

Security Models

Before discussing security models further, let's recall the three elements of the CIA triad: Confidentiality, Integrity and Availability. We've previously outlined what these elements are and their importance. However, there is a formal way of achieving this.

According to a security model, any system or piece of technology storing information is called an information system, which is how we will reference systems and devices in this task.

Let's explore some popular and effective security models used to achieve the three elements of the CIA triad.

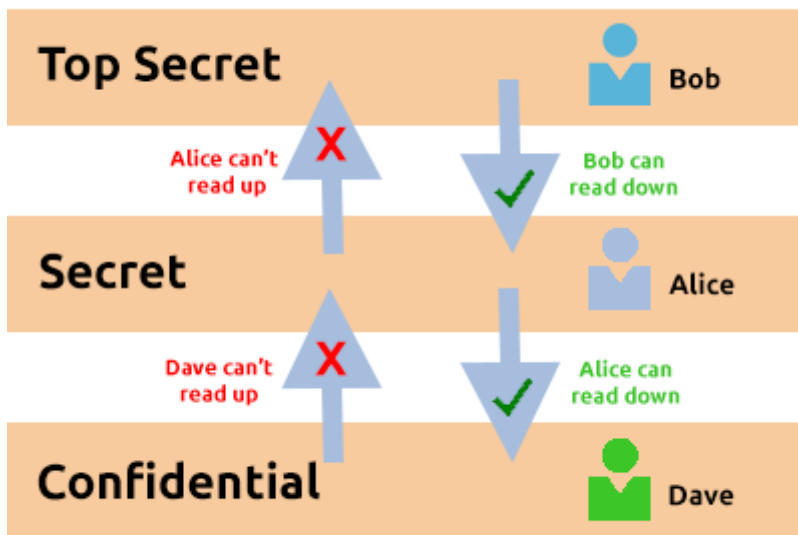
The Bell-La Padula Model

The Bell-La Padula Model is used to achieve confidentiality. This model has a few assumptions, such as an organisation's hierarchical structure it is used in, where everyone's responsibilities/roles are well-defined.

The model works by granting access to pieces of data (called objects) on a strictly need to know basis. This model uses the rule "no write down, no read up".

Advantages	Disadvantages
Policies in this model can be replicated to real-life organisations hierarchies (and vice versa)	Even though a user may not have access to an object, they will know about its existence -- so it's not confidential in that aspect.
Simple to implement and understand, and has been proven to be successful.	The model relies on a large amount of trust within the organisation.

The Bell LaPadula Model



The Bell LaPadula Model is popular within organisations such as governmental and military. This is because members of the organisations are presumed to have already gone through a process called vetting. Vetting is a screening process where applicant's backgrounds are examined to establish the risk they pose to the organisation. Therefore, applicants who are successfully vetted are assumed to be trustworthy - which is where this model fits in.

Biba Model

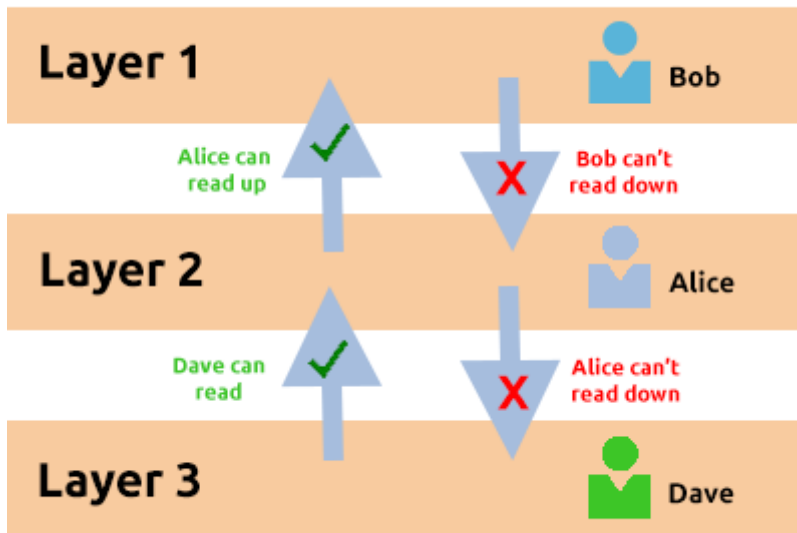
The Biba model is arguably the equivalent of the Bell-La Padula model but for the integrity of the CIA triad.

This model applies the rule to objects (data) and subjects (users) that can be summarised as "no write up, no read down". This rule means that subjects can create or write content to objects at or below their level but **can only** read the contents of objects above the subject's level.

Let's compare some advantages and disadvantages of this model in the table below:

Advantages	Disadvantages
This model is simple to implement.	There will be many levels of access and objects. Things can be easily overlooked when applying security controls.
Resolves the limitations of the Bell-La Padula model by addressing both confidentiality and data integrity.	Often results in delays within a business. For example, a doctor would not be able to read the notes made by a nurse in a hospital with this model.

The Biba Model



The Biba model is used in organisations or situations where integrity is more important than confidentiality. For example, in software development, developers may only have access to the code that is necessary for their job. They may not need access to critical pieces of information such as databases, etc.

Revision #2

Created 2023-02-11 20:55:04 UTC by Fettlaus

Updated 2023-02-11 21:16:51 UTC by Fettlaus