Bits especials

A més dels 9 bits de protecció bàsics, en l'inode rauen uns altres 3 bits per al control dels permisos d'accés. Aquests tres bits (*setuid*, *setgid* i *sticky*) són especials i una mica complexos però essencials per a una correcta administració. Els tres s'utilitzen principalment en programes executables i resulten potents i arriscats, ja que certs forats de seguretat es basen en la seva manipulació.
Si s'activa el bit *setuid* d'un programa executable s'aconsegueix que els permisos d'accés als arxius que gestiona aquest executable es contrastin no amb el compte des del qual es vol executar el programa sinó amb el propietari del programa executable. Aquesta funció permet saltar de forma controlada els permisos de certs programes. L'exemple més conegut és el del programa passwd que permet canviar i actualitzar les contrasenyes que resideixen en l'arxiu /etc/passwd. En principi, qualsevol hauria de poder escriure en aquest arxiu ja que té dret a canviar la seva clau d'accés. Tanmateix, aquest fet, sense una restricció addicional, representaria un perill enorme, ja que un usuari podria canviar les claus de qualsevol altre compte mitjançant un editor de text.
La solució a aquest conflicte és la utilització del bit *setuid* en el programa. L'usuari root és el propietari del programa i només el root té permís d'escriptura en l'arxiu /etc/passwd. Per tant no es pot escriure en aquest arxiu directament, però quan s'executa la comanda de canvi de clau, com aquest programa té activat el *setuid*. Els permisos que es verificaran seran els del seu propietari, que és root, i no els de l'usuari que vol canviar la clau. D'aquesta manera s'aconsegueix el permís d'escriptura de forma controlada. És a dir, gràcies al bit *setuid* s'aconsegueix escriure a l'arxiu, però només per mitjà d'aquest programa.
El bit *setgid* és similar al *setuid*, però referit als permisos de grup en lloc dels de propietari.
La funció del *sticky* bit és totalment diferent, encara que afecta també a programes executables. L'objectiu d'aquest bit és fixar el programa permanentment en la memòria per evitar els temps de càrrega posteriors. També és un bit perillós ja que els virus i derivats tenen precisament aquest objectiu, quedar-se residents en memòria.
L'activació i desactivació d'aquests bits és similar a la dels permisos. u+s activa el *setuid*, g+s activa el *setgid* i o+t l'*sticky*. Amb el signe menys es desactiven. Si desitgem modificar-los en manera numèrica hem d'usar un quart valor als tres ja coneguts, a l'esquerra dels anteriors. Per al càlcul del valor numèric *setuid* en val 4, *setgid* val 2 i *sticky* val 1.

Els bits especials en les carpetes

L'activació del *sticky* en un carpeta serveix per aconseguir que qui tingui dret d'escriptura en una carpeta no pugui esborrar els arxius que hi hagi en ell i que no siguin de la seva propietat. És comú utilitzar aquesta possibilitat en carpetes que contenen arxius temporals com /tmp i carpetes que contenen arxius amb característiques diverses de protecció.
Activant el bit *setgid* en una carpeta es pot aconseguir que els arxius que es vagin creant per sota d'aquesta carpeta heretin el grup propietari de la carpeta, que s'assignarà com a grup propietari de l'arxiu. Això és molt interessant quan treballaran en un projecte conjunt usuaris de diferents grups preassignats. En aquest cas es crearà un nou grup en el qual s'inclouran els comptes participants en el projecte. A continuació es crearà una carpeta arrel per al treball conjunt i, posteriorment, a aquesta carpeta se li assignarà com a grup propietari el nou grup i se li activarà el bit *setgid*. D'aquesta manera, quan participants del projecte creïn arxius i carpetes sota la carpeta principal el grup propietari que se li assignarà serà l'heretat, és a dir, el del projecte conjunt, i per tant els permisos de grup es comprovaran respecte al grup nou.

La representació d’aquests permisos en el resultat de la comanda ls –l és:

setuid	El caràcter **x** dels permisos del propietari es canvien per una **s** quan aquest permís està activat; una **S** significa que el permís en execució no està activat al mateix temps.
setgid	Igual que SUID però a nivell dels permisos del grup.
sticky	Una **t** indica en el lloc de la **x** a nivell dels permisos de l'entitat “others”. Si aquest permís és **T** significa que el permís **x** que està ocult no està actiu.

Resum:

Permís	Arxiu	Carpeta
setuid	executa l’arxiu amb la identitat del propietari de l’arxiu	
setgid	executa l’arxiu amb la identitat del grup de l’arxiu	els arxius creats en el directori hereten el grup del directori en lloc del grup principal de l’usuari
sticky	la imatge de l’executable segueix en memòria, la seva recàrrega és més ràpida	només el propietari de l’arxiu o del directori poden esborrar els arxius

Font:

Iñaki Agería Loinaz i altres: “Linux: Administración del sistema y la red” Ed. Pearson Prentice Hall. ISBN: 84-205-4848-0