Curso de doctorado
Seguridad en Redes de Ordenadores

Tema 3: La problemática de la seguridad en sistemas abiertos

¿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

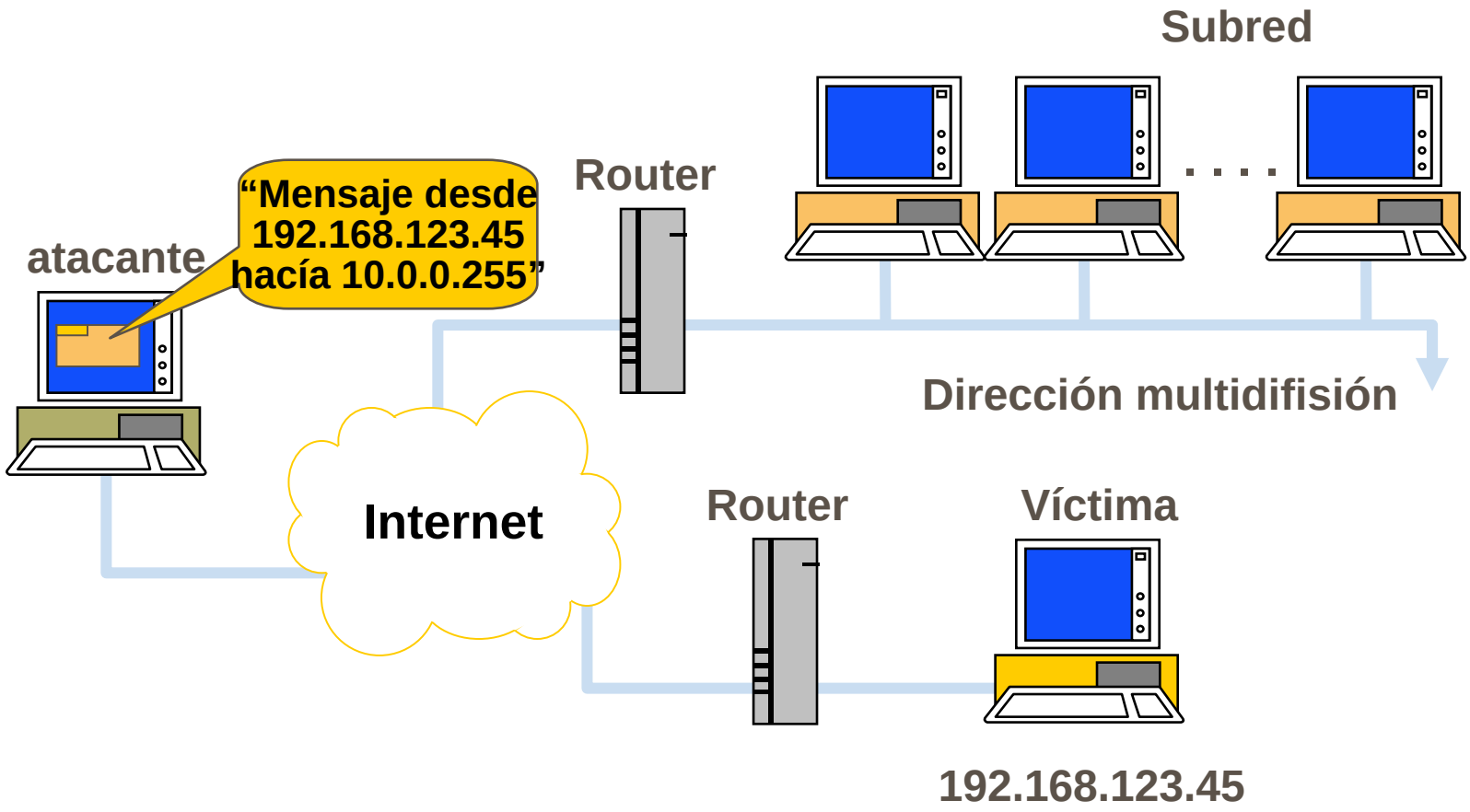
- Ataques a la autenticación
  - Suplantación de entidades en Internet
- Ataques a la disponibilidad
  - Inhabilitación remota de máquinas
- Ataques a la confidencialidad
  - Monitorización de conexiones de red
- Ataques a la Integridad
  - Sustitución de contenidos Web

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.

