1. Develop a construction to show that a system implementing the Chinese Wall model can support the Bell-LaPadula Model

Ans:

The Chinese Wall model and the Bell-LaPadula model are two different security models used in information security. The Chinese Wall model is a commercial security model that addresses the issue of conflict of interest. The Bell-LaPadula model is a military security model that deals with maintaining the confidentiality of information.

To show that a system implementing the Chinese Wall model can support the Bell-LaPadula model, we need to demonstrate how the principles of the Bell-LaPadula model can be enforced within the Chinese Wall model.

Here's a high-level construction:

1. **Bell-LaPadula Model Principles**:
    - The Simple Security Property (no read up): A subject at a given security level cannot read an object at a higher security level.
    - The *-property (no write down): A subject at a given security level cannot write to an object at a lower security level.
2. **Chinese Wall Model Implementation**:
    - The Chinese Wall model can be configured to have a hierarchical structure similar to the Bell-LaPadula model. This can be achieved by defining the security levels in the Chinese Wall model to match those in the Bell-LaPadula model.
    - The "no read up" principle can be enforced in the Chinese Wall model by preventing access to objects (information) that are within a higher conflict of interest class.
    - The "no write down" principle can be enforced by preventing a subject from writing to an object that is within a lower conflict of interest class.

This construction is a simplification and there are many complexities to consider when implementing these models in real-world systems. It's also important to note that while the Chinese Wall model can be configured to support the principles of the Bell-LaPadula model, it doesn't mean that it can fully replace the Bell-LaPadula model as they are designed to address different types of security concerns. The Bell-LaPadula model is primarily concerned with maintaining data confidentiality, while the Chinese Wall model is designed to prevent conflicts of interest in commercial environments. Therefore, the choice of model should depend on the specific requirements of the system.

2. Given the security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C, specify what type of access (read, write, both, or neither) is allowed in each of the following situations. Assume that discretionary access controls allow anyone access unless otherwise specified. a. Paul, cleared for (TOP SECRET, { A, C }), wants to access a document classified (SECRET, { B, C }). b. Anna, cleared for (CONFIDENTIAL, { C }), wants to access a document classified (CONFIDENTIAL, { B }). c. Jesse, cleared for (SECRET, { C }), wants to access a document classified (CONFIDENTIAL, { C }). d. Sammi, cleared for (TOP SECRET, { A, C }), wants to access a document classified (CONFIDENTIAL, { A }). e. Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (CONFIDENTIAL, { B }).

Ans:

Here's the type of access allowed in each situation according to the Bell-LaPadula model:

a. **Paul** is cleared for TOP SECRET with categories A and C. The document is classified as SECRET with categories B and C. Paul can **read** the document because his clearance level is higher than the document's classification level (no read up rule). However, he cannot **write** to the document because it contains a category (B) that he is not cleared for (no write down rule).

b. **Anna** is cleared for CONFIDENTIAL with category C. The document is classified as CONFIDENTIAL with category B. Anna cannot **read** or **write** to the document because it contains a category (B) that she is not cleared for.

c. **Jesse** is cleared for SECRET with category C. The document is classified as CONFIDENTIAL with category C. Jesse can **read** and **write** to the document because his clearance level is higher than the document's classification level and he is cleared for the document's category.

d. **Sammi** is cleared for TOP SECRET with categories A and C. The document is classified as CONFIDENTIAL with category A. Sammi can **read** and **write** to the document because her clearance level is higher than the document's classification level and she is cleared for the document's category.

e. **Robin** has no clearances and works at the UNCLASSIFIED level. The document is classified as CONFIDENTIAL with category B. Robin cannot **read** or **write** to the document because his clearance level is lower than the document's classification level.

Please note that these answers are based on the Bell-LaPadula model's mandatory access control rules and assume that discretionary access controls do not override these rules. In a real-world system, additional rules and exceptions may apply.

6. Declassification effectively violates the *-property of the Bell-LaPadula Model. Would raising the classification of an object violate any properties of the model? Why or why not?

