What are the access rights and privileges that control changing ownership of an object?

devblogs.microsoft.com/oldnewthing/20050818-09

August 18, 2005

Raymond Chen

Changing the ownership of an object (typically a file) is not difficult in principle: You call the `SetNamedSecurityInfo` function with the new security descriptor.

The hard part is getting to that point. (Thanks to John, a colleague in security, for correcting an earlier draft of this entry.)

If you have `WRITE_OWNER` access on an object, then you can change the owner of the object to yourself (or to any SID in your token that has the SE_GROUP_OWNER attribute): you can take ownership. However, you cannot change the owner to somebody else: you cannot give ownership to another person. Doing that would allow you to violate quota restrictions.

Imagine if this were possible, that you could change the ownership to something that you aren't a member of: Your account is at its disk quota. No problem, you just find somebody who isn't over quota (like Fred in Accounting) and take some of your biggest files and set their owner to Fred. This causes the disk space to be charged to its new owner Fred, without Fred even knowing that it has happened to him. If you put the file in a directory that Fred doesn't have access to, poor Fred will start getting "You are over disk quota" messages and have no way of finding this evil file that you charged to him. It's like stealing somebody's library card and checking out books with it.

In order to set the owner to somebody else, you need to assert SeRestorePrivilege, which by default is assigned to administrators and backup operators. Backup operators need to be able to set the owner to somebody else because restoring its security descriptor is an important part of the process of restoring a file from backup.

But what about SeTakeOwnershipPrivilege? That privilege is assigned to administrators, and it lets you act as if you had `WRITE_OWNER` access (but not SeRestorePrivilege) to everything. With SeTakeOwnershipPrivilege, you can take ownership of any file, but you can't assign it to somebody else.

And then there's the mysterious `CREATOR_OWNER` SID, described in a Knowledge Base article as well as in a blog entry by Larry Osterman. The important thing to remember is that granting `CREATOR_OWNER` SID to an object after it has been created doesn't actually grant anything to the creator or owner. Read the linked articles for more details.

Raymond Chen

Follow