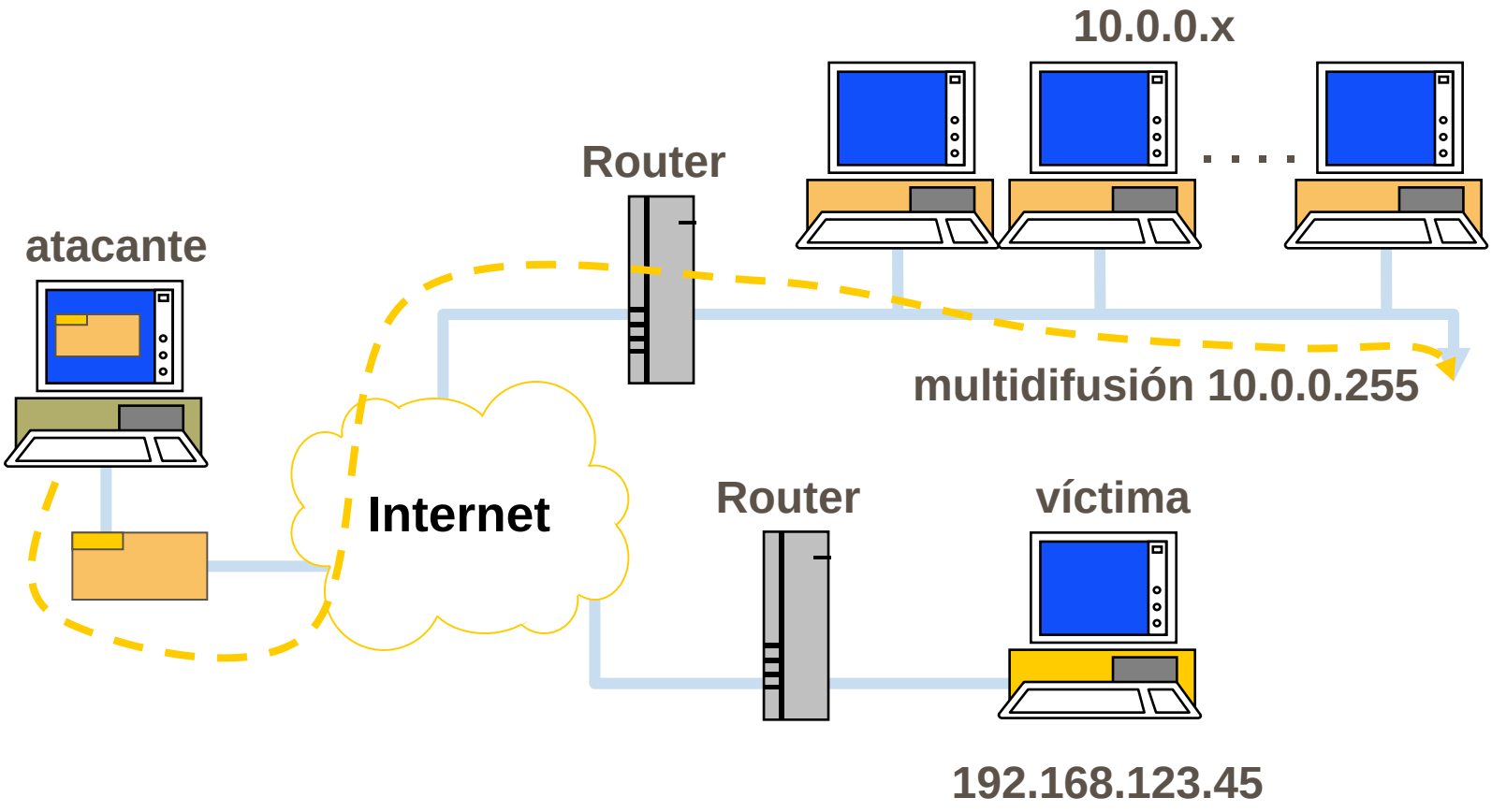
Ataques a la disponibilidad

Ataque de Denegación de Servicio



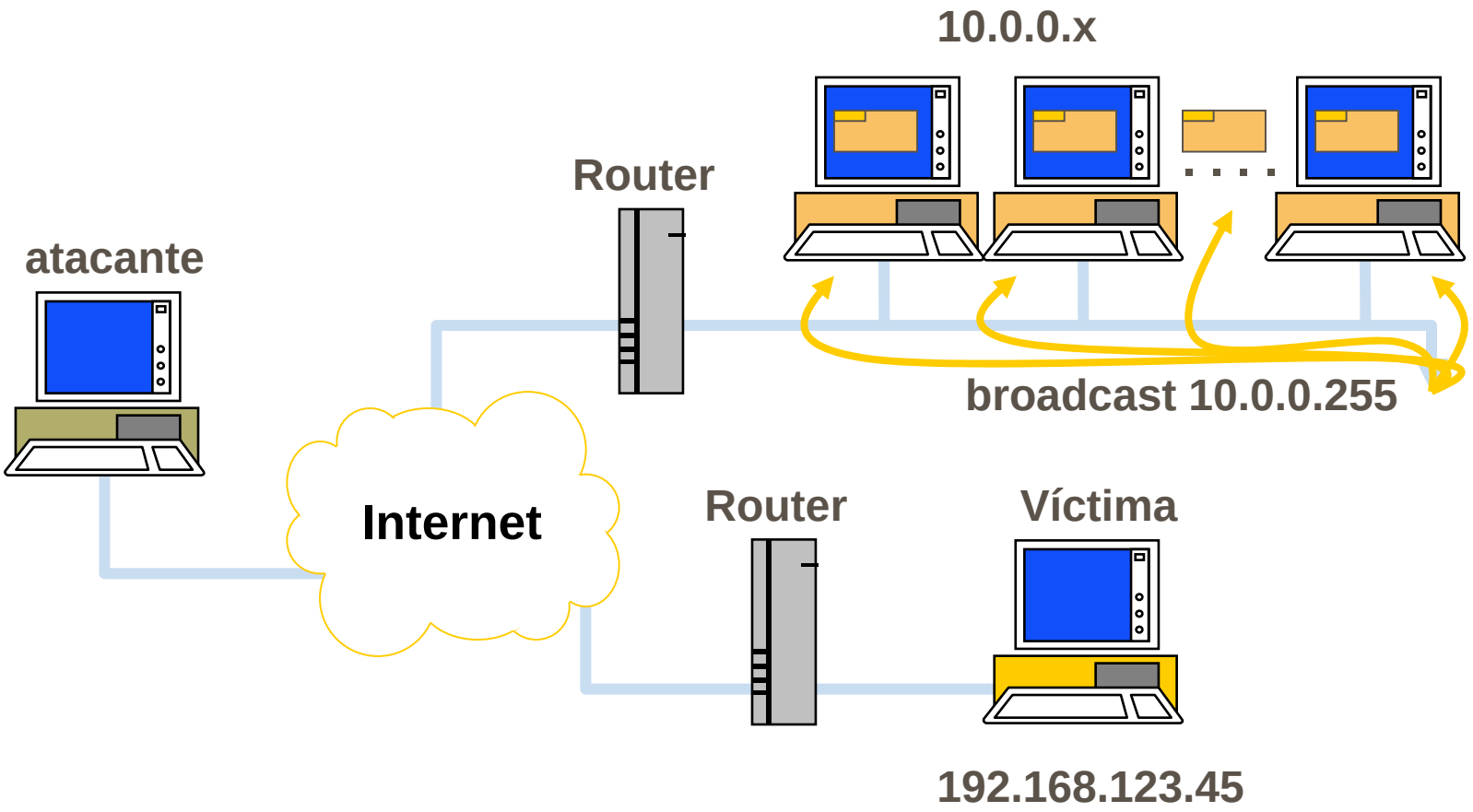
