Políticas de seguridad

Política de seguridad

Si consideramos a un sistema como un autómata finito con un conjunto de funciones que permiten cambiar de estado, entonces una política de seguridad es una declaración que particiona un sistema en dos conjuntos de estados:

- Autorizados (seguros): son los estados en los que el sistema puede entrar.
- No autorizados (no seguros): si el sistema entra en uno de estos estados habrá una violación de seguridad.

Definiciones

Sistema seguro

Es un sistema que comienza en un estado autorizado, y nunca entra en un estado no autorizado.

Un sistema seguro bajo una política puede no serlo bajo otra.

Problema de seguridad

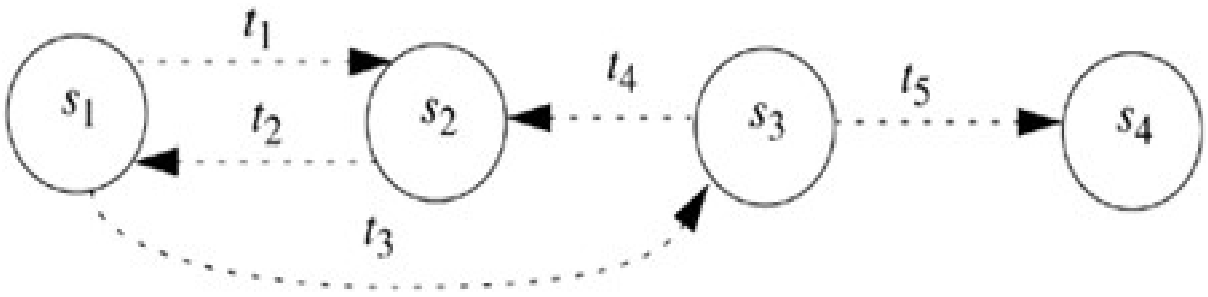
Cuando un sistema entra en un estado no autorizado entonces tenemos un problema de seguridad.

Ejemplo

- Dada la política de seguridad:

  A = { s_1, s_2 }

  NA = { s_3, s_4 }



- Este sistema no es seguro ya que desde un estado autorizado puede pasar a un estado no autorizado.
- Si el arco de s_1 a s_3 no estuviera presente sería un sistema seguro.

Confidencialidad

Sea *X* un conjunto de entidades e *I* una cierta información. Entonces *I* tiene la propiedad de confidencialidad con respecto de *X* si ningún $x \in X$ puede obtener información sobre *I*.

Por ejemplo:

- *X* conjunto de alumnos
- *I* respuestas de un examen
- *I* es confidencial con respecto de *X* si los alumnos no pueden obtener las respuestas del examen.

Integridad

Sea *X* un conjunto de entidades e *I* una cierta información. Entonces *I* tiene la propiedad de integridad con respecto de *X* si todos los $x \in X$ confían en *I*.

Tipos de integridad:

- Integridad de los datos: confiamos en que el medio de transporte o de almacenamiento no cambian la información.
- Integridad de origen: cuando la información es sobre el origen de algo o sobre identidad.

Disponibilidad

Sea *X* un conjunto de entidades e *I* una cierta información. Entonces *I* tiene la propiedad de disponibilidad con respecto de *X* si todos los $x \in X$ pueden acceder a *I*.

Tipos de disponibilidad:

- Tradicional: se accede o no a la información.
- Calidad de servicio: existe un nivel de servicio comprometido (SLA) que debe ser alcanzado.

Mecanismo

Un mecanismo de seguridad es una entidad o un procedimiento que hace cumplir una parte de la política de la seguridad.

Por ejemplo:

- Control de acceso (asignar permisos a los recursos)
- No permitir que las personas inserten CDs o dispositivos USB de almacenamiento en una computadora para controlar lo que ingresa a los sistemas.

Tipos de políticas

- Política de confidencialidad

  Desarrollada principalmente para proteger la confidencialidad.

