Tema 9
Seguridad y protección

Última modificación 31/05/07

E.T.S.I. Telecomunicaciones
José Luis Triviño Rodriguez

Introducción

- **Seguridad**. Hace referencia a los problemas relacionados con el acceso o modificación de la información. Incluye aspectos técnicos, administrativos, legales y políticos
- **Protección.** Conjunto de mecanismos específicos del SO que tienen como finalidad proporcionar seguridad

Seguridad

- Requisitos:
  - **Privacidad:** La información debe ser accesible sólo por entidades autorizadas.
  - **Integridad:** La información sólo debe poder ser modificada por entidades autorizadas.
  - **Disponibilidad:** Los elementos relacionados con la seguridad deben estar disponibles sólo para las partes autorizadas.

Principios de diseño para la seguridad

- Diseño abierto
- Negación en caso de duda
- Verificación completa
- Principio del menor privilegio
- Economía
- Aceptabilidad

Tipos de amenazas

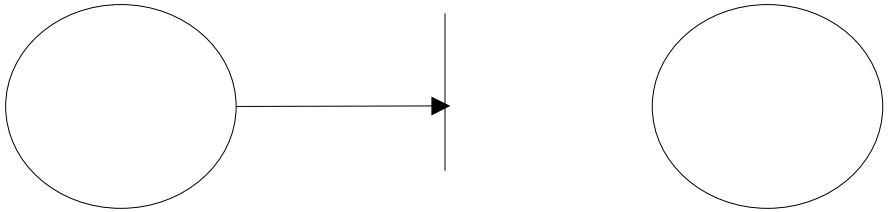
- Si se considera un sistema informático como una fuente de información, es posible considerar los distintos tipos de amenaza en función a como afecten a este flujo de información

Fuente de información

Destino de la información

Tipos de amenazas

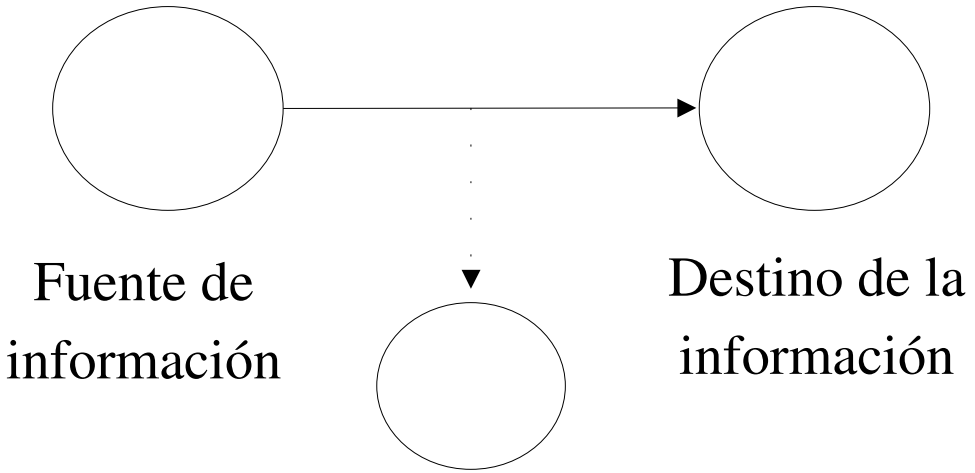
- Interrupción. Ataques de denegación de servicios (DoS)