Ataques a la disponibilidad

Ataque de Denegación de Servicio



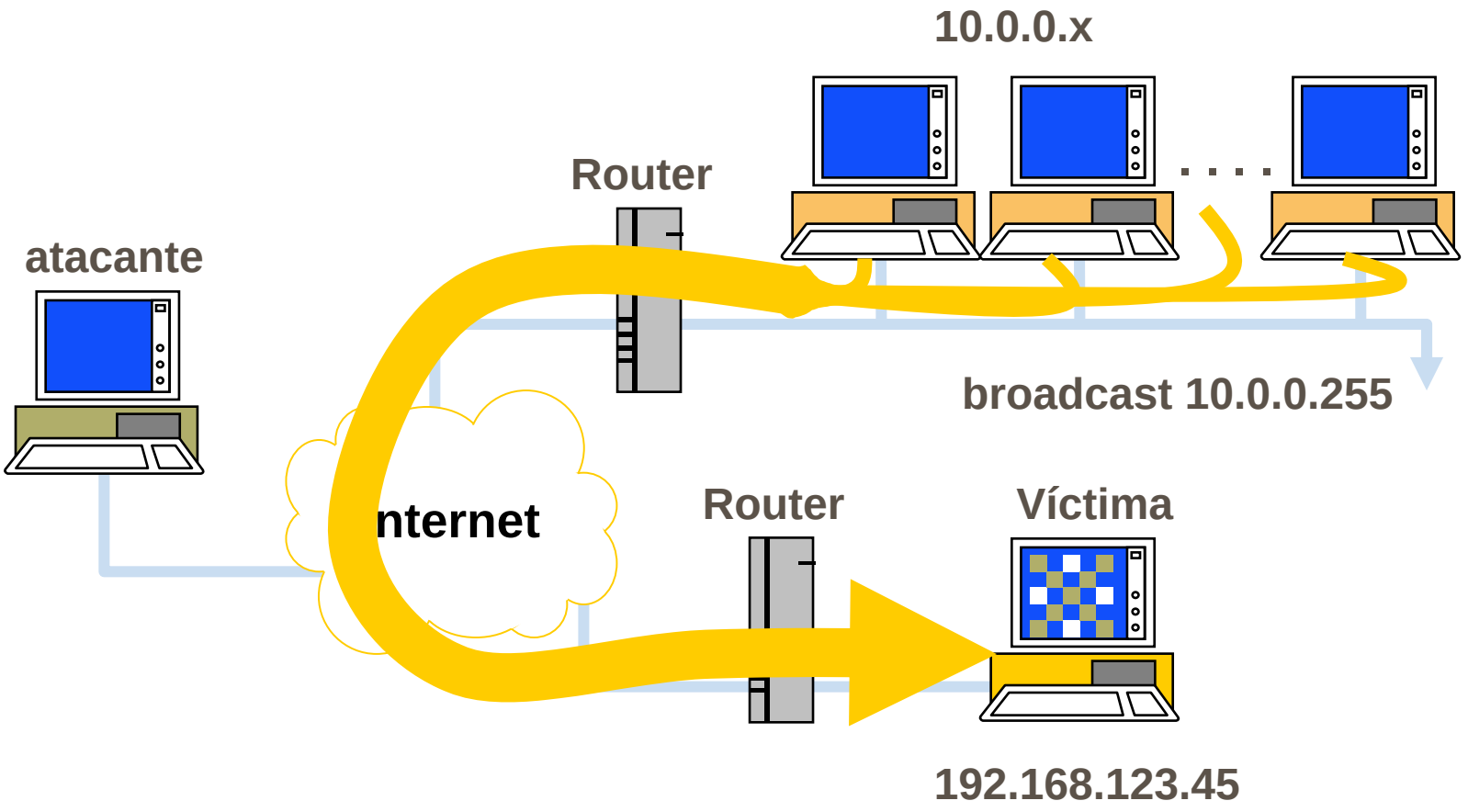
Ataques a la disponibilidad

