Semana de Ingeniería ELÉCTRICA Y ELECTRÓNICA 2002

11 abril 2002

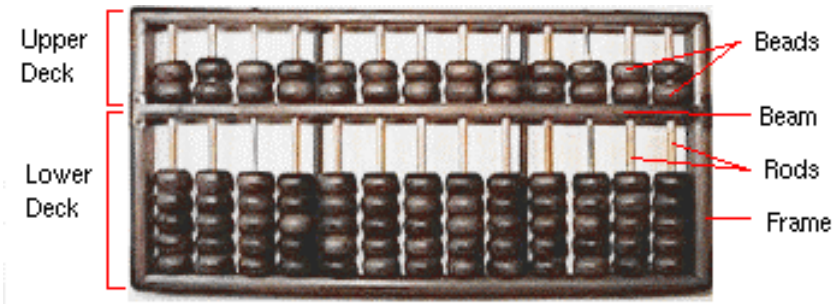
Panorama de la Seguridad en Redes

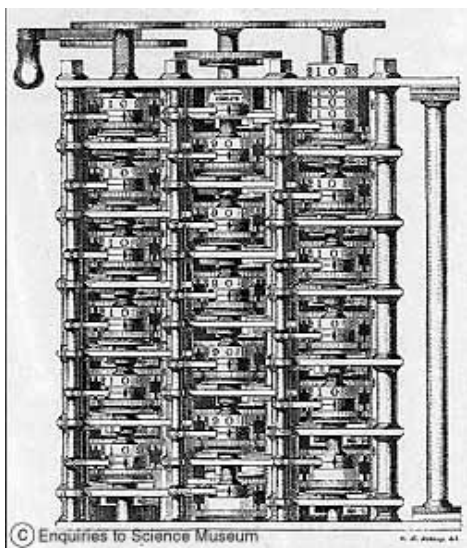
Roberto Gómez Cárdenas

rogomez@campus.cem.itesm.mx

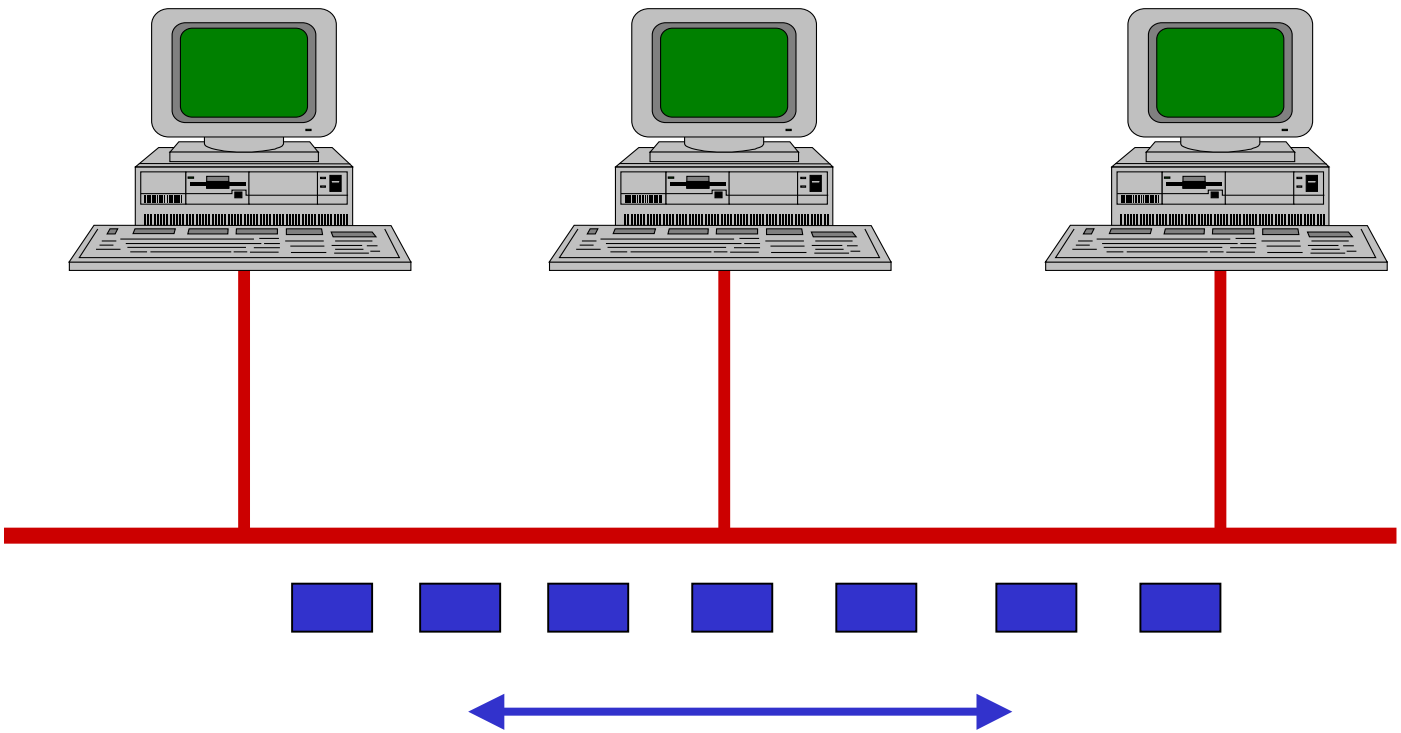
http://webdia.cem.itesm.mx/dia/ac/rogomez

Primeras computadoras

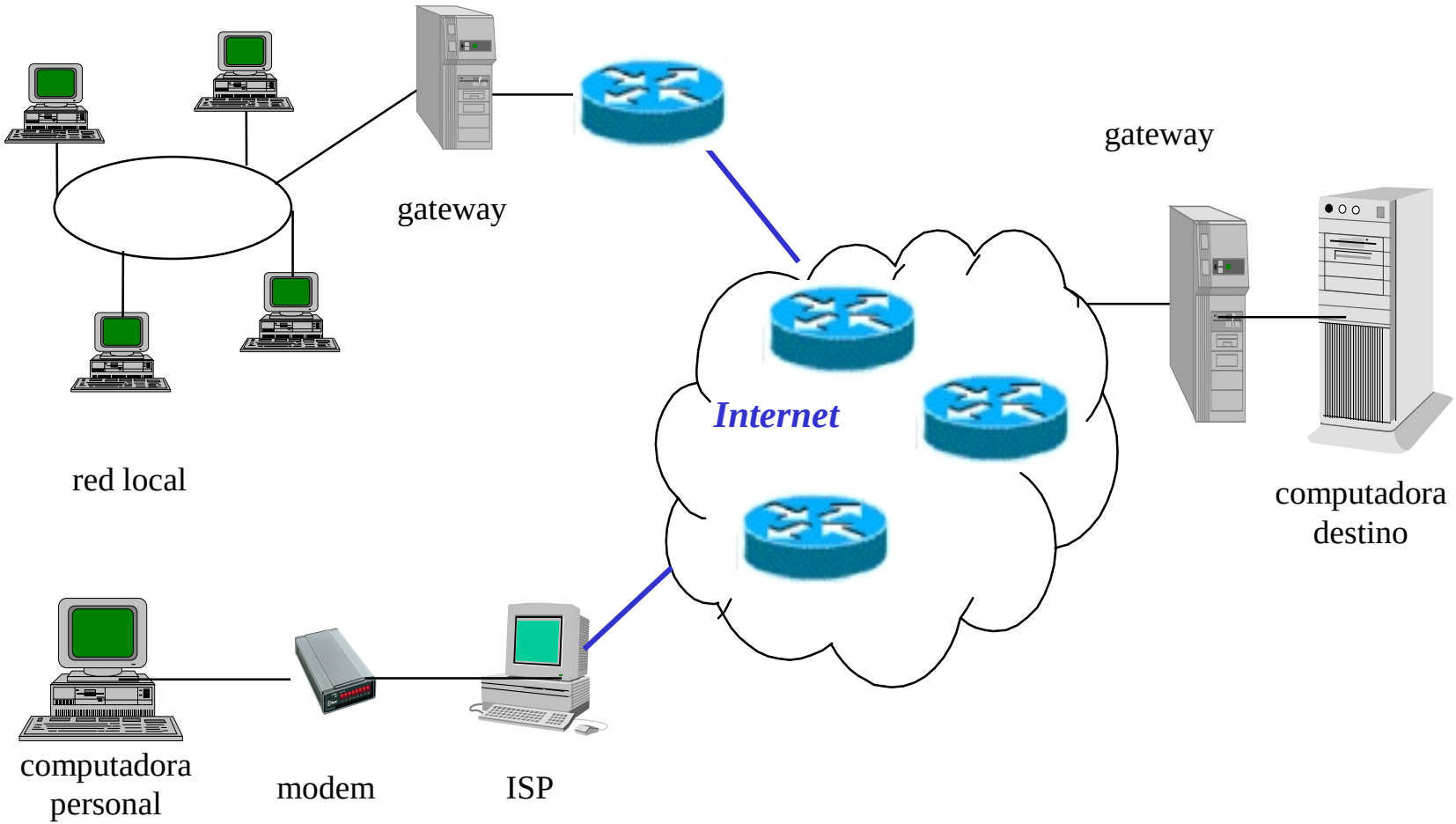




¿Y después?

