Seguridad y Protección

Sistemas Operativos

2° año Ing. en Sistemas de Información

Universidad Tecnológica Nacional Facultad Regional Villa María

Seguridad y Protección

Seguridad en los Sistemas

- Física
- **Lógica**

Seguridad y Protección

Requisitos básicos que rigen la seguridad

- Confidencialidad
- Integridad
- Disponibilidad
- Autenticación

Seguridad y Protección

Tipos de peligros

- Interrupción: ataque a la disponibilidad
- Intercepción: ataque a la confidencialidad
- Modificación: ataque a la integridad
- Fabricación: ataque a la autenticaicón

Seguridad y Protección

Componentes de un sistema informático

Tabla 16.1. Peligros de seguridad y componentes.

	Disponibilidad	Privacidad	Integridad/Autenticación
Hardware	Equipamiento robado o deshabitado, por lo tanto denegación de servicio.		
Software	Borrado de programas, denegación de acceso a los usuarios.	Copia no autorizada de software.	Modificación de un programa, bien para hacer que falle durante la ejecución o para que realice una tarea diferente.
Datos	Borrar ficheros, denegación de acceso a los usuarios.	Lectura no autorizada de datos. Un análisis estadístico de los datos que revele la información subyacente.	Modificación de los ficheros existentes o creación de nuevos ficheros.
Líneas de comunicación	Borrado o destrucción de mensajes. Las líneas de comunicación o redes no se encuentran disponibles.	Lectura de mensajes. Observación de los patrones de tráfico de mensajes.	Modificación, borrado, reordenación o duplicación de mensajes. Fabricación de mensajes falsos.

