1. Why is it meaningless to have compartments at the UNCLASSIFIED level (such as (UNCLASSIFIED, { NUC }) and (UNCLASSIFIED, { EUR }))?

   There are no reasons to have compartments, or categories, because of the fact that it is unclassified, everyone can have access to it.

2. Given the security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C, specify what type of access (read, write, both, or neither) is allowed in each of the following situations. Assume that discretionary access controls allow anyone access unless otherwise specified.

   Simple security property says that a subject can write to object if subject compartment dominates object compartment. *****-property says that subject can write to object if object compartment dominates subject compartment. Let (L,C) and (L', C') be compartments for different entities. ((L,C) *dominates* $(L',C') \Leftrightarrow L' \leq L$ and $C' \subseteq C$) is the principle we are going to apply to specify what type of access that the following sentences have.

   a. Paul, cleared for (TOP SECRET, { A, C }), wants to access a document classified (SECRET, { B, C }).
   Paul **cannot read** and **cannot write** to the document because Paul does not dominate document and also, document does not dominate Paul.

   b. Anna, cleared for (CONFIDENTIAL, { C }), wants to access a document classified (CONFIDENTIAL, {B }).
   Anna **cannot read** and **cannot write** to the document because Anna does not dominate document and also, document does not dominate Anna.

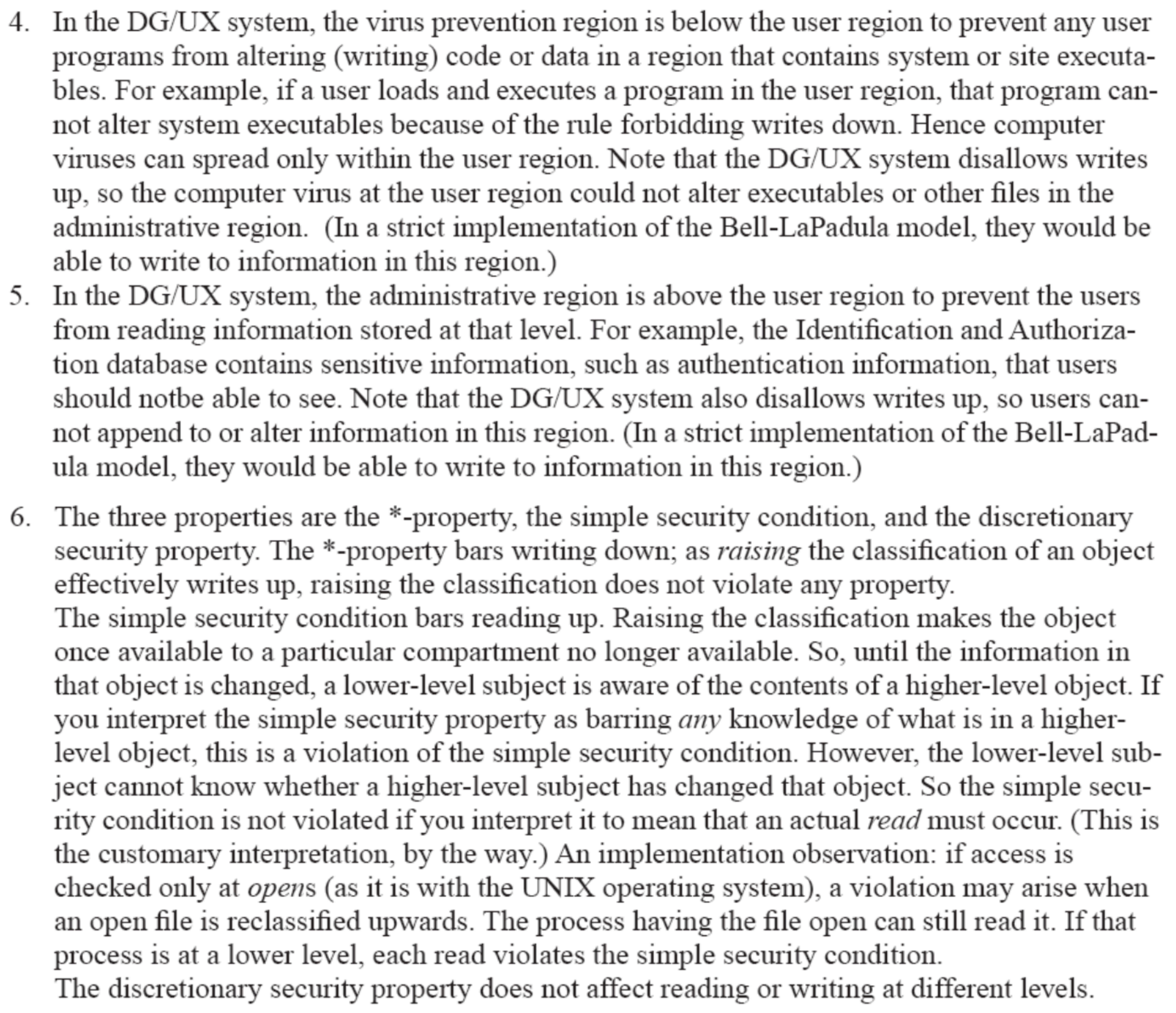
   c. Jesse, cleared for (SECRET, { C }), wants to access a document classified (CONFIDENTIAL, { C }).
   Jesse **can read** document because Jesse dominates document, but Jesse **cannot write** to the document because document does not dominate Jesse.

