13 de mayo de 2024

Clase 8

Seguridad Informática → preservar

Confidencialidad

Guardar info en secreto

(Acceso a autorizados)

Integridad

confiabilidad

- Integridad de datos
- Integridad de origen

Disponibilidad

Poder usar la info

Políticas Mecanismos

Qué acciones son seguras (permitidas) y qué acciones son inseguras (prohibidas)

Procedimiento, herramienta o método para garantizar cumplimiento de política

- Prevenir
- Detectar
- Recuperar

Tipos de Control de Acceso

Una política de seguridad puede usar

DAC

Discrecional

Basado en Identidad

Políticas se definen para el usuario

MAC

Mandatorio

Basado en Reglas

Políticas se definen para el sistema

Modelos de Seguridad

Un modelo de seguridad es una definición formal de una Política de Seguridad

A través de una sustentación formal, matemática se demuestra que el sistema es seguro.

Modelo de

Bell - LaPadula

Confidencialidad

Modelo de

Bíba

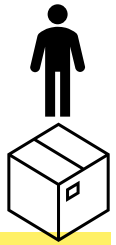
Integridad

Modelo de Bell - LaPadula

Objetivo: Prevenir el acceso no autorizado a la información.
las modificaciones no autorizadas son secundarias. (la parte de la integridad no es tan importante)

➢ Combina **acceso mandatorio** y **acceso discrecional**

Elementos:.



- ✓ Sujetos
- ✓ Objetos
- ✓ Modos de acceso = {read, write, ...}
- ✓ Clasificación de seguridad = {TS, S, C, U...}
- ✓ Niveles de seguridad = Clasificación x Categoría (red)

Ej: = {(Top Secret, {OTAN, MERCOSUR, ...})
(Confidencial, {MERCOSUR})...}

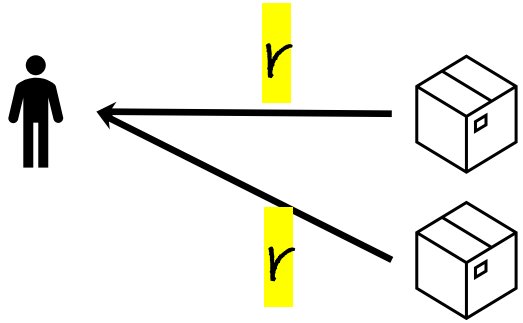
El verde es el acceso mandatorio y el amarillo el discrecional
Para que un sujeto S pueda acceder a un objeto O, entonces se tiene que cumplir tanto el acceso mandatorio como el discrecional.

Principios:.

Condición de Seguridad Simple - Read Down

El sujeto s puede leer el objeto o si y solo si

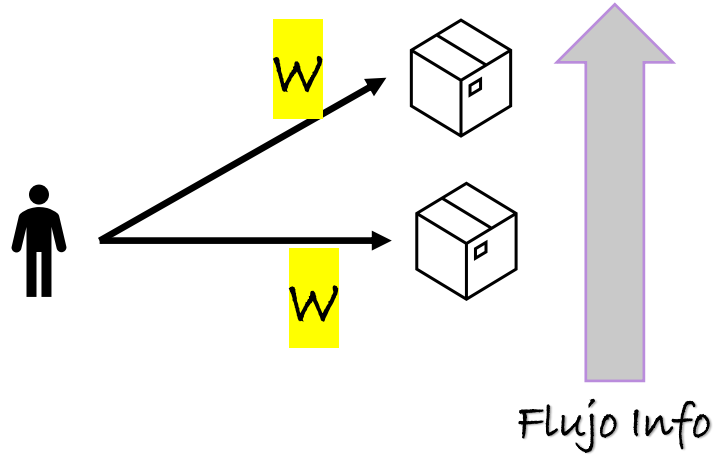
L(s) dom L(o) y s tiene permiso para leer o.



Propiedad * - Write Up

El sujeto s puede escribir el objeto o si y solo si

L(o) dom L(s) y s tiene permiso para escribir o.



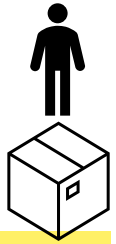
Dominancia:. (L,C) domina a (L',C') si y sólo si $L' \leq L$ y $C' \subseteq C$

Modelo de Biba

Objetivo: Preservar los datos y su integridad.
Identifica maneras autorizadas en las cuales la información puede ser alterada y cuáles son las entidades autorizadas para hacerlo.

Elementos:.

