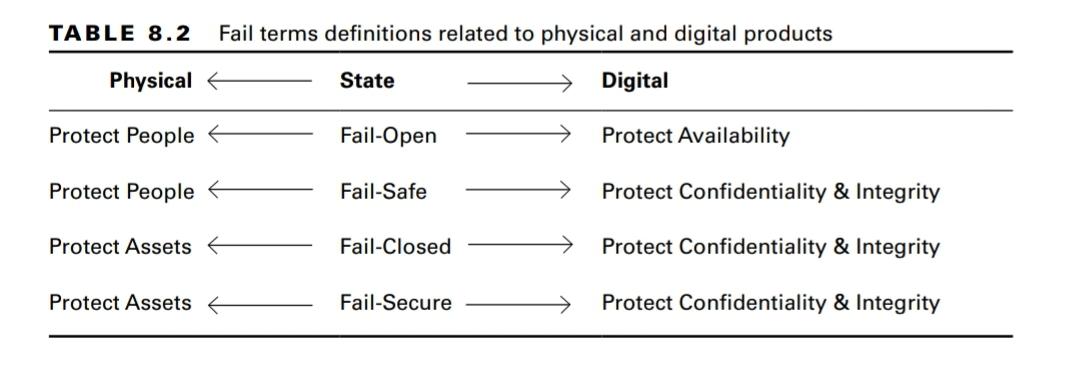
**Chapter 8: Principles of Security Models, Design, and Capabilities**

**Secure Design Principles**

* The **subject** is the active entity that makes a request to access a resource. The **object** is the passive entity that the subject wants to access.
* A **closed system** is designed to work well with a narrow range of other systems, generally all from the same manufacturer. The standards for closed systems are often proprietary and not normally disclosed. **Open systems**, on the other hand, are designed using agreed-upon industry standards and communicate using standard APIs. It is easier to exploit open systems if not implemented securely due to ease of information availability and interest gained from the attackers.
* **Secure Defaults** - Default settings should not be used
* **Fail Securely -**



* **Keep It Simple** - Avoid overcomplicating the environment, organization, or product design. The more complex a system, the more difficult it is to secure.
* **Zero Trust** - Zero trust is an alternate approach to security where nothing is automatically trusted including your internal network. Instead, each request for activity or access is assumed to be from an unknown and untrusted location until otherwise verified. The concept is “never trust, always verify.”
* **Privacy by Design** - design and implement privacy throughout SDLC.

**Techniques for Ensuring CIA**

* Process **confinement** allows a process to read from and write to only certain memory locations and resources. This is also known as sandboxing.
* The **bounds** of a process consist of limits set on the memory addresses and resources it can access.
* **Isolation** is the means by which confinement is implemented through the use of bounds.
* **Trust** can be built into a system by implementing specific security features, whereas **assurance** is an assessment of the reliability and usability of those security features in a real-world situation.