Ataque de Denegación de Servicio



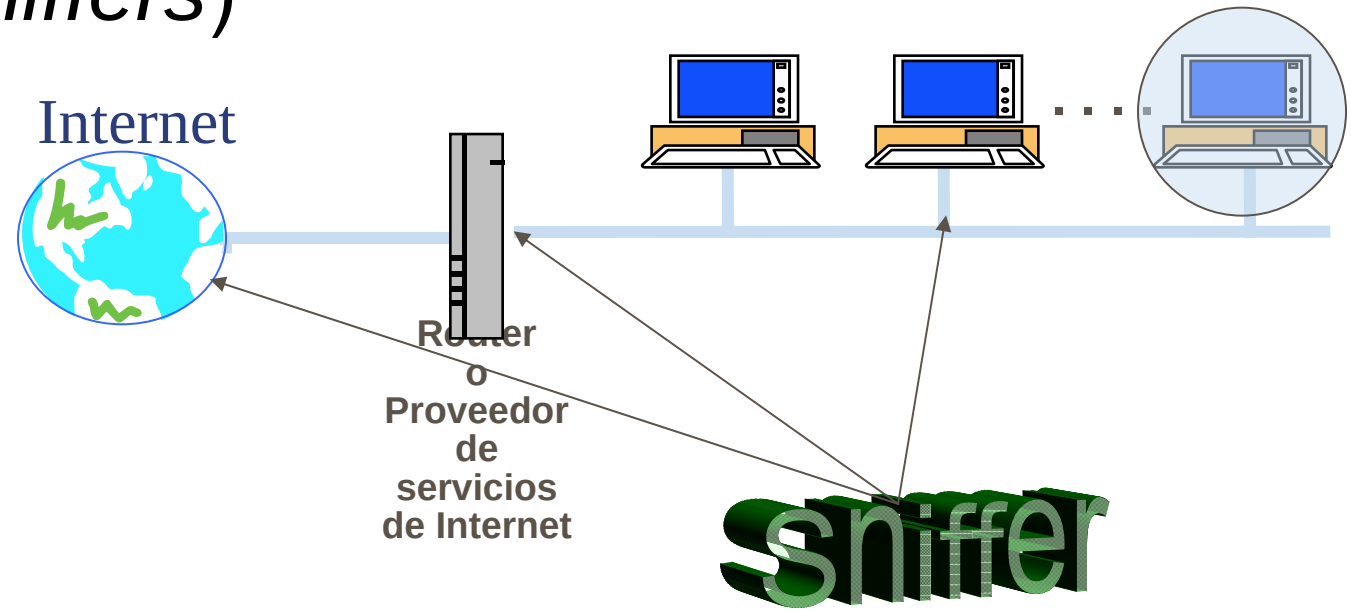
Ataques a la disponibilidad

Ataque de Denegación de Servicio