- ✓ Sujetos
- ✓ Objetos



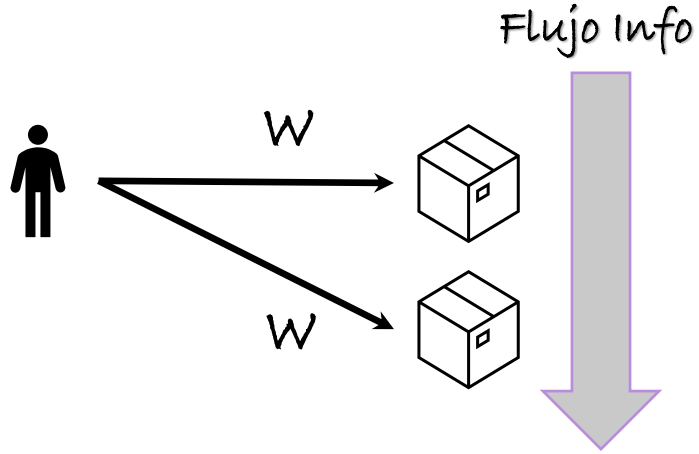
- ✓ Modos de acceso = {read, write, ...}
- ✓ Niveles de integridad = il() → a mayor nivel mayor confianza

Principios

Los principios son al reves que en Bell LaPadula.
Un sujeto puede escribir en un nivel de integridad menor o igual que el suyo.
Un sujeto puede leer en un nivel de integridad mayor o igual al suyo (en Biba Estricto)
Ademas de Biba Estricto, existen otros tipos de reglas

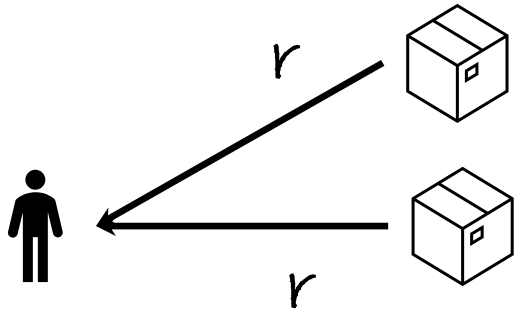
1. Escritura - Write Down

El sujeto s puede modificar el objeto o si y solo si $il(s) \geq il(o)$.



2. Lectura - Read Up (Biba Estricto)

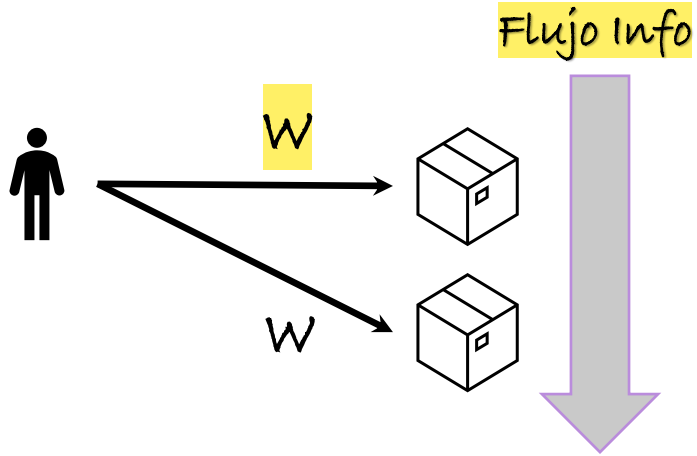
El sujeto s puede observar el objeto o si y solo si $il(o) \geq il(s)$



Principios

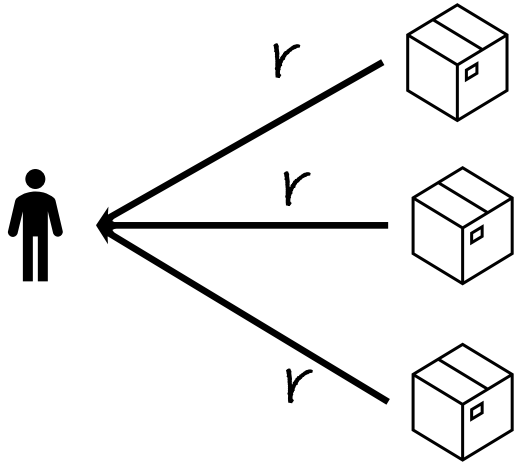
1. Escritura - Write Down

El sujeto s puede modificar el objeto o si y solo si $il(s) \geq il(o)$.



2. Lectura - Read (Biba Ring-Policy)

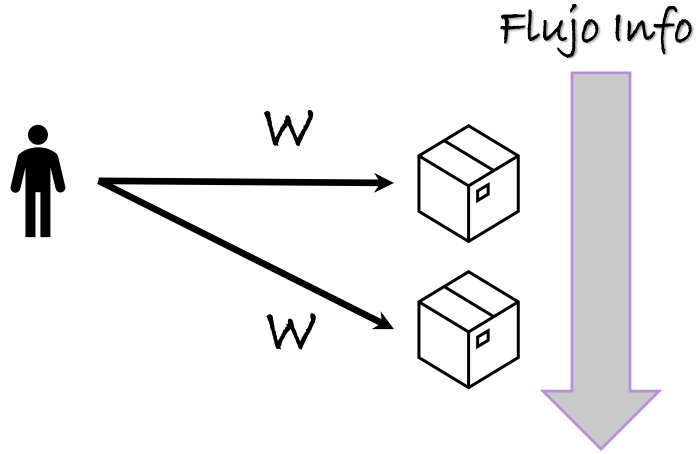
Cualquier s puede leer cualquier o.