Ans:

Raising the classification of an object does not violate any properties of the Bell-LaPadula model. Here's why:

The Bell-LaPadula model is primarily concerned with maintaining data confidentiality and preventing information leakage from higher to lower security levels. Its two main properties are:

1. The Simple Security Property (no read up): A subject at a given security level cannot read an object at a higher security level.
2. The *-property (no write down): A subject at a given security level cannot write to an object at a lower security level.

When the classification of an object is raised, it simply means that fewer subjects (those with the necessary higher clearance) will be able to access it. This change aligns with the principles of the Bell-LaPadula model because it further restricts access to the information, thereby enhancing its confidentiality.

On the other hand, declassification (lowering the classification of an object) can potentially violate the *-property (no write down) of the Bell-LaPadula model because it allows information to flow from a higher to a lower security level.

So, in summary, raising the classification of an object does not violate the Bell-LaPadula model's properties and, in fact, enhances the model's primary goal of maintaining data confidentiality. However, any change in classification should be handled with care in a real-world system to ensure that it does not inadvertently lead to information being inaccessible to subjects who need it for legitimate purposes.

3. A noted computer security expert has said that without integrity, no system can provide

confidentiality. a. Do you agree? Justify your answer.

Ans:

Yes, I agree with the statement. Here's why:

Integrity and **confidentiality** are two fundamental pillars of information security, often coupled with a third pillar, **availability**. These three principles are commonly referred to as the CIA triad in information security.

Confidentiality ensures that information is accessible only to those authorized to have access. It is about protecting data from unauthorized access.

Integrity, on the other hand, ensures that the information is accurate and reliable and is not altered without authorization. It guarantees that the data remains intact, unaltered, and consistent from when it was created until when it reaches its destination.

Without integrity, even if the data is confidential (i.e., protected from unauthorized access), it cannot be trusted. If data integrity is compromised, an unauthorized user could alter the data, making it unreliable or incorrect. Even if this altered data is kept confidential and only accessible to authorized users, it's of no use because it's not accurate or reliable. Hence, without integrity, confidentiality alone cannot fully secure a system.

Therefore, for a system to provide effective security, it must ensure both confidentiality and integrity of data. They are both crucial and interdependent aspects of information security. So, without integrity, no system can truly provide confidentiality. This is why I agree with the statement.

b. Can a system provide integrity without confidentiality? Again, justify your answer.

Ans:

Yes, a system can provide integrity without confidentiality. Here's why:

Integrity refers to the assurance that data is consistent, accurate, and trustworthy over its entire life cycle. It ensures that the data is not altered in transit and that it is kept safe from unauthorized changes, corruption, or loss.

Confidentiality, on the other hand, refers to the prevention of unauthorized access to information.

In some cases, data might not need to be confidential, but it still needs to maintain its integrity. For example, a public website may have information that is available to everyone (no confidentiality), but it is crucial that this information is not tampered with and remains accurate and reliable (integrity).

However, it's important to note that while a system can provide integrity without confidentiality, this doesn't mean that confidentiality isn't important. The significance of either depends on the specific requirements and context of the system. In many cases, both confidentiality and integrity are crucial for maintaining a secure system. But theoretically, a system can provide integrity without ensuring confidentiality. This is why I agree with the statement.

4.A cryptographer once claimed that security mechanisms other than cryptography were unnecessary because cryptography could provide any desired level of confidentiality and integrity. Ignoring availability, either justify or refute the cryptographer's claim.