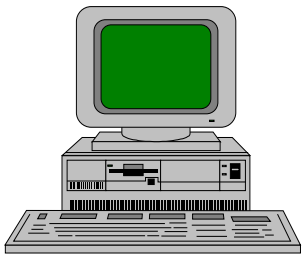


Expandiendo las redes

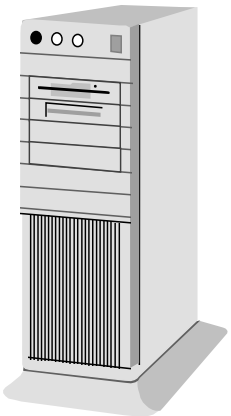


El esquema cliente/servidor

cliente



servidor



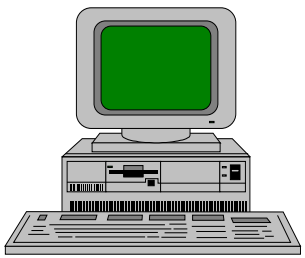
petición

procesamiento

respuesta

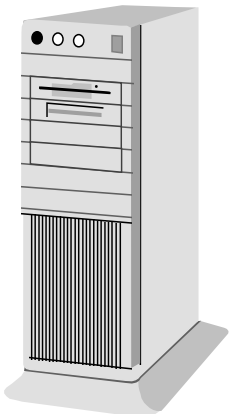
¿Y donde estan los malos?

cliente



¡de los dos lados!

servidor



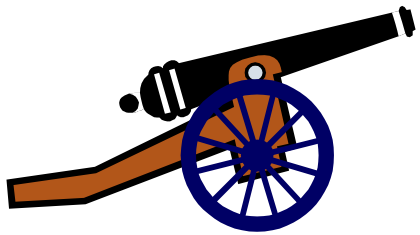
Haciendo cuentas ...

- Computación electrónica 50 años !
- Redes sólo tienen 30 años de vida !
- Seguridad 23 años !
- Internet 15 años !
- Web 6 años !
- Intranets 3 años...
- Extranets 2 años...

Seguridad Computacional

- El conjunto de políticas y mecanismos que nos permiten garantizar la confidencialidad, la integridad y la disponibilidad de los recursos de un sistema.

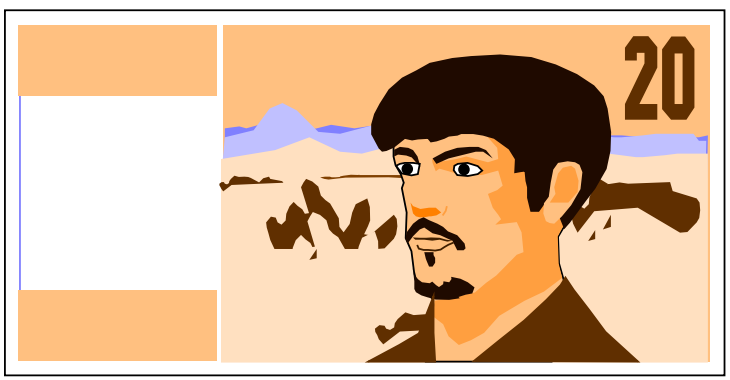
Confidencialidad



Un sistema posee la propiedad de *confidencialidad* si, la información manipulada por éste no es disponible ni puesta en descubierto para usuarios, entidades o procesos no autorizados.

Integridad

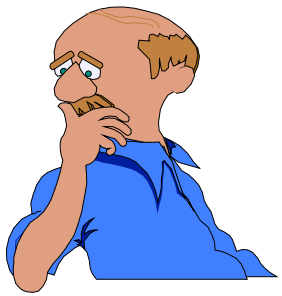
Un sistema posee la propiedad de integridad si los datos manipulados por éste no son alterados o destruidos por usuarios, entidades o procesos no autorizados.



Disponibilidad

Un sistema posee la propiedad de *disponibilidad* si, la información es accesible (está disponible) en el momento en que así lo deseen los usuarios, entidades o procesos autorizados.

¿Quien contra quien?



Amenazas
Vulnerabilidades
Ataques

Mecanismos y Políticas

Confidencialidad
Integridad
Disponibilidad

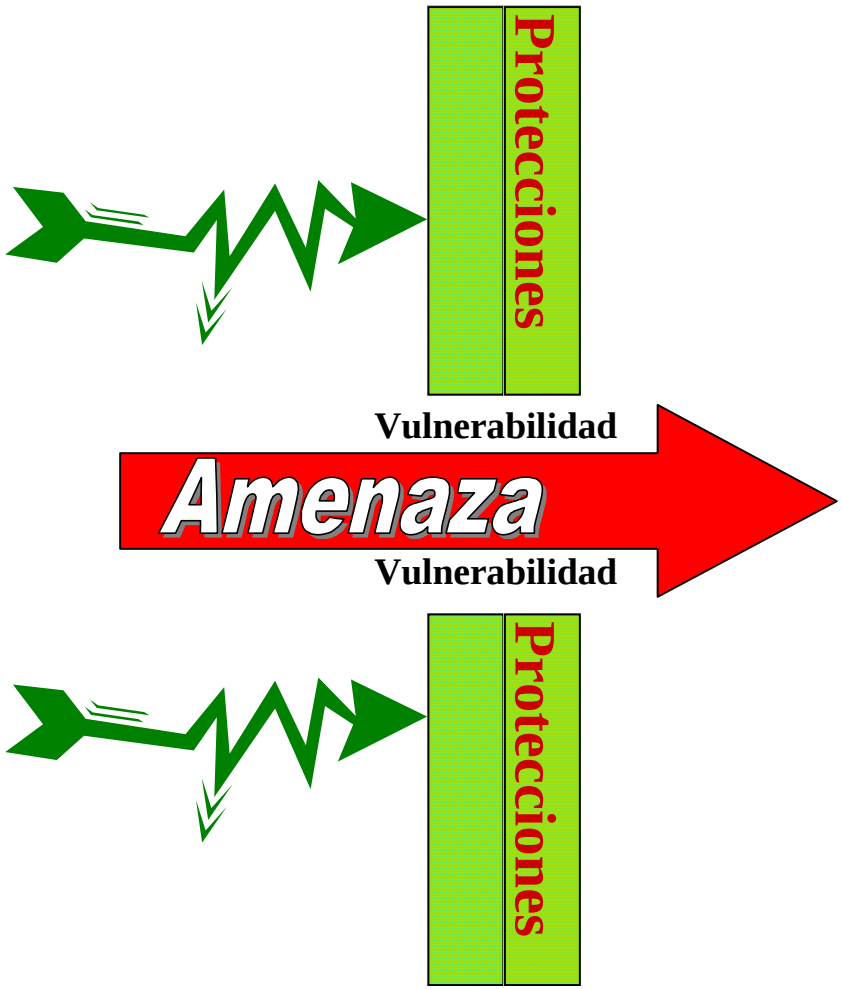
Amenaza

- Circunstancia o evento que puede causar daño violando la confidencialidad, integridad o disponibilidad
- Frecuentemente aprovecha una vulnerabilidad

Vulnerabilidad

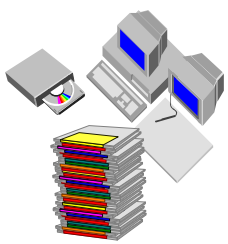
- Debilidad de un sistema informático que permite que sus propiedades de sistema seguro sean violadas.
- La debilidad puede originarse en el diseño, la implementación o en los procedimientos para operar y administrar el sistema.
- En el argot de la seguridad computacional una vulnerabilidad también es conocida como un *hoyo*.

Vulnerabilidad vs amenaza



Activos

Datos
Instalaciones
Hardware/Software



¿Qué es un ataque?

- Acción o acciones que previenen cualquier parte de un sistema de información automatizado, de funcionar de acuerdo con su propósito definido.
- El hecho de que se haga un ataque no necesariamente significa que tendrá éxito.
- Esto incluye cualquier acción que causa la destrucción, modificación o retraso del servicio no autorizado.

Mecanismos de Seguridad

- Es una técnica o método que implementa uno o más servicios de seguridad.
- Un servicio garantiza la seguridad de los datos que residen en un host o que circulan en una red.
- La mayoría de los mecanismos actuales se basan en la criptografía.

Política de Seguridad

- Definición del conjunto de reglas que deben respetarse para mantener la seguridad de la información.
- Depende de los objetivos y metas de la organización.
- Generalmente es expresada en un lenguaje o idioma.

Paradigmas

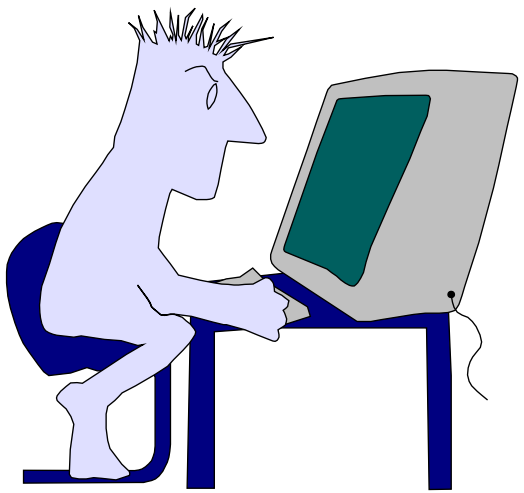
- *Paranoico*: Nada está permitido.
- *Prudente:* Lo que no está expresamente permitido, está prohibido.
- *Permisivo*: Lo que no está expresamente prohibido, está permitido.
- *Promiscuo:* Todo está permitido.

Ejemplo de Política (en lenguaje natural)

- Sólo se permitirá el intercambio de correo electrónico con redes de confianza.
- Toda adquisición de software a través de la red debe ser autorizada por el administrador de seguridad.
- Debe impedirse la inicialización de los equipos mediante disco.

¿De quien me debo cuidar?

- Los hackers
- Los crackers
- Los scripters



El Hacker: La Vieja Guardia

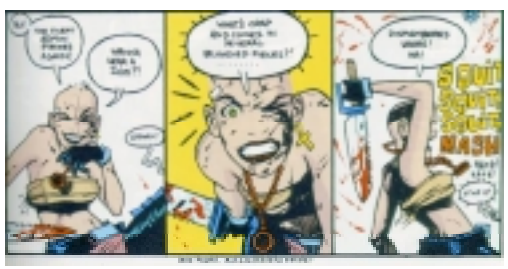
- Origen del término a finales de los 60.
- Programador con alto dominio de su profesión, capaz de solucionar problemas a través de hacks (segmentos de código muy ingenioso).
- Verdaderos conocedores de la tecnología de cómputo y telecomunicaciones (85-93).
- La búsqueda del conocimiento siempre fue su fuerza impulsora.

