IS-2150/TEL-2810 Introduction to Computer Security
Homework 4
Sample Solution

1. subject set $TS = \{st_1, st_2, \ldots, st_n\}$
   object set $TO = \{ot_1, ot_2, \ldots, ot_n\}$
   set of control rights $RC = \emptyset$
   set of inert rights $RI = \{r:c, w:c\}$ in owner-based the rights can be copyable

   create functions
   
   $$cc(st_i) = \{ot_i\}$$
   $$cr(st_i, ot_j) = \{ot_j/r:c, ot_j/w:c\}$$

   link and filter functions for Read
   
   $$link_{\text{read},i,j}(st_i, st_j) = \text{true}$$
   $$filter_{\text{read},(i,j)}(st_i, st_j) = \{ot_i/r:c, ot_2/r:c, \ldots, ot_i/r:c\}$$

   link and filter functions for Write
   
   $$link_{\text{write},i,j}(st_i, st_j) = \text{true}$$
   $$filter_{\text{write},(i,j)}(st_i, st_j) = \{ot_i/w:c, ot_{i+1}/w:c, \ldots, ot_n/w:c\}$$

2. Classify each of the following as an example of a mandatory, discretionary, or originator controlled policy, or a combination thereof. Justify your answers.

   a. discretionary
   b. originator
   c. mandatory
   d. discretionary + mandatory

3. Highlight the importance of the following (chapter 4) 

   Trust element with respect to the notion of Integrity Trust is crucial for Integrity. As explained on the example of a security patch you need a trusted entity from which you can receive the patch. You need a trust worthy connection that you can make sure that the patch you receive is not poisoned with any code which would open new wholes in the security of the system. Furthermore the patch it self needs to be of a high integrity that with any given
input it produces a secure output within the boundaries of the system otherwise the patch itself would be a new security problem. In addition the vendor on which integrity you trust must ensure a robust testing of the patch on a comparable system to which you use to ensure the quality of the patch. The patch also needs to be correctly installed by a trustworthy person.

*Time element* with respect to the notion of *Confidentiality* and *Availability* Time has different effects considering confidentiality on the one hand and on the other hand availability. Some information is only under confidentiality for a certain amount of time or to a certain point in time. E.g. construction plans of a tank or mission plans of World War II are in most cases not anymore confidential as the technology is outdated and most of the people who were involved are very old or dead. Availability on the other hand comes in to play if you want to make a system not only secure but also at least to some extend precise. You can make any system secure by just giving nobody access to the data but as that is obviously not the purpose of a security policy availability is also a big issue. Availability does not only describe to whom a system is available (the users) but also the time in which the information are available. E.g. in a hospital it is not acceptable that everyone has access to all patient records but on the other hand in case of an emergency patient records have to be available in a short time frame and not hours later.

*(Submitted by Thomas Ehmer)*