

What is a security model?

A computer security policy consists of a clearly defined and precise set of rules, for determining authorization as a basis for making access control decisions. A security policy captures the security requirements of an establishment or describes the steps that have to be taken to achieve the desired level of security.

A security policy is typically stated in terms of subjects and objects, Given the desired subject and object there must be a set of rules that are used by the system to determine whether a given subject can be given access to a specific object.

A security model is a formal or an informal way of capturing such policies. Security models are an important concept in the design of a system. The implementation of the system is then based on the desired security model. Formal security models such as BLP have a prominent place in high assurance security evaluations. Informal models, such as Clark-Wilson, are a more of a descriptive framework for expressing security policies.

Most security models cannot support a wide range of security policies. They either support static policies or a limited set of security policies.

The goal of the Bell-LaPadulla model

BLP is a state machine model capturing the confidentiality aspects of access control. BLP addresses security policy goal of preventing from unauthorized disclosure and declassification of information. BLP prevents information flowing downwards from high security level to a low security level.

Informal description of BLP

BLP defines security as the property of states. It consists of three properties:

1. *The simple security property: (ss-property)* The ss-property defines no-read up. Therefore a subject is not allowed to read an object higher than its own security level.

E.g. A user cleared for Secret information may not read information that is classified as Top-Secret.

However if a low level subject can read a high level object it could create a (high-level) Trojan horse, which can read high-level objects, an copy the information into a low-level object.

Thus BLP has to control the write access through the *-property.

2. *The star-property: (*-property)* A subject may not write to an object with a lower classification that the subject has clearance for. Therefore it prevents an authorized subject (user) from declassifying higher-level information and prevents against Trojan-horse attacks.

In addition a higher-level subject is not able to send messages to a lower level subject. However there are two ways this restriction can be escaped:

-Temporarily downgrade a high-level subject, which assumes that a subject forgets all it knew at a higher level, at the moment it is downgraded.

-Identify a set of trusted subjects that can be relied on not to compromise the information.

3. *Discretionary security property: (ds-property)* Defines a policy where access control is based on named users and named objects. Subject holding an access permission may pass that permission on to other subjects at their discretion.

Comments on BLP

The BLP model has been criticised for the following:

- Too restrictive and too concerned with military security policy, which may not be applicable for the enterprise environment.
- BLP only deals with confidentiality and declassification of data. In many enterprise environments integrity of data can be more valuable.
- BLP has no policy for changing access rights. This is to retain the properties of the basic security theorem. It assumes *tranquility*. The property that security levels and access rights never change. Thus BLP is intended for systems with static security levels. Again the enterprise environment is a more diverse one than a military one. Thus management of access control is not addressed.
- BLP has been also criticised that it contains covert channels. A low subject can detect the existence of a high-level object when it is denied access. Covert channels is the communications channels that allow transfer of information in a manner that violates the systems's security policy.

However some of the criticisms are not a flaw of the BLP model but a feature. It was originally designed for a military environment and not for supporting a diverse range of policies.

The Biba integrity model

Biba is a state machine model similar to BLP. Biba however addresses integrity policies, in terms of access to objects from subjects.

In an integrity lattice information may only flow downwards.

Static integrity levels

Mirroring the tranquility property of BLP, we can state policies where integrity levels never change.

- Simple integrity property: (No write-up) Subjects cannot write objects with higher integrity level.
- Integrity *-property: (No read down) Subject cannot read an object with lower integrity level.

Dynamic Integrity levels

Similar to the Chinese-Wall model, the next two integrity properties automatically adjust the integrity level of an entity if it has come into contact with a low-level information.

- Subject low watermark property: A subject can read an object at any integrity level. The new integrity level of the subject is $\inf(fs(s), fo(o))$ where $fs(s)$ and $fo(o)$ are the integrity levels before the operation.
- Object low watermark property: A subject can modify an object at any integrity level. The new integrity level of the object is $\inf(fs(s), fo(o))$ where $fs(s)$ and $fo(o)$ are the integrity levels before the operation.

Policies for invocation

The Biba model can be extended to include an access operation *invoke*. A subject can invoke another subject e.g. A software tool, to access an object. A distinct policy must then exist for invocation. Two additional properties add this functionality.

- Invoke property: Subjects are only allowed to invoke tools at a lower level. Otherwise a dirty (low-level) subject could invoke a clean (high-level) tool and contaminate a clean object. Alternatively we might want to do this. Dirty subjects will be able to access clean objects but only if they use a clean tool to do so. This tool may perform a number of consistency checks to ensure that the object remains clean. In this scenario we would not want a dirty subject to use a dirty tool and we

could adopt the Ring Property.

- Ring property: A subject can read objects at all integrity levels. It can only modify objects if the integrity level of the object is lower/equal than the subject. And it can invoke a subject only if the subjects integrity level is higher than itself.

The last two properties are highly application specific.

Brief description of the Clark-Wilson model

The Clark-Wilson model addresses the security requirements of commercial applications. It states the goal of a commercial system concerned with the integrity of data, which ensures that a user cannot modify data in a manner that would result in the loss or corruption of system asset data (like financial records).

The restriction applies to authorized users as well as unauthorized. The goal of the C-W model is to maintain the internal data and its external (user's) expectation of data.

CW uses two mechanisms for maintaining integrity.

- Well-formed transactions

Well formed transactions ensure that a user cannot alter data arbitrarily. Instead data can only be altered in specified way in order to preserve its internal consistency. This principle requires that any modification to accounting data, for example, must be accomplished in two parts. If a withdrawal from an account is made, an appropriate entry must also appear in another location, such as a payable account. If the transaction does not appear in both locations when the books are balanced, it will be detected. Performing the steps in order, performing exactly the steps listed and authenticating the individual who performs the steps constitutes a well-performed transaction.

In computer systems, well-formed transactions result in the identification of the program that may modify the data. The programs must be validated and audited beforehand to ensure they perform the right operations.

CW uses programs as an intermediate layer between subjects and objects. Subjects and objects are labelled with programs.

In CW integrity means being authorised to apply a program to a data item that may be accessed through this program. Subjects must be identified and authenticated and objects may only be manipulated by a restricted set of programs. In addition subjects can only execute a restricted set of programs. The system must be certified to work properly.

- Separation of duties

Separation of duty attempts to maintain consistency of data objects by separating all operations into several parts and requiring each part to be performed by the appropriate subject.

BLP and CW differences

- BLP controls for military security and CW for commercial security
- The way data is being treated
 - In BLP data is assigned a security level and the mode of access granted depends on this level and the level of the subject.
 - In CW, data is associated with a set of programs that which are allowed to access and manipulate it. Subjects are not given authority to access objects but instead are given permission to access certain programs that in turn access specific data.
 - In BLP user is constrained by the data they can access, while in CW they are constrained by the programs they can execute.
 - BLP deals with confidentiality and information declassification, while CW with system integrity.