El cracker

- Aquella persona que en forma persistente realiza intentos hasta obtener acceso a sistemas computacionales.
- Una vez logrado el acceso produce daños a los recursos del sistema atacado.
- No necesariamente tiene el mismo nivel de conocimientos que el hacker.

El Hacker: la nueva generación o los ¨Script-kidies¨

- Gente con la capacidad de buscar un programa en la red y ejecutarlo.
- No hay una meta fija.
- Necesidad de pertenencia, aunque sea al *inframundo*.
- No hay preocupación por las consecuencias reales de sus actos.
- Se sienten muy ¨cool¨.



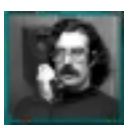
El Hacker: La Visión del Resto de los Usuarios

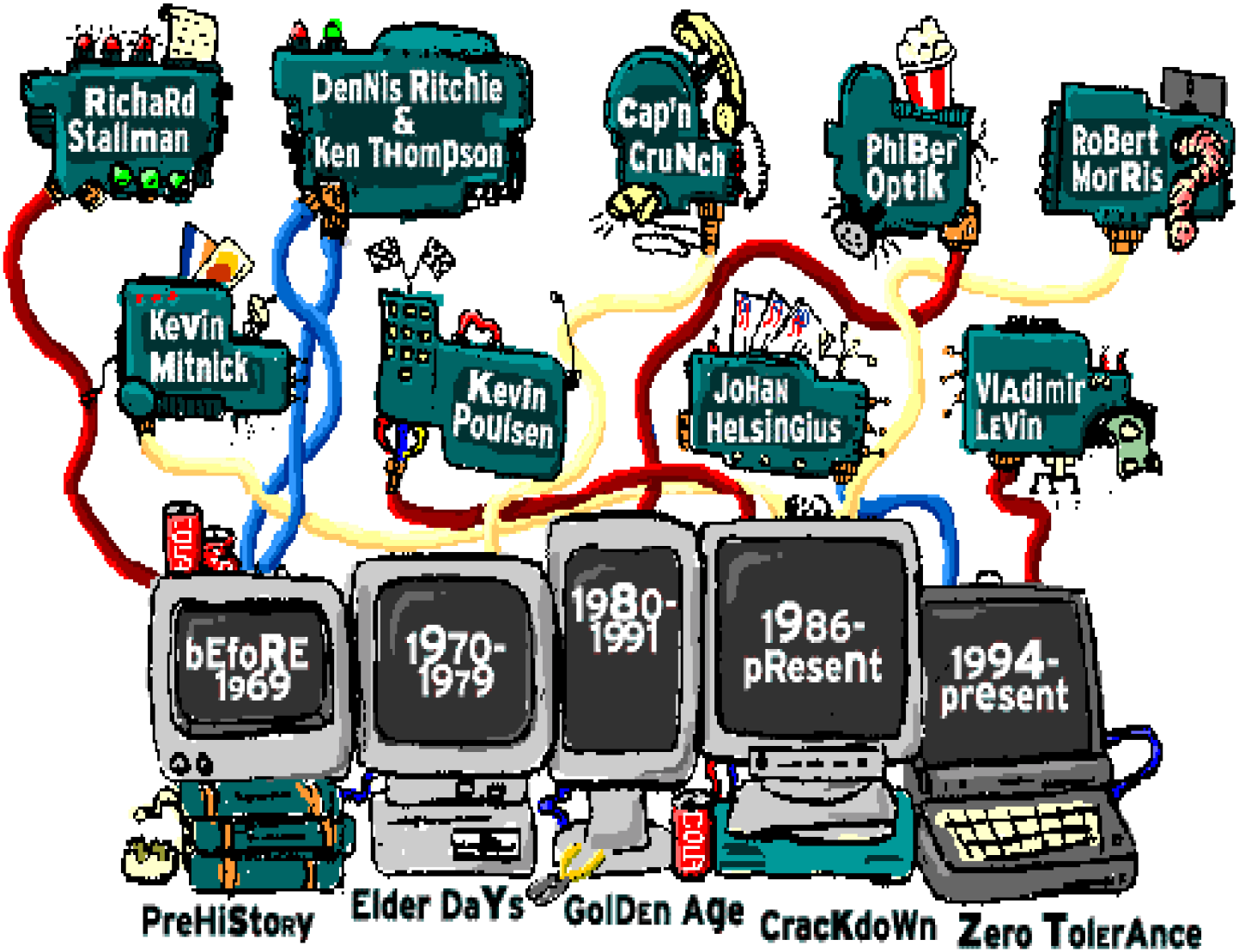
- ¿Qué es eso?
- Eso pasa solo en las películas.
- Así como los de ¨The Net¨
- Yo soy hacker.
- Yo apenas sé como se usa una computadora.
- Bill Gates se va a encargar de ellos.

El hall de la fama de los hackers











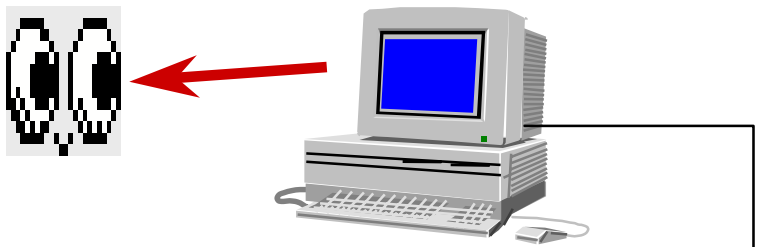


www.discovery.com/area/technology/hackers/hackers.html

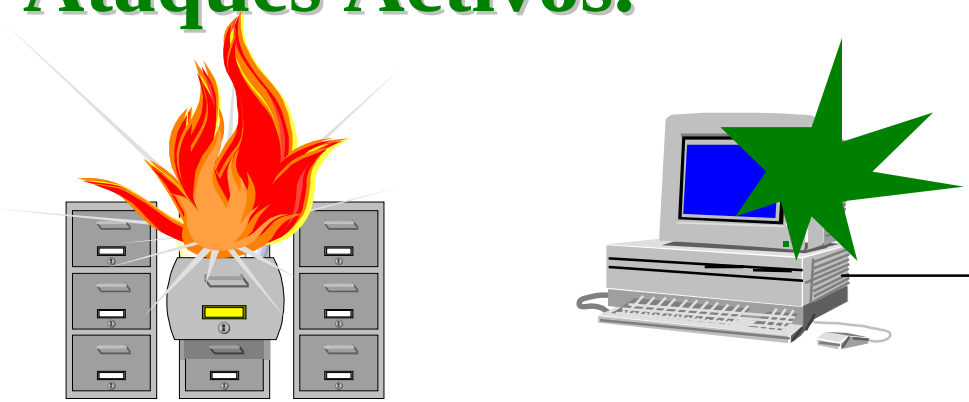
El hacker Kevin Mitnick

Tipos de Ataques

Ataques Pasivos.



Ataques Activos.

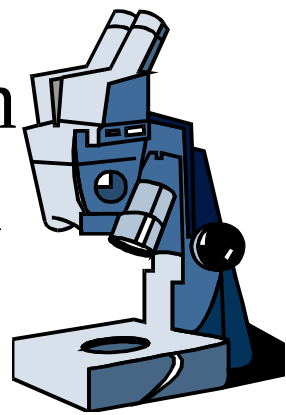


Principales Ataques

- Virus
- Caballo de Troya
- Gusanos (Worms)
- Bugs
- Trapdoors
- Stack overflow
- Pepena
- Bombas lógicas
- Secuestro sesiones
- Dedos inexpertos
- Falsificación
- Usurpación
- Sniffers
- Spoofing
- Spam
- Grafiti
- Ingeniería Social
- Negación de servicio

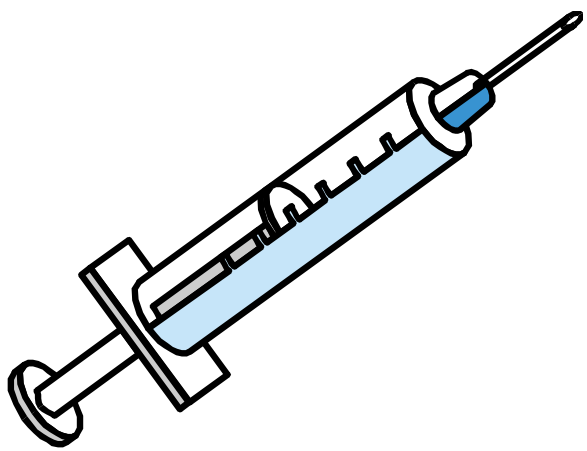
Virus

- Un virus se define como una porción de código de programación cuyo objetivo es implementarse a si mismo en un archivo ejecutable y multiplicarse sistemáticamente de un archivo a otro.
- Además de esta función primaria de "invasión" o "reproducción", los virus están diseñados para realizar una acción concreta en los sistemas informáticos..



Virus

- Esta acción puede ir desde la simple aparición de un mensaje en la pantalla, hasta la destrucción de toda la información contenida en el sistema.