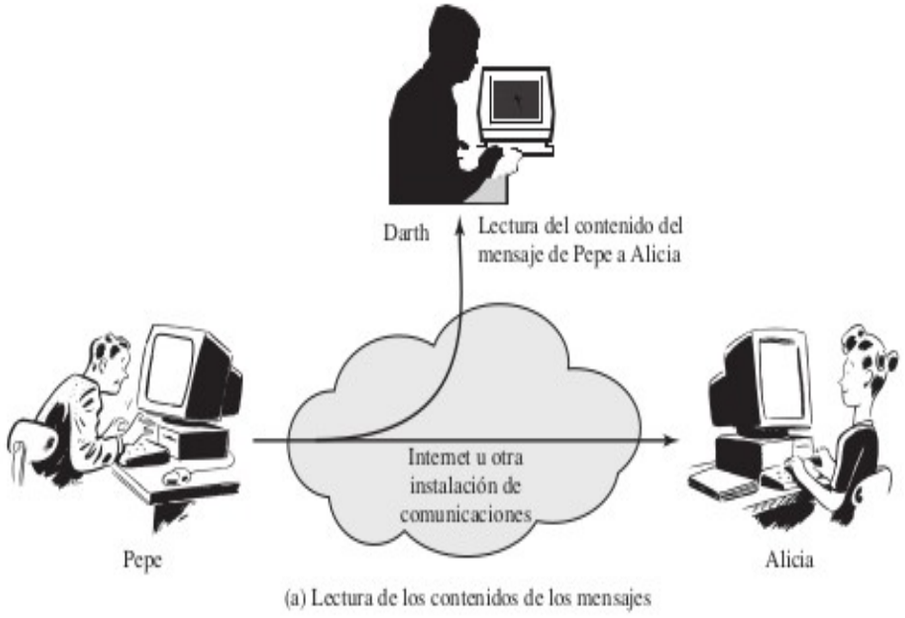
Seguridad y Protección

Tipos de ataques

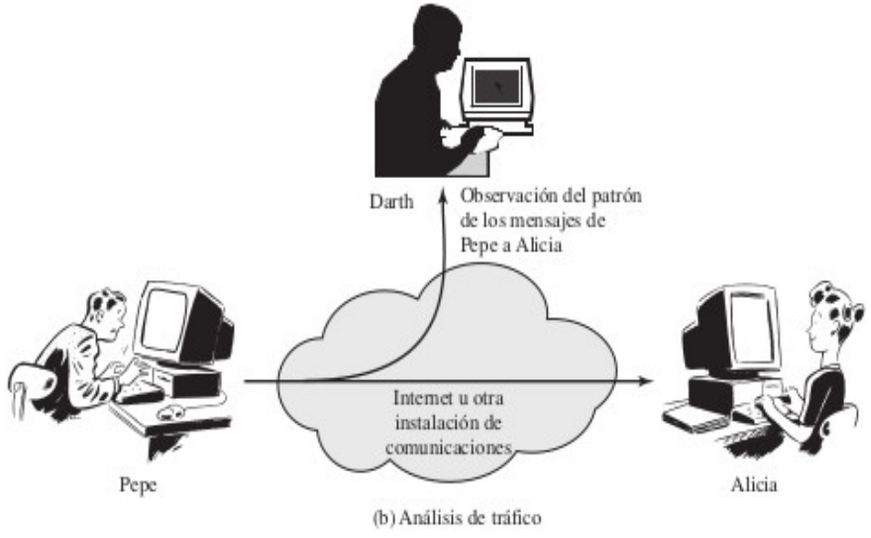
- Ataques pasivos
  - Lectura de contenidos
  - Análisis de tráfico
- Ataques activos
  - Enmascaramiento
  - Reenvío
  - Modificaciones
  - Denegación de servicio

Seguridad y Protección

- Ataques pasivos



(a) Lectura de los contenidos de los mensajes

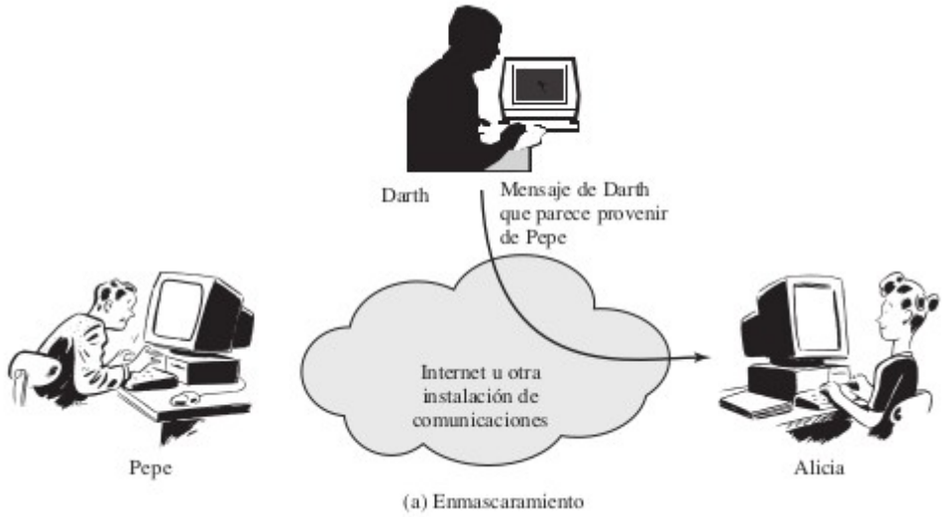


(b) Análisis de tráfico

Figura 16.3. Ataques pasivos.

