Sistemas Operativos

Seguridad en Sistemas Operativos: Introducción

Curso 2024

Facultad de Ingeniería, UDELAR

Agenda

- Seguridad: conceptos básicos
- Motivación
- Mecanismos de seguridad en S.O.

Seguridad: conceptos básicos

Definiciones

Seguridad

- La **seguridad** trata sobre la protección de **activos**
- Debemos conocer cuáles son los activos y su **valor** para la organización
- Las medidas de protección se clasifican en:
  - Prevención
  - Detección
  - Reacción

Seguridad de la información

- Cuando el activo a proteger es "información",
- vamos a querer protegerla de ataques a la:
  - confidencialidad
  - integridad
  - disponibilidad

Seguridad Computacional

- *"Mecanismos y controles que permitan preservar la confidencialidad, integridad y disponibilidad de los activos de los sistemas de información; incluyendo hardware, software, firmware, y la información procesada, almacenada y comunicada"* (NIST.IR.7298r2, Mayo 2013)
- *"Mecanismos necesarios para proveer protección y seguridad de un sistema computacional."*
- *"Computer security deals with the prevention and detection of* **unauthorized actions** *by users of a* **computer system**."
- *"Computer security is concerned with the measures we can take to deal with intentional actions by parties behaving in some unwelcome fashion."*

Confidencialidad, Integridad y Disponibilidad

- **Confidencialidad**, este término cubre dos conceptos relacionados:
  - **Confidencialidad de los datos**: prevención que la información privada o confidencial no se revele a personas no autorizadas
  - **Privacidad**: asegurar que los individuos controlen o influyan en qué información relacionada con ellos se puede recopilar y almacenar por quién y a quién se puede divulgar esa información

Confidencialidad, Integridad y Disponibilidad

- **Integridad**, este término cubre dos conceptos relacionados:
  - **Integridad de los datos**: garantiza que la información y los programas se modifiquen únicamente en una forma especificada y autorizada.
  - **Integridad del sistema**: asegura que un sistema realiza su función prevista sin impedimentos, libre de manipulación no autorizada deliberada o inadvertida del sistema.
- **Disponibilidad**: prevención de apropiación no autorizada de información o recursos

Terminología

- **Política de seguridad**: Un conjunto de reglas y prácticas que especifican o regulan cómo un sistema u organización proporciona servicios de seguridad para proteger los recursos sensibles y críticos (activos) del sistema.
- **Activo**: Datos contenidos en un sistema de información; o un servicio proporcionado por un sistema; o una capacidad del sistema, como potencia de procesamiento o ancho de banda de comunicación; o un elemento del equipo del sistema (es decir, un componente del sistema: hardware, firmware, software o documentación); o una instalación que alberga operaciones y equipos del sistema.