Ejemplos de virus

- El caballo de Troya
- El pakistaní
- El cascada
- El Alabama
- El Jerusalén
- El Miguel Angel
- El ping pong
- El Viena
- El natas
- El dos piernas
- El stoned noit
- El DARK AVEGER
- El ping pong
- El I love you
- El trojan
- El killer

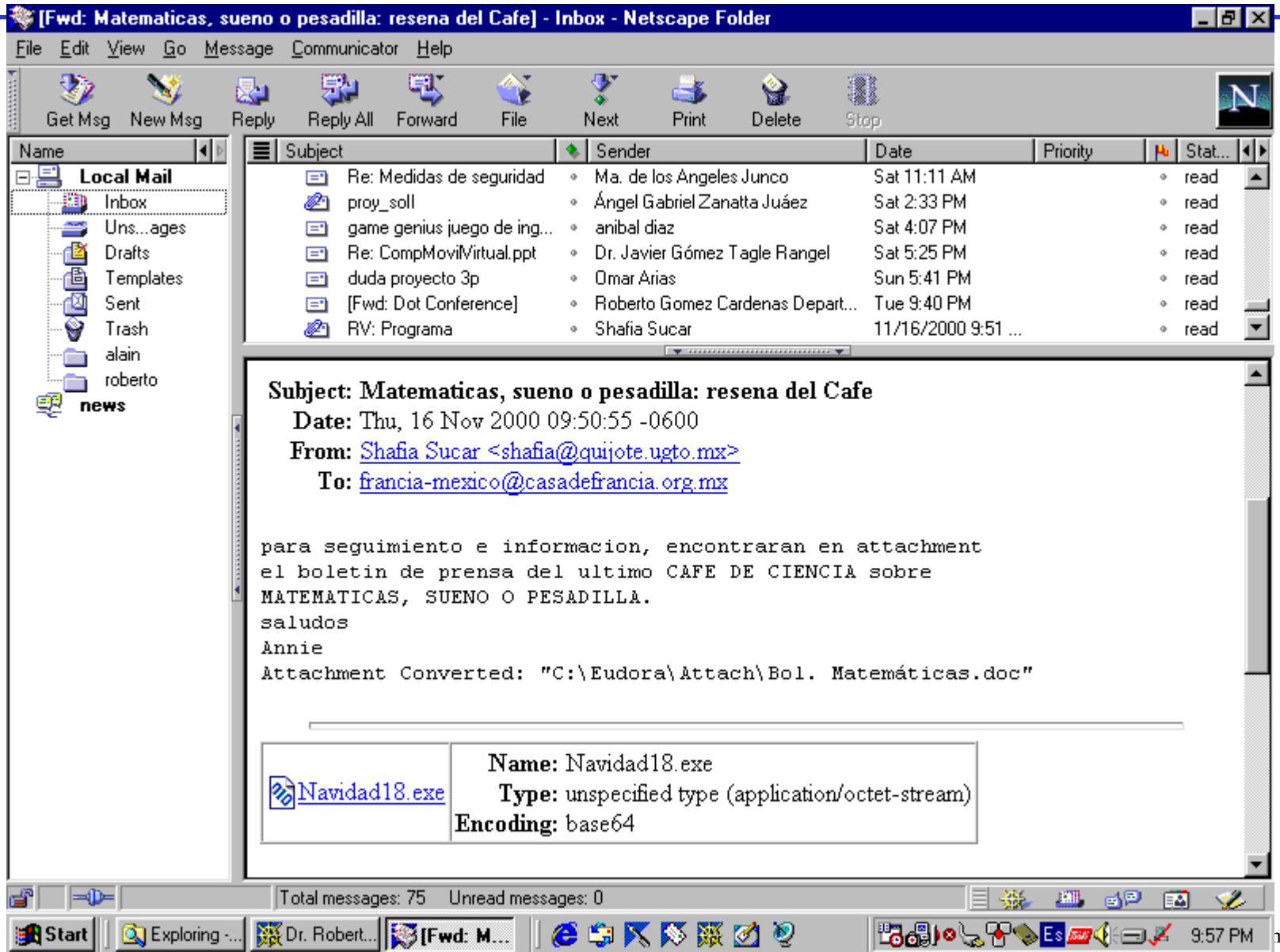
Variantes relacionadas con virus

- En ocasiones se habla de estas variantes como si se tratara de virus , cuando en realidad son conceptualmente diferentes.
- Algunos antivirus pueden detectarlos.
- Estas variantes son:
  - Troyanos
  - Gusanos
  - Bomba lógica

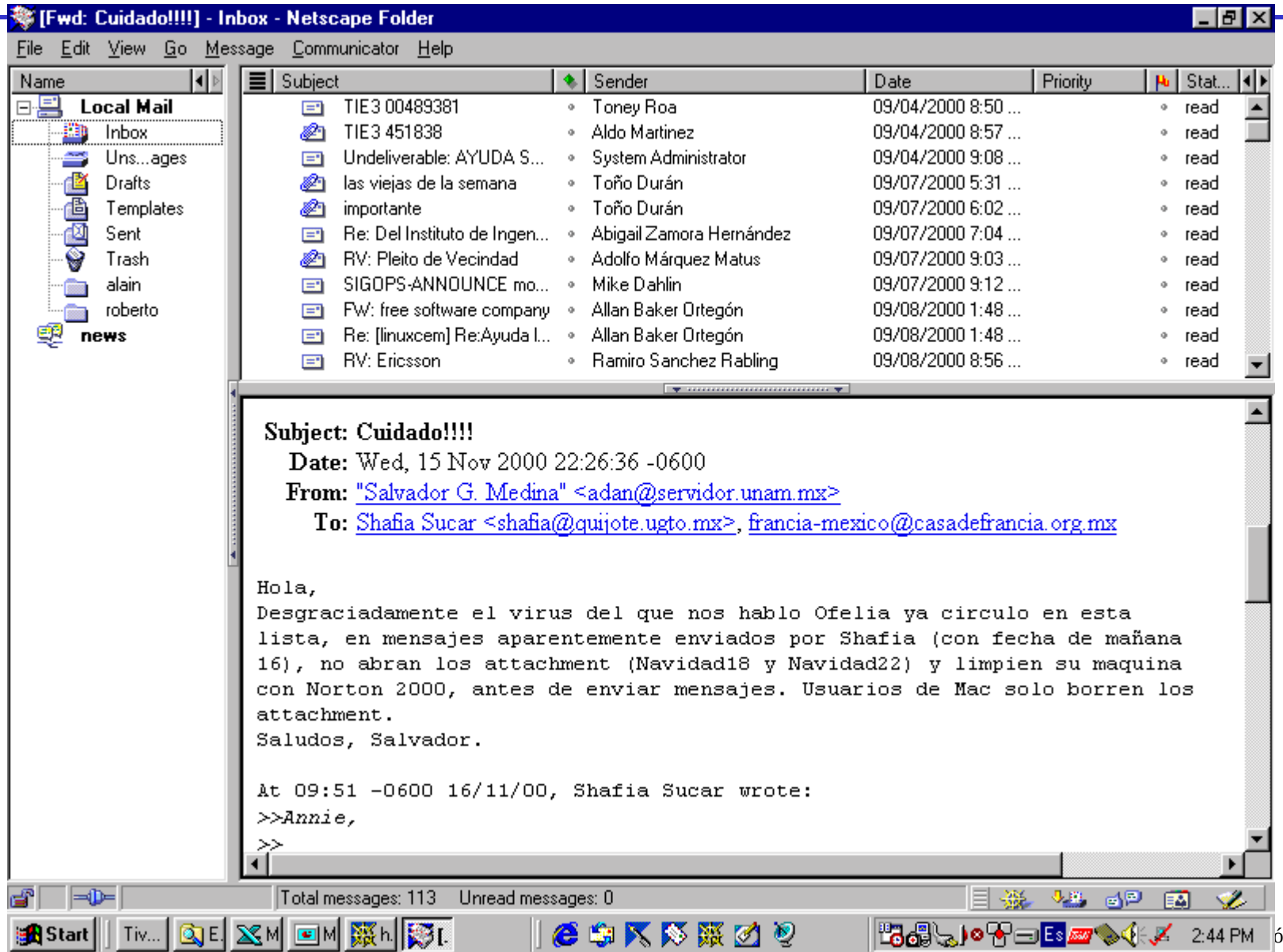
Los gusanos

Es un programa que produce copias de sí mismo de un sistema a otro a través de la red; en las máquinas que se instala, produce enormes sobre-cargas de procesamiento que reducen la disponiblidad de los sistemas afectados.

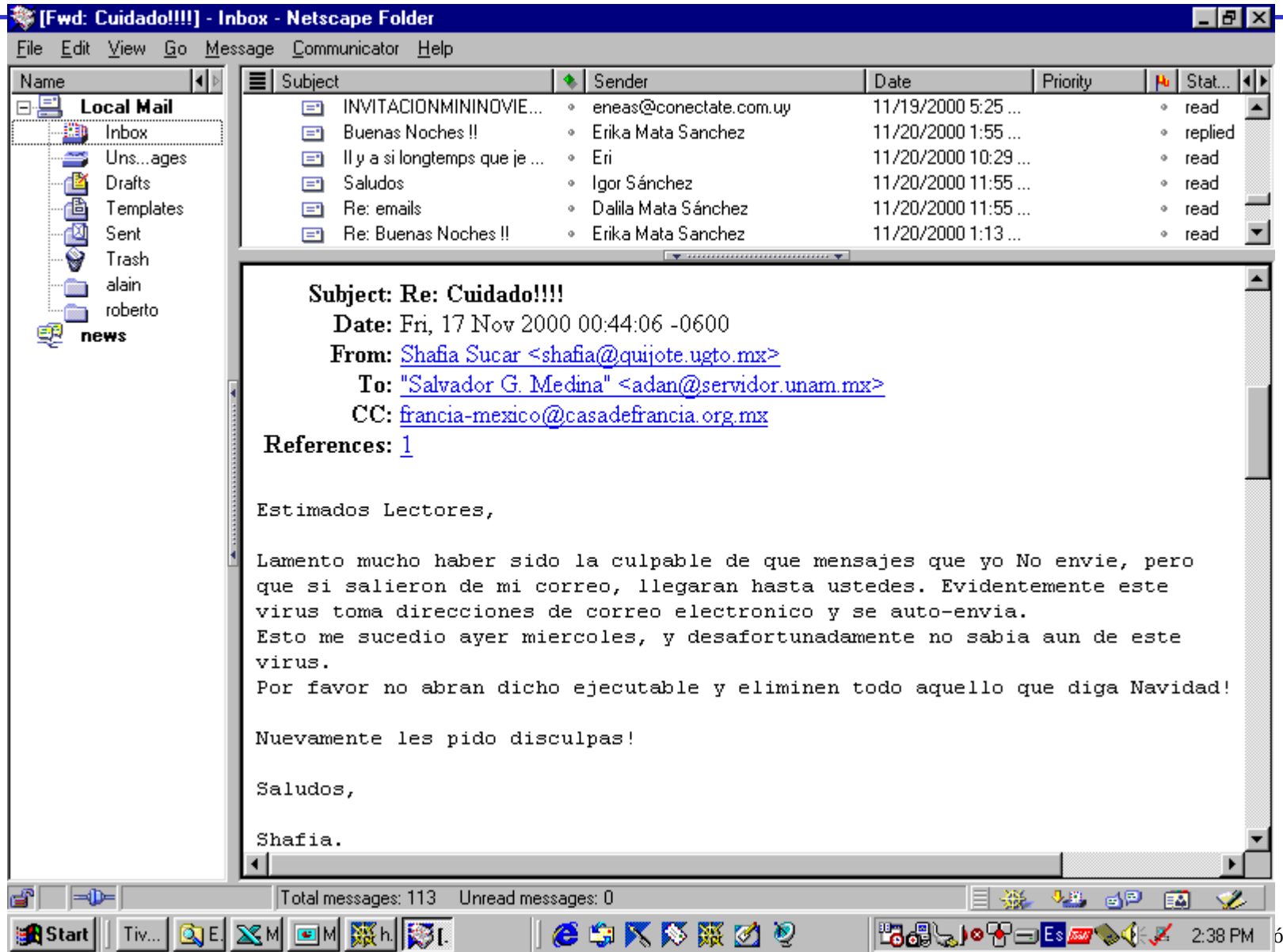
El gusano navidad.exe (1)



