

## Final Exam

### Exercise 1: (06 pts)

The Bell-LaPadula (BLP) model is a security model designed to enforce access control. Given in a system, the following subjects and their Security Levels: Ali= Confidential, Bachir = Secret, and Omar = Top Secret. Objects and Their Security Levels: X = Unclassified, Y = Secret, and Z = Top Secret. Security Levels: Top Secret > Secret > Confidential > Unclassified.

1. Explain the two main properties the model is based on.
2. Create a diagram representing subjects (Ali, Bachir, Omar) and objects (X, Y, Z) with their respective security levels.
3. For each of the following operations, determine if it is **allowed** under the Bell-LaPadula model and **justify** your answer based on the two Properties: **Ali reads Y, Ali writes to Z, Bachir reads X, Bachir reads Z, Omar writes to X, Omar reads Z.**

### Exercise 2: (04 pts)

In a product company, various **roles** are defined to manage the store. Each role has specific permissions associated with it, governing what actions they can perform.

- Store Manager: have all employee permissions.
- Employee: view store status.
- Visitor: view products list and prices.
- Sales Representative: view store status and manage sales and process refunds.
- Purchasing Manager: view store status manage purchases.
- Warehouse Staff: view store status and manage inventory.
- Customer Service Representative: process refunds.
- Client: View product details and place orders.

#### Question:

1. Draw an RBAC Hierarchy Diagram (note: R1 → R2: R2 has also the rights of R1).
2. Can the following roles do the corresponding permission?
  - Sales Representative processes refunds.
  - Store Manager manages purchases.
  - Customer Service Representative manages sales.
  - Visitor views store status.
  - Customer Service Representative manages inventory.
  - Client places an order.

### Exercise 3: (10 pts)

For each question, choose one, two, three, or four good answers.

- 1- The **top four** measures for prevention:
  - a) Patch operating systems and applications using auto update.
  - b) Performing regular backups of data.
  - c) Restrict admin privileges to users who need them.
  - d) White-list approved applications.
- 2- Operating systems additional security tools are:
  - a) Anti-virus.      B) Firewalls.      C) Planning process.      D) Risk assessment.
- 3- The reactive control that can only inform you about bad things that have already happened is called:
  - a) Logging,    b) Testing,    c) backup,    d) Assessment.
- 4- Security maintenance includes:
  - a) Monitoring and analyzing logging information
  - b) Specifying appropriate data storage areas for application
  - c) Encrypting files and directories
  - d) Regularly testing system security
- 5- The process of making copies of data at regular intervals is called:
  - a) Planning.    b) Backup.      c) Logging.      d) Encryption.
- 6- Intruder classes:
  - a) Misfeasor.      b) Clandestine user.      c) masquerader.      D) Virus.
- 7- Intruder Behavior patterns:
  - a) Criminal.      B) Worm.      C) Phishing.      D) Insider attack.
- 8- Intrusion detection system types:
  - a) Host-based.      B) Session-based.      C) Application-based.      D) Network-based.
- 9- IDS Logical components:
  - a) Sensors.      B) User Interface.      C) Audit records.      D) Hosts.
- 10-Intrusion detection systems:
  - a) Metasploit.      B) Mitre.      C) Suricata.      D) Snort.

# System security final Exam correction

## Exercise 1:

The Bell-LaPadula (BLP) model is a security model designed to enforce access control. Given in a system, the following subjects and their Security Levels: Ali= Confidential, Bachir = Secret, and Omar = Top Secret. Objects and Their Security Levels: X = Unclassified, Y = Secret, and Z = Top Secret. Security Levels: Top Secret > Secret > Confidential > Unclassified.

1. Explain the two main properties the model is based on.
  - **No read up:** A subject cannot read data at a higher security level than its own.
  - **No write down:** A subject cannot write data to a lower security level than its own
2. Create a diagram representing subjects (Ali, Bachir, Omar) and objects (X, Y, Z) with their respective security levels.

Top Secret	Top Secret	File Z
Secret	Bachir	File Y
Confidential	Ali	
Unclassified		File X

3. For each of the following operations, determine if it is allowed under the Bell-LaPadula model and justify your answer based on the two Properties: **Ali reads Y, Ali writes to Z, Bachir reads X, Bachir reads Z, Omar writes to X, Omar reads Z.**
  - **Ali reads X:** YES. Ali (Confidential) wants to read file X (Unclassified). According to the Simple Security Property (No read up), this is allowed because Confidential is higher than Unclassified.
  - **Ali writes to Z:** NO. Ali (Confidential) wants to write to file Z (Top Secret). According to the Star Property (No write down), this is not allowed because Confidential is lower than Top Secret.
  - **Bachir reads X:** YES. Bachir (Secret) wants to read file X (Unclassified). According to the Simple Security Property (No read up), this is allowed because Secret is higher than Unclassified.
  - **Bachir reads Z:** NO. Bachir (Secret) wants to read file Z (Top Secret). According to the Simple Security Property (No read up), this is not allowed because Secret is lower than Top Secret.
  - **Omar writes to X:** NO. Omar (Top Secret) wants to write to file X (Unclassified). According to the Star Property (No write down), this is not allowed because Top Secret is higher than Unclassified.
  - **Omar reads Z:** YES. Omar (Top Secret) wants to read file Z (Top Secret). According to the Simple Security Property (No read up), this is allowed because Top Secret is equal to Top Secret.