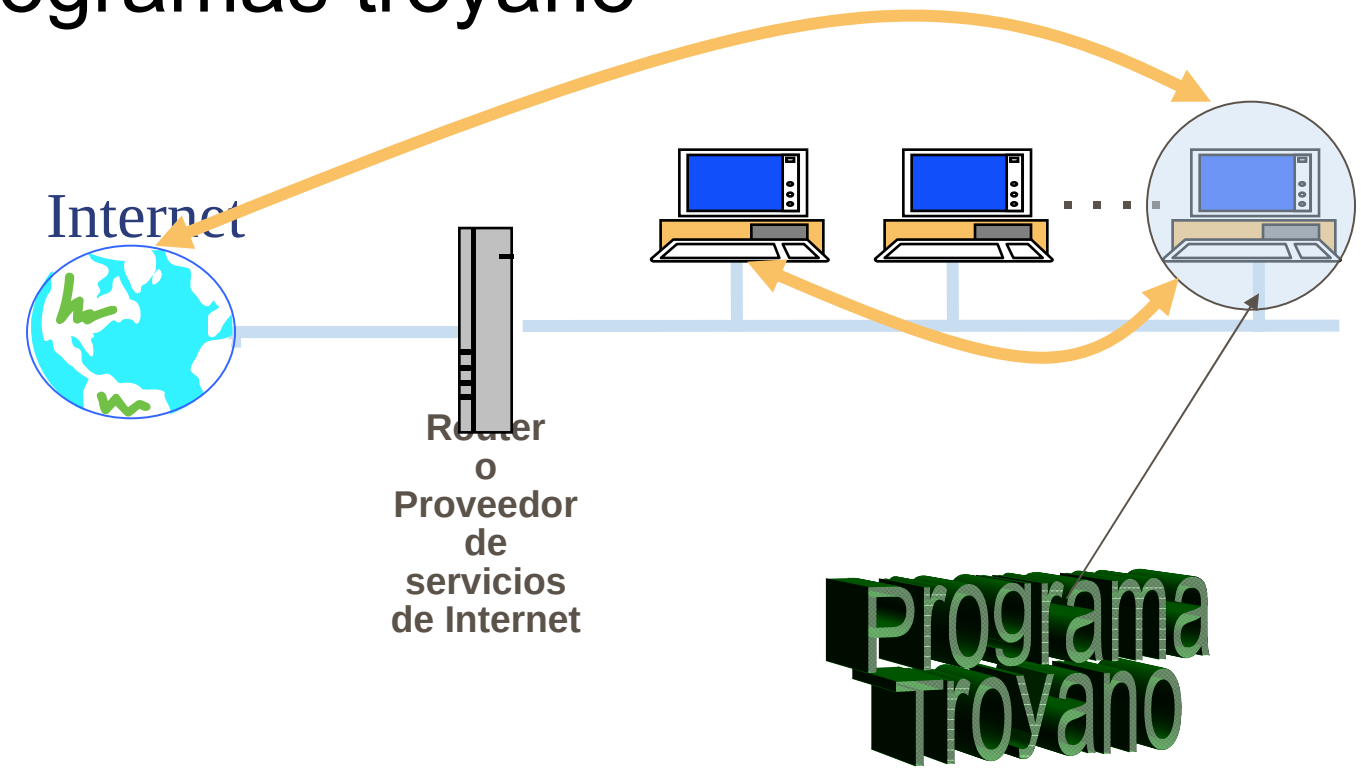
Ataques a la confidencialidad

- Utilización de analizadores de red (*sniffers*)