Principios

1. Escritura - Write Down

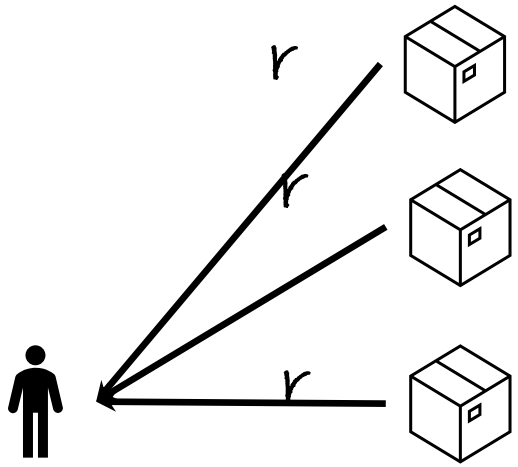
El sujeto s puede modificar el objeto o si y solo si $il(s) \geq il(o)$.



2. Lectura - Read (Biba Low-Watermark)

Si s lee o, $il(s) = min(il(s), il(o))$.

Si un sujeto lee algo de menor nivel de integridad, entonces baja su nivel de integridad.
Esto trae problemas a la larga, porque va bajando el nivel de todos los sujetos.

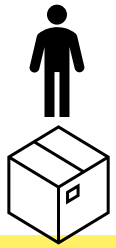


Modelo de Muralla China

Objetivo: Resolver situaciones de conflicto de interés.

Este modelo apunta a las dos cosas, pero mas a confidencialidad

Elementos:.



- ✓ Sujetos
- ✓ Objetos
- ✓ CD = Company Dataset:
  - contiene objetos relacionados con una compañía
- ✓ COI = Clase de Conflicto de Interés
  - contiene CD de compañías que compiten entre sí.
- ✓ Cada objeto pertenece a una sola clase de COI.

Principios

1. Condición de seguridad simple:

El sujeto s **puede leer** o si y sólo si:

- $\exists\ o' / s$ ha leído o' y $CD(o') = CD(o)$

(si ya leyo algo del company dataset)

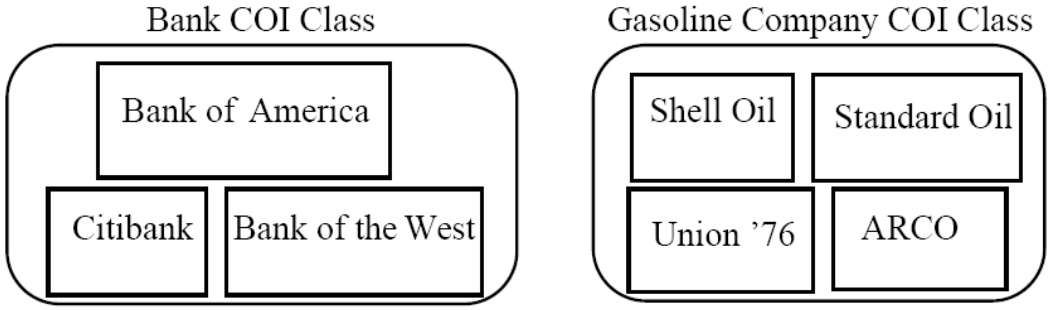
o bien:

- $\forall\ o' : o' \in PR(s) \Rightarrow COI(o') \neq COI(o)$

(si todos los objetos que leyo no son del mismo COI que el que quiere leer)

o bien:

- o es un objeto esterilizado (público)



2. Propiedad * :

El sujeto s **puede escribir en** o si y sólo si:

- S puede leer o por condición de seguridad simple

Y

- $\forall\ o'$ no esterilizado, si s puede leer $o' \Rightarrow CD(o') = CD(o)$

Si el objeto no es publico y lo puede leer, entonces tiene que ser del mismo CD que los otros que leyo

Lectura Recomendada:

- Bell76.pdf
  (Documento original Modelo Bell-LaPadula)
- Biba75.pdf
  (Documento original Modelo Biba)
- Brewer_nash_89.pdf
  (Documento original Modelo Muralla China)
- Modelo Biba.pdf
  (Acerca del Modelo Biba, en castellano)