El gusano navidad.exe (2)



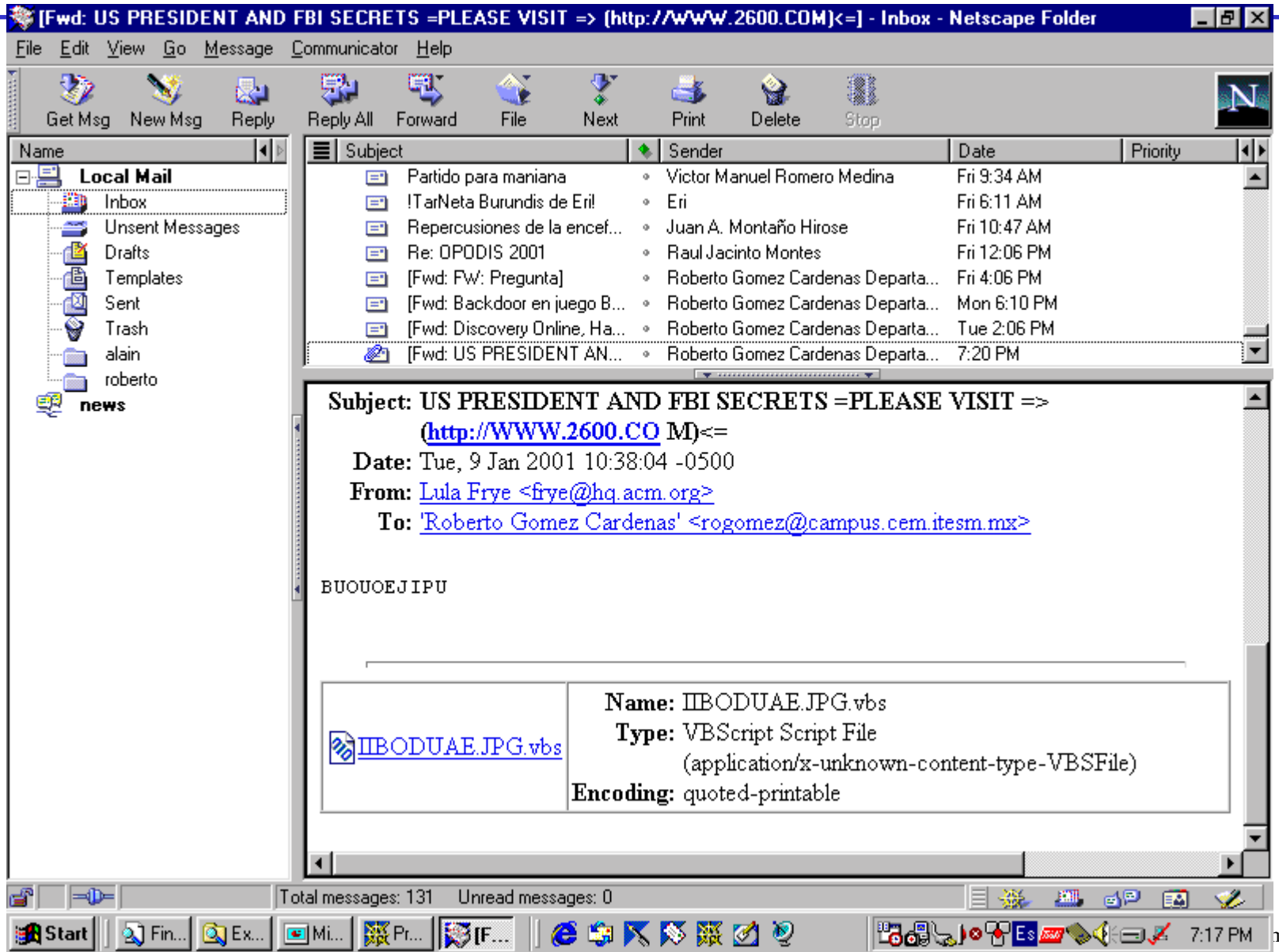
El gusano navidad.exe (3)



Lo bueno y lo malo de navidad

- Lo malo del Navidad es que contiene rutinas destructivas que se activan, al menos en teoría, el 25 de diciembre.
- Lo bueno es que debido a errores en el procedimiento de instalación, quizá nunca llegue a activarse la rutina destructora.
- Lo malo es que después de instalarse, no funcionará prácticamente ningún programa del usuario

Otro ejemplo virus/gusano



¿Cúal es el problema?

```
rem  ==========================================================
rem  "Plan Colombia" virus v1.0
rem  by Sand Ja9e Gr0w   (www.colombia.com)

rem  Dedicated to all the people that want to be hackers or crackers, in Colombia
rem  This program is also a protest act against the violence and corruption that
rem  Colombia lives  I always wanting that all this finishes, I have said...
rem  Santa fe de Bogotá 2000/09
rem  I dedicate to all you the song "GoodBye" of Andreas Bochelli
rem  ==========================================================
rem  Thanks God..!
rem  A greeting for "Lina María" from "Santa fe de Bogotá"
rem  A greeting for "Tizo" from "Spain"
rem  And One kicked of tail to my friends, "eL ChE" and "ThE SpY"

rem  okay, ok...
rem  my baby start here...
```

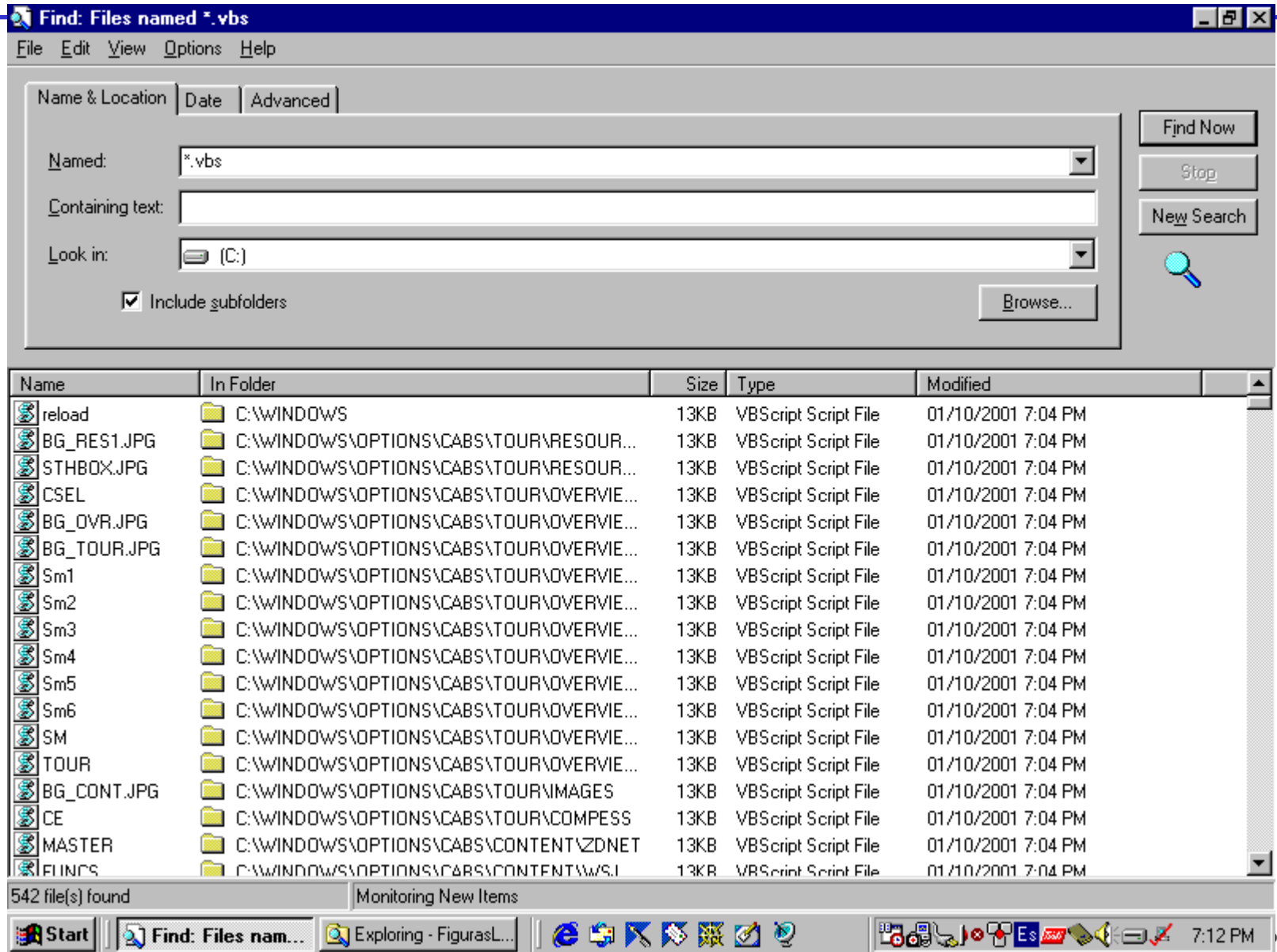
¿Y que hace?

```
if(ext="js") or (ext="jse") or (ext="css") or (ext="wsh") or (ext="sct")
                or (ext="hta") then
  set ap=fso.OpenTextFile(f1.path,2,true)
  ap.write vbscopy
  ap.close
  bname=fso.GetBaseName(f1.path)
  set cop=fso.GetFile(f1.path)
  cop.copy(folderspec&"\"&bname&".vbs")
  fso.DeleteFile(f1.path)
 else
   :
   :

rem  bye net connection ...              :-(
Set WSHNetwork=Nothing

end sub
```

Viendo las consecuencias ...



