Grupo de Seguridad Informática

Fundamentos de Seguridad Informática

Sistemas Operativos

Plan

- **Motivación**
- **Introducción**
- *Principals (UID / GID)*
- Sujetos (PID)
- Objetos (files)
- Control de acceso
- Políticas de complejidad de claves

Motivación / Introducción

- ¿Que es un Sistema Operativo?
- Principios de Seguridad
- Mecanismo de Seguridad de S.O.
  - Identificación y Autenticación
  - Control de Acceso
  - Sujetos, objetos
  - Autorización
  - Auditoría y Registro de Eventos
  - Sandboxing

Sistema Operativo Definición

Es un intermediario entre el hardware y los usuarios del sistema, encargado de realizar:

- la asignación eficiente de recursos entre los procesos o programas y usuarios del sistema
- proteger el sistema de programas (y usuarios) incorrectos o maliciosos
- mantener y proteger espacios de usuarios disjuntos o separados

Sistema Operativo Definición (cont)

- 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 inicia hasta que es apagado.

Sistemas Operativos

- Recursos controlados y protegidos por el Sistema Operativo
  - CPU (Gestor de procesos)
  - Memoria (Gestor de memoria)
  - Almacenamiento en disco (File System)
  - Terminales, Impresoras
  - Acceso a la red / Ancho de banda (Networking)

Sistemas Operativos

¿Cual es limite entre el sistema operativo y las aplicaciones?

En algunos casos, este limite no esta claro.

Trusted Computing Base (TCB)

- Porción de un sistema o aplicación en el cual tenemos que confiar en su seguridad.
- La TCB debería ser:
  - tan pequeña como sea posible
  - tan confiable como sea posible
- Típicamente el Sistema Operativo (o una gran parte de él) forma parte de la TCB

Principios 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
- KISS (Keep It Simple)
- Mantener secretos es difícil
  (Security Through Obscurity)

Principios de Seguridad

Se pueden aplicar a distintos niveles, por ejemplo:

- a nivel de una sola aplicación
- entre distintas aplicaciones
- Sistema operativo
- Networking
- Organizacional

Problemas de seguridad a nivel de S.O.

- ¿Como controlamos que personas pueden utilizar el sistema?
- ¿Como controlar los procesos que un usuario puede ejecutar?
- ¿Como controlar los recursos que un proceso puede acceder?
- ¿Como proteger entre sí a los procesos que comparten recursos del sistema?

Mecanismos de seguridad ofrecidos por los S.O.

- Capa de abstracción sobre el hardware
  - esconder los detalles de bajo nivel permite prevenir el acceso y el abuso de los mismos
  - pero las capas de abstracción pueden ser evitadas ...
- Procesos
- kernel vs user mode (modos de ejecución)

Mecanismos de seguridad ofrecidos por los S.O.

- Memoria Virtual
- File Systems
- Autenticación
- Control de Acceso y Autorización

Plan de presentación

Como seguimos?

Objetivo: presentar mecanismos los conceptos básicos de control de acceso ofrecidos por los sistemas:

- UNIX like
- MS Window 2000 (en adelante)