Security Principles

CIA

CIA is a security triad, below is what each one stands for and why:

- **Confidentiality** ensures that only the intended persons or recipients can access the data.
- **Integrity** aims to ensure that the data cannot be altered; moreover, we can detect any alteration if it occurs.
- **Availability** aims to ensure that the system or service is available when needed.

For example in a patient records:

- **Confidentiality**: According to various laws in modern countries, healthcare providers must ensure and maintain the confidentiality of medical records. Consequently, healthcare providers can be held legally accountable if they illegally disclose their patients' medical records.
- **Integrity**: If a patient record is accidentally or maliciously altered, it can lead to the wrong treatment being administered, which, in turn, can lead to a life-threatening situation. Hence, the system would be useless and potentially harmful without ensuring the integrity of medical records.

- **Availability**: When a patient visits a clinic to follow up on their medical condition, the system must be available. An unavailable system would mean that the medical practitioner cannot access the patient's records and consequently won't know if any current symptoms are related to the patient's medical history. This situation can make the medical diagnosis more challenging and error-prone.

Beyond the CIA we have authenticity and nonrepudiation:

- **Authenticity**: Authentic means not fraudulent or counterfeit. Authenticity is about ensuring that the document/file/data is from the claimed source.
- **Nonrepudiation**: Repudiate means refusing to recognize the validity of something. Nonrepudiation ensures that the original source cannot deny that they are the source of a particular document/file/data. This characteristic is indispensable for various domains, such as shopping, patient diagnosis, and banking.

There is a six security element model made by Donn Parker which is:

1. Availability
2. Utility
3. Integrity
4. Authenticity

5. Confidentiality
6. Possession

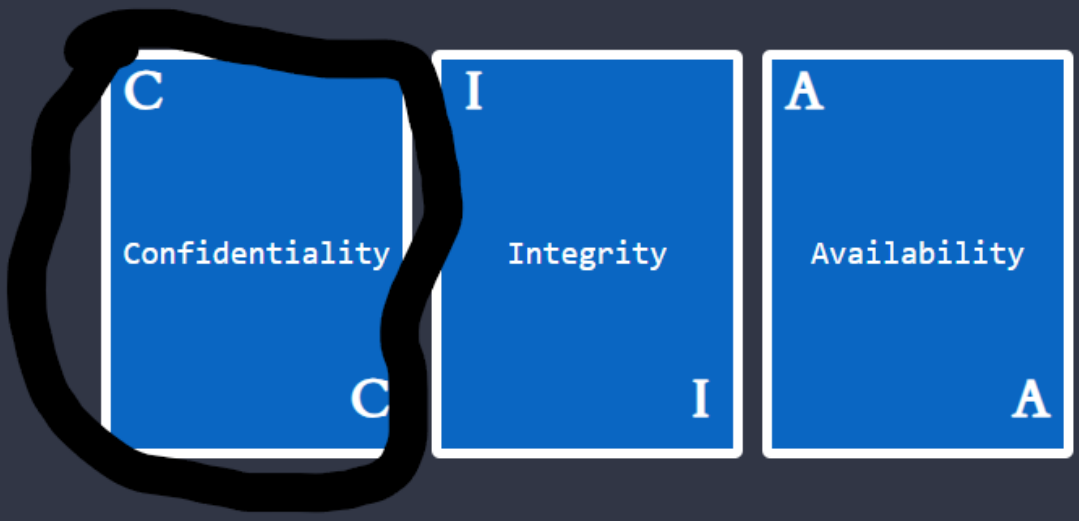
- **Utility**: Utility focuses on the usefulness of the information. For instance, a user might have lost the decryption key to access a laptop with encrypted storage. Although the user still has the laptop with its disk(s) intact, they cannot access them. In other words, although still available, the information is in a form that is not useful, i.e., of no utility.
- **Possession**: This security element requires that we protect the information from unauthorized taking, copying, or controlling. For instance, an adversary might take a backup drive, meaning we lose possession of the information as long as they have the drive. Alternatively, the adversary might succeed in encrypting our data using ransomware; this also leads to the loss of possession of the data.

Now we have to do a challenge to get the flag we have 5 questions and have to select which part of the CIA triad it is.

