TEMA 1
Modelo OSI de Seguridad

José María Sierra

Departamento de Informática
Universidad Carlos III de Madrid

Introducción

- Necesidad de seguridad de una organización
  - Evaluar su nivel de seguridad
  - Aplicar mejoras
  - Evaluación períodica de su nivel de seguridad
- Recomendación X.800 de la ITU
  - Visión general de la seguridad
  - Centrada en:
    - Ataques a la seguridad
    - Mecanismos de seguridad
    - Servicios de seguridad

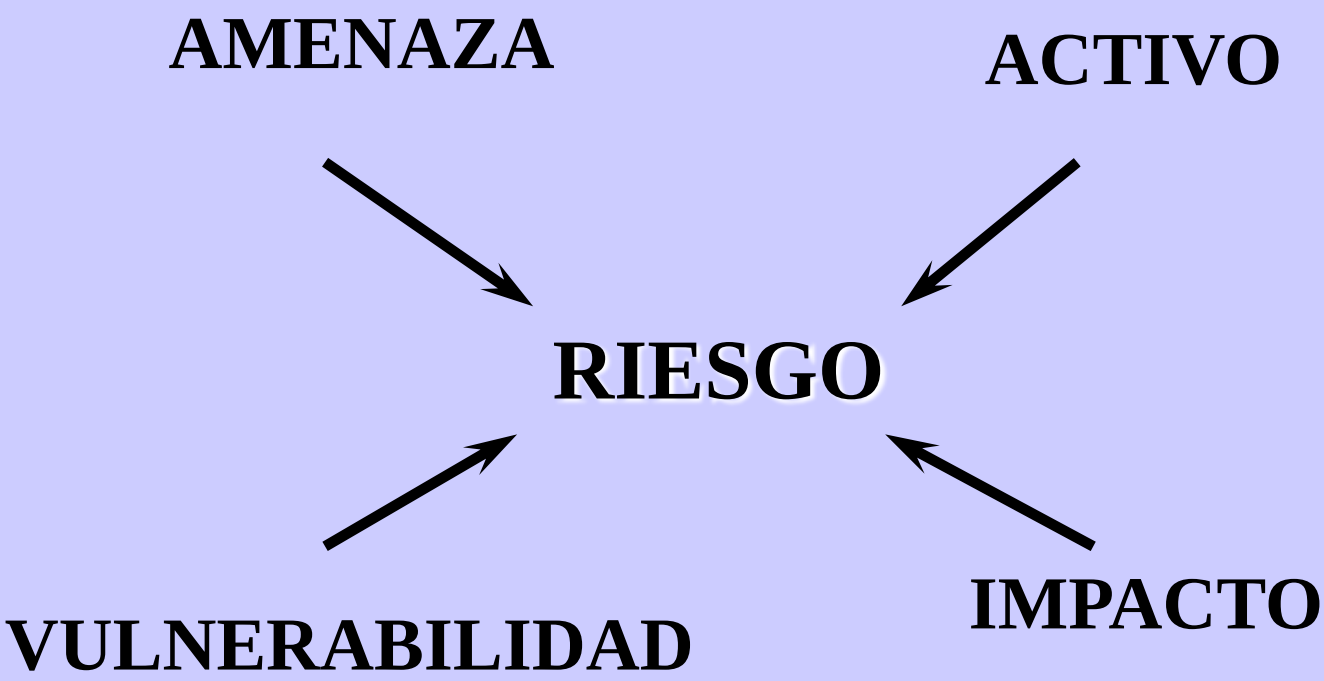
Ataques a la seguridad

- Asalto deliberado a la seguridad del sistema
  - Eludir las protecciones
  - Hacer uso inadecuado de los recursos
- Ataques pasivos
  - Escucha u observación no autorizada de las comunicaciones
  - Difíciles de detectar
  - Tipos
    - Obtención de los contenidos de los mensajes
    - Análisis de tráfico

Ataques a la seguridad

- Ataques Activos
  - Modificación del flujo de datos o elaboración de flujos falsos
  - Difíciles de evitar (Detección)
  - Tipos
    - Suplantación
    - Repetición
    - Modificación de los mensajes
    - Interrupción del servicio

Elementos de la seguridad en S.I.



Elementos de la seguridad en S.I.

