COM-301 Computer Security
Exercise sheet: Mandatory access control

1. Recall that Bell LaPadula has two key properties to support MAC: the ss-property (No Read Up), and the *-property. Why it is not a problem that Write up is permitted in Bell LaPadula?

2. Given the classifications TOP SECRET, SECRET, CONFIDENTIAL and UNCLASSIFIED (ordered from highest to lowest) and two categories: Nuclear and Army.

   We consider four subjects:

   - the president has a TOP SECRET clearance for Nuclear and Army
   - the colonel has SECRET clearance for Army and Nuclear
   - the major has only CONFIDENTIAL clearance for Army
   - the soldier has only UNCLASSIFIED clearance for Nuclear

   We also have some objects (documents):

   - the army position at classifications SECRET
   - the number of army units at classifications CONFIDENTIAL
   - the number of nuclear units at classifications CONFIDENTIAL
   - the costs of the nuclear program at classifications UNCLASSIFIED
   - the costs of the army at classifications UNCLASSIFIED
   - the nuclear code at classifications TOP SECRET

   Answer with justifications the following questions based on the BellLaPadula model:

   (a) Can the president compute the overall defense costs (army + nuclear)?

   (b) Can the colonel compute the total number of nuclear and army units?

   (c) Can the major change the nuclear code?

   (d) Can the soldier compute the cost of army?

   (e) Can the soldier compute the number of nuclear units?

3. To make sure that the privacy of the students is preserved in our assignment submission system, we model it using the Bell LaPadula model. Students are assigned the lowest clearance, TAs medium, and the Professor the highest (Student < TA < Professor). The assignments are submitted to the TAs, who send an ACK to the students. The TAs correct the assignment and submit the correction to the Professor, who does the grading and gives the grade to the students.

   (a) In the description above, is there any flow of information that contradicts the BLP rules? If yes, what process would the lab need to implement to make it safe?

   (b) The Professor is worried that the TAs may give hints to the students about their performance before they receive the grades using the ACKs as a covert channel (agreeing on specific delays to convey if they have passed the assignment or not). For each of the following policies, discuss if they would totally prevent the possibility of a covert channel (justify your answer):

      i. Intercept the ACKs the TAs send and delay them by 10 minutes.
      ii. Buffer the ACKs of the TAs and send them at the end of the day.
      iii. Intercept the ACKs the TAs send and delay them by a random amount selected uniformly at random between 0 and 10 minutes.
      iv. Send ACKs to all students every hour

4. Mosaicing is a process by which a rectangular grid is superimposed over an image and the color values of the pixels within each grid cell are averaged to obtain a mosaiced image [1]. A strategy to declassify texts is converting them to an image and deducting sensitive parts with black rectangles. Do you think replacing black rectangles with mosaicing is a better declassification mechanism? Justify.(Remember the strategic adversary knows the mosaicing technique)

5. Consider a system that used the Bell-LaPadula model to enforce confidentiality and the Biba model to enforce integrity.

   (a) If the confidentiality levels were the same as integrity levels, what objects could a given process (with some confidentiality level that also served as its integrity level) access?

   (b) Why is this scheme not used in practice?

6. Is the following statement right or wrong? why?
   "Classic BIBA makes sense for the case where a malware that in order to work needs to download a configuration file from the network, manages to infiltrate a "high"-integrity level, because it cannot read from a low integrity level, thus preserving data integrity at the high level."

[1] `https://petsymposium.org/2016/files/papers/On_the_(In)effectiveness_of_Mosaicing_and_Blurring_as_Tools_for_Document_Redaction.pdf`

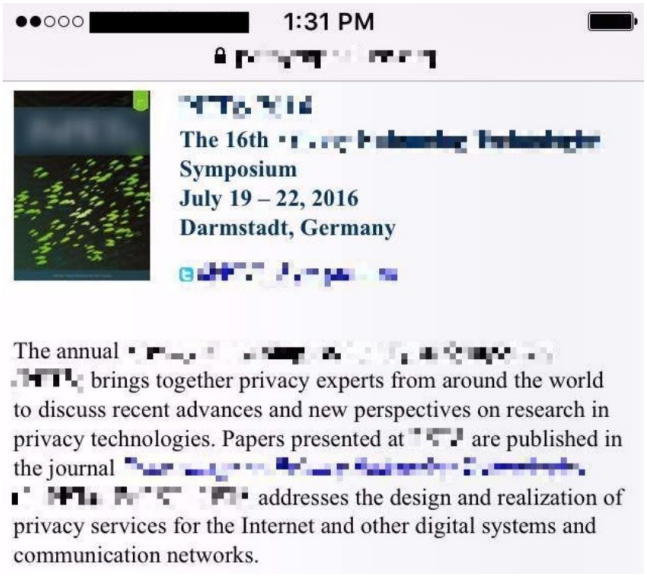

Figure 1: An example of mosaicing

7. A list of phone numbers needs to be sanitized. What checks should be performed?

8. Suppose you work for a company with a Chinese Wall security policy with clients in the following conflict classes:

   - { Cadbury, Nestle }
   - { Ford, Chrysler, GM }
   - { Citicorp, Credit Lyonnais, Deutsche Bank }
   - { Microsoft }

   You have previously worked on cases for Nestle and Citicorp, and you are ready for a new assignment. List any of your company's clients for whom you cannot work in your next assignment. (You can work for a client for whom you have previously worked, as no flow is generated.)