Ans:

While cryptography is a powerful tool for ensuring confidentiality and integrity, it's not a silver bullet that can address all security concerns. Here's why:

1. **User Management**: Cryptography doesn't manage users or their access rights. Systems need mechanisms to manage user identities, authenticate users, and control their access rights.
2. **Physical Security**: Cryptography can't protect against physical attacks, such as someone gaining unauthorized access to a device or data center.
3. **Social Engineering**: Cryptography can't prevent social engineering attacks, where an attacker manipulates individuals into revealing confidential information.
4. **Insider Threats**: Cryptography can't prevent insider threats. A malicious insider with the right cryptographic keys can still cause harm.
5. **Software Vulnerabilities**: Cryptography can't protect against software vulnerabilities. If an attacker can exploit a vulnerability in the system, they can bypass cryptographic protections.
6. **Key Management**: Cryptography introduces the problem of key management. Protecting, storing, and managing cryptographic keys is a complex problem itself.
7. **Human Error**: Cryptography can't prevent human errors. Users might choose weak passwords, fail to protect their cryptographic keys, or accidentally disclose sensitive information.

So, while cryptography is essential for providing confidentiality and integrity, it's just one part of a multi-layered defense strategy. Other security mechanisms are necessary to provide a comprehensive security solution. Therefore, I would refute the cryptographer's claim. Security is a multi-faceted problem that requires a multi-faceted solution. Cryptography is a crucial part of this solution, but it's not the only part. It needs to be complemented with other security mechanisms to effectively protect a system.

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

a. The file access control mechanisms of the UNIX operating system b. A system in which no memorandum can be distributed without the author's consent c. A military facility in which only generals can enter a particular room d. A university registrar's office, in which a faculty member can see the grades of a particular student provided that the student has given written permission for the faculty member to see them.

Ans:

Here's the classification for each scenario:

a. **The file access control mechanisms of the UNIX operating system**: This is an example of a **discretionary access control** policy. In UNIX, the owner of a file can set permissions (read, write, execute) for themselves, their group, and others. This is discretionary because the owner has the discretion to set these permissions.

b. **A system in which no memorandum can be distributed without the author's consent**: This is an example of an **originator controlled** policy. The author (originator) of the memorandum controls who can distribute it.

c. **A military facility in which only generals can enter a particular room**: This is an example of a **mandatory access control** policy. In this case, access to the room is mandated by a higher authority (the military organization) and is not left to the discretion of individuals.

d. **A university registrar's office, in which a faculty member can see the grades of a particular student provided that the student has given written permission for the faculty member to see them**:

This is a combination of **discretionary** and **originator controlled** policies. The student (originator) controls who can see their grades (originator controlled), and the faculty member, once given permission, can choose whether or not to view them (discretionary).

Please note that these classifications are based on the general principles of mandatory, discretionary, and originator controlled policies. The actual implementation of these policies can vary depending on the specific system and its requirements.

1. Consider a computer system with three users: Alice, Bob, and Cyndy. Alice owns the file alicerc, and Bob and Cyndy can read it. Cyndy can read and write the file bobrc, which Bob owns, but Alice can only read it. Only Cyndy can read and write the file cyndyrc, which she owns. Assume that the owner of each of these files can execute it. a. Create the corresponding access control matrix. b. Cyndy gives Alice permission to read cyndyrc, and Alice removes Bob's ability to read alicerc. Show the new access control matrix.

Ans:

a. The access control matrix for the initial scenario would look like this:

Table

	alicerc	bobrc	cyndyrc
Alice	RWE	R	
Bob	R	RWE	
Cyndy	R	RW	RWE

Here, R stands for Read, W for Write, and E for Execute.

b. After Cyndy gives Alice permission to read cyndyrc, and Alice removes Bob's ability to read alicerc, the access control matrix would look like this:

Table

	alicerc	bobrc	cyndyrc
Alice	RWE	R	R
Bob		RWE	
Cyndy	R	RW	RWE

In this updated matrix, Alice now has read access to cyndyrc, and Bob no longer has read access to alicerc. The other permissions remain unchanged.

Stallings

1 Explain the differences among the terms security class, security level, security clearance, and security classification.

