

# “Process user” control -- su, SUID and sudo

David Morgan

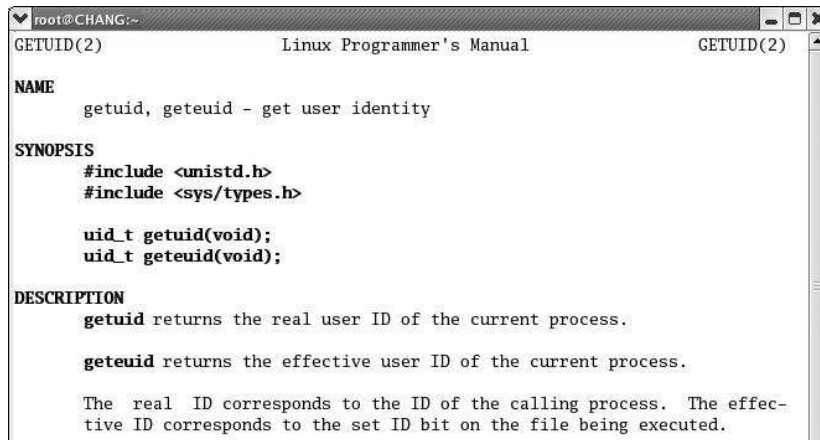
© David Morgan 2003,2006

## Processes and users

- running processes are associated with user(s)
  - real user/UID –id of user running process
  - effective user/UID – id of user owning executable
- process’s real and effective UIDs are same, usually
- check with `getuid( )` and `geteuid( )`

© David Morgan 2003,2006

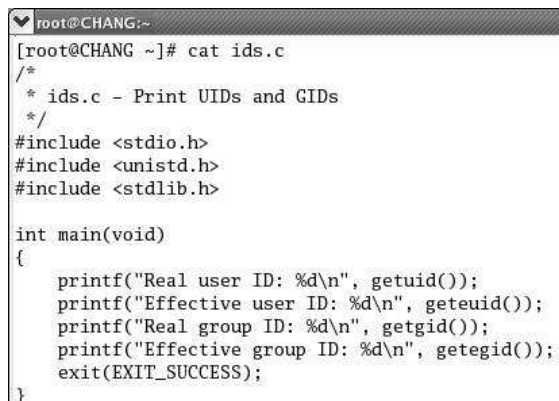
## Process gets from caller/parent, gives to called/child



```
root@CHANG:~  
GETUID(2) Linux Programmer's Manual GETUID(2)  
  
NAME  
  getuid, geteuid - get user identity  
  
SYNOPSIS  
  #include <unistd.h>  
  #include <sys/types.h>  
  
  uid_t getuid(void);  
  uid_t geteuid(void);  
  
DESCRIPTION  
  getuid returns the real user ID of the current process.  
  
  geteuid returns the effective user ID of the current process.  
  
  The real ID corresponds to the ID of the calling process. The effective ID corresponds to the set ID bit on the file being executed.
```

© David Morgan 2003,2006

## Diagnostic UID revealer program



```
root@CHANG:~  
[root@CHANG ~]# cat ids.c  
/*  
 * ids.c - Print UIDs and GIDs  
 */  
#include <stdio.h>  
#include <unistd.h>  
#include <stdlib.h>  
  
int main(void)  
{  
    printf("Real user ID: %d\n", getuid());  
    printf("Effective user ID: %d\n", geteuid());  
    printf("Real group ID: %d\n", getgid());  
    printf("Effective group ID: %d\n", getegid());  
    exit(EXIT_SUCCESS);  
}
```

another revealer: `ps -eo pid,ruid,euid,command`

© David Morgan 2003,2006

# Controlling a process's UIDs

- su
- suid
- sudo

© David Morgan 2003,2006

## su syntax

su <-c command> <user>

- defaults
  - omit user: root
  - omit command: bash
- password prompt: for *other user's* password, not yours

© David Morgan 2003,2006

## Run ids – where does it pick up its ids from?

- 2 diff logins
- Some single login
  - Run su as some other user
  - Run fork9a as that user, then ids from fork9a

© David Morgan 2003,2006

## SUID – exception to the rule

- SUID – a permission characteristic of files
- changes the effective UID of file's process when run
  - from UID of user who runs the program
  - to UID of user who “owns” the file

© David Morgan 2003,2006

## SUID – exception to the rule

- WHAT – “When a SUID file is run, the process involved takes on an *effective UID* that is the same as the owner of the file.”
- WHY – “Sometimes, unprivileged users must be able to accomplish tasks that require privileges.
- EXAMPLES – passwd, mail

© David Morgan 2003,2006

## SUID shell scripts

- BAD
  - DON'T
  - Security flaw – launches SUID shell to run script
- 
- most modern unix's now ignore SUID on a script

© David Morgan 2003,2006

## sudo – secure solution

- lets certain user(s) run certain program(s) as another user
- user runs program indirectly under sudo's control: `sudo <targetprogram>`
- sudo configuration defines who can run what as whom

© David Morgan 2003,2006

## sudo syntax

`sudo <-u user> command`

- defaults
  - omit user: root
  - omit command: *not optional*
- password prompt: for *your* password, not other user's (you don't know who that is)

© David Morgan 2003,2006

## sudo config file: /etc/sudoers

- privilege specifications
- other specifications
  - User aliases – named groups of “by” users
  - Runas aliases – named groups of “as” users
  - Cmnd aliases – named groups of commands

© David Morgan 2003,2006

## What?

- What is a “ ‘by’ user” ?? an “ ‘as’ user” ??
- default: command runs as whoever launched it
- sudo purpose: let a command launched by one user run as another
  - “by” user is the one who launches the command
  - “as” user is the one the command runs as, as if he had actually launched it (even though he didn’t)

© David Morgan 2003,2006

## sudo config file: /etc/sudoers

- privilege specifications
- other specifications
  - User aliases – named groups of “by” users
  - Runas aliases – named groups of “as” users
  - Cmnd aliases – named groups of commands

© David Morgan 2003,2006

## sudoers privilege specifications

<who by> <where>=(<who as>) <what>

© David Morgan 2003,2006