Última modificación 31/05/07

Tipos de amenazas

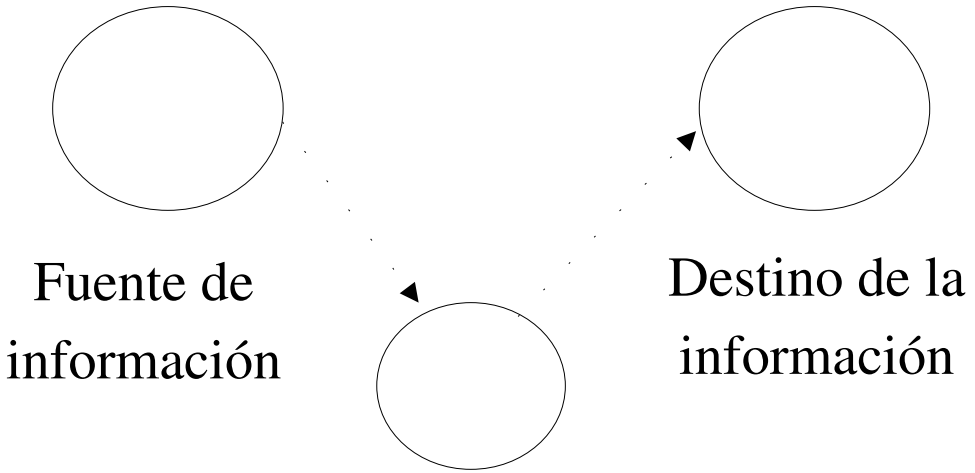
- Intercepción. Amenaza a la privacidad



Última modificación 31/05/07

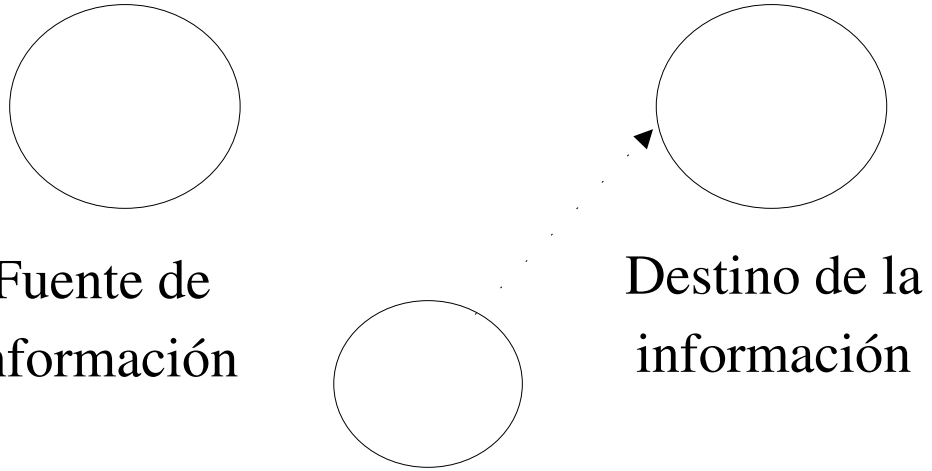
Tipos de amenazas

- Modificación. Amenaza a la integridad



Tipos de amenazas

- Fabricación. Amenaza a la identidad.



Origen de la amenaza

- Fortuitos. Solucionables mediante backups
  - Desastres: icendios, terremotos, etc.
  - Errores hardware o software.
  - Errores humanos
- Intencionados
  - Usuarios no técnicos movidos por la curiosidad
  - Personal cualificado como reto personal
  - Intento de obtener beneficios económicos
  - Espionaje

Ataques genéricos a la seguridad

- Solicitar páginas de memoria o bloques de disco y leer su contenido
- Ejecutar llamadas al sistema ilegales
- Intentar romper un proceso de autentificación
- Intentar modificar las estructuras del SO
- Engañar al usuario con falsos programas
- Soborno

Amenazas de origen software

- No autoreplicantes
  - Caballo de Troya
  - Bomba lógica
  - Puertas traseras
- Autoreplicantes
  - Virus
    - Mochila
    - De sector de arranque
  - Gusanos

Protección

- El papel de la protección en un Sistema Informático es proporcionar un conjunto de mecanismos que permitan llevar a cabo un política de protección de recursos
- Dos aspectos:
- **Sistema de protección**: determina **como** proteger un recurso
- **Política**: determinan **que** recursos hay que proteger

Dominios de protección

- Se utilizan para especificar las políticas de protección de un sistema
- Un *dominio de protección* está formado por un conjunto de pares *objeto-derechos*
- Cada par especifica las operaciones que se pueden realizar sobre un objeto
- Todo proceso se ejecuta siempre dentro de un dominio concreto que puede cambiar a lo largo de su vida

Dominios de protección

- Dependiendo del sistema, un dominio de protección se puede hacer corresponder con diferentes entidades:
- Usuario
- Proceso
- Procedimiento

Matriz de acceso

- El conjunto de todos los dominios en un sistema se representa mediante una *matriz de acceso*
- Una matriz de acceso es una tabla donde cada fila representa un dominio y cada columna un objeto del sistema. En cada celda se almacena las operaciones válidas para un objeto en el dominio correspondiente

