



Zmiany `uid` w programach

- ▶ Programy typu `set-user-id` w szczególny sposób muszą sprawdzać prawa dostępu do plików, urządzeń itp.
- ▶ Najlepsza metoda – korzystać ze specjalnych uprawnień tylko wtedy, gdy jest to niezbędne i rezygnować z nich kiedy tylko się da.
- ▶ Przykład serwera pocztowego:
 - ▶ Startuje jako program `suid`
 - ▶ Zmienia `uid` na `nobody`, by przeczytać plik konfiguracyjny.
 - ▶ Zmienia `uid` na 0, by zacząć nasłuchiwać na porcie 25 (lub innym, określonym w konfiguracji)
 - ▶ Zmienia `uid` na `nobody` i działa dalej
 - ▶ Przyjmuje pocztę, wysyła dalej
 - ▶ Zapis poczty do kolejki wymaga zmiany grupy na `mail`, po zapisaniu można z tej grupy zrezygnować.
 - ▶ Zapis poczty do skrzynki użytkownika wymaga ponownej zmiany `uid` – na `root` lub (znacznie bezpieczniej) – ID użytkownika
 - ▶ Po zapisaniu poczty do skrzynki – powrót do ID `nobody`
- ▶ Trzy niezależne wartości UID:
 - ▶ `uid` – effective uid (efektywny numer użytkownika)
 - ▶ `ruid` – real uid (rzeczywisty numer użytkownika)
 - ▶ `suid` – saved uid (zachowany numer użytkownika)