Precauciones a tomar con correos electrónicos

- Usar un antivirus
- Si recibe un correo, con un archivo en attach, de una fuente desconocida simplemente borrelo.
- Los virus y programas troyanos contienen código que es necesario ejecutar para poder infectar
  - si hace doble-click sobre un archivo que viene en forma de attach dentro de un correo, esta ejecutando código y puede infectar su máquina
  - ningún antivirus es capaz de “scanear” estos archivos antes de abrirse

Antivirus y vacunas

- Programa encargado de la detección de virus.
- Algunos intentan parar el virus en el momento en que se produce el ataque (sistemas de prevención)
  - la mayoría vigilan la entrada desde disco pero no desde internet
- Otros comprueban el código del programa antes de que se ejecute.
  - usuario puede ser avisado de los posibles peligros del programa que va a ejecutarse
  - el proceso se conoce vulgarmente como “escaneado”
- Una vacuna esta diseñada para limpiar un virus en concreto, solamente un virus

Por último, pero no menos importante

- Mantener al día el antivirus
  - algunos lo hacen de forma automática
- Nunca instalar y ejecutar más de un antivirus
- Usar sentido común
  - ¿vale la pena examinar lo que me llego por correo electrónico?
  - verificar el origen del correo
  - ¿conozco a la persona que lo envio?
  - ¿en realidad necesito el archivo que viene con el correo?
  - ¿acaso yo pedi dicho archivo?

Los plugins

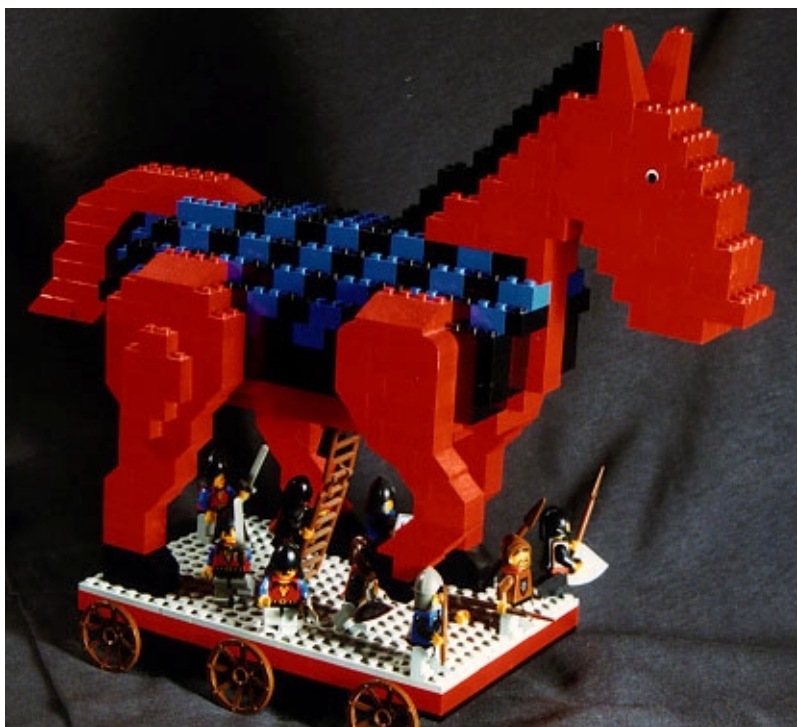
- Distribución de SW por Internet
- Plug-ins desarrollados por terceros diferentes a los creadores de los browsers, que toman el control de la máquina
- Ofrecen soporte de nuevos formatos de archivos y aplicaciones
  - acroread, real player, etc
  - fondos de pantalla
  - protectores de pantalla

Riesgos plugins

- Afectan configuraciones de otros productos ya instalados.
- Posibilidad de que el software realice más actividades que las originales.
  - caballos de troya
  - puertas traseras (backdoors, trapdoors)

El Caballo de Troya

- Objetivo principal: recuperación información confidencial de un organismo o un usuario.
- Se basa en substituir un programa de servicio común por uno alterado por el intruso para recuperar información.



Un ejemplo de caballo de Troya

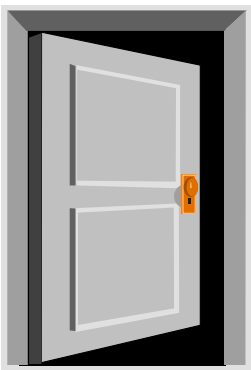
- El Caballo de Troya por login es uno de los más comunes.
- En este ataque, el usuario encuentra su estación de trabajo con una pantalla solicitándole su login.
- El usuario inadvertido teclea su login y su password como de costumbre; esta vez recibiendo un mensaje de error.

```
login: mbui
Password:
Login incorrect
```

Continuación del ejemplo

- En el segundo intento, el usuario logrará acceder al sistema.
- El no sabe que su password fue almacenado en algún archivo donde, más tarde, el creador del Caballo de Troya lo recuperará.
- El falso programa de login, después de almacenar el password robado, invoca el verdadero programa de login, dejando al usuario actuar con una nueva sesión de login.

Trapdoors, backdoors o puertas traseras



- Es frecuentemente creado por el diseñador del sistema; sin embargo, en ocasiones existe por accidente.
- Algunas veces es creado durante las pruebas de implementación de un sistema y después es olvidado.
- Otras veces, es usado por el proveedor para “atar” al cliente que compro dicho sistema.

Ejemplo puerta trasera

- Programa buscaminas de Windows 2000
- Correr Minesweeper, teclear “xyzzy” y presionar Shift + Enter.
- Buscar un pixel blanco en la parte superior izquierda de la pantalla
  - si no se ve configurar pantalla
  - conforme se mueve el raton por las celdas del buscaminas el pixel desaparece y aparece: desaparece cuando hay una mina en la celda y viceversa

Puerta trasera en buscaminas (1)

Puerta trasera en buscaminas (2)

Puerta trasera en buscaminas (3)

Puerta trasera en buscaminas (4)

Precauciones a tomar en cuenta

- Estar seguros de que en realidad se necesita el software
- No pueden proporcionarmelo en el área de sistemas.
- Preguntar si alguien más lo ha usado y si ha tenido problemas.
- De preferencia que se software recomendado por la misma marca del browser.

Hoax (engaño, burla, petardo)

- Tipicamente son alertas de peligro, o peticiones de ayuda, empezadas por gente maliciosa - y divulgadas por usuarios inocentes que piensan que estan ayudando a la comunidad al espacir la advertencia.
- El incremento de virus y programas troyanos muchos usuarios han usado Internet como un medio para alertar a amigos y colegas de trabajo acerca de estos menesteres.

Algunos ejemplos de hoax

- A Virtual Card For You
- A.I.D.S. Virus Hoax
- ANTHRAX Virus Hoax
- Anticristo Virus Hoax
- AOL4FREE
- ASPARTAME HOAX
- Big Brother Hoax
- BLOAT VIRUS HOAX
- BUDSAVER.EXE
- SULFNBK Hoax
- Win A Holiday
- Celulares Hoax
- D@fit Hoax
- Dangerous HIV Hoax
- Death Ray
- Deeyenda Virus Hoax
- NEW YORK BIG DIRT HOAX
- Perrin Hoax
- PIKACHUS BALL HOAX
- PKZ300 Warning

1er. ejemplo Hoax

Mr. Xxxxx wrote:

Unanse a esta buena causa:

SE TRATA DE LA PEQUEDA LLAMADA JESSICA MYDEK TIENE SIETE ANOS DE EDAD Y SUFRE DE UN AGUDO Y MUY RARO CASO DE CARCINOMA CEREBRAL ESTA ENFEREMEDAD TERMINAL PROVOCA LA APARICION DE DIVERSOS TUMORES MALIGNOS EN EL CEREBRO.

LOS DOCTORES LE HAN PRONOSTICADO A JESSICA SEIS MESES DE VIDA, Y COMO PARTE DE SUS ULTIMOS DESEOS ELLA QUIZO INICIAR UNA CADENA DE E-MAILS INFORMANDO DE SU CONDICION Y ENVIAR EL MENSAJE A LA GENTE PARA QUE VIVA AL MAXIMO Y DISFRUTEN DE CADA MOMENTO DE SU VIDA, UNA OPORTUNIDAD QUE ELLA NUNCA TENDRA.

ADICIONALMENTE, LA SOCIEDAD AMERICANA DE LUCHA CONTRA EL CANCER, JUNTO CON OTRAS EMPRESAS PATROCINADORAS, ACORDARON DONAR TRES CENTAVOS QUE SERAN DESTINADOS A LA INVESTIGACION DEL CANCER POR CADA PERSONA QUE ENVIE ESTE MENSAJE. POR FAVOR, DENLE A JESSICA Y A TODAS LAS VICTIMAS DEL CANCER UNA OPORTUNIDAD.