   d. Sammi, cleared for (TOP SECRET, { A, C }), wants to access a document classified (CONFIDENTIAL, {A }).
   Sammi **can read** document because Sammi dominates document, but Sammi **cannot write** to the document because document does not dominate Jesse.

   e. Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (CONFIDENTIAL, { B }).
   Robin **cannot read** document because Jesse does not dominate document, but Robin **can write** to the document because document dominates Jesse.

(adapted from Aref Al-Kamel)

ex3



4. In the DG/UX system, the virus prevention region is below the user region to prevent any user programs from altering (writing) code or data in a region that contains system or site executables. For example, if a user loads and executes a program in the user region, that program cannot alter system executables because of the rule forbidding writes down. Hence computer viruses can spread only within the user region. Note that the DG/UX system disallows writes up, so the computer virus at the user region could not alter executables or other files in the administrative region. (In a strict implementation of the Bell-LaPadula model, they would be able to write to information in this region.)
5. In the DG/UX system, the administrative region is above the user region to prevent the users from reading information stored at that level. For example, the Identification and Authorization database contains sensitive information, such as authentication information, that users should notbe able to see. Note that the DG/UX system also disallows writes up, so users cannot append to or alter information in this region. (In a strict implementation of the Bell-LaPadula model, they would be able to write to information in this region.)
6. The three properties are the *-property, the simple security condition, and the discretionary security property. The *-property bars writing down; as *raising* the classification of an object effectively writes up, raising the classification does not violate any property.
   The simple security condition bars reading up. Raising the classification makes the object once available to a particular compartment no longer available. So, until the information in that object is changed, a lower-level subject is aware of the contents of a higher-level object. If you interpret the simple security property as barring *any* knowledge of what is in a higher-level object, this is a violation of the simple security condition. However, the lower-level subject cannot know whether a higher-level subject has changed that object. So the simple security condition is not violated if you interpret it to mean that an actual *read* must occur. (This is the customary interpretation, by the way.) An implementation observation: if access is checked only at *open*s (as it is with the UNIX operating system), a violation may arise when an open file is reclassified upwards. The process having the file open can still read it. If that process is at a lower level, each read violates the simple security condition.
   The discretionary security property does not affect reading or writing at different levels.

ex7

Declassification effectively violates the *-property of the Bell-LaPadula Model. Would raising the classification of an object violate any properties of the model? Why or why not?

Answer:

The principle of tranquility states that subjects and objects may not change their security levels once they have been instantiated[2]. Declassification violates the *-property of the Bell-LaPadula Model which states that S can write O if and only if $l_s \leq l_o$ and S has discretionary write over O and in other words it is “no writes down”. A declassification makes information available to subjects who did not have access to it before and rendering a “high” subject unable to write on the “low” object. However, the principle of weak tranquility does provide flexibility by allowing “trusted entities” to declassify information by removing sensitive elements. For example, the UK government declassified two (of the many) papers written by Alan Turing in breaking the Enigma code after more than 70 years since the end of the second world war[3].

Raising the classification of an object is not a violation as the Bell-LaPadula model as the model does not state how to classify the information but instead describes how to manage the information based on its classification. Raising the classification enforces the control of “no reading up” for the lower level subjects. However, the information which has been previously accessed by subjects of that security level is no longer “confidential” despite raising its classification as the information has already been accessed. Therefore, raising the classification of an object does not violate the Bell-LaPedula model as the confidentiality of the object is not valid.

ex8
ex9
ex10
ex11
ex12不用看