## Exercise 2: (04pts)

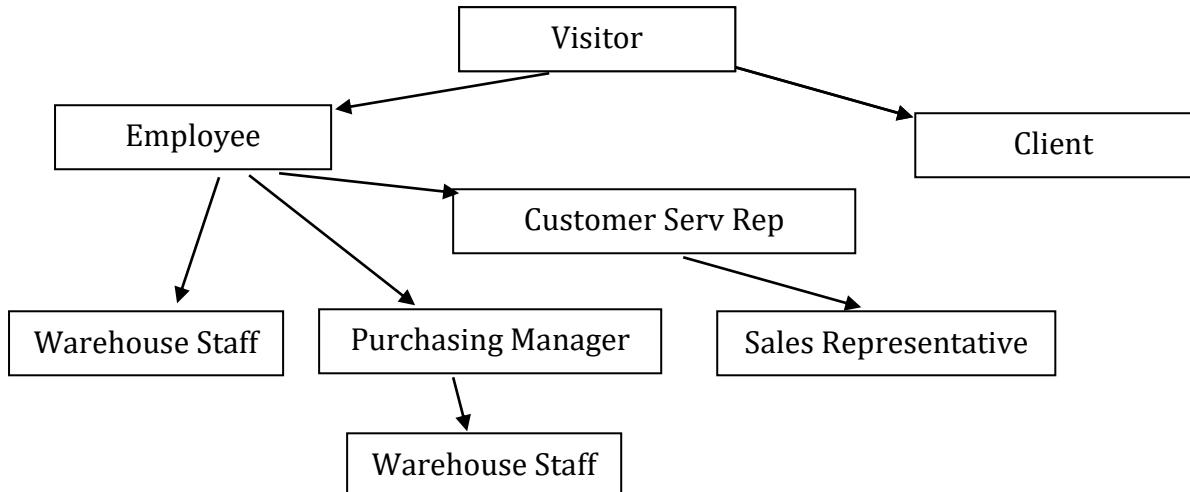
In a product company, various **roles** are defined to manage the store. Each role has specific permissions associated with it, governing what actions they can perform.

- Store Manager: have all employee permissions.

- Employee: view store status.
- Visitor: view products list and prices.
- Sales Representative: view store status and manage sales and process refunds.
- Purchasing Manager: view store status manage purchases.
- Warehouse Staff: view store status and manage inventory.
- Customer Service Representative: process refunds.
- Client: View product details and place orders.

**Question:**

1. Draw an RBAC Hierarchy Diagram (note: R1 → R2: R2 has also the rights of R1).



2. Can the following roles do the corresponding permission?

- Sales Representative processes refunds. **YES**
- Store Manager manages purchases. **YES**
- Customer Service Representative manages sales. **NO**
- Visitor views store status. **NO**
- Customer Service Representative manages inventory. **NO**
- Client places an order. **YES**

**Exercise 3: (10pts)**

For each question, choose one, two, three, or four good answers.

11-The **top four** measures for prevention:

- a) **Patch operating systems and applications using auto update.**
- b) Performing regular backups of data.
- c) **Restrict admin privileges to users who need them.**
- d) **White-list approved applications.**

12-Operating systems additional security tools are:

- a) **Anti-virus.**
- b) **Firewalls.**
- c) Planning process.
- d) Risk assessment.

13-The reactive control that can only inform you about bad things that have already happened is called:

a) **Logging**, b) Testing, c) backup, d) Assessment.

14-Security maintenance includes:

**a) Monitoring and analyzing logging information**

b) Specifying appropriate data storage areas for application

c) Encrypting files and directories

**d) Regularly testing system security**

15-The process of making copies of data at regular intervals is called:

a) Planning.

**b) Backup.**

c) Logging.

d) Encryption.

16-Intruder classes:

**a) Misfeasor.**

**b) Clandestine user.**

**c) masquerader.**

D) Virus.

17-Intruder Behavior patterns:

**a) Criminal.**

B) Worm.

C) Phishing.

**D) Insider attack.**

18-Intrusion detection system types:

**a) Host-based.**

B) Session-based.

C) Application-based.

**D) Network-based.**

19-IDS Logical components:

**a) Sensors.**

**B) User Interface.**

C) Audit records.

D) Hosts.

20-Intrusion detection systems:

a) Metasploit.

B) Mitre.

**C) Suricata.**

**D) Snort.**