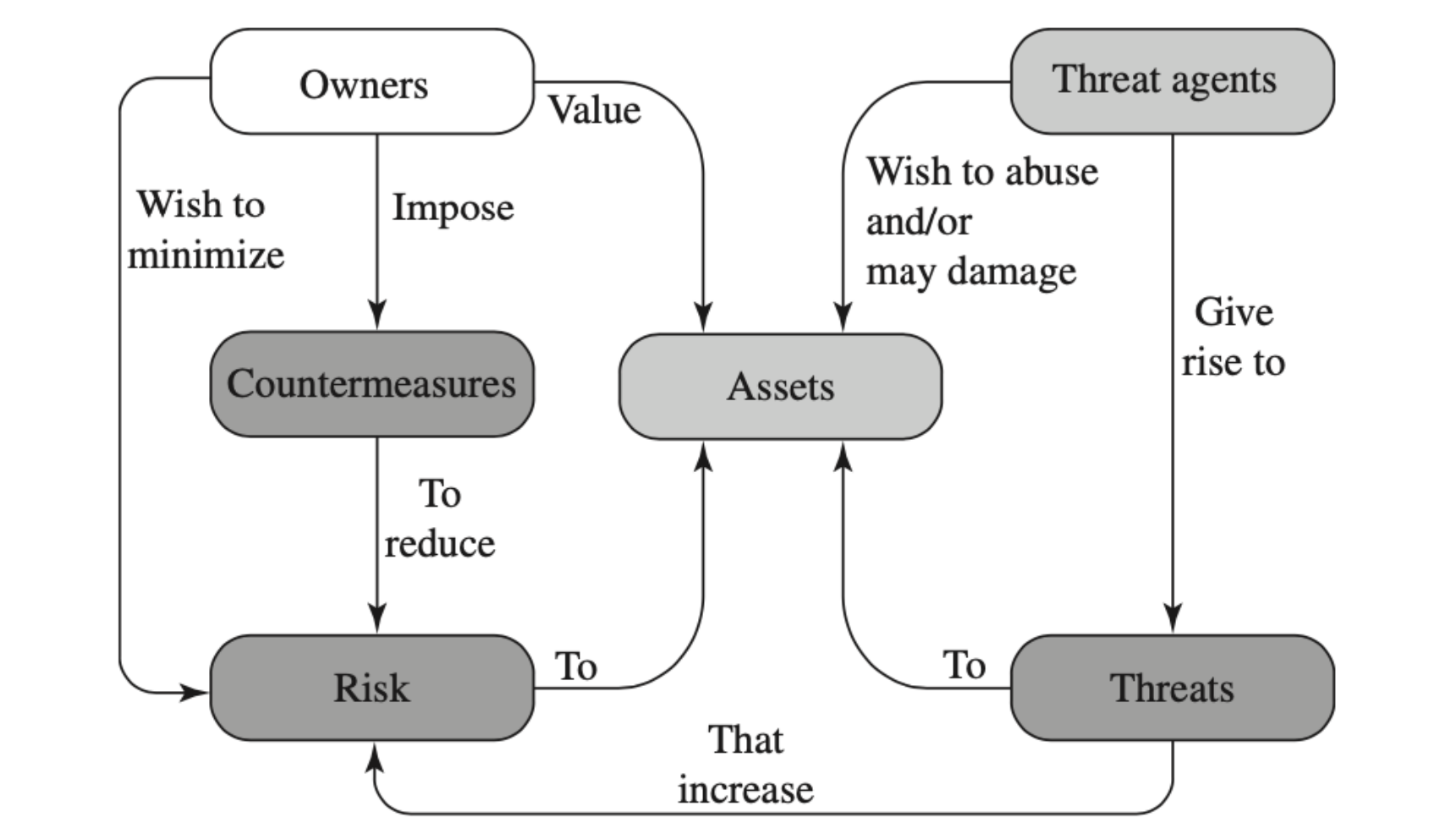
Terminología

- **Amenaza**: Un potencial de violación de la seguridad, que existe cuando hay una circunstancia, capacidad, acción o evento que podría violar la seguridad y causar daño. Es decir, una amenaza es un posible peligro que podría explotar una vulnerabilidad.
- **Vulnerabilidad**: Una falla o debilidad en el diseño, implementación u operación y administración de un sistema que podría explotarse para violar la política de seguridad del sistema.
- **Adversario** Una entidad que ataca o es una amenaza para un sistema.

Terminología

- **Ataque**: Una violación a la seguridad del sistema que se deriva de una amenaza inteligente; es decir, un acto inteligente que es un intento deliberado (especialmente en el sentido de un método o técnica) para evadir los servicios de seguridad y violar la política de seguridad de un sistema.
- **Contramedida**: Una acción, dispositivo, procedimiento o técnica que reduce una amenaza, una vulnerabilidad o un ataque eliminando o previniéndola, minimizando el daño que puede causar, o descubriéndola y reportándola para que se puedan tomar acciones correctivas.