Matriz de acceso

- En la práctica no es viable almacenar una matriz de acceso porque es grande y contiene muchos huecos
- Dos alternativas:
  - Lista de control de acceso: almacena la matriz de acceso por columnas. Es el caso de UNIX
  - Lista de capacidades: almacena la matriz de acceso por filas. Es el caso de Windows

Criptografía

- La criptografía es un elemento fundamental de la protección de un sistema para evitar el acceso o la modificación no autorizada de información
- Definiciones:
  - **Cifrado**: proceso de “disfrazar” información para convertirla en ininteligible
  - **Descifrado**: proceso de conversión de información cifrada a información legible

Criptografía

- Definiciones:
  - **Criptografía:** ciencia que estudia como mantener la seguridad de la información
  - **Criptoanálisis:** ciencia que estudia como romper la información cifrada
  - **Criptología:** criptografía + criptoanálisis
  - **Esteganografía:** ciencia que estudia como "esconder" el significado de los mensajes

Conceptos básicos

- Una función de cifrado E opera sobre el mensaje M para producir el texto cifrado (o criptograma) C:

$$E(M) = C$$

- Una función de descifrado D opera sobre C para producir el mensaje M:

$$D(C) = M$$

- El objetivo del cifrado y del posterior descifrado de un mensaje es obtener el texto original:

$$D(E(M)) = M$$

- Algoritmo criptográfico o cifrado: Función utilizada para cifrar y descifrar

Conceptos básicos

- Tanto las operaciones de cifrado como de descifrado pueden utilizar una clave K

$$E_K(M) = C \quad D_K(C) = M \quad D_K(E_K(M)) = M$$

- Dos tipos de algoritmos
  - **Simétricos**: utilizan la misma clave para cifrar y descrifrar
  - **Asimétricos**: utilizan una clave diferente para cifrar y otra para descrifrar

Algoritmos de cifrado clásicos

- Algoritmos de sustitución
  - Monoalfabéticos:
    - Sustitución afín (caso general del Algoritmo del César)