Ataques a la confidencialidad

- Programas troyano

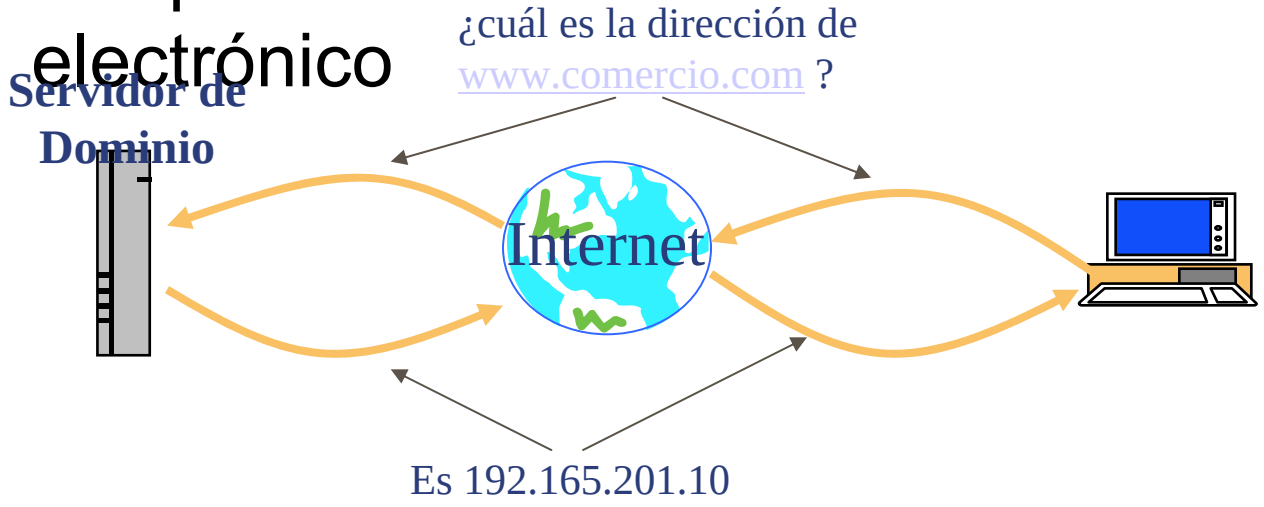


Ataques a la Integridad

- 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)