Conceptos y sus relaciones



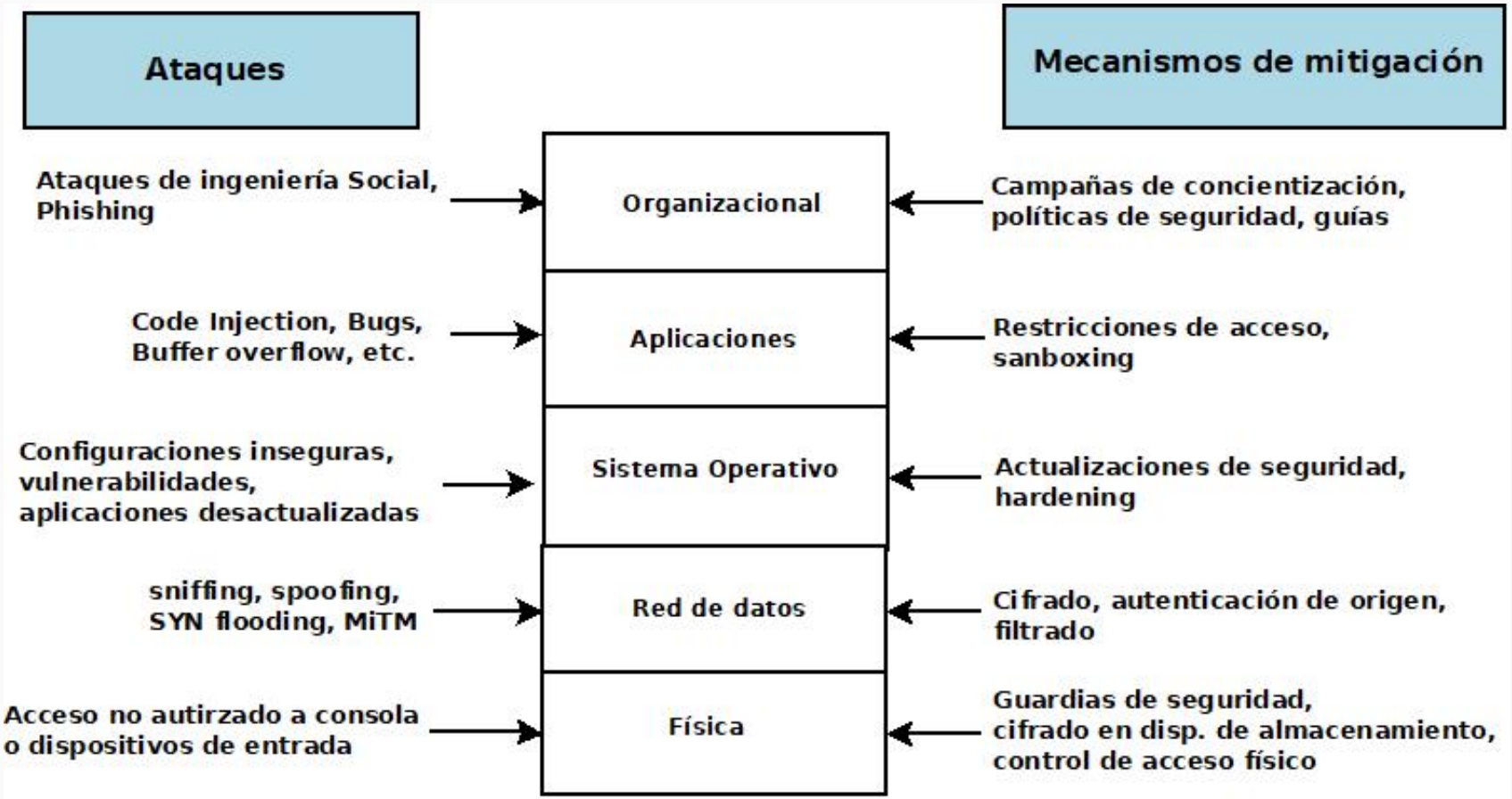
Principios de Seguridad

Lineamientos o principios metodológicos que sirven de guía para implementar controles de seguridad

- Asegurar el eslabón (punto) más débil
- Defensa en profundidad
- Principio de menor privilegio
- Reducir la superficie de ataque
- Compartimentar (sandboxing)
- Asegurar los valores por defecto
- Fallar en forma segura
- Security Through Obscurity

Principios de Seguridad

Debemos aplicarlo con una visión integral



Motivación

¿Por qué es necesario?

Intermediario entre el hardware y los usuarios del sistema, encargado de:

- asignación eficiente de recursos entre los procesos y usuarios del sistema
- **proteger** el sistema de programas (y usuarios) maliciosos
- **mantener y proteger** espacios de usuarios disjuntos
- **permitir** a los usuarios el **acceso** a datos, programas y otros **recursos**
- ejecutar programas de usuarios
- optimizar la eficiencia total del sistema
- gestionar dispositivos de entrada y salida

Desde que el sistema se inicia hasta que es apagado

¿Por qué es necesario?

Recursos:

- CPU (Gestor de procesos)
- Memoria virtual o de swap (Gestor de memoria)
- Almacenamiento secundario en disco (File System)
- Terminales, impresoras, dispositivos de I/O
- Acceso a la red, ancho de banda (Networking)

Todos ellos pueden ser mal utilizados o dañados intencionalmente o no.