$$E_{(a,b)}(M)= (aM+b) \bmod N$$

  - Polialfabético:
    - Cifrado de Vigenere

$$E_k(m_i)=(m_i+k_{(i \bmod d)}) \bmod n$$

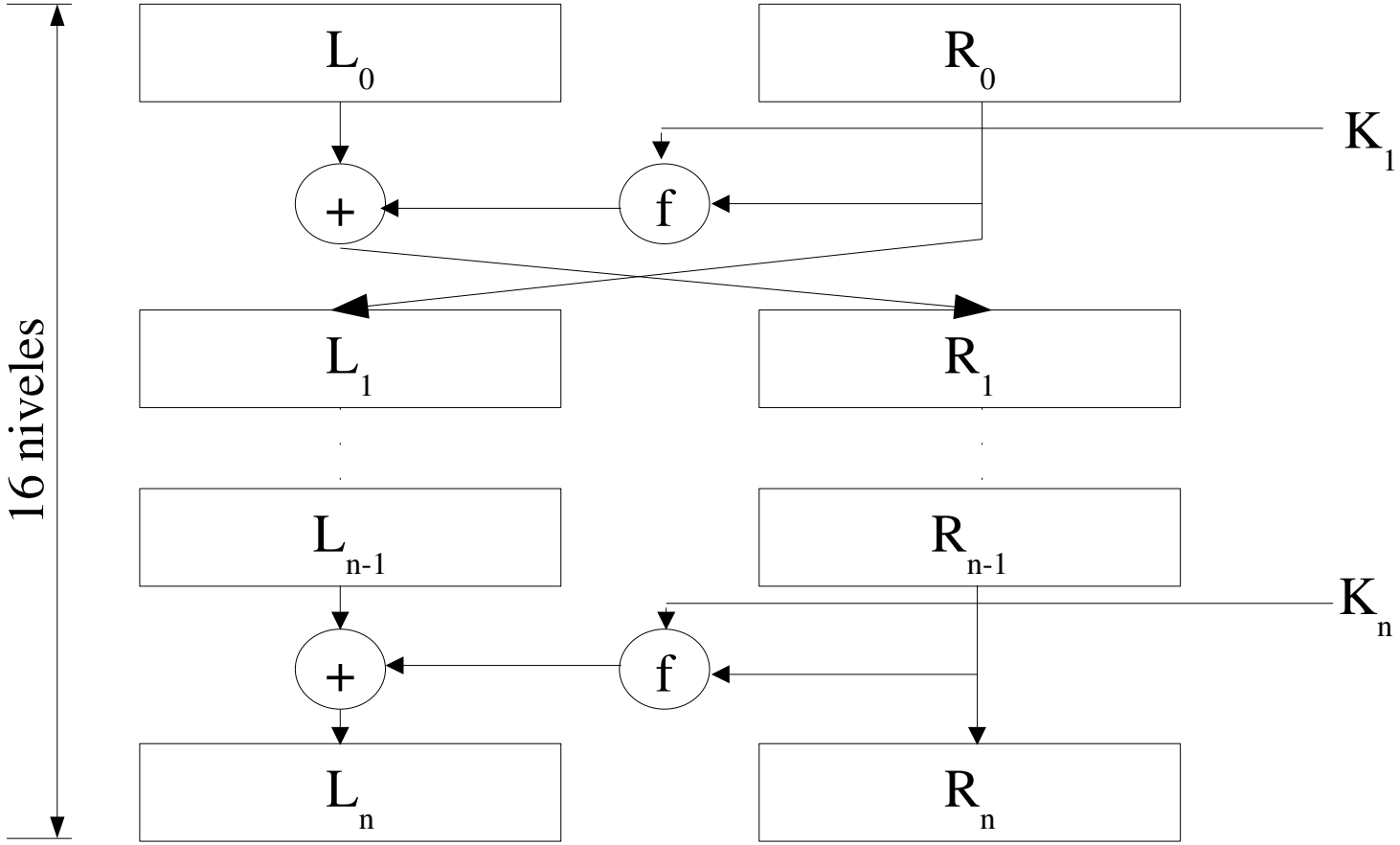
Algoritmos de cifrado clásicos

- Algoritmos de transposición
  - Por tablas. El mensaje se escribe en horizontal en una tabla de n columnas y se lee en vertical
  - Por matrices. Se utiliza una matriz de transposición donde cada celda contiene el elemento del mensaje que se debe colorcar en ese lugar
- Máquinas de rotores (Máquina Enigma)