Security Principles

Question 1/5

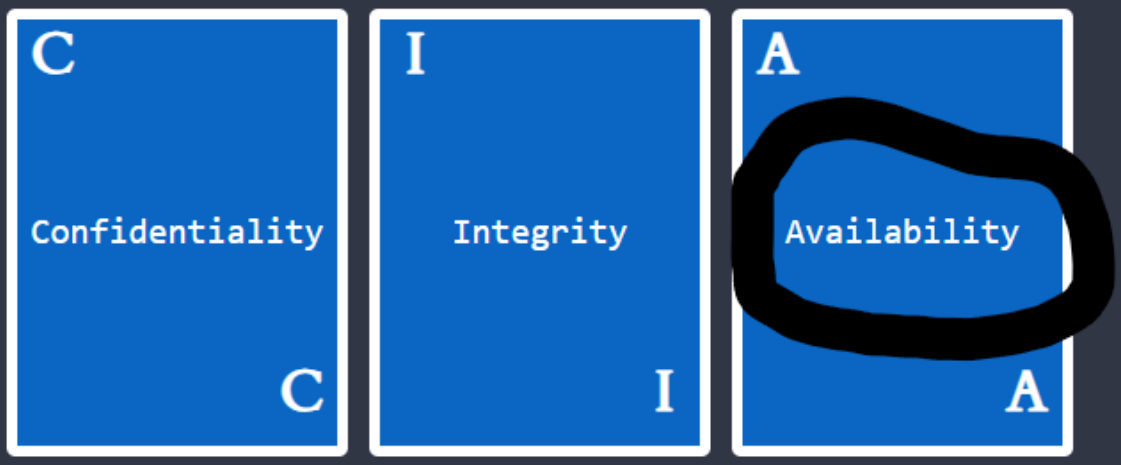
As the troops got deployed, the leader stressed that they should not communicate their location to anyone while the mission was ongoing. Which security function did the leader want to have?



Security Principles

Question 2/5

One hotel is stressing that the Internet over its WiFi network must be accessible 24 hours a day, seven days a week. Which security pillar is the hotel requiring?