Mecanismos de seguridad en S.O.

¿Qué podemos hacer a nivel de los S.O.?

Controlar:

- qué personas (usuarios) pueden utilizar el sistema
- qué programas un usuario puede ejecutar (procesos)
- los recursos que los procesos pueden acceder

Proteger:

- procesos entre si, que comparten recursos del sistema
- integridad del sistema operativo (todo?)

Auditar

- La actividad de los usuarios (procesos), así como
- cumplimiento (validez) de los controles

Mecanismos de seguridad

¿Qué mecanismos ofrecen?

- Procesos
- Modos de ejecución (Kernel vs User Mode)
- Sistema de memoria virtual
- Sistema de gestión de archivos (File Systems)
- Identificación y Autenticación (IA)
- Control de acceso y autorización
- Registrar la actividad (auditoría)
- Virtualización / Sandboxing

Procesos

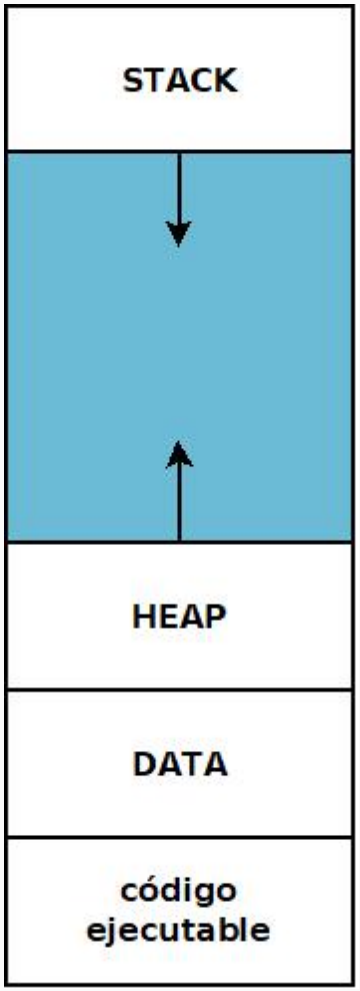
- Son la abstracción central en el sistema operativo
- Es la forma en que que los usuarios interactúan en el sistema
- Son independientes, y no deberían influenciarse directamente unos a otros
- El control de acceso es **organizado en torno a los procesos** = programas en ejecución
- Se identifican con un identificador único de proceso (Process ID o PID)

Procesos

El sistema operativo mantiene la siguiente información:

- Código (del programa) que está ejecutando
- Memoria asignada
- Valor del *program counter*
- Valor de los registros
- Stack de ejecución
- Otros recursos asignados como p.e. archivos abiertos

Proceso en memoria



Código vulnerable

```
#include <stdio.h>
int main(int argc, char **argv)
{
    char buf[8]; // buffer for eight characters
    gets(buf); // read from stdio (sensitive fu
    printf("%s\n", buf); // print out data stor
    return 0; // 0 as return value
}
```

Procesos: problemas de seguridad

Malware:
Programa que es insertado en forma encubierta dentro de otro programa con el objetivo de destruir datos, ejecutar programas destructivos o intrusivos; o que comprometan la confidencialidad, integridad o disponibilidad de los datos, aplicaciones o el propio sistema operativo de la victima. (Def. según NIST SP 800-83r1)

Formas de malware

- Virus
- Worms (gusanos)
- Ransomware

Modos de ejecución: User vs Kernel mode

- La mayoría de los S.O. distinguen diferentes modos de ejecución o niveles de privilegio
  - **Kernel**, supervisor o system mode
  - **User** mode
- El modo kernel ofrece privilegios sobre las funciones del sistema
  - acceso completo a toda la memoria,
  - todas las instrucciones soportadas por el CPU
  - y demás recursos gestionados por el S.O.
- User mode ofrece un ámbito de ejecución para procesos no críticos
- En general estos modos cuentan con soporte de hardware (flags a nivel de registros de ejecución del procesador)

Modos de ejecución: Invocaciones controladas

- Se producen cuando un proceso en modo usuario requiere ejecutar una operación que requiere modo supervisor
- debido al riesgo de estas operaciones, es necesario:
  - que el sistema ejecute solo un conjunto de operaciones predefinidas (limitadas y bien definidas) y una vez finalizada
  - controlar que el proceso vuelva a User Mode antes de devolver el control al usuario

Modos de Invocación: objetivos de seguridad

- El kernel del S.O. ejecuta en modo kernel
- Es importante proteger:
  - integridad de los procesos ejecutando en modo kernel
  - al sistema operativo de malware

Gestor de memoria

Es responsable de:

- asignar memoria a los procesos (in a fair way)
- el manejo de memoria virtual en sus distintas formas:
  - segmentos de largo fijo (paginado),
  - largo variable
  - o swapping

Debe garantizar protección de memoria, esto es:

- Procesos no deberían poder acceder a la memoria de otros procesos o del propio S.O.