- Política de integridad

  Desarrollada principalmente para proteger la integridad.

- Política híbrida

Políticas de Confidencialidad: Modelo Bell-Lapadula

Política de confidencialidad

Objetivo: Prevenir el acceso no autorizado a la información. Las modificaciones no autorizadas son secundarias.

Controla el Flujo de información.

Los modelos de seguridad multinivel son los ejemplos más comunes.

El Modelo Bell-Lapadula (década del 70) es la base para la mayoría de estos modelos.

Modelo Bell-Lapadula

- Combina acceso Mandatorio y acceso Discrecional

- Niveles de clasificación de seguridad ordenados
  - Alto Secreto: Nivel más alto
  - Secreta:
  - Confidencial
  - No clasificada: nivel más bajo

- Los sujetos tienen habilitaciones de seguridad *L(s)*
- Los objetos tienen clasificaciones de seguridad *L*(*o*)

Cuando nos referimos a ambos, hablamos de clasificaciones.

Ejemplo

Clasificación de Seguridad	***sujeto***	***objeto***
Alto Secreto	Tamara	Legajos de Personal
Secreto	Samuel	Archivos correo Electrónico
Confidencial	Claire	Logs de Actividad
No clasificado	Ulaley	Guía Telefónica

- Tamara puede leer todos los archivos.
- Claire no puede leer los legajos de personal o los archivos de correo electrónico.
- Ulaley solo puede leer la guía telefónica.

Bell-Lapadula

- Ante un requerimiento, el sistema lo admite o rechaza considerando la habilitación del sujeto que lo solicita y la clasificación de seguridad del objeto solicitado.

- Para esto se aplican dos principios:
  - Read down
  - Write up

Acceso de lectura la información

Condición simple de Seguridad, versión preliminar

- El sujeto *s* puede leer el objeto *o* sii $L(o) \leq L(s)$ y *s* tiene permiso para leer el objeto *o*
  - Nota: el modelo combina control de acceso mandatorio (relaciones entre niveles de seguridad) y control discrecional (el permiso requerido)
- Conocida como la Regla de “Read Down”

Escritura de Información

Propiedad *, versión preliminar

- El sujeto *s* puede escribir el objeto *o* sii $L(s) \leq L(o)$ y *s* tiene permiso de escritura para *o*
  - Nota: el modelo combina control de acceso mandatorio (relaciones entre niveles de seguridad) y control discrecional (el permiso requerido)

- Conocida como la Regla de “Write up”

Modelo Bell-Lapadula, extendido

- Se expande el concepto agregando categorías.
- Las categorías representan distintas áreas de información dentro de un mismo nivel, y no responden a un esquema jerárquico.
- El nivel de seguridad es (*habilitación*, *conjunto de categorías*)
- Ejemplos
  - (Alto Secreto, { NATO, MERCOSUR, NOFORN })
  - (Confidencial, { MERCOSUR, NOFORN })
  - (Secreto, { NATO, NOFORN })

Niveles y dominancia

- Dominancia: (A, C) *dom* (A', C') sii $A' \leq A$ y $C' \subseteq C$
- Ejemplos:
  - (Alto Secreto, {NATO, NOFORN}) *dom* (Secreto, {NATO})
  - (Secreto, {NATO, Mercosur}) *dom* (Confidencial, {NATO, Mercosur})
  - (Alto Secreto, {NATO}) ¬*dom* (Confidencial, {Mercosur})

Bell-Lapadula

Condición simple de Seguridad, versión Extendida

- El sujeto *s* puede leer el objeto *o* sii *L*(*s*) *dom L*(*o*) y *s* tiene permiso para leer *o*
  - Nota: el modelo combina control de acceso mandatorio (relaciones entre niveles de seguridad) y control discrecional (el permiso requerido)

- Conocida como la Regla de “Read Down”

Bell-Lapadula

Propiedad *, versión extendida

- El sujeto *s* puede escribir el objeto *o* sii *L*(*o*) *dom L*(*s*) y *s* tiene permiso para escribir *o*
  - Nota: el modelo combina control de acceso mandatorio (relaciones entre niveles de seguridad) y control discrecional (el permiso requerido)
- Conocida como la Regla de “Write up”

Covert channel

- Un covert channel o canal secreto es un mecanismo de comunicación que no fue diseñado para ser utilizado con ese fin.