Servicios de Seguridad

- Servicio suministrado por uno o más niveles de un sistema abierto de comunicación, que garantiza la seguridad del sistema y de las transferencias de datos.
- Servicio de Autenticación (entidades o datos)
  - Autenticación de entidades (con conexión)
  - Autenticación del origen de datos (sin conexión)
- Servicio de Control de acceso
  - Prevención del uso no autorizado de un servicio
- Servicio de Confidencialidad
  - Confidencialidad de la conexión
  - Confidencialidad no orientada a conexión
  - Confidencialidad de campos seleccionados
  - Confidencialidad del flujo del tráfico

Elementos de la seguridad en S.I.

Servicios de Seguridad

- Servicio de Integridad de los datos
  - Integridad de la conexión con recuperación
  - Integridad de la conexión sin recuperación
  - Integridad de la conexión de campos seleccionados
  - Integridad no orientada a conexión
  - Integridad no orientada a conexión de campos seleccionados
- Servicio de No repudio
  - No repudio en origen
  - No repudio en destino
- Servicio de Disponibilidad
  - Cualidad de estar accesible y utilizable a petición de una entidad autorizada

Elementos de la seguridad en S.I.

Mecanismos de seguridad

- Cifrado
- Firma digital
- Control de Acceso
- Integridad de los datos
- Intercambio de autenticación
- Relleno de tráfico
- Control de encaminamiento
- Notarización

Problemas de Protección de los sistemas distribuidos

¿Es Internet seguro?

- Diseño con 30 años de antigüedad
- Incremento exponencial del número de ordenadores conectados
- Incremento exponencial de usuarios
- Transmisión de informaciones sensibles
- Decremento de los requisitos para la realización de ataques remotos

Amenazas de seguridad en Internet

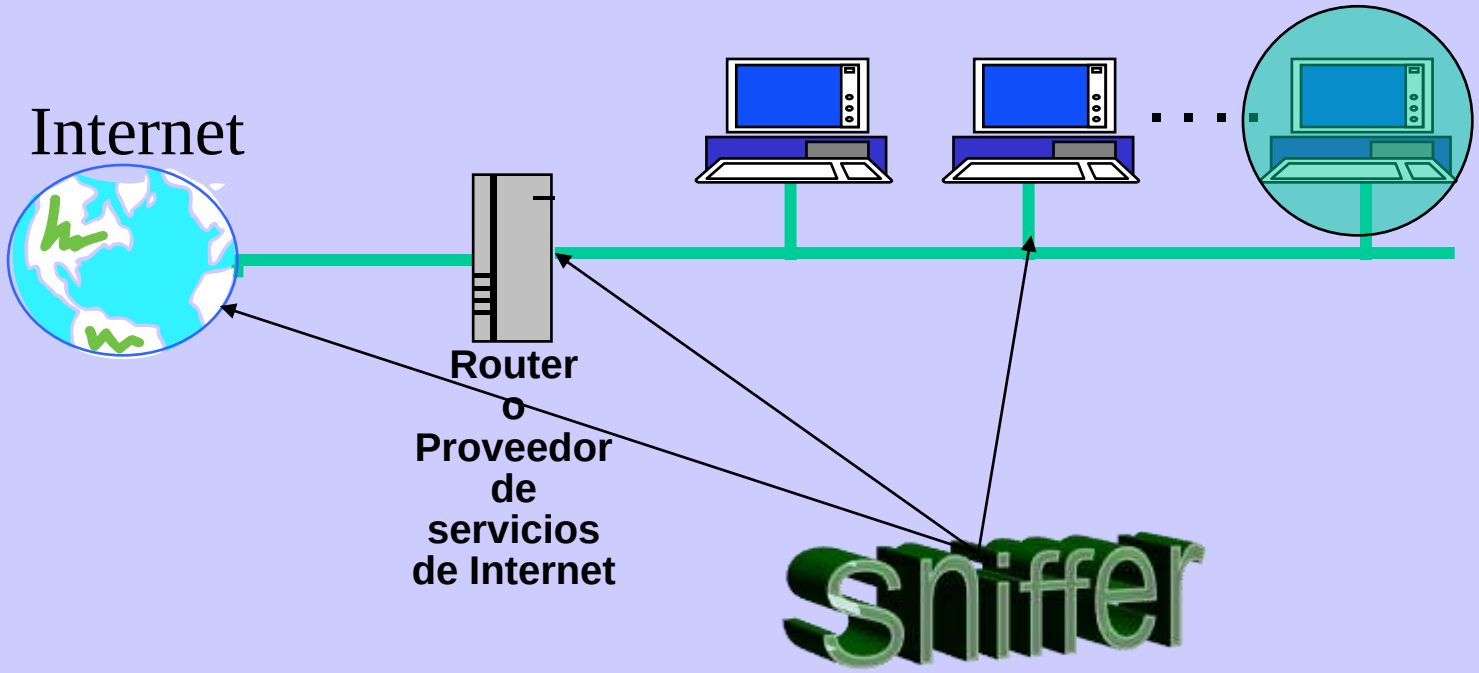
- Ataques a la autenticación
  - Suplantación de entidades en Internet
- Ataques a la disponibilidad
  - Inhabilitación remota de máquinas
- Ataques a la confidencialidad
  - Monitorización de conexiones de red
- Ataques a la Integridad
  - Sustitución de contenidos Web