Security Principles

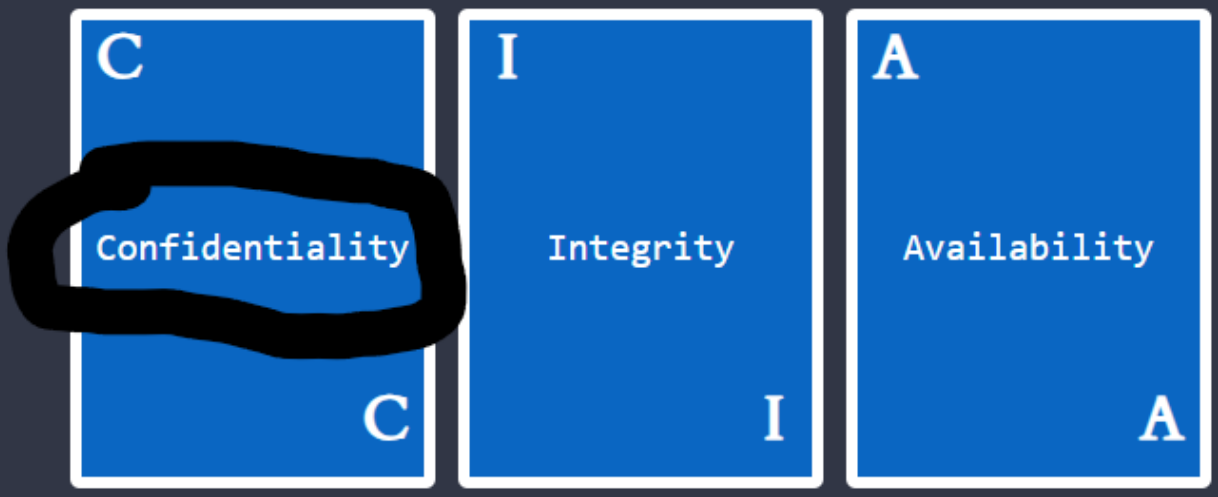
Question 3/5

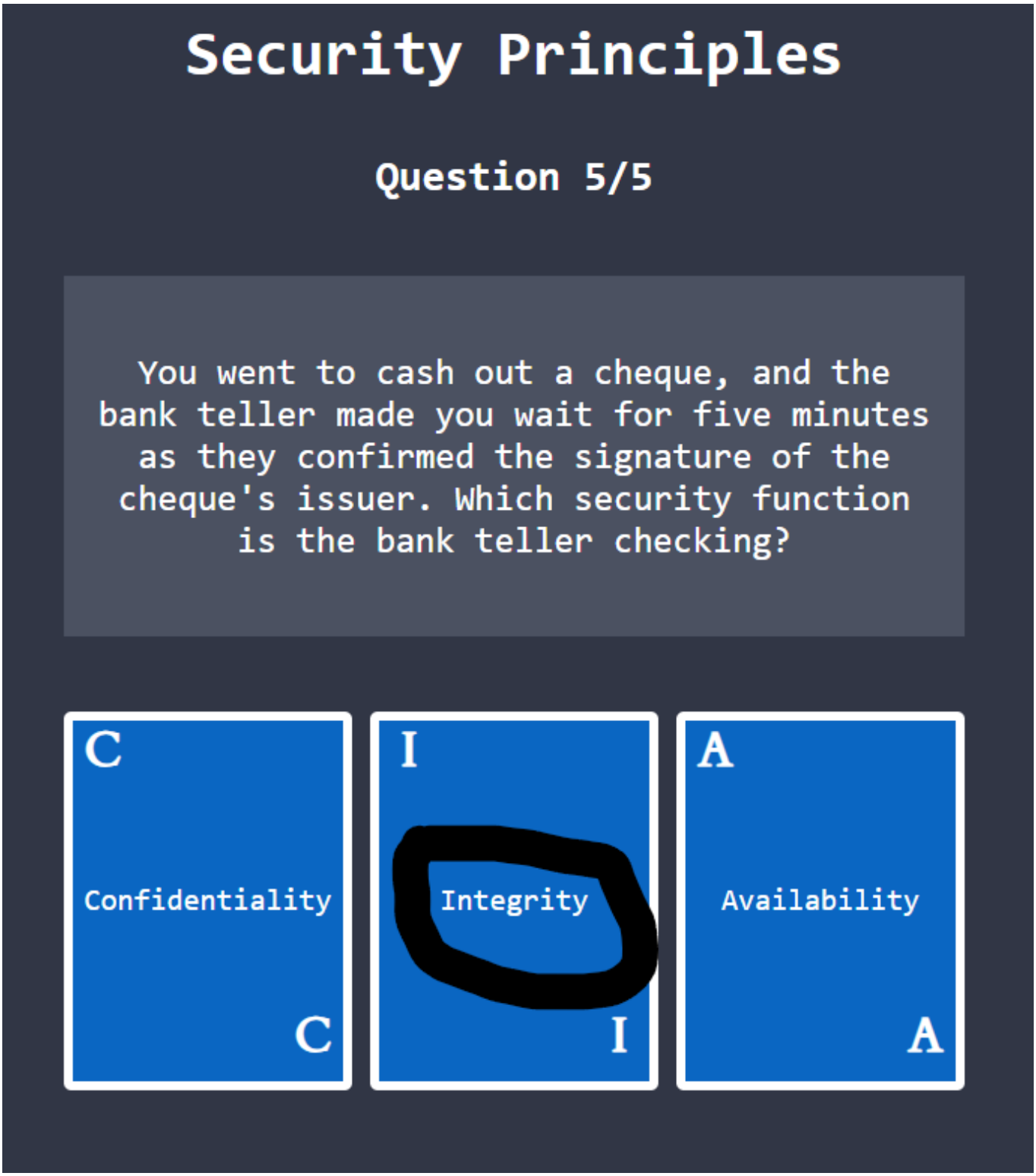
At a police checkpoint, the police officer suspected that the vehicle registration papers were fake. Which security function does the officer think is lacking?

Security Principles

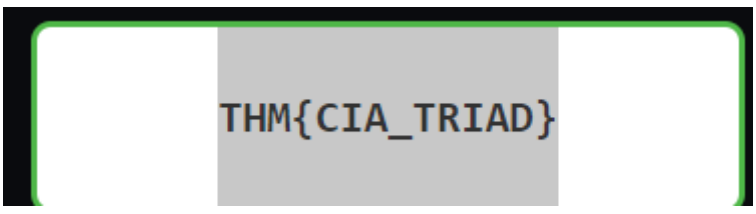
Question 4/5

Two companies are negotiating a certain agreement; however, they want to keep the details of the agreement secret. Which security pillar are they emphasizing?