Seguridad y Protección

- Ataques activos



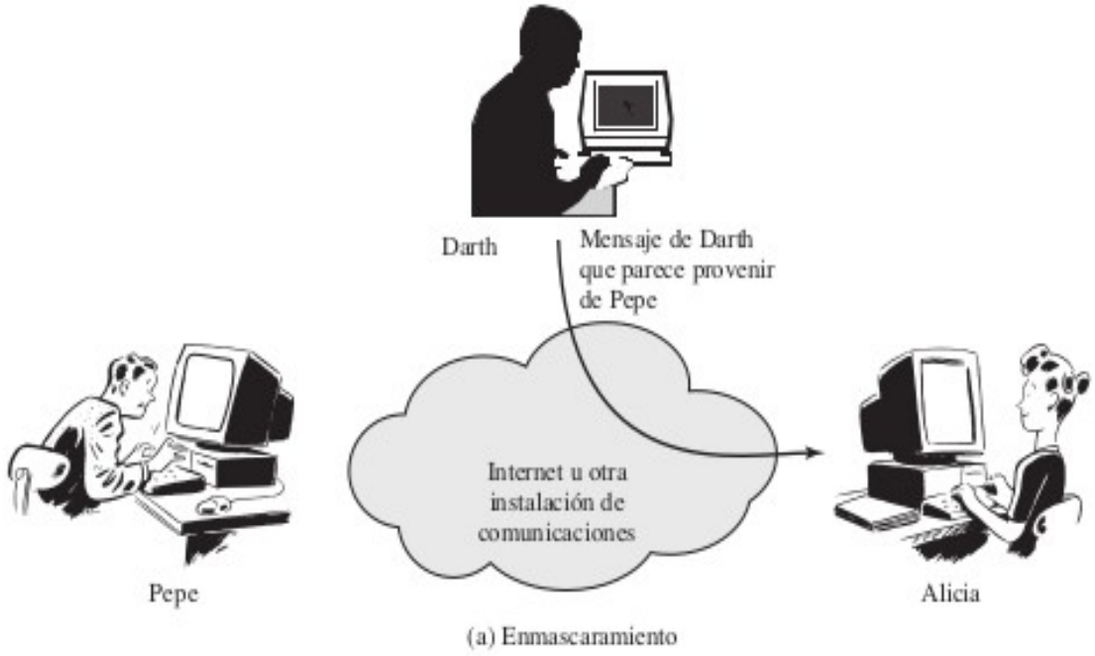
(a) Enmascaramiento

Seguridad y Protección

- Ataques activos

Seguridad y Protección

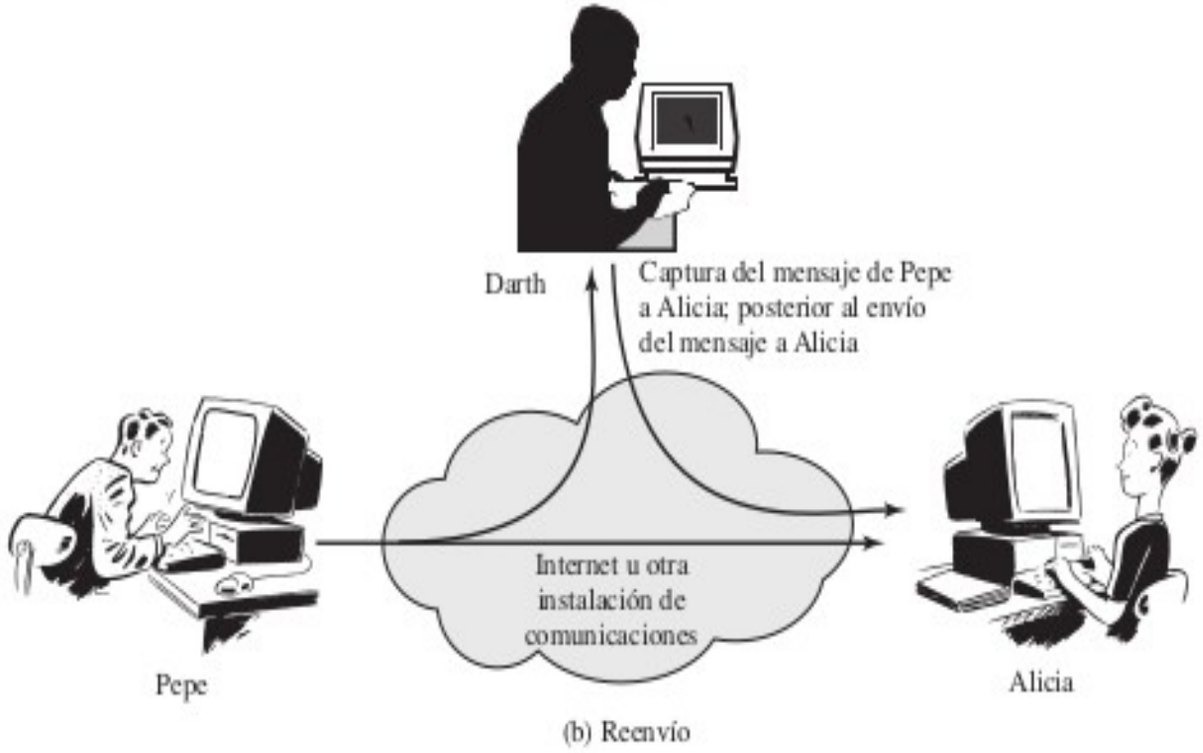
- Ataques activos



(a) Enmascaramiento

Seguridad y Protección

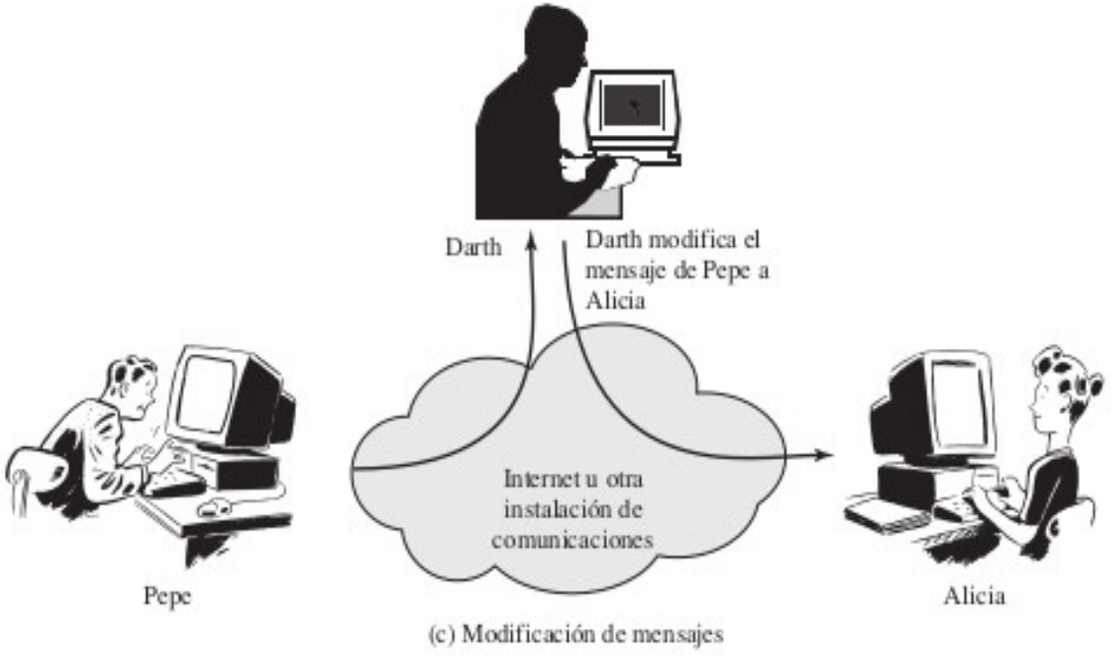
- Ataques activos



(b) Reenvío

Seguridad y Protección

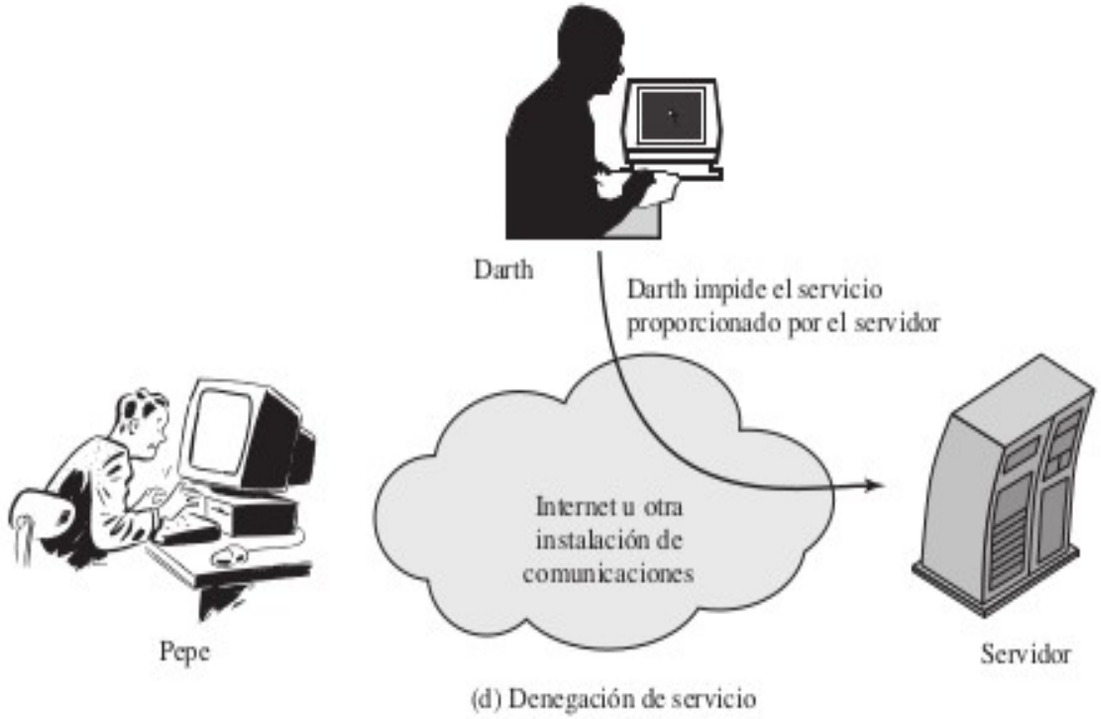
- Ataques activos



(c) Modificación de mensajes

Seguridad y Protección

- Ataques activos



(d) Denegación de servicio

Seguridad y Protección

- Protección
  - La multiprogramación permite compartir:
    - Memoria
    - Dispositivos E/S
    - Programas
    - Datos

    Para ello se debe se necesita protección !

