GRUPO DE SEGURIDAD INFORMÁTICA

Fundamentos de la Seguridad Informática

Seguridad en Sistemas Windows

Introducción

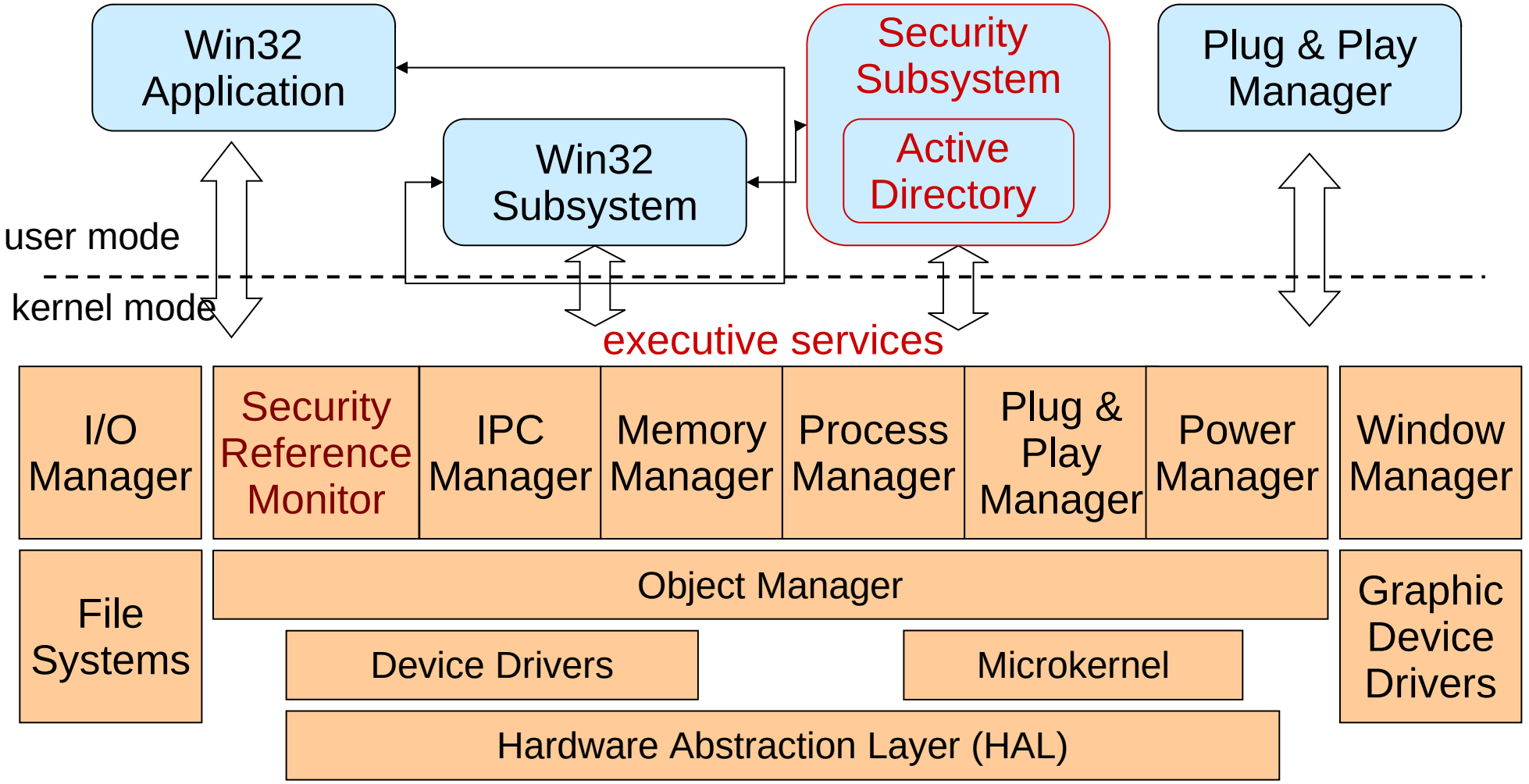
Introducción

- En **Unix**, todos los objetos son tratados uniformemente como recursos
- **Sin embargo en Windows,** el control de acceso puede ser ajustado individualmente a los distintos tipos de objetos

Plan

- Arquitectura de Windows
  - El registro (registry)
  - Dominios
  - Active Directory
- Control de acceso (componentes, algoritmo)
- Contextos restringidos
- Security templates / Group Policy Objects
- Gestión de logs y auditoría

Arquitectura



Arquitectura (2)

- Los usuarios hacen llamadas a API's para invocar los servicios del Sistema Operativo
- El cambio de contexto entre *user* y *kernel* mode es manejado a través de *Local Procedure Call*
- Los componentes del subsistema de seguridad en modo usuario son:
  - El proceso de *Logon* (*winlogon*) => autentica
  - *Local Security Authority* => crea un *access token*
  - *Security Account Manager* => mantiene BD usuarios

Grupo de Seguridad Informática

El registro (registry)

- Es la base central de datos de configuración de Windows
- Para modificar/desplegar el contenido usamos el editor de registro: **regedit.exe** o **regedt32.exe**
- Una entrada o nodo del registro es un grupo de claves, subclaves y valores

El registro (2)

- Claves de más “alto nivel” predefinidas de la registry
  - HKEY_CLASSES_ROOT asociación de extensiones de archivos
  - HKEY_CURRENT_USER configuración del usuario actualmente logueado
  - HKEY_LOCAL_MACHINE configuración de la computadora
  - HKEY_USERS profiles de los usuarios cargados en el sistema
  - HKEY_CURRENT_CONFIG *profile* del hardware del sistema usado por la computadora cuando se inicia

El registro (3)

Entradas relevantes para la seguridad del sistema

- HKEY_LOCAL_MACHINE\SAM
- HKEY_LOCAL_MACHINE\Security
- HKEY_LOCAL_MACHINE\Software
- HKEY_CURRENT_CONFIG
- HKEY_USERS\DEFAULT

El registro (4)

- Modificando el registro, un atacante puede modificar el comportamiento del sistema
- Es necesario proteger la integridad del registro
- Un problema potencial es cuando una clave no está definida explícitamente, p.e.:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ SecurePipeServers\Winreg

  Si **NO** existe la clave, se permite acceder remotamente al registro sin realizar chequeos!!

Dominios

- Definición: Colección de máquinas que comparten la base de cuentas de usuarios y políticas de seguridad
- Pueden formarse jerarquías de dominios
- Existe un *Domain Controller* (DC), luego otras máquinas se unen al dominio
- Pueden haber más de un DC
- Las actualizaciones son propagadas usando el modelo de *multimaster replication*

Active Directory

- Implementación de servicio de directorio en W2K
- Árbol de objetos con tipo
- Los objetos se identifican con GUID (*Global Unique Identifier*)
- Los contenedores son objetos que pueden contener otros objetos

Control de Acceso

- Más complejo que el control de acceso en un filesystem típico
- Los objetos sobre los que se aplica son: archivos, claves del registro, objetos del AD, etc.
- *Mecanismos para estructurar políticas:* ***grupos****,* ***roles*** *y* ***herencia***