After guessing all of these correctly we get a flag:



DAD

The DAD is the security of a system is attacked through many means. This is the opposite of the CIA triad:

- **Disclosure** is the opposite of confidentiality. In other words, disclosure of confidential data would be an attack on confidentiality.
- **Alteration** is the opposite of Integrity. For example, the integrity of a cheque is indispensable.
- **Destruction/Denial** is the opposite of Availability.

Referring back to the CIA with patient records this is the DAD with patient records:

- **Disclosure:** As in most modern countries, healthcare providers must maintain medical records' confidentiality. As a result, if an attacker succeeds in stealing some of these medical records and dumping them online to be viewed publicly, the health care provider will incur a loss due to this data disclosure attack.
- **Alteration:** Consider the gravity of the situation if the attacker manages to modify patient medical records. This alteration attack might lead to the wrong treatment being administered, and consequently, this alteration attack could be life-threatening.
- **Destruction/Denial:** Consider the case where a medical facility has gone completely paperless. If an attacker

manages to make the database systems unavailable, the facility will not be able to function properly. They can go back to paper temporarily; however, the patient records won't be available. This denial attack would stall the whole facility.

The attacker managed to gain access to customer records and dumped them online. What is this attack?
Disclosure

A group of attackers were able to locate both the main and the backup power supply systems and switch them off. As a result, the whole network was shut down. What is this attack?
Destruction/Denial

Fundamental Concepts of Security Models

Bell-LaPadula Model

The Bell-LaPadula Model aims to achieve **confidentiality** by specifying three rules:

- **Simple Security Property**: This property is referred to as "no read up"; it states that a subject at a lower security level cannot read an object at a higher security level. This rule prevents access to sensitive information above the authorized level.
- **Star Security Property**: This property is referred to as "no write down"; it states that a subject at a higher security

level cannot write to an object at a lower security level. This rule prevents the disclosure of sensitive information to a subject of lower security level.

- **Discretionary-Security Property**: This property uses an access matrix to allow read and write operations. An example access matrix is shown in the table below and used in conjunction with the first two properties.

Biba Model

The Biba Model aims to achieve **integrity** by specifying two main rules:

- **Simple Integrity Property**: This property is referred to as “no read down”; a higher integrity subject should not read from a lower integrity object.
- **Start Integrity Property**: This property is referred to as “no write up”; a lower integrity subject should not write to a higher integrity object.

These two properties can be summarized as “read up, write down.” This rule is in contrast with the Bell-LaPadula Model, and this should not be surprising as one is concerned with confidentiality while the other is with integrity.

Biba Model suffers from various limitations. One example is that it does not handle internal threats (insider threat).

Clark-Wilson Model

The Clark-Wilson Model also aims to achieve integrity by using the following concepts:

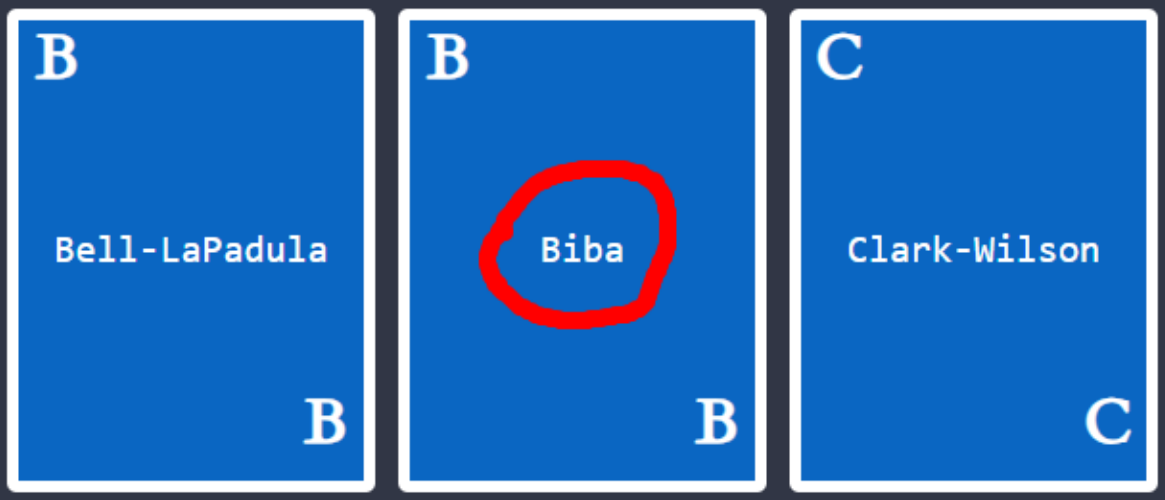
- **Constrained Data Item (CDI)**: This refers to the data type whose integrity we want to preserve.
- **Unconstrained Data Item (UDI)**: This refers to all data types beyond CDI, such as user and system input.
- **Transformation Procedures (TPs)**: These procedures are programmed operations, such as read and write, and should maintain the integrity of CDIs.
- **Integrity Verification Procedures (IVPs)**: These procedures check and ensure the validity of CDIs.

