

Question

Hi,

I often confuse between real and effective user id of a process. Could you please clarify me what is the difference between them and give an example where we can clearly see the difference.

regads

Ananta

Answer

Each UNIX proces has 3 UIDs associated to it. Superuser privilege is UID=0.

Real UID

This is the UID of the user/process that created THIS process. It can be changed only if the running process has EUID=0.

Effective UID

This UID is used to evaluate privileges of the process to perform a particular action. EUID can be change either to RUID, or SUID if EUID!=0. If EUID=0, it can be changed to anything.

Saved UID

If the binary image file, that was launched has a Set-UID bit on, SUID will be the UID of the owner of the file. Otherwise, SUID will be the RUID.

What is the idea behind this?

Normal programs, like "ls", "cat", "echo" will be run by a normal user, under that users UID. Special programs that allow user to have controlled access to protected data, can have Set-UID bit to allow the program to be run under privileged UID.

An example of such program is "passwd". If you list it in full, you will see that it has Set-UID bit and the owner is "root". When a normal user, say "ananta", runs "passwd", passwd starts with:

Real-UID = ananta

Effective-UID = ananta

Saved-UID = root

The the program calls a system call "seteuid(0)" and since SUID=0, the call will succede and the UIDs will be:

Real-UID = ananta

Effective-UID = root

Saved-UID = root

After that, "passwd" process will be able to access /etc/passwd and change password for user "ananta". Note that user "ananta" cannot write to /etc/passwd on it's own. Note one other thing, setting a Set-UID on a executable file is not enough to make it run as privileged process. The program itself must make a system call.

That is the idea.

Nix.