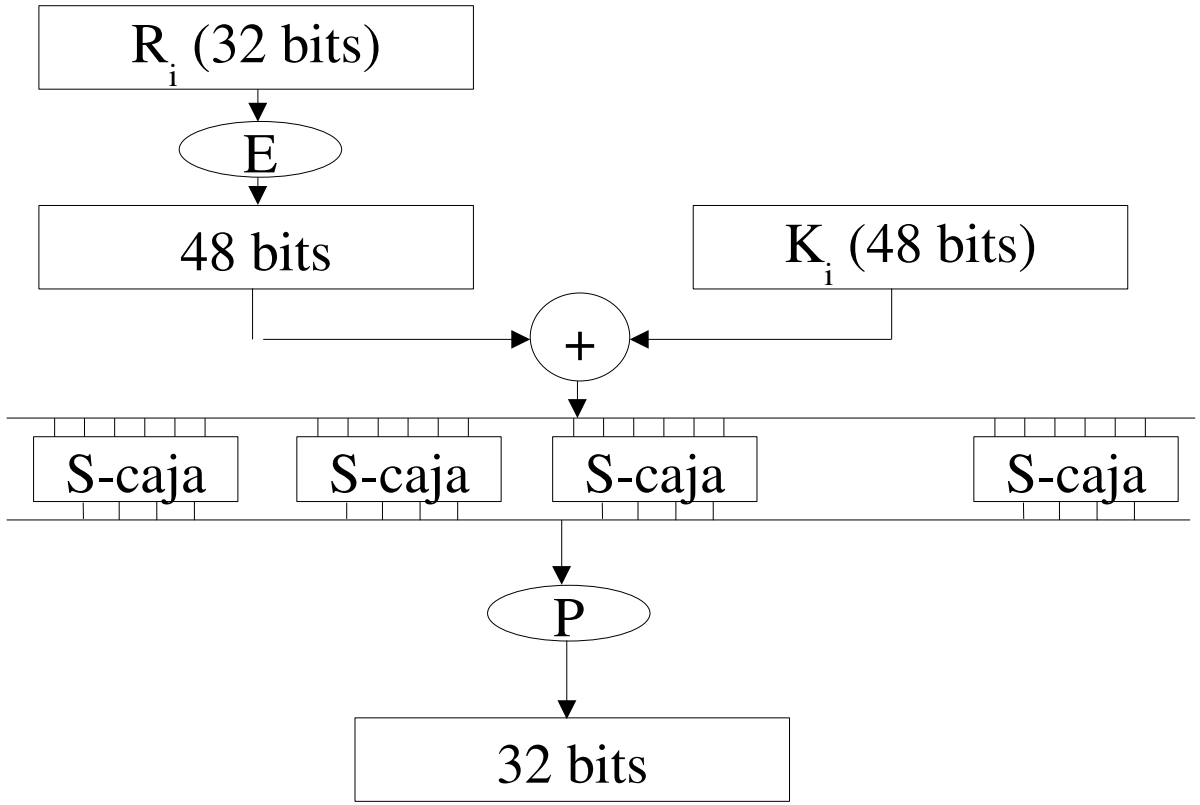
Algoritmos de cifrado simetricos

- Utilizan la misma clave para cifrar y descifrar
- Ejemplos:
  - DES
  - DES triple
  - GDES
  - NEWDES
  - FEAL (Fast Encryption Algorithm)
  - IDEA (International Data Encryption Standard)

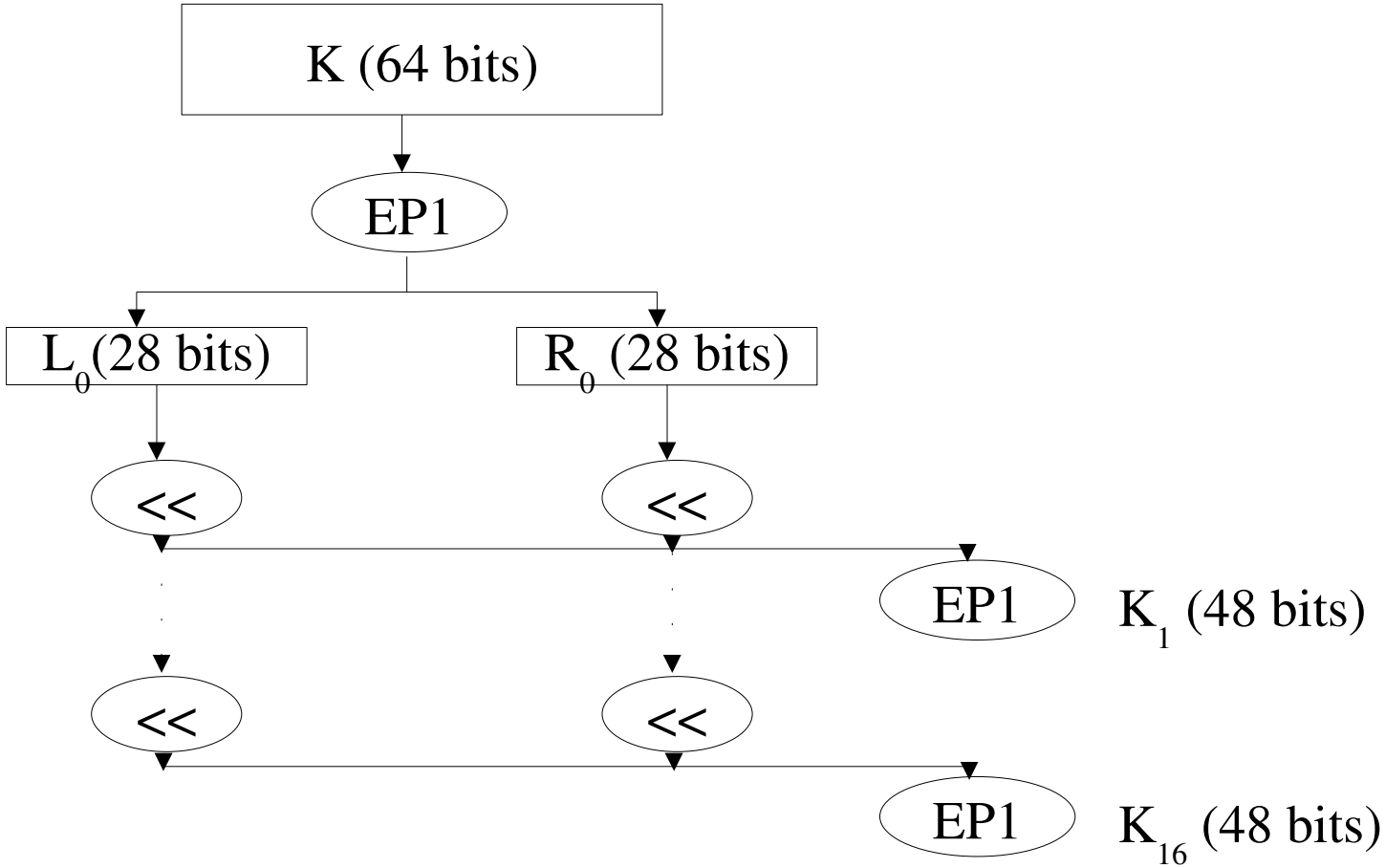
Red de Feistel (DES)