Ataques a la autenticación

- Suplantación de entidades en Internet
  - Mediante:
    - Falsificación de las direcciones origen de los mensajes (IP-spoofing)
  - Permite:
    - Suplantar a otras máquinas
      - Es posible acceder a sistemas de información protegidos
    - Suplantar a otras entidades
      - Envío de mensajes de correo electrónico con identidades falsas.

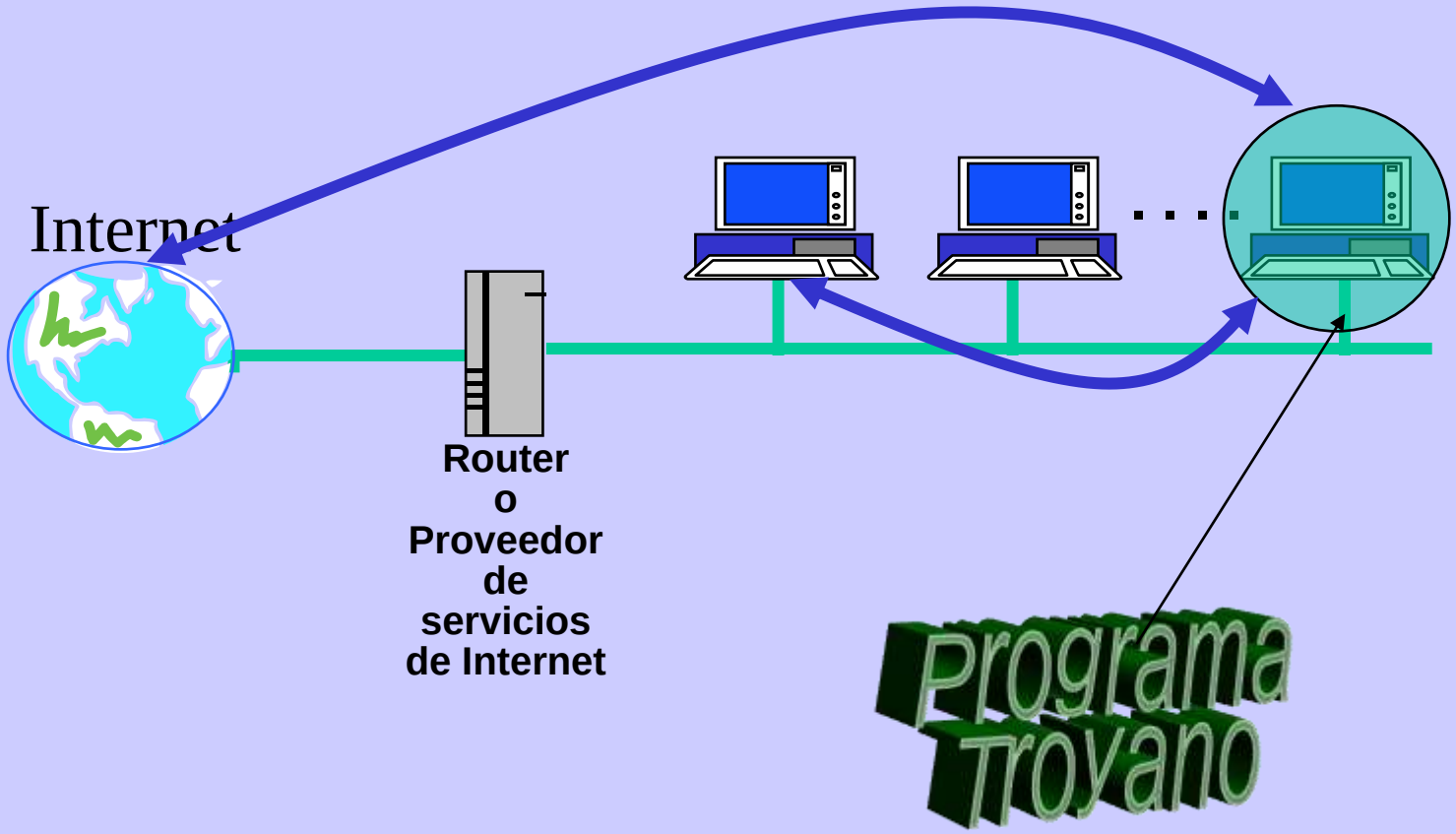
Ataques a la confidencialidad