- Ej: Problema del directorio y solución en DG/UX B2.

Política de integridad

Objetivo: Preservar los datos y su integridad.

Para establecer una política de integridad hay que identificar las maneras autorizadas en las cuales la información puede ser alterada y cuales son las entidades autorizadas para alterarla.

Modelos Biba y Clark-Wilson

Principios de operación

- **Separación de tareas**

  Ejemplo: pasar un sistema del entorno de desarrollo al entorno de producción.

- **Separación de funciones**

  Ejemplo: los sistemas se programan y prueban en el entorno de desarrollo no en el de producción.

- **Auditabilidad**

  Ejemplo: el proceso de pasar un sistema a producción debe ser auditado, los auditores deben tener acceso al estado del sistema y a los logs.

Modelo BIBA

Niveles de integridad: Cuanto más alto el nivel de integridad, más confianza en que:

- Un programa ejecutara correctamente
- La información es correcta y/o confiable.

Read up:

Un sujeto S puede leer un objeto *o* sii $i(s) \leq i(o)$

Write down:

Un sujeto *S* puede escribir un objeto o sii $i(o) \leq i(s)$

Transacciones

- Algunas políticas de integridad (Clark-Wilson) utilizan la noción de transacción.
  - Comenzar en un estado inicial consistente
  - Realizar una serie de acciones (*transacción*)
    - Las acciones no pueden ser interrumpidas.
    - Si se completan el sistema está en un estado consistente.
    - Si no se completan el sistema vuelve al estado inicial.

El rol de la confianza

- Las políticas de integridad tratan el tema de la confianza

- El modelo Biba se basa en integridad multinivel
- El modelo Clark-Wilson hace foco en las transacciones y la separación de tareas.

El rol de la confianza

Supongamos que ha aparecido una vulnerabilidad en el sistema operativo que usamos en nuestra PC.

- Obtenemos el parche de seguridad correspondiente.
- Lo instalamos.
- Elevamos el nivel de seguridad de nuestra PC.
- Confiamos en que ya no es vulnerable.

El rol de la confianza

Pero además implícitamente confiamos en:

- Que el parche viene del vendedor del sistema operativo y que no fue modificado.
- Que el vendedor probó correctamente el parche antes de liberarlo.
- Que el ambiente de prueba del vendedor se corresponde con nuestro ambiente.
- Que el parche se instaló correctamente.

El rol de la confianza

- Cualquier política, mecanismo, o procedimiento de seguridad está basado en asumir hechos que, de ser incorrectos, destruyen todo lo construido.

- Hay que tener esto en mente, porque si no entendemos en que se basa la política, el mecanismo, o el procedimiento de seguridad, se pueden asumir cosas inválidas y llegar a conclusiones erróneas.

Políticas Híbridas:
Pared China (CW)

Pared - China

Problema:

- Armando es un analista de mercado que asesora al Banco Mayo en temas de planes corporativos de negocios.
- Se le solicita que también aconseje al Banco Junio en los mismos temas.
- Se produce un **Conflicto de interés**, porque al tener información interna de uno de ellos, como ser planes, estado financiero, etc, puede obtener ventajas en la forma en la que asesora al otro.