Gestor de memoria: problemas de seguridad

- Los mecanismos de protección no previenen que un proceso acceda a la memoria de otro luego que este último la libera
- Usuarios o procesos maliciosos pueden buscar datos sensibles en memoria recién asignada a estos
- el disco duro puede contener páginas de memoria de procesos, incluso después de apagado el computador (*swap*)

Sistema de archivos

- Mecanismo de abstracción sobre dispositivos de almacenamiento **persistente**
- Puede usarse como capa de abstracción de otros dispositivos de I/O (teclado, pantalla, interfaz de red, etc)
- La **persistencia** es una característica
  - buena para implementar disponibilidad
  - mala para implementar confidencialidad
- Capa de abstracción usada como base para el **control de acceso**

  quien tiene los permisos para acceder a **cuales** archivos o directorios

Sistema de archivos: problemas de seguridad

- Los mecanismos de control de acceso y seguridad que provee el S. O. pueden ser anulados retirando el disco duro

Contramedida: cifrar disco duro

- debemos tener cuidado con el manejo de claves
- Criptografía puede resolver algunos problemas de seguridad, pero siempre introduce uno nuevo: el manejo de claves

Sistema de archivos: problemas de seguridad

- El borrado en la mayoría de los File Systems de S.O. no hace un borrado físico!
  - Journaling, registros de transacciones, papeleras de reciclaje
  - Caches, swap o archivos de paginado
  - Datos viejos que quedan en bloques del File System en disco
  - Sectores del disco sin asignar o marcados como dañados o defectuosos
- Necesitamos políticas para el manejo de dispositivos viejos o defectuosos

Control de acceso y Autorización

- Establecer los permisos de acceso ("access rights") es equivalente a especificar:

  Quien puede hacer **que** sobre (**quien** o **que**)

- Hacerlos cumplir (**enforcement**)

