

NAME

cr_canseeothergids - determine if subjects may see entities in a disjoint group set

SYNOPSIS

int

cr_canseeothergids(*struct ucred *u1, struct ucred *u2*);

DESCRIPTION

This function is internal. Its functionality is integrated into the function `cr_bsd_visible(9)`, which should be called instead.

This function checks if a subject associated to credentials *u1* is denied seeing a subject or object associated to credentials *u2* by a policy that requires both credentials to have at least one group in common. For this determination, the real and supplementary group IDs are used, but not the effective group IDs, as per `realgroupmember(9)`.

This policy is active if and only if the `sysctl(8)` variable `security.bsd.see_other_gids` is set to zero.

As usual, the superuser (effective user ID 0) is exempt from this policy provided that the `sysctl(8)` variable `security.bsd.suser_enabled` is non-zero and no active MAC policy explicitly denies the exemption (see `priv_check_cred(9)`).

RETURN VALUES

The `cr_canseeothergids()` function returns 0 if the policy is disabled, the credentials share at least one common group, or if *u1* has privilege exempting it from the policy. Otherwise, it returns ESRCH.

SEE ALSO

`cr_bsd_visible(9)`, `realgroupmember(9)`, `priv_check_cred(9)`