Which access rights bits belong to whom?

devblogs.microsoft.com/oldnewthing/20031204-00

December 4, 2003

Raymond Chen

Each ACE in a security descriptor contains a 32-bit access mask. Which bits belong to whom? The access rights mask is a 32-bit value. The upper 16 bits are defined by the operating system and the lower 16 bits are defined by the object being secured. For example, consider the value 0x00060002 for the access rights mask. This breaks down as the system-defined access rights WRITE_DAC (0x00040000), READ_CONTROL (0x00020000), and one object-defined access right 0x0002. The object-defined access right 0x0002 depends on the object. This particular access right might mean any of the following:

meaning	if the object is a…
FILE_WRITE_DATA	file
FILE_ADD_FILE	directory
PROCESS_CREATE_THREAD	process
THREAD_SUSPEND_RESUME	thread
JOB_OBJECT_SET_ATTRIBUTES	job object
EVENT_MODIFY_STATE	event
SEMAPHORE_MODIFY_STATE	semaphore
TIMER_MODIFY_STATE	timer
IO_COMPLETION_MODIFY_STATE	I/O completion port
KEY_SET_VALUE	registry key
TOKEN_DUPLICATE	token
WINSTA_READATTRIBUTES	windowstation
DESKTOP_CREATEWINDOW	desktop

or it could mean something else entirely if it's an object of a type not listed above. If you ask the ConvertSecurityDescriptorToStringSecurityDescriptor function to convert a security descriptor to a string security descriptor, it tries to guess what the object is, but since there is so little information to go on, it usually guesses wrong. The access rights mask above, for example, would be rendered by SDDL as "DCRCWD". The rights RC = READ_CONTROL, WD = WRITE_DAC are standard across all objects, so there is no guessing there. But SDDL guessed that 0x0002 was DC = ADS_RIGHTS_DS_DELETE_CHILD.

Notice that there are some system-defined access rights that are named "GENERIC", such as GENERIC_READ and GENERIC_WRITE. Each object exposes different "read-like", "write-like", and possibly "execute-like" access rights (for example, registry keys have KEY_QUERY_VALUE and KEY_SET_VALUE), but they all have to define which ones are read-like, which ones are write-like, and which ones are execute-like, so that you can request one of the GENERIC access masks and get access appropriate to the type of object you are opening.

Raymond Chen

Follow