1er. ejemplo Hoax (cont)

Lo unico que tienen que hacer para incrementar el numero de personas en esta cadena es:

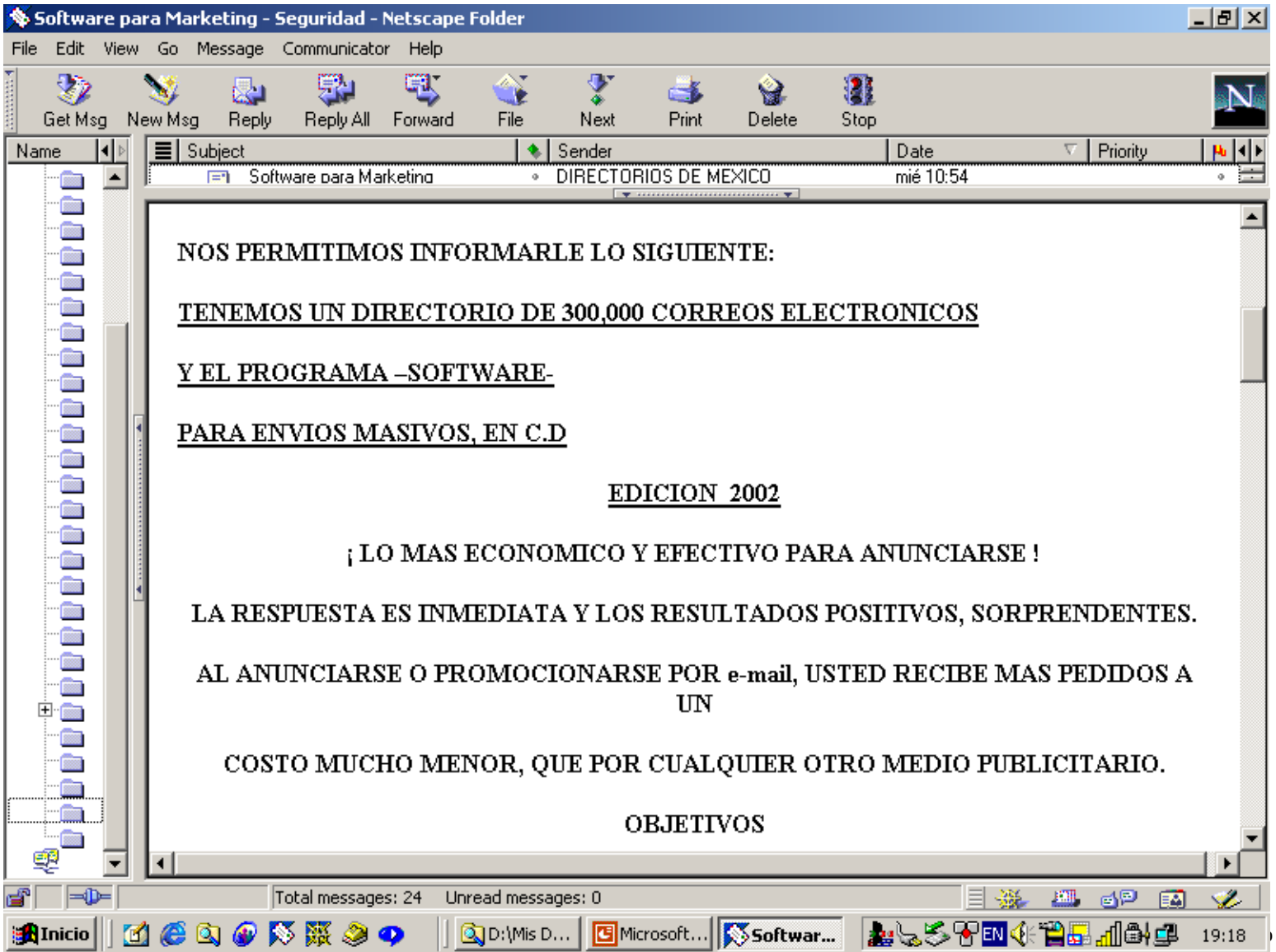
Primero: dirija este e-mail a ACS@aol.com

Segundo: en la parte donde dice CC agregue los e-mails de todos los amigos y colegas que conozca

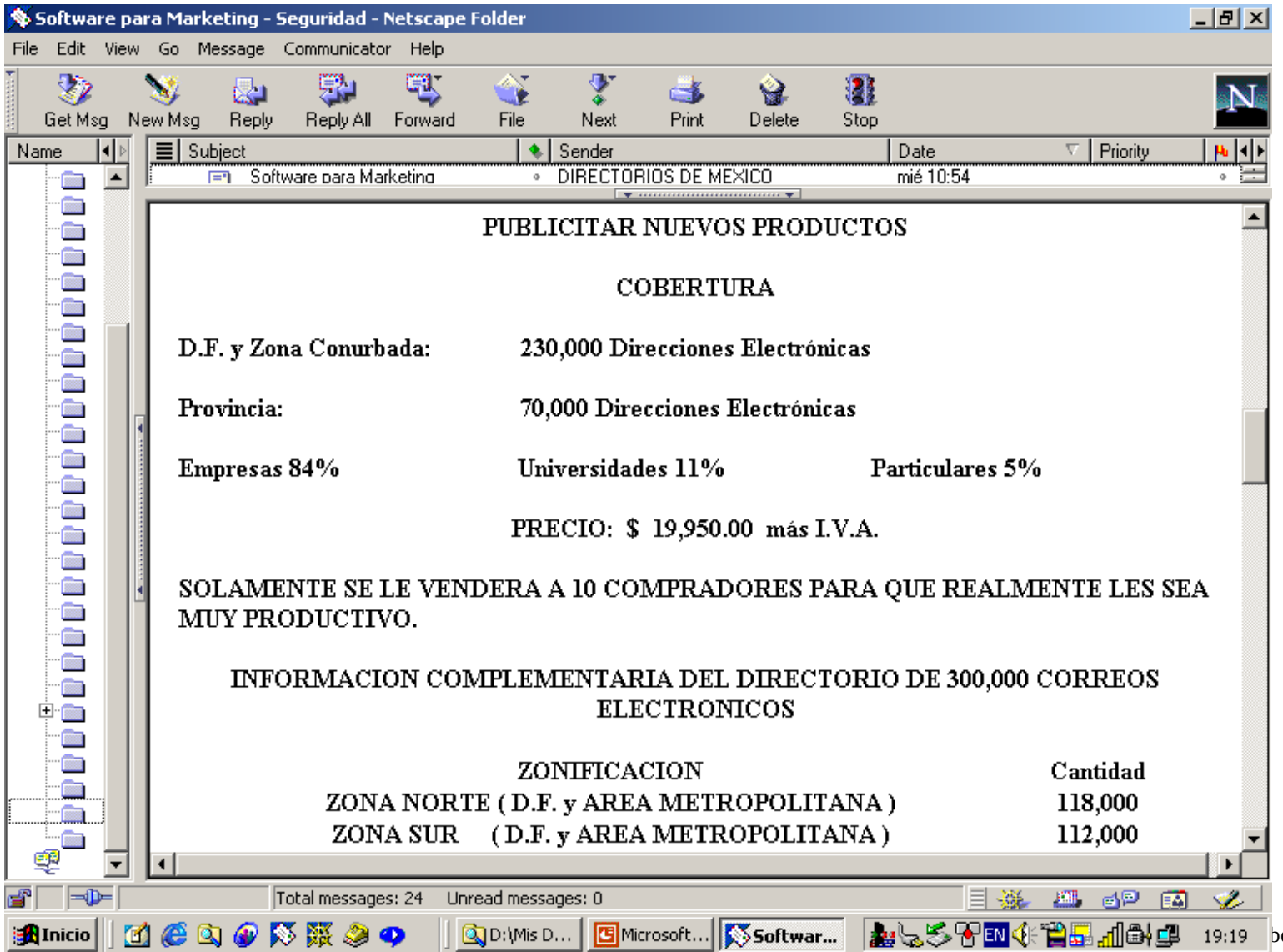
Saludos cordiales,

Alfonso

¿Y para que quiere alguien direcciones electrónicas?



¿Y eso es negocio?



2do. ejemplo hoax

Este reenvio lo recibí de un amigo hoy y es verdad lo busqué con estas instrucciones y lo encontré,lo tenía sin saberlo.
No lo detecta el Norton 2001 ni McAfee, los tengo instalado y pasó igual Un virus está llegando a través de los mails de modo oculto.
Gracias a un aviso pude detectarlo (lo tenía sin saberlo) y eliminarlo.
Buscarlo del siguiente modo:

1. Ir a Inicio
2. Luego: Buscar
3. Archivo o carpeta
4. Tipear el archivo: sulfnbk.exe
5. Eliminar (NO ABRIRLO)
6. Eliminar de la papelera de reciclaje