We now have another activity which we have to click the right model for the four questions to get the flag

Security Principles

Question 1/4

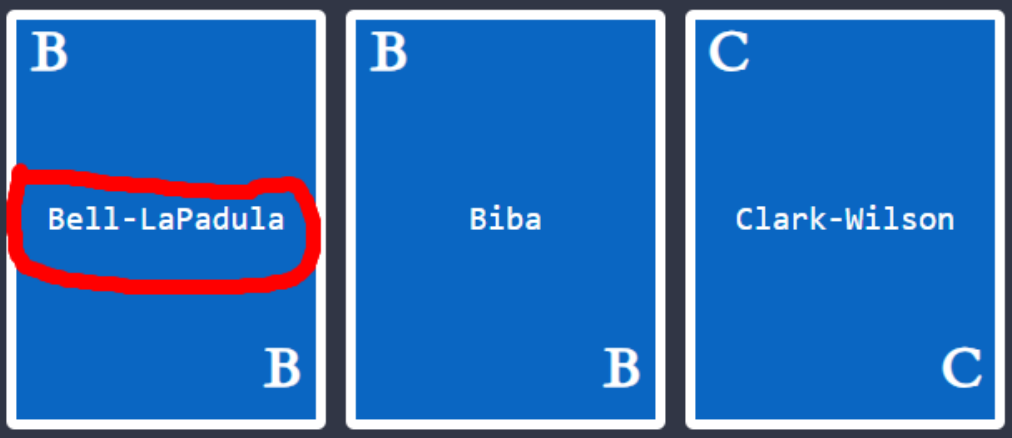
Which model dictates “no read down”?



Security Principles

Question 2/4

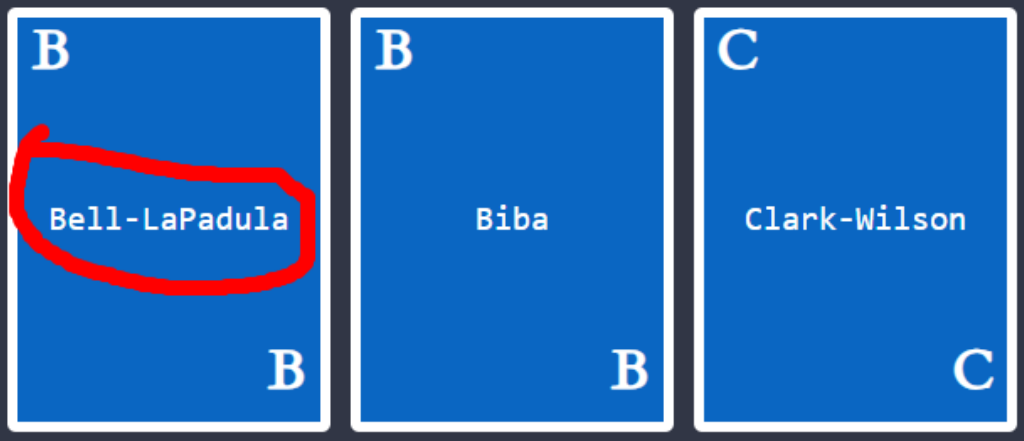
Which model states “no read up”?