  Hacer chequeos antes de cualquier operación

- Auditar

  Registrar y chequear los logs o registros de las acciones

Concepto aplicable no solo a S.O. sino que también a aplicaciones

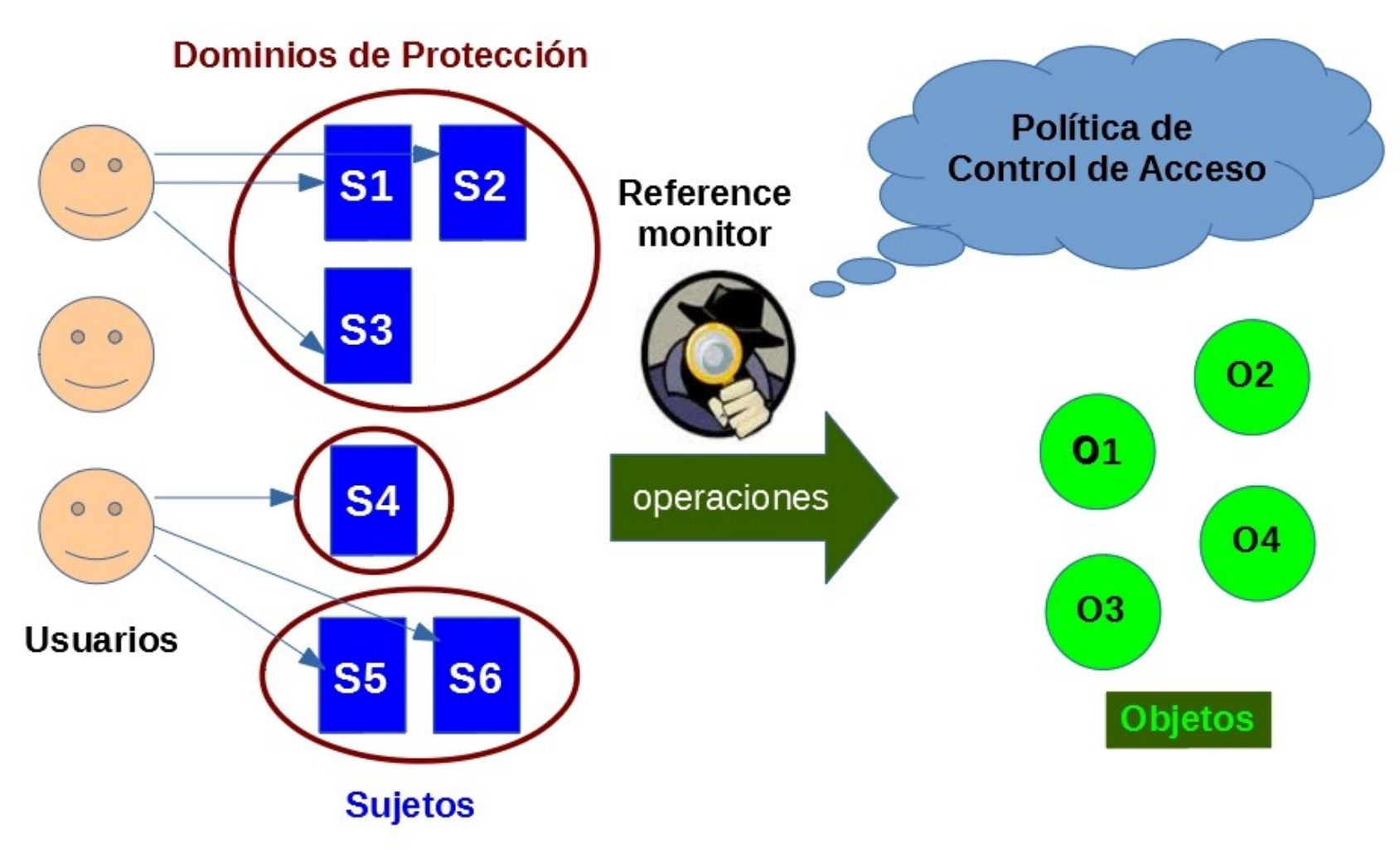
Control de acceso: definiciones

- Seguridad $\equiv$ Regular el acceso a los activos del sistema
- Identificación: forma en que una persona (principal) se identifica ante un sistema (*username*)
- Autenticación: proceso de verificación de la identidad (pretendida) de un usuario (principal) ante un sistema a través de algo que se sabe, se tiene o se es
- Objeto: entidad pasiva que requiere acceso controlado (por ejemplo archivos, impresora, etc.)
- Operaciones de acceso: formas de acceder a los objetos

Control de acceso: definiciones

- Usuarios inician sesiones/sujetos en computadoras que van a acceder a objetos a través de operaciones de acceso
- Sesiones con los mismos permisos son agrupados en dominios de protección
- La política de un sistema nos dice que permisos tiene cada dominio de protección
- Llamamos "reference monitor" a la entidad que hace que se cumpla (*enforce*) la política de seguridad en cada intento de acceso a los objetos

Control de acceso y dominios de protección



Control de acceso: DAC vs MAC

Discretionary Access Control (DAC)
Si un usuario individual puede gestionar el mecanismo de control de acceso para permitir o denegar acceso a un recurso, ese mecanismo constituye un control de acceso discrecional (DAC), también llamado control de acceso basado en identidad (IBAC)

Mandatory Access Control (MAC)
Cuando un mecanismo de un sistema controla accesos a un objeto y un individuo (principal o sujeto) no puede alterar ese acceso, entonces el control de acceso es mandatorio (MAC) (ocasionalmente llamado control de acceso basado en reglas)

Bibliografía

- A.Silberschatz, P.Galvin and G. Gagne, Operating Systems Concepts, 9th edition, Editorial Wiley, 2014. Cap 14 y 15.
- M. Souppay, K. Scarfone, Guide to Malware Incident Prevention and Handling for Desktop and Laptops, NIST Special Publication SP 800-53. Cap. 2
- R. Kissel, Glossary of Key Information Security Terms, NIST Internal Report, 7298 Rev. 2 (NIST.IR 7298r2),2 May 2013.
- W. Stallings, Lawrie Brown; Computer Security Principles and Practice, Third Edition, 2018.