CS526 Information Security
Assignment 5 Solutions

ZHONGSHU GU
CAREER:GU16

1 Answer

a False. [redacted]

release-read: a subject releases a read right from itself. In rescind-read, a subject cancels a read right from the set of rights of another subject.

b True. According to the 3 rules of Biba's strict integrity model, there is no rule to change the integrity level of subjects. So the integrity level is static.

2 Answer

a Proof:

(1) we consider the situation that H has multiple nodes.

According to the definition of hierarchy, it has fulfilled that the tree should be connected.

There are only three situations which will violate the requirement of a tree.

1. Left: The dash line is pointing to the node on the next level and the node which is poited already has a inbound edge.
2. Middle: The dash line is pointing to the node on the higher level and it is NOT in the path from its source node to the root.
3. Right: The dash line is pointing to the node on the higher level and it is in the path from its source node to the root.

Please look at Figure 1.

1. Property 1 can rule out the left structure because if $o_i \neq o_j$, their children set can not have intersection. It means all the node in the graph can only have one parent.
2. Property 1 can rule out the middle structure because if $o_i \neq o_j$, their children set can not have intersection. It means all the node in the graph can only have one parent.
3. Property 2 can rule out the right structure because it does not permit an edge back to its ancestor.

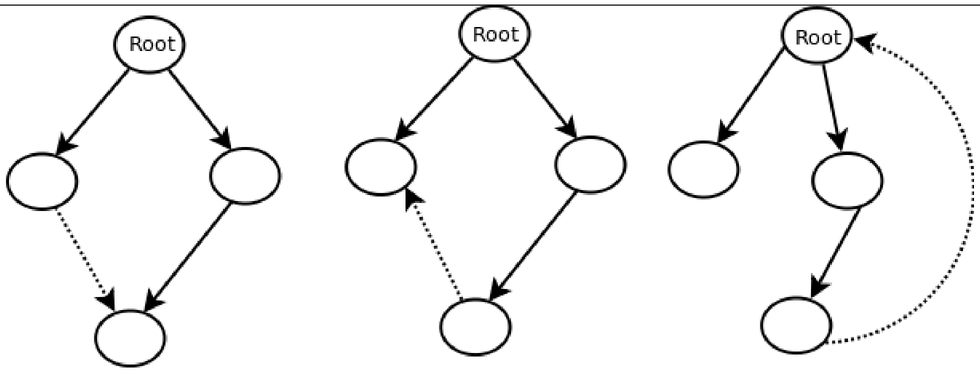

Figure 1: Two situations that will violate the condition

(2) Then we consider that there is only one single node for H.

As it has only one node, it fulfill the two properties.

So the H should be a tree or a single node.

b If the hierarchy of objects is like the left or middle situation of Figure 1, it is a dag and one node has two parents. For example in the file system, it means that there is a file and there are two directories that contain this file. When we want to modify the file, first we need the priviledge to write the parent directory of this file. But in this situation, it has two parent directories and the permission of parents may be conflict with each other. For example, one normal user want to read a file and this file has two parent directory. The first directory requires that only the root user can read the files under it. The second directory does not have this requirement. In this case, normal user can read the file through the second directory. The requirement for the root permission in the first directory is useless. Confidentialality policy is violated.

3 Answer

In this example,
$i(s) = high\ i(o) = higher$
$l(s) = high\ l(o) = higher$
$``higher''\ dominates\ ``high''$

We should discuss it in two conditions. The first is $high < higher$ and the second is $high = higher$.

(1) For $high < higher$:

If s wants to read o, according to the ssc of bell-lapadula model, l(o) $\leq$ l(s) does not comply with the condition of the example.

If s wants to write o, according to the Biba strict integrity model, i(o) $\leq$ i(s) does not comply with the condition of the example.

If s wants to append o, the analysis is the same as write as it does not comply with Biba model.

We assume S $\subseteq$ O, if s wants to execute o, according to Biba model, i(o) $\leq$ i(s) does not comply with the condition in example.

It is not possible for this situation.

(1) For $high = higher$:

We can hold both Bell-Lapadula and Biba models because the security level and integrity level is the same for subject and object. Both models can satisfy their conditions only when the security level and integrity level is the same.

It is possible for this situation.

4 Answer

Low-Water-Mark policy is suitable for this self-destructive operating system.

Because ring policy and Biba strict integrity policy does not have the rule to change the subject's integrity level.

For low-water-mark policy, if a subject s reads object o, it will lower its integrity level to the same as object's integrity level if object's integrity level is less than subject's. It satisfies the requirement that process should change its integrity level when reading user submitted data with lower integrity level.