NAME

vaccess_acl_posix1e - generate a POSIX.1e ACL access control decision using vnode parameters

SYNOPSIS

#include <sys/param.h>
#include <sys/vnode.h>
#include <sys/acl.h>

int
vaccess_acl_posix1e(*enum vtype type, uid_t file_uid, gid_t file_gid, struct acl *acl, accmode_t accmode, struct ucred *cred, int *privused*);

DESCRIPTION

This call implements the logic for the UNIX discretionary file security model with POSIX.1e ACL extensions. It accepts the vnodes type *type*, owning UID *file_uid*, owning GID *file_gid*, access ACL for the file *acl*, desired access mode *accmode*, requesting credential *cred*, and an optional call-by-reference *int* pointer returning whether or not privilege was required for successful evaluation of the call; the *privused* pointer may be set to NULL by the caller in order not to be informed of privilege information, or it may point to an integer that will be set to 1 if privilege is used, and 0 otherwise.

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_acl_posix1e**() 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_acl_posix1e**() is based on the POSIX.1e ACL evaluation algorithm. The algorithm selects a *matching* entry from the access ACL, which may then be composed with an available ACL mask entry, providing UNIX security compatibility.

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_acl_posix1e() 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(9), vnode(9), VOP_ACCESS(9)

AUTHORS

This manual page and the current implementation of **vaccess_acl_posix1e**() were written by Robert Watson.

BUGS

This manual page should include a full description of the POSIX.1e ACL evaluation algorithm, or cross reference another page that does.