  /* execute the shell script */
exit(1);
}
```

- Compile and link execsh.c using the command:

```
cc -o execsh execsh.c
```

- Set the owner of the execsh to root and the SETUID bit on

```
chown root execsh
chmod 4755 execsh
```

The SETUID behavior has not changed for compiled programs, so execsh will 'effectively' become root when it is executed, and will pass these credentials to shell.sh.

10/01/96,

Reader's Comments

Please fax this form to (512) 823-4009, attention "AIXServ Information". You may also e-mail comments to: elizabet@austin.ibm.com. These comments should include the same customer information requested below.

Use this form to tell us what you think about this document. If you have found errors in it, or if you want to express your opinion about it (such as organization, subject matter, appearance) or make suggestions for improvement, this is the form to use.

If you need technical assistance, contact your local branch office, point of sale, or 1-800-CALL-AIX (for information about support offerings). These services may be billable. Faxes on a variety of subjects may be ordered free of charge from 1-800-IBM-4FAX. Outside the U.S. call 415-855-4329 using a fax machine phone.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Note: If you have a problem report or item number, supplying that number may help us determine why a procedure did or did not work in your specific situation.

Problem Report or Item #: Branch Office or Customer #:

Be sure to print your name and fax number below if you would like a reply:

Name: Fax Number:

10/01/96,

END OF DOCUMENT (suid.script.cmd)