Ans:

Sure, here are the differences among these terms:

1. **Security Class**: This refers to a grouping of information based on similar levels of sensitivity and the need for protection. Information within the same security class will have similar requirements for confidentiality, integrity, and availability.
2. **Security Level**: This is a measure of the sensitivity of an object (such as data) or a subject (such as a user or process). It often includes a hierarchical classification (such as Top Secret, Secret, Confidential, Unclassified) and a set of categories (such as Nuclear, Chemical, Biological).
3. **Security Clearance**: This is the level of trust given to an individual, typically after a background check, which determines the highest security level of data they can access. For example, a person with a “Top Secret” clearance can access data classified at the “Top Secret” level and below.
4. **Security Classification**: This is the process of assigning a security level to an object. It determines the sensitivity of the data and the extent to which it needs to be protected. The classification is typically assigned by the data owner based on laws, regulations, or policies.

Each of these terms plays a crucial role in defining and implementing an organization’s information security policy. They help ensure that sensitive information is only accessible to authorized individuals and that it is protected from unauthorized access or disclosure.

13.2 What are the three rules specified by the BLP model?

Ans:

The Bell-LaPadula (BLP) model specifies three rules for maintaining data confidentiality in a system:

1. **Simple Security Property (No Read Up, or NRU)**: A subject cannot read an object at a higher security level. This prevents information flow from a higher security level to a lower one.
2. ***-property (No Write Down, or NWD)**: A subject cannot write to an object at a lower security level. This prevents information at a higher security level from being written to a lower security level where it could be read by subjects not cleared for the higher level.
3. **Strong Tranquility Property**: The security level of a subject or object does not change while it is being accessed by a subject. This ensures that the security level of an object or subject doesn't change in a way that violates the first two properties during processing.

These rules are designed to prevent unauthorized information flow in a system, particularly to prevent information from flowing from a higher security level to a lower one. They form the basis of many secure systems and are fundamental to understanding computer security.

13.3 How is discretionary access control incorporated into the BLP model

Ans:

The Bell-LaPadula (BLP) model primarily focuses on mandatory access control, which is based on the classification of information and the security clearances of

users. However, it can be extended to include discretionary access control (DAC).

In a system with DAC, the owner of the information or resource has the discretion to grant or revoke access permissions to other users. This is typically implemented using Access Control Lists (ACLs) or capability lists.

In the context of the BLP model, discretionary access control can be incorporated as follows:

- The owner of a document (or any object) can set discretionary access permissions for that document. These permissions specify which users (or groups of users) can read or write the document.
- These discretionary permissions are checked in addition to the mandatory access control rules of the BLP model. That is, a user can access a document only if both the mandatory and discretionary access control checks pass.
- For example, even if a user has the necessary security clearance to access a document based on the BLP model's rules, they would still need the appropriate discretionary permissions set by the document's owner.

So, while the BLP model is primarily a mandatory access control model, it can incorporate elements of discretionary access control to provide more flexible and fine-grained

access control. However, it's important to note that the discretionary controls must not violate the mandatory access control rules of the BLP model. For instance, a user should not be able to grant a higher level of access to another user than they themselves possess. This ensures the model's primary goal of maintaining data confidentiality is not compromised.

13.5 What are the three rules specified by the Biba model?

Ans:

The Biba model, a formal state transition system of computer security policy that describes a set of access control rules, is designed to ensure data integrity. Here are the three main principles or rules of the Biba model:

1. **Simple Integrity Axiom (No Read Down)**: A subject at a given integrity level cannot read an object at a lower integrity level. This prevents a subject from reading information that could have been tampered with by a less trusted subject.
2. ***-Integrity Axiom (No Write Up)**: A subject at a given integrity level cannot write to an object at a higher integrity level. This prevents a subject from corrupting data that is trusted by subjects at a higher integrity level.
3. **Invocation Property**: A subject at a given integrity level cannot request service (invoke) from a subject at a lower

integrity level. This prevents a higher integrity subject from being influenced by a lower integrity subject.

These rules are designed to prevent unauthorized users from making modifications, and they help to maintain the integrity of data in a system.