Niektóre operacje w systemie wymagają wyższych uprawnień niż posiadane przez użytkownika, np.: zmiana hasła, nagranie płyty CD.

Ze względów bezpieczeństwa niektóre operacje wykonywane są z niższymi uprawnieniami, np.: wysyłanie i odbieranie poczty.

Tutaj mamy przykłady dwóch programów z flagą SUID (Switch User ID) i SGID (Switch Group ID):

```
sirius$ ls -l /usr/bin/passwd /usr/bin/cdrw /usr/sbin/sendmail
-r-sr-sr-x 1 root sys     22644 sier 7 2009 /usr/bin/passwd
-rwsr-xr-x 1 root bin       54K maj 22 2008 /usr/bin/cdrw
-r-xr-sr-x 1 root smmsp    1,3M lip 24 2015 /usr/sbin/sendmail
```

W miejscu `x` w zestawie user jest `s` - to jest właśnie ustawiona flaga SUID. W programie `passwd` mamy także `s` w zestawie group zamiast `x`. To jest flaga SGID. Uruchomienie programu z ustawioną flagą SUID powoduje, że proces uzyska efektywne UID właściciela pliku. Analogicznie flaga SGID powoduje, że po uruchomieniu programu, efektywna grupa procesu będzie taka jak grupa programu. Flagi SUID i SGID mają jedynie sens, gdy odpowiednio mamy możliwość uruchamiania przez właściciela i grupę, to znaczy gdy mamy `u+x` i `g+x`.

Flagę SUID można ustawić numerycznie podając 4 jako pierwszą cyfrę przed 3 cyframi oznaczającymi uprawnienia, natomiast SGID ustawia się podając 2 jako pierwszą cyfrę. Zauważmy, że są to kolejne potęgi 2, a więc kolejne bity w parametrze numerycznym. Kombinację SUID i SGID uzyskujemy zatem podając 6:

```
chmod 6555 /usr/bin/passwd
chmod 4755 /usr/bin/cdrw
chmod 2555 /usr/sbin/sendmail
```

To samo można uzyskać symbolicznie używając `+s` w następujący sposób;

```
chmod u=rx+s,g=rx+s,o=rx /usr/bin/passwd
chmod u=rwx+s,g=rx,o=rx /usr/bin/cdrw
chmod u=rx,g=rx+s,o=rx /usr/sbin/sendmail
```

Zwróćmy uwagę, gdzie pojawia się `+s`. Dopisanie `+s` dla user ustawia flagę SUID, natomiast dopisanie `+s` w group ustawia flagę SGID.

Wyzerowanie flagi SUID, czy SGID uzyskujemy przez `-s`.

Ustawienie flagi SGID dla katalogu powoduje, że pliki tworzone w tym katalogu odziedziczą GID tego katalogu, to znaczy będą w tej samej grupie co dany katalog.

Załączony program `xuid` wyświetla UID oraz efektywne UID procesu. Warto go sobie skompilować i uruchamiać modyfikując flagi SUID i SGID, aby zobaczyć jak zmienia się efektywne UID i GID procesu.

Załączony program `xfile` próbuje zapisać `Hello world!` w pliku `/tmp/testfile`. Jeśli, na przykład, ustawimy uprawnienia dla tego pliku następująco:

```
chown root:root /tmp/testfile
chmod 0640 /tmp/testfile
```

to tylko `root` ma prawo zapisu do tego pliku. Po skompilowaniu `xfile`, gdy nadamy mu uprawnienia:

```
chown mariusz:staff /tmp/xfile
chmod 0755 /tmp/xfile
```

to nie uda się nim zapisać pliku `/tmp/testfile`. Ale, gdy zmienimy właściciela i ustawimy SUID w następujący sposób:

```
chown root /tmp/xfile
chmod u+s /tmp/xfile
```

to program `xfile` może modyfikować zawartość `/tmp/testfile`.