    El Sistema Operativo manejará diferentes niveles de protección sobre los recursos compartidos

Seguridad y Protección

- Protección (enfoques)
  - Protección a la memoria en la muliprogramación
  - Control de acceso orientado a usuario
    - Identifación usuario / password
    - Arquitectura Single sign on
  - Control de acceso orientado a datos
    - Una vez logueado se utiliza un perfil
    - Acl
    - Tickets (kerberos)

Seguridad y Protección

- Intrusos (clases)
  - Enmascarado: individuo externo que se aprovecha de una cuenta de un usuario legítimo
  - Trasgresor: interno, accede a recuros no autorizados o si está autorizado lo hace de forma maliciosa
  - Usuario clandestino: evade auditoría, accede y elimina registros de acceso.

Seguridad y Protección

- Técnicas de intrusión
  - Ingeniería social
- Protección de contraseñas
  - Buena prácticas (ingresar como usuario plano)
  - Técnicas para generar contraseñas robustas
- Detección de intrusos
  - Bitácoras (registros de sucesos y logs)
  - Detección
  - Prevención

Seguridad y Protección

- Software Malicioso (malware) vs antivirus
  - Puertas secretas
  - Bomba lógica: se planifica para que en cierta condición se ejecute
  - Troyano: parece ser otra cosa
  - Virus: infecta a otros programas y archivos
  - Gusanos: se replican por la red. Ej email se comporta como un virus.
  - Zombie: toma el control de otros oredenadores y realiza DoS descentralizada