- Utilización de analizadores de red (*sniffers*)



Ataques a la confidencialidad

- Programas troyano



Ataques a la Integridad

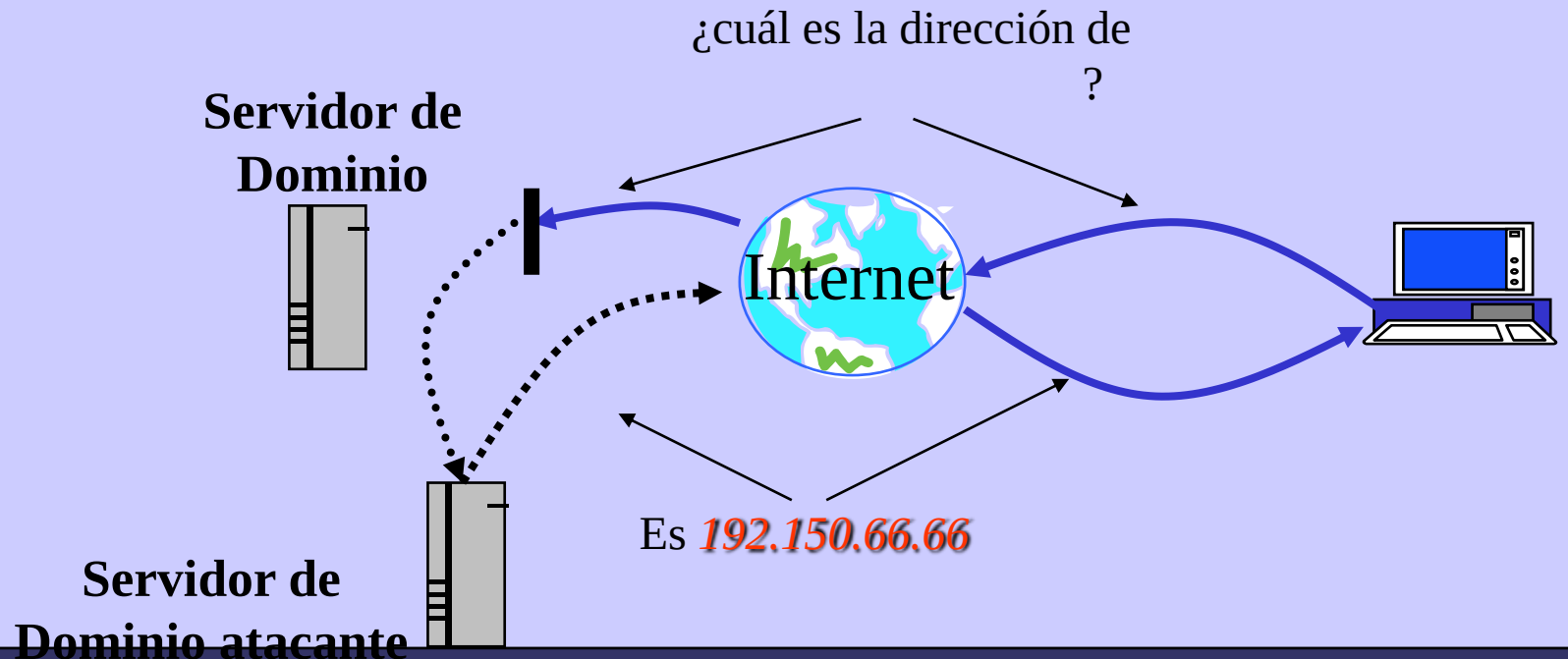
- Ruptura de servidores Web
  - Mediante:
    - Ejecución de ficheros "*cgi*"
    - Fallos en los programas servidores
  - Es posible:
    - Cambio de contenidos web
      - Control total del servidor
      - Modificación del contenido de ficheros (normalmente imágenes)