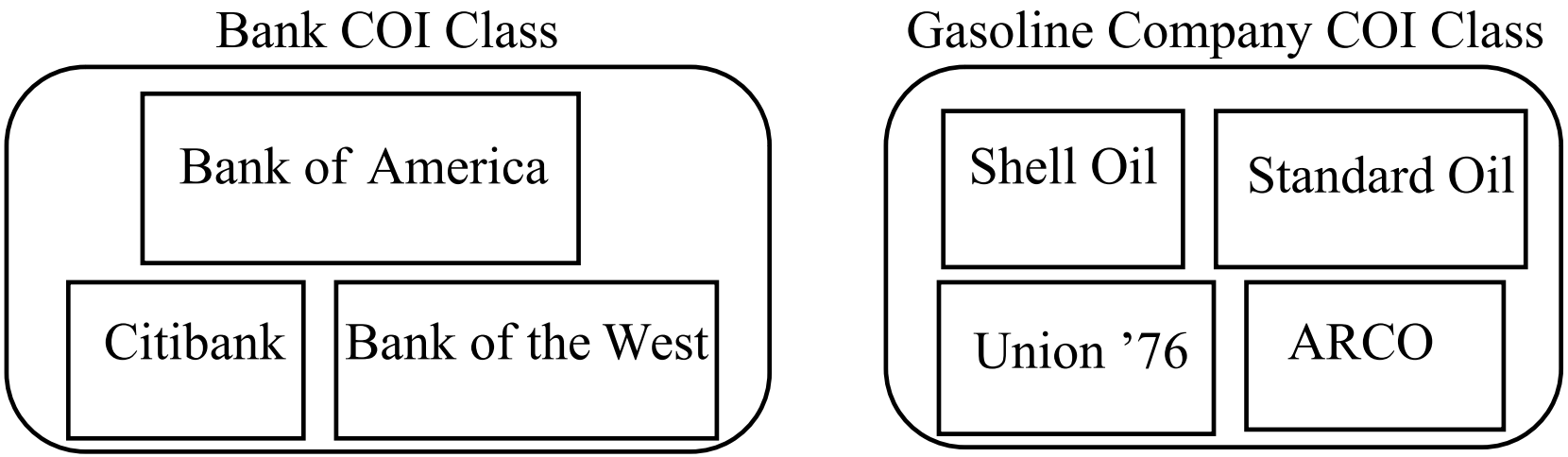
Pared - China

- Organiza entidades en clases de “conflicto de interés”
- Controla el acceso de los sujetos a cada clase.
- Controla la escritura a todas las clases para asegurarse que la información no es pasada de una a otra violando las reglas.
- Permite que todos vean la información “esterilizada” (por ejemplo, los balances, que son públicos)

Pared - China

- *Objetos*: Elementos de información relacionados con una compañía.
- *Company dataset* (CD): Contiene objetos relacionados con una compañía
  - Se escribe *CD*(*O*)
- *Clase de Conflicto de Interés* (COI): contiene datasets de compañías que compiten entre si.
  - Se escribe *COI*(*O*)
  - Se asume que cada objeto pertenece a una sola clase de *COI*.

Ejemplo


Bank COI Class
Bank of America
Citibank
Bank of the West
Gasoline Company COI Class
Shell Oil
Standard Oil
Union ’76
ARCO

Elemento Temporal

- Si Armando lee cualquier CD en un COI, no podrá NUNCA leer otro CD en ese COI.
  - Es posible que la información que obtuvo anteriormente le sirva para decisiones posteriores.
  - sea *PR*(*S*) el conjunto de objetos que *S* ya leyó

Condición de seguridad simple

- *s* puede leer *o* sii alguna de estas condiciones se cumple:
  1. Existe un objeto *o´* tal que *s* ha leído *o´* y *CD*(*o´*) = *CD*(*o*)
     - Es decir, s leyó previamente algún dato en el dataset de la compañía.
  2. Para todo *o´* ∈ *O*, *o´* ∈ *PR*(*s*) ⇒ *COI*(*o´*) ≠ *COI*(*o*)
     1. Es decir, s no leyó ningún objeto de algún CD(o) en la misma COI.