Función f (DES)



Cálculo de K_i (DES)



Algoritmos de cifrado asimétricos

- Utilizan una clave distinta para cifrar y otra para descifrar
- Ejemplos: Algoritmo RSA
- Características:
  - Ninguna de las claves se puede calcular a partir de otra
  - Las claves suelen ser de gran tamaño
  - Son computacionalmente más costosos que los algoritmos simétricos

Algoritmo RSA

- Se basa en la complejidad de factorizar grandes número
- Cálculo de las claves:
  - Escoger 2 números primos grandes *p* y *q*
  - *n = p * q*
  - Escoger número *e* grande y primo relativo con *(p-1)*(q-1)*
  - Calcular *d* como la inversa de *e* módulo *(p-1)*(q-1)*
  - Claves (e,n) y (d,n)

Algoritmo RSA

- Codificar el mensaje m:

$$c = m^e \pmod{n}$$

- Decodificar c:

$$m = c^d \pmod{n}$$

Última modificación 31/05/07

Cálculo de la inversa de e mod n

- Algoritmo extendido de euclides

```
ALGORITMO euclides_ext( n: Z; a: Z ) : Z
  VAR
    c, i: Z
  INICIO
    g[0]= n; u[0]= 1; v[0]= 0
    g[1]= a; u[1]= 0; v[1]= 1

    i= 1
    MIENTRAS (g[i]≠0) HACER
      c= g[i-1]/g[i]
      g[i+1]= g[i-1] MOD g[i]
      u[i+1]= u[i-1]-c*u[i]
      v[i+1]= v[i-1]-c*v[i]
      INC( i )
    FINMIENTRAS

    DEVOLVER (v[i-1] MOD n
  FIN
```

Caso de estudio. Windows XP

- Windows NT utiliza un esquema de protección uniforme para controlar los accesos a recursos: se aplica igual a todos los objetos del sistema
- El control de acceso está basado en dos entidades:
  - Token de acceso asociado a cada proceso
  - Descriptor de seguridad asociado a cada objeto

Estructura del token de acceso

- Identificador de seguridad (Security ID o SID): identifica a un usuario
- Identificadores de grupo (Group SIDs): lista de grupos a los que pertenece el usuario
- Privilegios: lista de servicios del sistema que el usuario puede solicitar
- Propietario por defecto: normalmente, el propietario de un proceso es el del usuario lo crea
- Lista de control de accesos por defecto: indica las protecciones aplicadas inicialmente a los objetos que crea el proceso

Estructura del descriptor de seguridad

- Lista de control de acceso del sistema (System Acces Control List o SACL): Especifica las operaciones sobre el objeto que deberían de generar mensajes de auditoría
- Propietario (puede ser un individuo o un grupo)
- Lista de control de acceso discrecional (Discretionary Access Control List): Indica qué usuarios y grupos pueden acceder al objeto y con qué operaciones. Consiste en una lista de entradas de control de acceso (ACE)
- Indicadores (definen el tipo y contenidos del descriptor de seguridad)

Estructura de la Lista de Control de Acceso

- Cada Lista de Control de Acceso contiene una cabecera y una o varias ACEs
- Cada ACE especifica un SID individual o de grupo y una máscara de acceso que define los derechos permitidos para el SID

Funcionamiento de de las Listas de Control de Acceso

- Cuando un proceso intenta acceder a un objeto, el gestor de objetos de Windows 2000/ XP lee los SID individual y de grupo del token de acceso y realiza una búsqueda en la DACL del objeto

- Si se encuentra una ACE cuyo SID coincida con uno de los del token de acceso, entonces el proceso tiene los derechos de acceso especificados en la máscara de acceso de la ACE