Ataques a la Integridad

- Ruptura de Servidores de Dominio (DNS)
  - Ataques sobre servidores de comercio electrónico

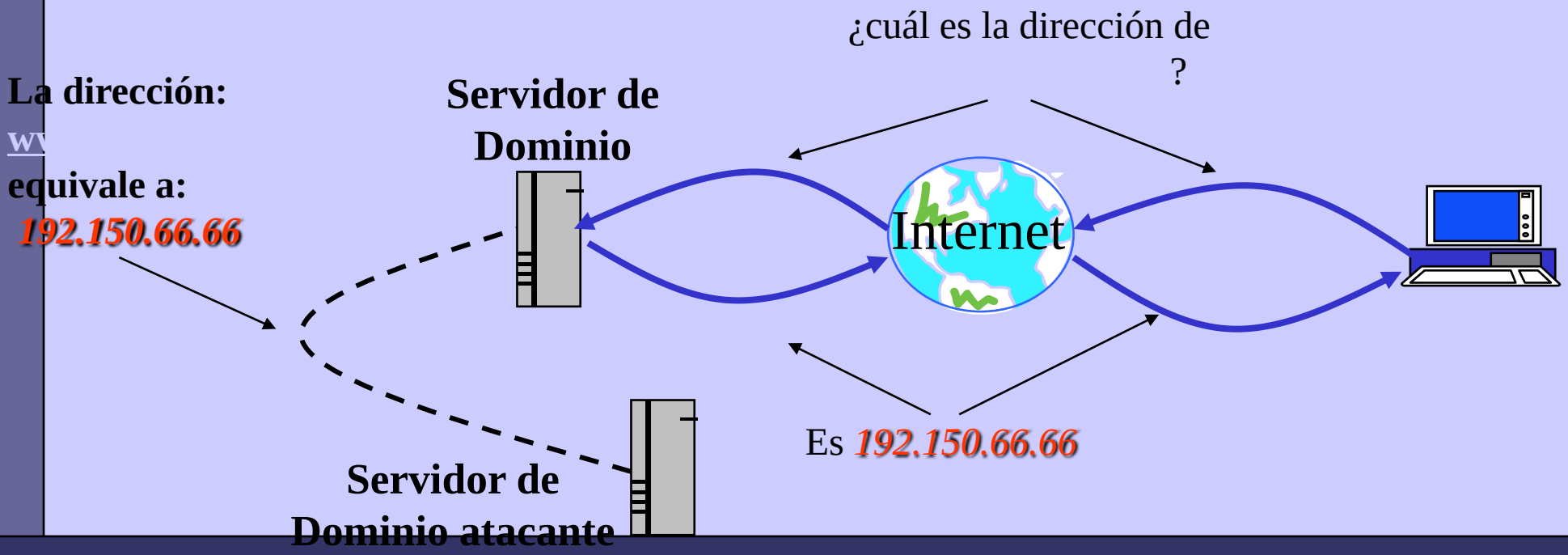
Ataques a la Integridad

- Ruptura de Servidores de Dominio (DNS)
  - Re-direccionamiento de las peticiones



Ataques a la Integridad

- Ruptura de Servidores de Dominio (DNS)
  - Sabotaje de la información del servidor de dominio



¿Qué nos espera?

- Incremento de usuarios
- El crecimiento de los clientes potenciales
  - Los vendedores deben actuar rápido
  - Los usuarios demandan mejor precio en los productos y no seguridad en las transacciones
- Mayor interconexión con clientes, proveedores y empresas afines
- Difícil de determinar qué es intranet y qué internet
- Los ordenadores inseguros suponen una amenaza para el resto

Buenas noticias

- Nuevo protocolo para Internet (IPv6)
  - Incorpora mecanismos de seguridad
    - Autenticación, Integridad y Confidencialidad
- Sistemas más volcados en la interconexión
  - Concienciación de la importancia de la seguridad
  - Cambio de mentalidad
    - Inversión ←→ Ahorro potencial