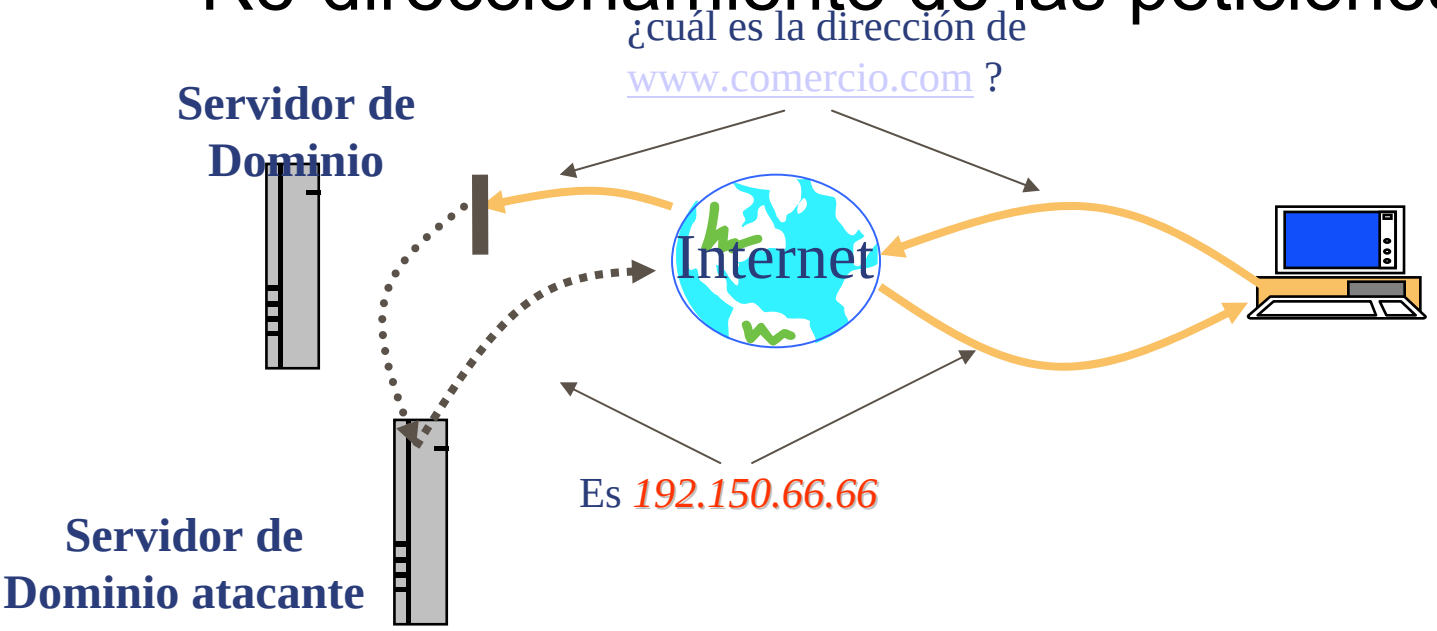
Ataques a la Integridad

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



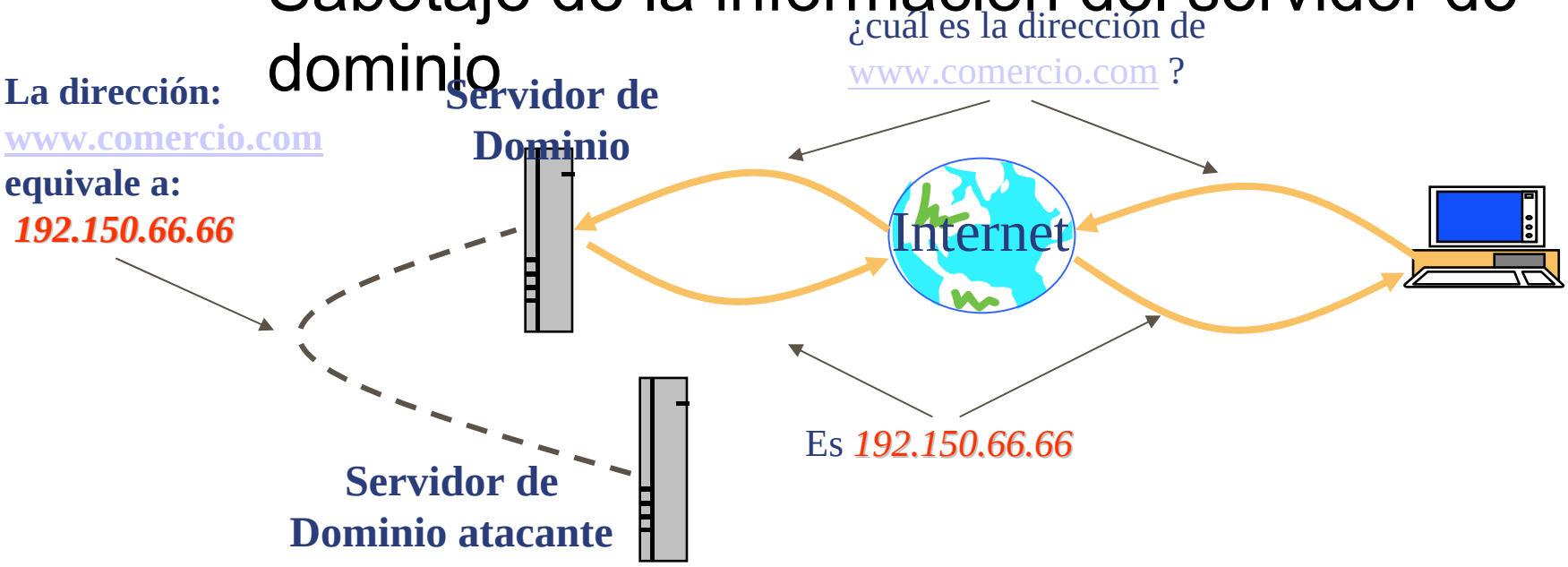
Ataques a la Integridad

- 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



Actualidad de Internet

- Cambio de contenidos del periódico *New York Times* en Internet (sept. 1998)
- Ataque informático al Ministerio del Interior (oct. 1998)
- Ataques de Denegación de servicio sobre empresas de comercio electrónico (feb. 2000)
- Telefónica permitió acceder a facturas de clientes desde Internet (feb. 2000)
- Datos personales de los aspirantes a “Gran Hermano” (ene. 2001)

