COM-301 Computer Security
Exercise 3: Security Models

October 5, 2023

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?

   Solution:
   Bell LaPadula has preserving confidentiality as the goal. Thus, while Write up could tamper with the integrity of information at higher levels, it is not a concern within this security model because lower clearance subjects can still not read highly classified objects.

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?

Solution:

(a) Yes, the president can compute the total cost, since he has clearance (T, {A, N}), which dominates both the army cost, classified as (U, {A}), and the nuclear cost, classified as (U, {N}).

(b) Yes, the colonel can read these numbers, since read-below is allowed and he has clearance (S, {A, N}), which dominates both the number of army units, classified as (C, {A}), and the number of nuclear units, classified as (C, {N}).

(c) No, there is no relation between the clearance of the major (C, {A}) and the nuclear code classified as (T, {N}).

(d) No, the clearance of the soldier (U, {N}) does not include the army category to access the army cost classified as (U, {A}).

(e) No, the clearance of the soldier (U, {N}) is below the required security of the number of nuclear units classified as (C, {N}).

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

Solution:

(a) Yes, the Professor sending grades to the students and the TAs sending ACKs to the students are violations of the No Write Down property in BLP. The lab needs to implement declassification, i.e., removing the classification label, for the grades and the ACKs.

(b) i. Does not prevent the channel. The TAs can still transmit their bit. The students just need to subtract 10 minutes to recover the bit.

ii. This completely prevents the channel. The sending time of the acknowledgment is independent of when the assignment was submitted and the moment when the TA sends the ACK. [Note: the TA could still use this channel by delaying the ACK for more than one day, but then the students would get nervous about maybe not having submitted correctly.]

iii. Does not *completely* prevent the channel. Now it is more difficult for the students to know what is the delay with which the TA has sent the ACK. Yet, on average, they can still detect ACKs sent with delay.

iv. Does not prevent the channel. These ACKs do not hide the real ACKs and the real ACKs' delay. Also, they will annoy the students.

Note that the TAs can still find other covert channels, e.g., sending 2 acks instead of 1 when the exercise is correct. Can you think of more schemes to transmit 1 bit?

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)

Solution:
No, it is not. An adversary knowing the technique can recover the characters/words using brute force: if you suspect a word is being mosaiced, apply the mosaicing algorithm and check if the result is similar to what you see in the declassified document

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

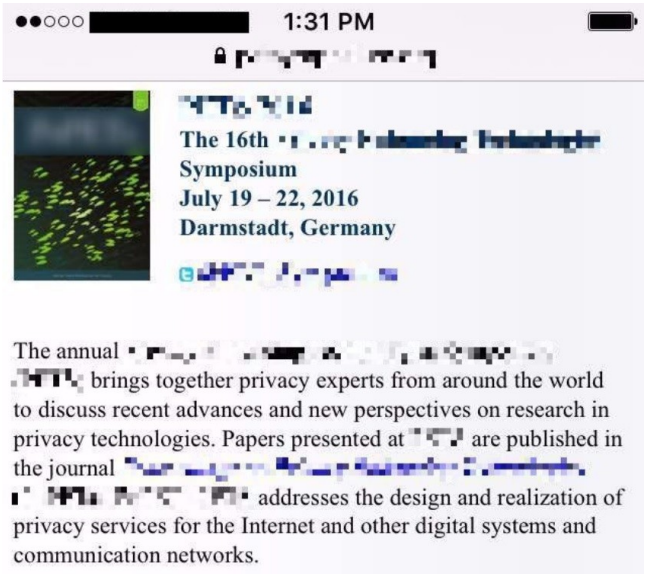

Figure 1: An example of mosaicing

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?

   Solution:

   (a) Assume the confidentiality levels were the same as the integrity levels. Let A and B be the labels of security compartments, where A dominates B. Then under the Bell-LaPadula model, a subject with label B cannot read an entity with label A. Under Biba's model, a subject with label A cannot read an entity with label B. A similar set of conditions holds for writing. However, if A = B, then both models allow reads and writes. And, of course, if there is no dominance relation between any two labels, entities with those labels can neither read nor write one another. Thus, if the confidentiality levels are the same as the integrity levels, a given process can only access objects in its own compartment (level).

   (b) This scheme is far too restrictive to be used in practice. The processes are completely confined to their compartments, and often processes

need to be able to read data in compartments that their compartment dominates. This is not possible in this scheme.

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."

   Solution:
   It is right. Following the BIBA model, once the malware has infiltrated the high integrity level, it **cannot** read down (in order to avoid that low-level information pollutes the high level). Thus, it cannot access the network, at a lower level. Therefore, the malware cannot obtain the configuration file it needs to operate, i.e., it cannot do anything. As a result, the integrity of the high level is preserved.

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

   Solution:
   One should make checks to ensure that the received number belongs to the universe of good telephone numbers:

   - It contains only numbers
   - Format restrictions depending on the country. In Switzerland "A complete telephone number consists of ten digits: 0xx xxx xx xx. Two formats are distinguished: three digits for the NDC and seven digits for the subscriber number, and four digits for the NDC and six digits for the subscriber number." (`https://en.wikipedia.org/wiki/Telephone_numbers_in_Switzerland`)

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.)

   Solution:
   I cannot work with any company that has a conflict of interest with the companies I have already worked with. Thus, given that I have already worked with Nestle and Citicorp I cannot work with:

- Cadbury: This company generated a Conflict of Interest with Nestle, as indicated in the first class.
- Credit Lyonnais or Deutsche Bank: These companies generate a Conflict of Interest with Citicorp.