1. Ignora datos esterilizados (ver más adelante)
2. Inicialmente, *PR(s)* = ⊘, por eso la petición de lectura inicial es concedida.

Esterilización

- La información Publica puede pertenecer a un CD
  - Como está disponible públicamente, no surge ningún conflicto de intereses.
  - Por eso, no debería ser restringido el acceso de ningún analista.
  - Típicamente, toda la información sensible de esa información es removida antes de hacerla pública (esterilización o sanitizing).
- Se agrega una tercer condición a la CW-condición de Seguridad Simple:

  3. o es un objeto esterilizado

Escritura

- Armando y Nancy trabajan en la misma agencia financiera.
- Armando puede leer el CD del Banco 1, y el CD de la compañía de Gas.
- Nancy puede leer el CD del Banco 2, y el CD de la compañía de Gas.
- Si Armando pudiera escribir al CD de GAS, Nancy podría Leerlo.
  - Indirectamente, Nancy podría leer información sobre el Banco 1, un claro conflicto de intereses.

Propiedad *

- *s* puede escribir en *o* sii se cumples ambas premisas:
  - La CW-condición simple de seguridad permite a *s* leer *o*; y
  - Para todo objeto no esterilizado *o´*, si *s* puede leer *o´*, entonces *CD*(*o´*) = *CD*(*o*)
- En otras palabras, s puede escribir un objeto si todos los objetos (no esterilizados) que puede leer están en el mismo dataset.

ORCON (Originator controlled)

- **Problema:** Se quiere controlar la diseminación de los documentos generados en la organización.

- **Ejemplo:** El secretario de defensa escribe un memo para distribuir a sus subordinados directos, y estos no deben distribuirlo sin su autorización. Este es un ejemplo de control del “originador”.

DRM

- **Digital Rights Management**

- Control de acceso usado por editoriales y titulares de derechos de autor para limitar el uso de medios o dispositivos digitales a personas o equipos no autorizados.

Políticas de seguridad
Sistemas de información clínica

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

- **Para uso con registros médicos**
  - El problema crítico es la confidencialidad del paciente, la autenticidad e integridad de los registros.
- **Entidades:**
  - Pacientes
  - Información personal de salud: incluye información sobre la salud del paciente y sus tratamientos, que pueden ser usados para identificar al paciente.
  - Médico, puede acceder a la información personal de salud mientras trabaja.

Acceso

- **Principio 1:** Cada registro médico tiene una lista de control de acceso que incluye los individuos o grupos que pueden leer y agregar información al registro. El sistema debe controlar que sólo aquellos en la lista pueden acceder al registro.
- **Principio 2:** Uno de los médicos en la ACL, denominado médico responsable, debe tener permisos para agregar a otros médicos a la ACL.
- **Principio 3:** El médico responsable debe notificar al paciente los nombres en la ACL cada vez que abre su registro médico. Salvo casos explícitos en estatutos, o en casos de emergencia, el médico responsable debe obtener el consentimiento del paciente.
- **Principio 4:** El nombre del médico, la fecha y hora de acceso a un registro médico debe ser registrado. También el borrado de información.

Otros principios

- Definen la forma en que se crean registros, cuando se puede borrar los mismos, como se agrega información de un registro médico a otro, como se fuerza el cumplimiento de estos principios, etc.

Ref: https://www.hhs.gov/hipaa/index.html

Ejemplo Implementación MAC

SELinux y Windows Integrity Control

SELinux

Security Enhanced Linux (SELinux) es una extensión al Kernel de Linux que fue diseñada para forzar políticas de control de acceso estrictas (MAC).

Difundido por la NSA en el 2000, y creado con el aporte de, o mecanismo deentre otros, NAI Labs, Secure Computing Corporation y MITRE Corporation. El código es liberado a la comunidad Open Source.