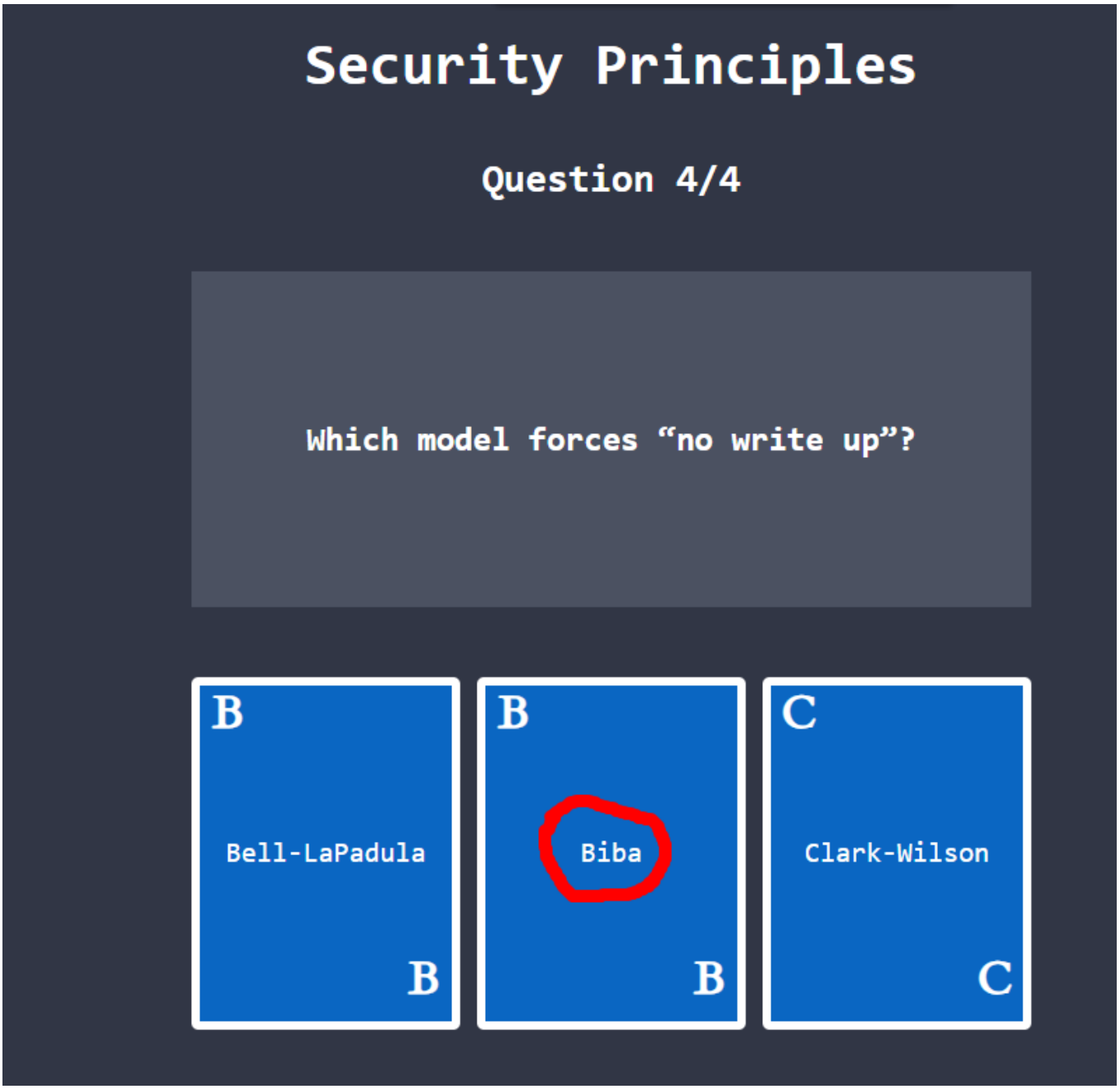


Security Principles

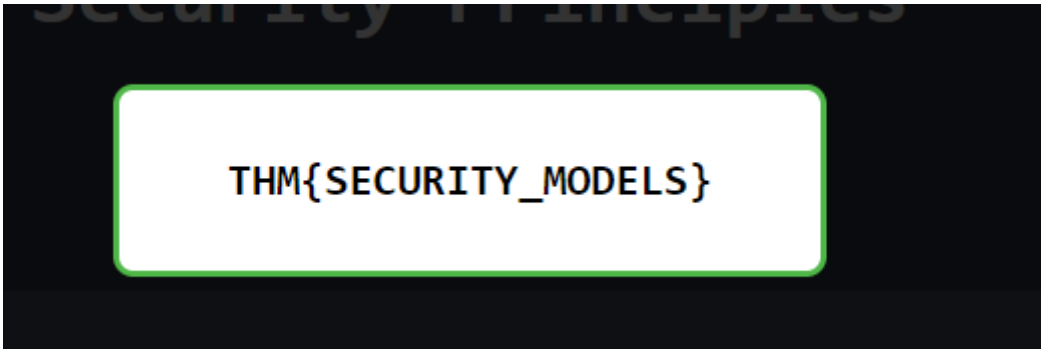
Question 3/4

Which model teaches “no write down”?