**Fundamentals of Security Models (OS architecture design)**

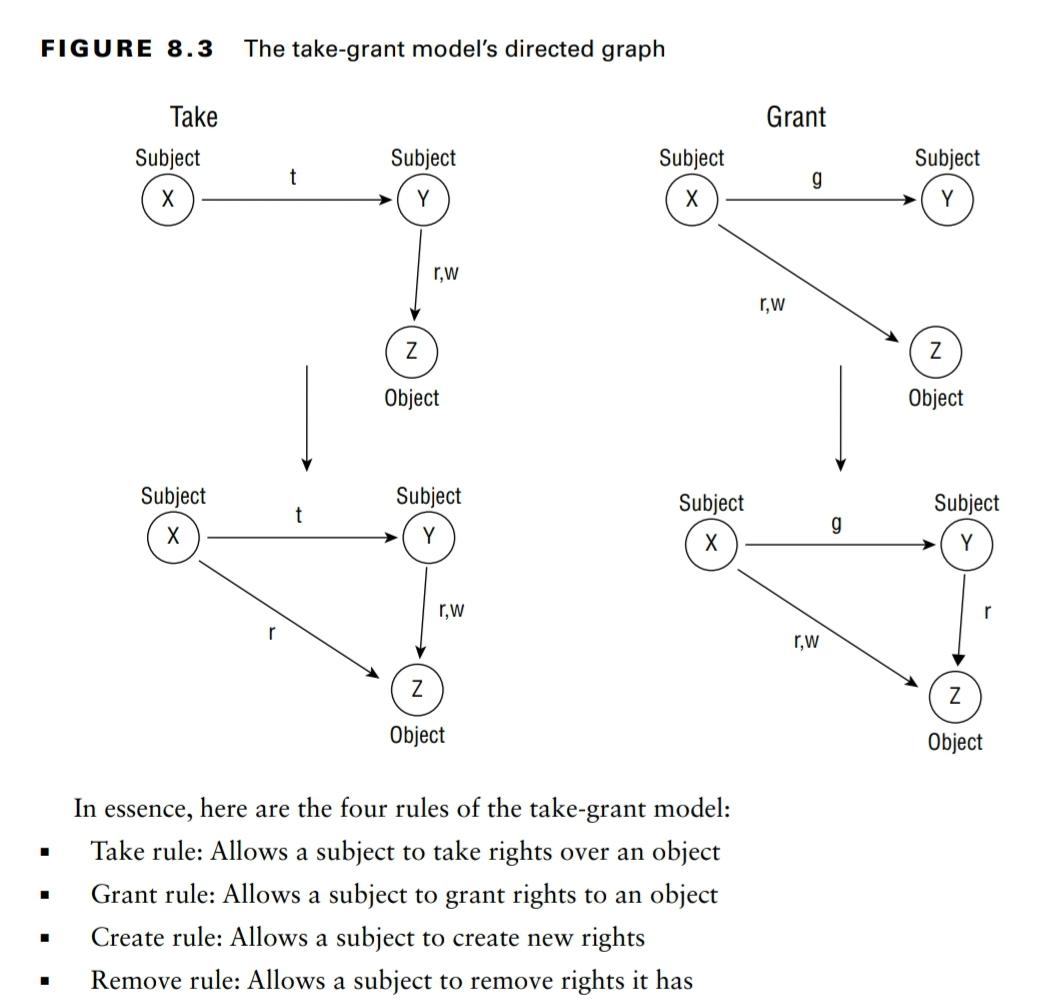
* The **trusted computing base** **(TCB)** design principle is the combination of hardware, software, and controls that work together to form a trusted base to enforce your security policy. It is the responsibility of TCB components to ensure that a system behaves properly in all cases and that it adheres to the security policy under all circumstances.
* The **security perimeter** of your system is an imaginary boundary that separates the TCB from the rest of the system.
* The part of the TCB that validates access to every resource prior to granting access requests is called the **reference monitor**. The reference monitor is a concept or theory that is put into practice via the implementation of a **security kernel** in software and hardware.

**State Machine Model** - A **secure state machine** model system always boots into a secure state, maintains a secure state across all transitions, and allows subjects to access resources only in a secure manner compliant with the security policy. It is based on a finite state machine where all transitions result in a new state, and the new state is the function of the current state and input provided. All state transitions are evaluated to ensure they result in a secure state. Many successive models such as Bell-Lapadulla and Biba are based on this model.

**Information Flow Model** - Information flow models are designed to prevent unauthorized, insecure, or restricted information flow, often between different levels of security (known as multilevel models).

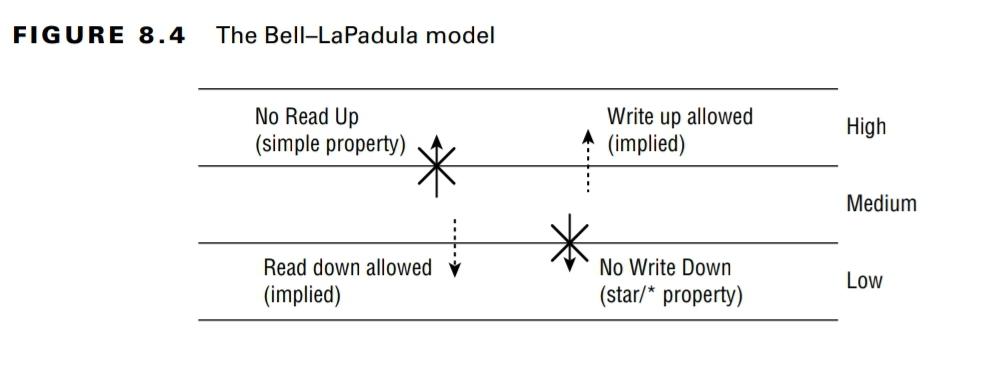
**Noninterference Model** - Actions of subject A (high level) should not affect or **interfere** with the actions of subject B (low) or even be noticed by subject B. If such violations occur, subject B may be able to deduce or infer information about a higher level of classification. This is a type of information leakage and implicitly creates a covert channel.

