

W2003 Security by Using Access Control

Determining Access to NTFS files on Windows NT, W2000, Windows XP, and Windows 2003 Access Control.

There are three rules that Windows systems use to determine access to an object. These rules are “**mutually exclusive and exhaustive**” so that only one rule occurs in each request to access an object, no matter what the request is.

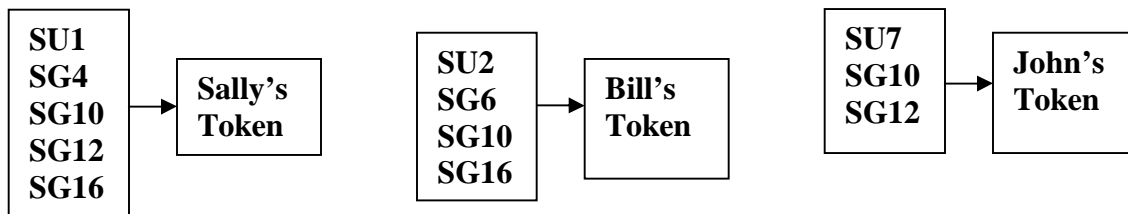
In each rule, your search starts at the first Access Control Entry in the object’s DACL.

Rule 1: As you go through the DACL, before getting all the permissions you seek, you find an ACE that denies you a permission you seek. In this case, you are denied access to that object.

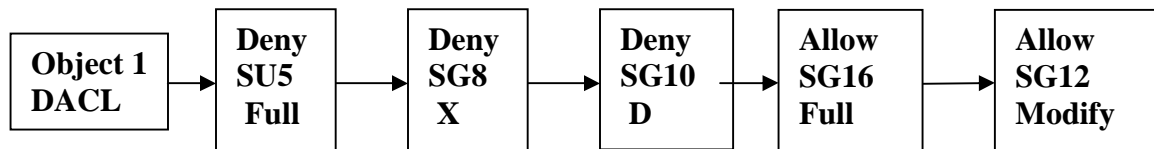
Rule 2: Rule 1 does not apply, and you go through the entire DACL and still do not discover an ACE that gives you a desired permission. You are denied access to that object.

Rule 3: As you go through the DACL, Rule 1 never applies, i.e., you are not denied a permission you seek. You find each and every permission you seek. You are granted a handle to that object.

Below are three tokens, belonging to users Sally, Bill, and John. SU1, SU2, and SU7 are the individual user SIDs for Sally, Bill, and John. SG4, SG6, SG8, SG10, SG12, and SG16 are group SIDs.



Permissions are: R=Read, W=Write, X=Execute, D=Delete, O=Take Ownership, P=Change Permissions, Modify=RWXD, and Full=RWXDOP.



First Question
Sally's Request

Second Question
Bill's Request

Sally wants to *delete Object 1*.
Allowed or denied?
What Rule Applies? 1, 2, or 3?

Bill wants to *Execute Object 1*.
Allowed or denied?
What Rule Applies? 1, 2, or 3?

The tables below show step-by-step results of the searches for the two questions' access requests.

Question 1 Analysis for Sally's Request to Delete Object 1

SU5	<i>Does Not apply, since not in Sally's token</i>
SG8	<i>Not in Sally's token, so it also does not apply.</i>
SG10	<i>This SID is Sally's token, so her request is Denied.</i>
Result	Access is Denied via Rule 1.

Question 2 Analysis for Bill's Request to Execute Object 1

SU5	<i>Does Not apply, since not in Bill's Token</i>
SG8	<i>Also does not apply, since not in Bill's token.</i>
SG10	<i>This SID is in Bill's token, but Bill is not trying to execute.</i>
SG16	<i>In Bill's Token and gives Bill the Access he desires.</i>
Result	Access is Allowed via Rule 3.

Question 3- John's Request to Change Permissions on Object 1

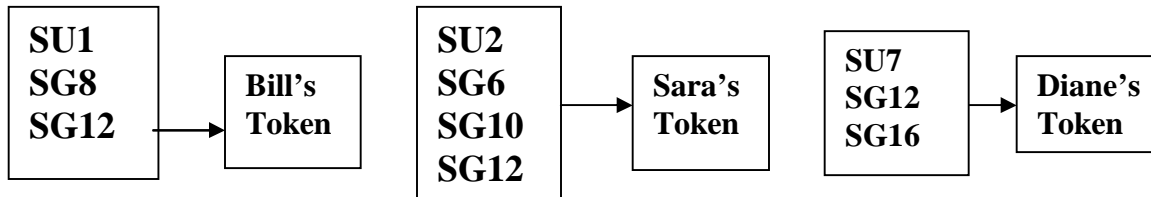
**John wants to Change the Permissions on Object 1?
 Allowed or denied?
 Which Rule Applies? 1, 2, or 3?**

Question 3 Analysis for John's Request to Change Permissions

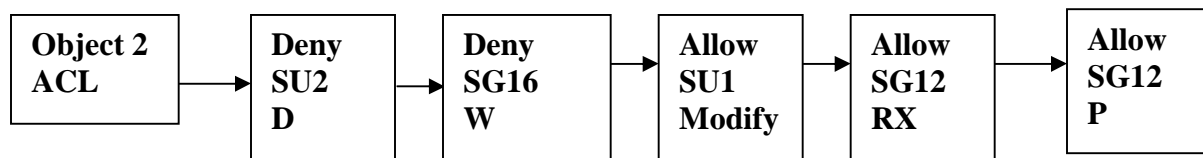
SU5	<i>Does Not apply, since not in John's token</i>
SG8	<i>Also does not apply, since not in John's token.</i>
SG10	<i>This SID is in John's token, but John is not trying to Delete object.</i>
SG16	<i>Not in John's Token, so it does not Apply to this Search.</i>
SG12	<i>In John's Token, but since it gives Modify (RWXD), John is seeking to Change Permissions, P. Thus this ACE does not give John the permission he is seeking.</i>
Result	Access is DENIED via Rule 2. No more Aces to Search.

Second Set of Access Control Problems – Homework for you!!

The user tokens are now shown as follows:



In this problem, we have another object, Object 2, whose DACL is shown below.



First Question

**Bill wants RWX to Object 2.
Allowed or Denied?
Which Rule Applies? 1, 2, or 3?**

Second Question

**Sara wants RX to Object 2.
Allowed or Denied?
Which Rule Applies? 1, 2, or 3?**

Third Question

**Sara wants to Delete Object 2.
Allowed or denied?
Which Rule Applies? 1, 2, or 3?**

Fourth Question

**Diane wants to Write to Object 2.
Allowed or denied?
Which Rule Applies? 1, 2, or 3?**

Fifth Question

**Diane wants to delete Object 2.
Allowed or denied?
Which Rule Applies? 1, 2, or 3?**

Sixth Question

**Bill wants to delete Object 2.
Allowed or denied?
Which Rule Applies? 1, 2, or 3?**