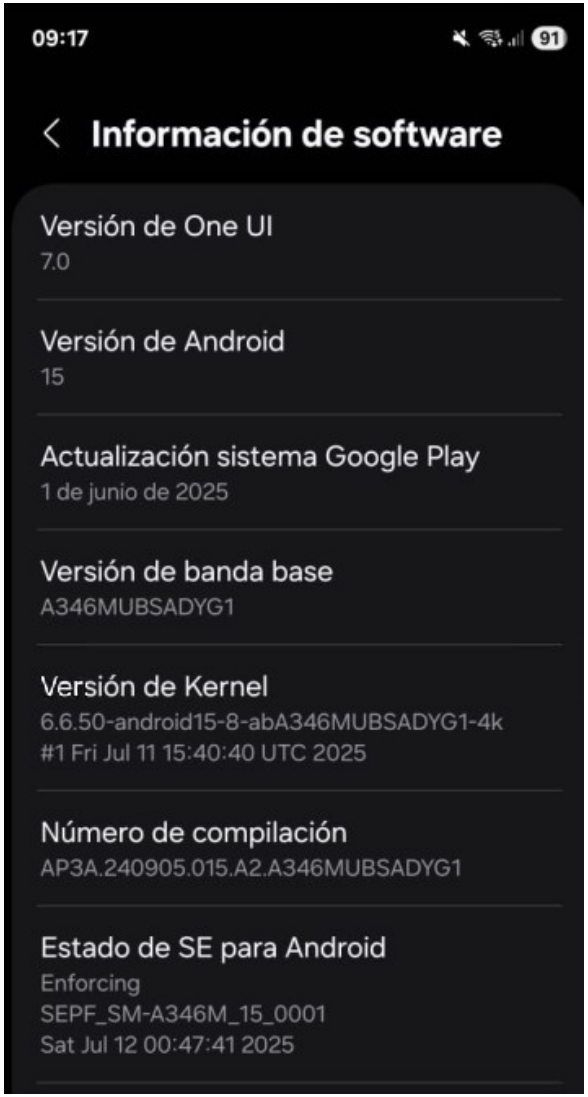
Integrado al Kernel 2.6 de Linux.

Muy utilizado en distribuciones basadas en RedHat Linux y en todos los dispositivos con android.

Otras distribuciones pueden usar SELinux, pero por defecto usan otra implementación de MAC: AppArmor

Ref: https://source.android.com/docs/security/features/selinux

SELinux


09:17
91
Información de software
Versión de One UI
7.0
Versión de Android
15
Actualización sistema Google Play
1 de junio de 2025
Versión de banda base
A346MUBSADYG1
Versión de Kernel
6.6.50-android15-8-abA346MUBSADYG1-4k
#1 Fri Jul 11 15:40:40 UTC 2025
Número de compilación
AP3A.240905.015.A2.A346MUBSADYG1
Estado de SE para Android
Enforcing
SEPF_SM-A346M_15_0001
Sat Jul 12 00:47:41 2025

Windows Mandatory Integrity Control

Implementado a partir de windows vista (2007).

Se basa en el modelo Biba de control de Integridad.

Define cuatro niveles de integridad

Archivos, carpetas, usuarios, procesos, todos tienen niveles de integridad.

El nivel medio es el nivel por defecto para usuarios estándar y objetos sin etiquetas.

El usuario no puede darle a un objeto un nivel de integridad más alto que el suyo.

Windows Mandatory Integrity Control

Nivel	**Uso**
Low	Used by Protected Mode Internet Explorer; blocks write access to most objects (such as files and registry keys) on the system.
Medium	Used by normal applications being launched while UAC is enabled.
High	Used by administrative applications launched through elevation when UAC is enabled, or normal applications if UAC is disabled and the user is an administrator
System	Used by services and other system-level applications (such as Wininit, Winlogon, Smss, etc.)

Ref: https://learn.microsoft.com/en-us/windows/win32/secauthz/mandatory-integrity-control