

1. Introducción

La protección es un problema interno mientras que la seguridad considera el entorno exterior dentro del cual opera el sistema.

Una política de seguridad es qué se hace y los mejoramientos cómo se hace.

2. Protección

Un sistema es una colección de procesos y objetos donde cada uno tiene nombre único y operaciones propias. Si embargo, hay que asegurar que cada objeto es accesible correctamente sólo por quien lo tiene permiso.

· Dominio de protección: conjunto de objetos juntos con sus derechos de acceso para realizar una operación

Un proceso se ejecuta dentro de un dominio cuya asociación puede ser crítica (conjunto de objetos disponibles fijo) o dinámica.

Las entidades que pueden determinar un dominio son:

- Cada user (depende de la identidad del usuario)
- Cada proceso (depende de la identidad del proceso).
- Cada procedimiento (sus variables locales)

Matriz de acceso

Modelo que nos proporciona un mecanismo apropiado para especificar distintas políticas, y definir e implementar un control estrecho.

Objeto Dominio	F1	F2	F3	F4	F5	Impr.
D1	leer	leer escribir				
D2			leer ejecutar		escribir	
D3	ejecutar			leer escribir ejecutar		

Incluir dominios como objetos (anterior para entrada)

Objeto Dominio	F1	F2	F3	F5	Impres.	D1	D2	D3
D1	leer	leer propriet.	escribir				Comutar	
D2				leer*		escr		
D3	eje.			leer escrib. ejec.			Comutar Control	

Como implementación:

i) Tabla global: $\text{set} < \text{dominio, objeto, conjunto_derechos} \rangle$

- Gran tamaño \rightarrow no cabe en RAM
- Difícil de agrupar dominios o objetos

ii) Listas de acceso para objetos: almacena la lista por dominios.

$\text{Dom} \rightarrow \text{list} < \text{pair} < \text{dominio, conjunto_derechos} \rangle \rangle$

- Fácil de agrupar dominios

• Saber el conjunto de objetos, conjunto_derechos es complicado para dominio.

iii) Listas de capacidades para dominios: matriz por filas

$\text{Dom} : i \rightarrow \text{list} < \text{objeto, conjunto_derechos} \rangle$

- Cada elemento se determina capacidad
- Las listas de capacidades deben protegerse por el so.

iv) Corrijo - Clave

Objeto $i \rightarrow$ lista de posibles combinaciones binarias (corrijos)

Rea $i \rightarrow$ otra lista

Un proceso en un dominio puede acceder a un objeto si tiene una clave que se corresponda con una de las corrijos del objeto.

Normalmente usan i y iii)

3. Seguridad

Un sistema es seguro si sus recursos son utilizados y accedidos como se espera en todas las circunstancias. Sin embargo, se suele intentar saltarse la protección de recursos. Tres requisitos, bajas confidencialidad, integridad y disponibilidad de la información.

Vulneraciones:

- Accidentales
- Provocadas

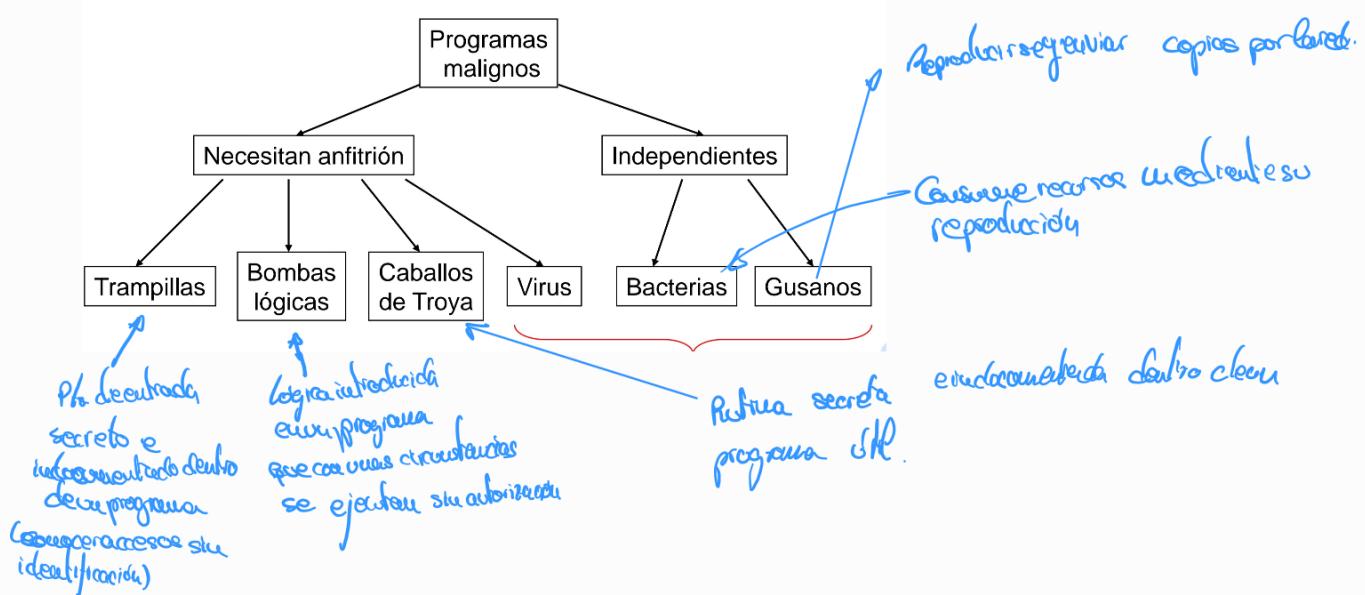
Medidas a tener en cuenta:

- Físico: protección física del sistema
- Humano: autorización, evitando el uso de usuarios
- Sistema Operativo: identificación (identifica programas, procesos y usuarios combinando la posesión de un objeto, atributo del usuario, conocimiento del usuario)

Para proteger contraseñas se suelen usar cifrados y guardar encriptada las passwords del sistema que puede ser privada o pública.

Técnicas de infusión

- Clasificación general de las amenazas por software:



Para mejorar la seguridad

1. Monitorizar la posibilidad de amenazas (patrones de actividad sospechosa)
2. Prevención de la infidelidad (guardar todos los accesos a un objeto y si hubiere uno. Si se ha violado la seguridad se puede saber cuando adentro del objeto, recuperarse, desarrollar mejor seguridad.)
3. Explorar aspectos del sistema para entorpecer.
4. Encriptar los datos