**Take-Grant Model**



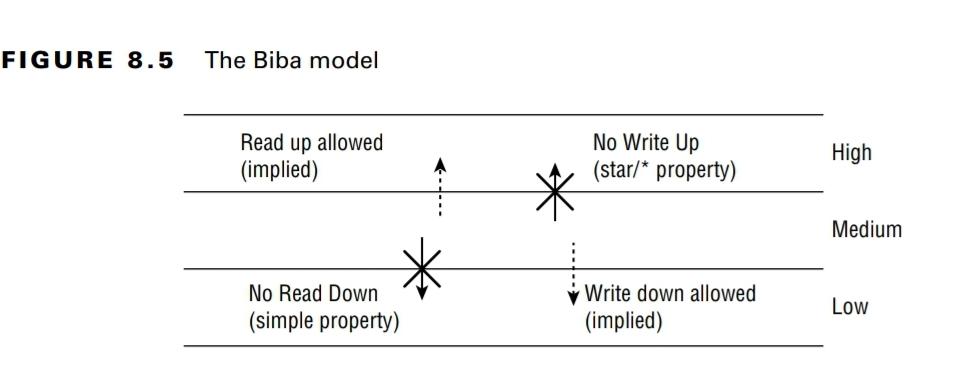
**Access Control Matrix** - An access control matrix is a table of subjects and objects that indicates the actions or functions that each subject can perform on each object.

**Bell–LaPadula Model** - It is a confidentiality focused model. Simple rule to enforce confidentiality is to not allow read up.



* Simple property is always about reading and star property is always about writing.

**Biba Model** - It is an integrity focused model. Star rule to enforce integrity is to not allow write up.



**Clark–Wilson Mode**l - It is an integrity focused model and uses an access control triplet. Subjects do not have direct access to objects. Objects can be accessed only through program interface or access portal. Each program has specific limitations on what it can and cannot do to an object. This effectively limits the subject’s capabilities. This model also provides separation of duties.

**Brewer and Nash Model** - This model uses the principle of data isolation to prevent any subject to access data that belongs to the same conflicting class. Metaphorically, this puts a wall around all other information in any conflict class. Because company relationships change all the time, there happens dynamic updates to the members of and definitions for conflict classes.

**Graham–Denning Model** - The Graham–Denning model is focused on the secure creation and deletion of both subjects

and objects. It's also focused on securely providing read, delete, grant and transfer access rights.

The **Common Criteria (CC)** defines various levels of testing and confirmation of systems’

security capabilities, and the number of the level indicates what kind of testing and confirmation has been performed. It helps to win customer's confidence while selling the product.

* **Security targets (STs)** - claims of security from the vendor that are built into TOE
* **Protection profiles (PPs)** - security requirements and protections required for a product

For many environments, it is necessary to obtain an official approval to use secured equipment for operational objectives. This is often referred to as an Authorization to Operate (ATO).

There are **four types of ATOs**, Authorization to operate, common control authorization, authorization to use, and denial of authorization.

A TPM is an example of a hardware security module (HSM). It is placed on the motherboard and is used to store cryptographic keys used for full disk encryption in modern systems.

Windows Blue Screen of Death (BSoD) stops all processing when a critical failure occurs in Windows. This is an example of a fail-secure approach.

Declassification is the process of moving an object into a lower level of classification once it is determined that it no longer justifies being placed at a higher level.

Only the Bell–LaPadula model addresses data confidentiality. The Biba and Clark–Wilson models address data integrity. The Brewer and Nash model prevents conflicts of interest.