

NAME

vaccess - generate an access control decision using vnode parameters

SYNOPSIS

```
#include <sys/param.h>
```

```
#include <sys/vnode.h>
```

int

```
vaccess(enum vtype type, mode_t file_mode, uid_t file_uid, gid_t file_gid, accmode_t accmode,  
        struct ucred *cred);
```

DESCRIPTION

This call implements the logic for the UNIX discretionary file security model common to many file systems in FreeBSD. It accepts the vnodes type *type*, permissions via *file_mode*, owning UID *file_uid*, owning GID *file_gid*, desired access mode *accmode* and requesting credential *cred*.

This call is intended to support implementations of VOP_ACCESS(9), which will use their own access methods to retrieve the vnode properties, and then invoke **vaccess()** in order to perform the actual check. Implementations of VOP_ACCESS(9) may choose to implement additional security mechanisms whose results will be composed with the return value.

The algorithm used by **vaccess()** selects a component of the file permission bits based on comparing the passed credential, file owner, and file group. If the credential's effective UID matches the file owner, then the owner component of the permission bits is selected. If the UID does not match, then the credential's effective GID, followed by additional groups, are compared with the file group--if there is a match, then the group component of the permission bits is selected. If neither the credential UID or GIDs match the passed file owner and group, then the other component of the permission bits is selected.

Once appropriate protections are selected for the current credential, the requested access mode, in combination with the vnode type, will be compared with the discretionary rights available for the credential. If the rights granted by discretionary protections are insufficient, then super-user privilege, if available for the credential, will also be considered.

RETURN VALUES

vaccess() will return 0 on success, or a non-zero error value on failure.

ERRORS

[EACCES] Permission denied. An attempt was made to access a file in a way forbidden by its file access permissions.

[EPERM] Operation not permitted. An attempt was made to perform an operation limited to processes with appropriate privileges or to the owner of a file or other resource.

SEE ALSO

vaccess_acl_nfs4(9), vaccess_acl_posix1e(9), vnode(9), VOP_ACCESS(9)

AUTHORS

This manual page and the current implementation of **vaccess()** were written by Robert Watson.