# Exercises - Week 3
# Security Models

**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?**

*Bell LaPadula has as goal preserving confidentiality. 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 security levels 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, and**
- **the soldier has only UNCLASSIFIED clearance for Nuclear.**

**We also have some objects (documents):**

- **the army position at security level SECRET,**
- **the number of army units at security level CONFIDENTIAL,**
- **the number of nuclear units at security level CONFIDENTIAL,**
- **the costs of the nuclear program at security level UNCLASSIFIED,**
- **the costs of the army at security level UNCLASSIFIED, and**
- **the nuclear code at security level TOP SECRET.**

**Answer with justifications the following questions based on the BellLaPadula model:**
**[Hint: draw the lattice, it should help]**

**(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?**

*(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. Consider a system that used the Bell-LaPadula model to enforce confidentiality and the Biba model to enforce integrity.**
**a. If the security classes were the same as integrity classes, what objects could a given process (with some security class that also served as its integrity class) access?**
**b. Why is this scheme not used in practice?**

*a. Assume the security classes were the same as the integrity classes. Let A and B be the labels of security compartments, where A dom 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 security classes are the same as the integrity class, a given process can only access objects in its own compartment (class).*

*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*

**4. Discuss this statement: "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 preserves data integrity at the high level." Is it right or wrong? why?**

*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.*

**5. A list of phone numbers needs to be *sanitized*. What checks should be performed on the phone numbers before publishing the list?**

*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)*

**6. 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 are <u>not</u> able to work as your next assignment. Assume you can work for a client for whom you have previously worked.**

*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 indicated in the first class.*
- *Credit Lyonnais or Deutsche Bank: These companies generate a Conflict of Interest with Citicorp.*