¿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

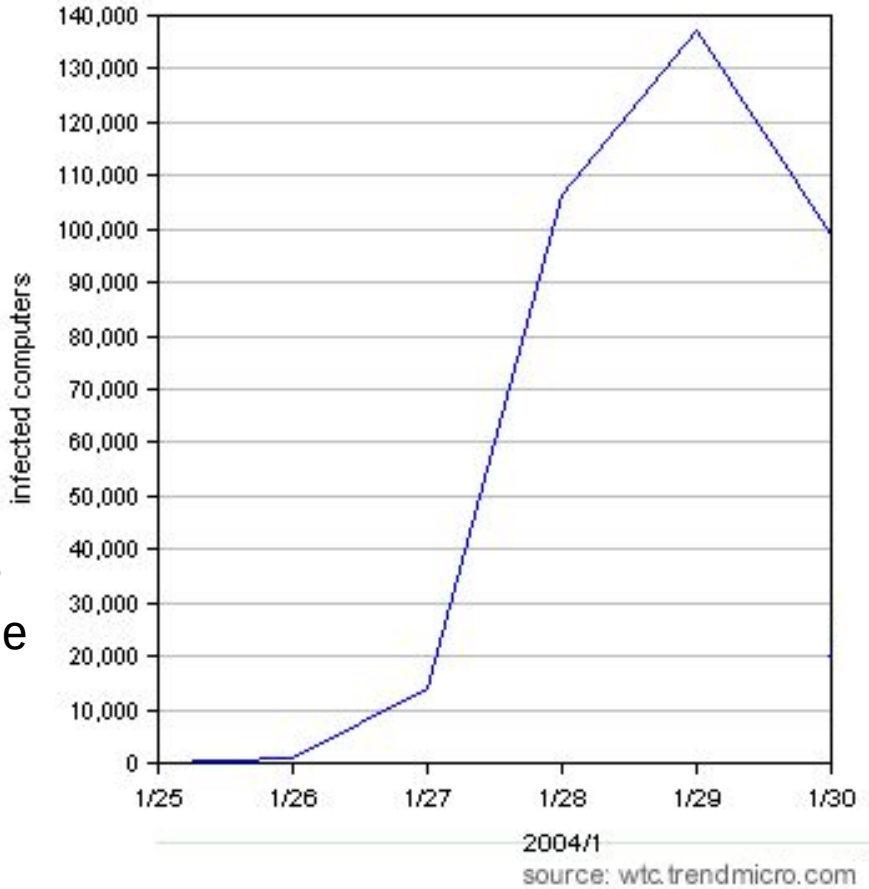
¿Qué nos espera?

- Cambio de filosofía del software malicioso:

Virus destructivo → Programa espía

Expansión de Virus rápida

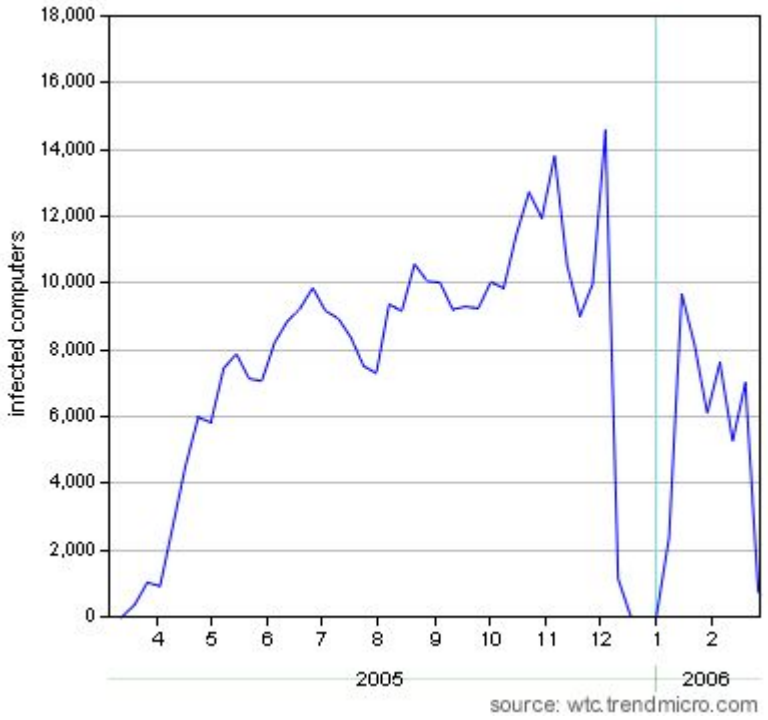
- 26/ene/2004, MyDoom worm
  - Internet worm contra sistemas Microsoft Windows
  - Correo electrónico basado en ingeniería social
    - Mensajes localizados en 142 países
    - Hasta uno de cada 3 mensajes tiene el virus (CNN)
    - > 400.000 ordenadores afectados
  - Ataques DoS programados:
    - 1/Feb/2004: www.sco.com
    - 3/feb/2004: www.microsoft.com



Expansión lenta

- 24/mar/2005, SPYW_DASHBAR
  - Entra por Internet Explorer sin acción del usuario.
  - Instala un toolbar de búsqueda

  - Casi 400.000 ordenadores infectados



Ordenadores Zombies

- Según datos de TechNewsWorld, se crearon 7.6 millones de nuevos zombies en Diciembre 2005.
- Esto supone más de **250.000 nuevos** PCs comprometidos, cada día.
- La mayoría de los ordenadores zombies permanecen encendidos 24 horas al día corriendo programas de intercambio de archivos. Estás siempre preparados para ser utilizados en acciones fraudulentas.

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