Now we have answered all questions correctly we have received the flag:



Defence-in-Depth

Defence-in-Depth refers to creating a security system of multiple levels; hence it is also called Multi-Level Security.

ISO/IEC 19249

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have created the ISO/IEC 19249.

There are 5 Architecture principles to this:

- **Domain Separation**: Every set of related components is grouped as a single entity; components can be applications, data, or other resources. Each entity will have its own domain and be assigned a common set of security attributes.
- **Layering**: When a system is structured into many abstract levels or layers, it becomes possible to impose security policies at different levels; moreover, it would be feasible to validate the operation.
- **Encapsulation**: In object-oriented programming (OOP), we hide low-level implementations and prevent direct manipulation of the data in an object by providing specific methods for that purpose.
- **Redundancy**: This principle ensures availability and integrity. There are many examples related to redundancy. Consider the case of a hardware server with two built-in

power supplies: if one power supply fails, the system continues to function. Consider a RAID 5 configuration with three drives: if one drive fails, data remains available using the remaining two drives. Moreover, if data is improperly changed on one of the disks, it would be detected via the parity, ensuring the data's integrity.

- **Virtualization**: With the advent of cloud services, virtualization has become more common and popular. The concept of virtualization is sharing a single set of hardware among multiple operating systems. Virtualization provides sandboxing capabilities that improve security boundaries, secure detonation, and observance of malicious programs.

Here are the 5 design principles:

- **Least Privilege**: The principle of least privilege teaches that you should provide the least amount of permissions for someone to carry out their task and nothing more.
- **Attack Surface Minimisation**: Every system has vulnerabilities that an attacker might use to compromise a system.
- **Centralized Parameter Validation**: Many threats are due to the system receiving input, especially from users. Invalid inputs can be used to exploit vulnerabilities in the system, such as denial of service and remote code execution. Parameter validation is a necessary step to ensure the correct system state.

- **Centralized General Security Services**: As a security principle, we should aim to centralize all security services.
- **Preparing for Error and Exception Handling**: Whenever we build a system, we should take into account that errors and exceptions do and will occur.

Which principle are you applying when you turn off an insecure server that is not critical to the business?
2 - Attack Surface Minimisation

Your company hired a new sales representative. Which principle are they applying when they tell you to give them access only to the company products and prices?
1 - Least Privilege

While reading the code of an ATM, you noticed a huge chunk of code to handle unexpected situations such as network disconnection and power failure. Which principle are they applying?
5 - Preparing for Error and Exception Handling

Zero Trust versus Trust but Verify

Trust but Verify: This principle teaches that we should always verify even when we trust an entity and its behaviour. An entity might be a user or a system. Verifying usually requires setting up proper logging mechanisms; verifying indicates going through the logs to ensure everything is normal. In reality, it is not feasible to verify everything; just think of the work it takes to

review all the actions taken by a single entity, such as Internet pages browsed by a single user. This requires automated security mechanisms, such as proxy, intrusion detection, and intrusion prevention systems.

Zero Trust: This principle treats trust as a vulnerability, and consequently, it caters to insider-related threats. After considering trust as a vulnerability, zero trust tries to eliminate it. It is teaching indirectly, “never trust, always verify.” In other words, every entity is considered adversarial until proven otherwise. Zero trust does not grant trust to a device based on its location or ownership. This approach contrasts with older models that would trust internal networks or enterprise-owned devices. Authentication and authorization are required before accessing any resource. As a result, if any breach occurs, the damage would be more contained if a zero trust architecture had been implemented.

Threat Versus Risk

- **Vulnerability**: Vulnerable means susceptible to attack or damage. In information security, a vulnerability is a weakness.
- **Threat**: A threat is a potential danger associated with this weakness or vulnerability.
- **Risk**: The risk is concerned with the likelihood of a threat actor exploiting a vulnerability and the consequent impact on the business.