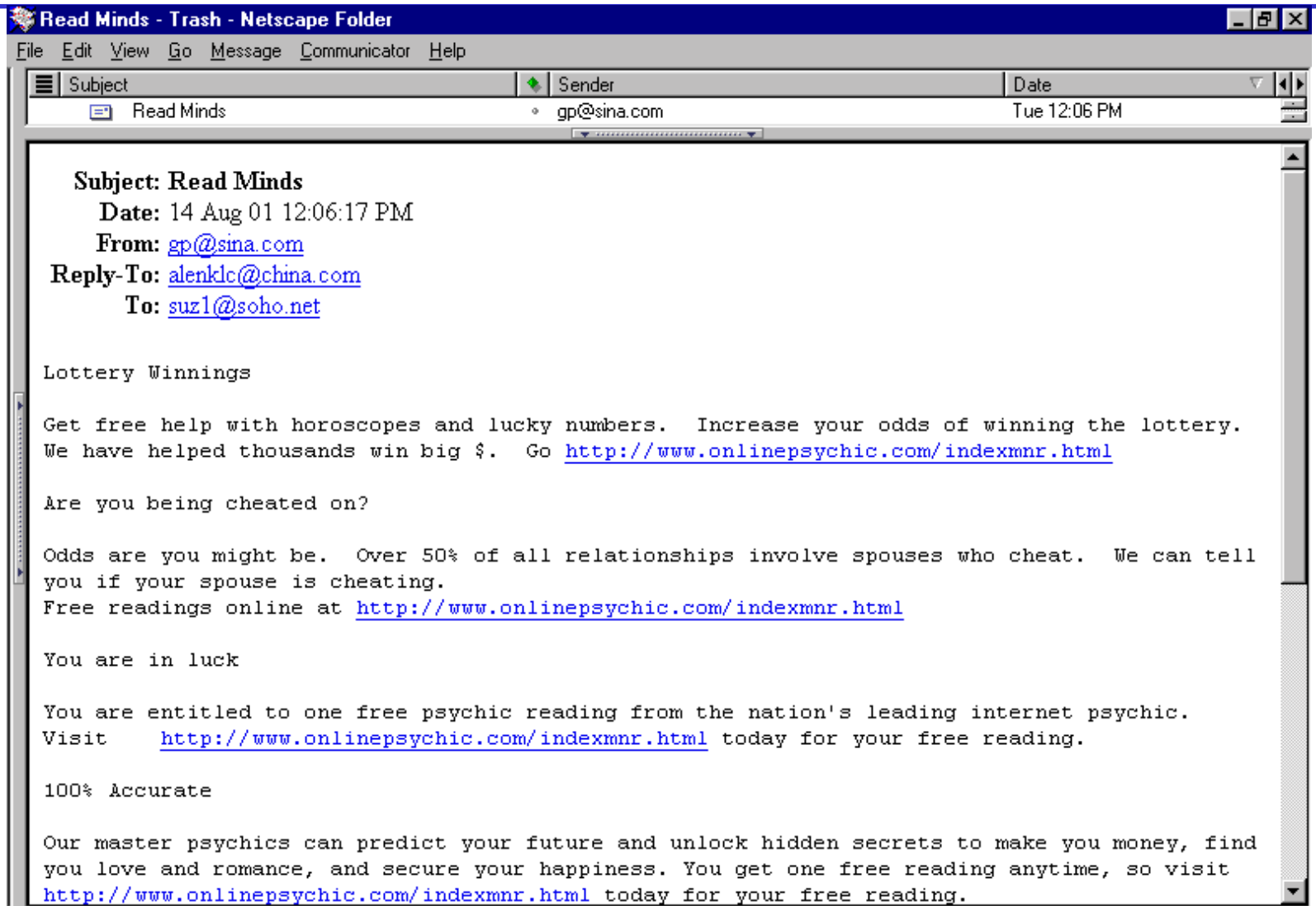
Gracias a estas instruciones lo eliminé..

suerte..

Spam

- Intento de entregar un mensaje, a través de Internet, a una persona que de otra forma no hubiera elegido recibirlo.
- Cada vez recibimos más correos no deseados:
  - Ventas.
  - Insultos.
  - Bombardeos.
  - Pornografía
  - Hoax

Ejemplo spam



Aclaración sobre SPAM

¿Qué hacer con los hoaxes/spams?

- No redireccionar mensajes de este tipo.
  - sistema correo puede colapsar debido al redireccionamiento de este tipo de mensajes
- Los corporativos pueden confrontar este tipo de problemas, con un politicas del estilo:
  - usuarios finales no deben difundir alertas de viurs
  - cualquier informe de virus se debe enviar al departamento de sistemas de información

Ingeniería Social.

Es una de las formas más comunes para penetrar sistemas de “alta seguridad”.

- Uso de trucos psicologicos, por parte de un atacante externo, sobre usuarios legitimos de un sistema para obtener información (usenames y passwords) necesaria para acceder a un sistema.
- Se basa en ataques como: usurpación de identidad, pepena, inocencia de la gente, relaciones humanas, etc.

Ejemplo ingeniería social

"Hi Bev, this is Sam from the IS Department. We just got in a new corporate screensaver and since you're the VP's secretary you will get it first. It's really cool wait 'till you see it. All I need is your password so I can log on to your PC from the computer center and install it.

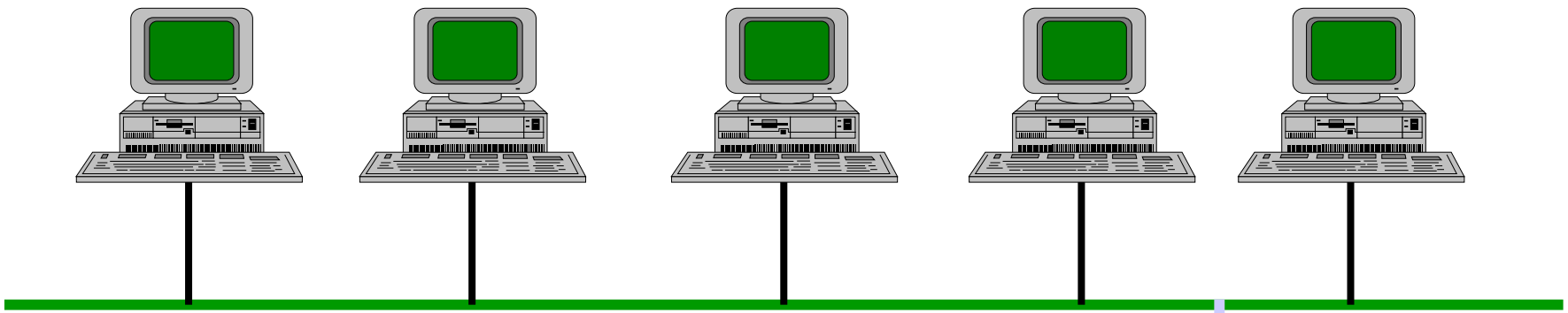
Oh Great!!!!! My password is rover. I can't wait to see that new screen saver!!!!!"

Medidas a tomar

- Verificar la identidad de la persona con la que estamos conversando.
- Verificar la información transmitida con las fuentes
- Reportar cualquier anomalia

Sniffers

¿Cómo se comunican dos computadoras en una red local?

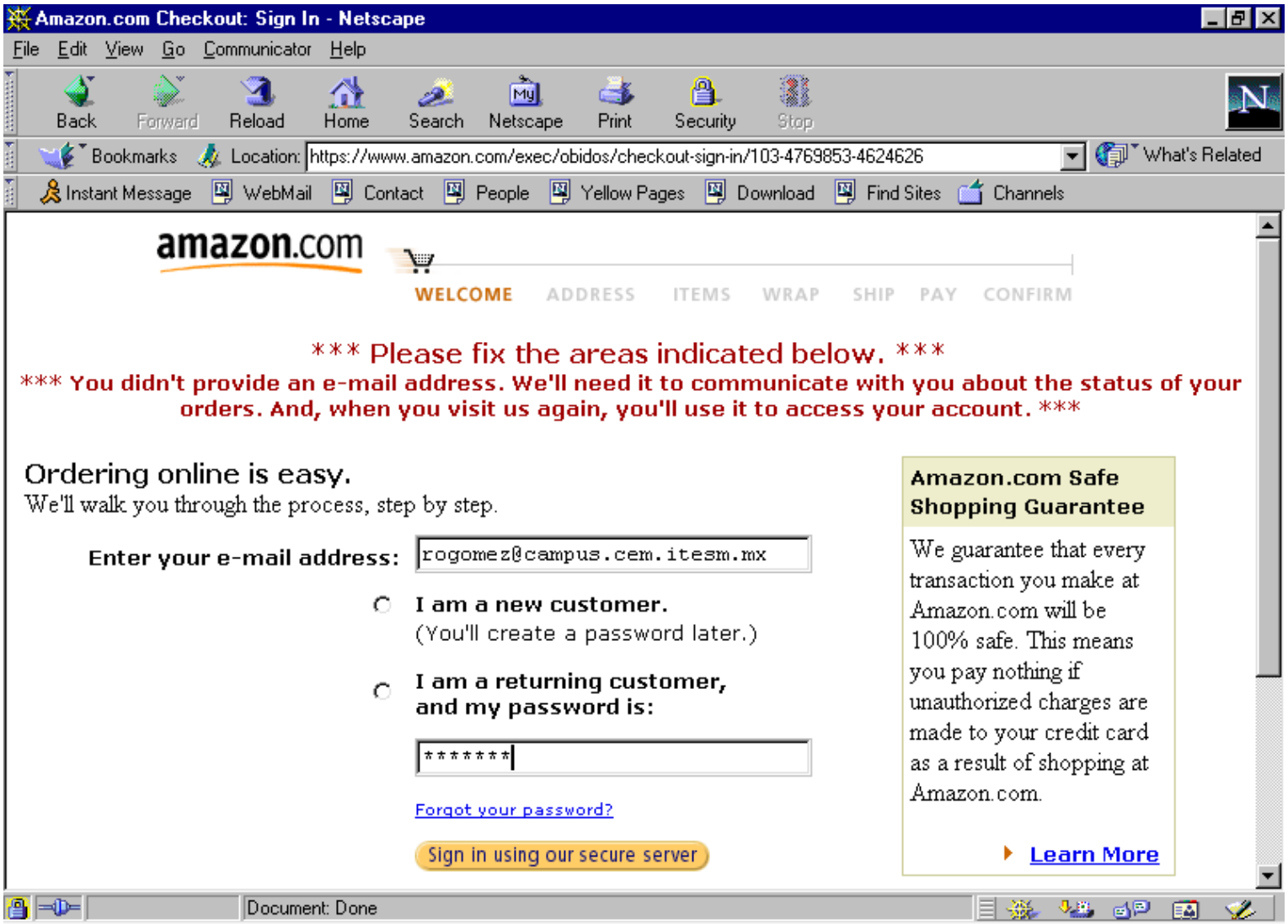


computadora en
modo promiscuo

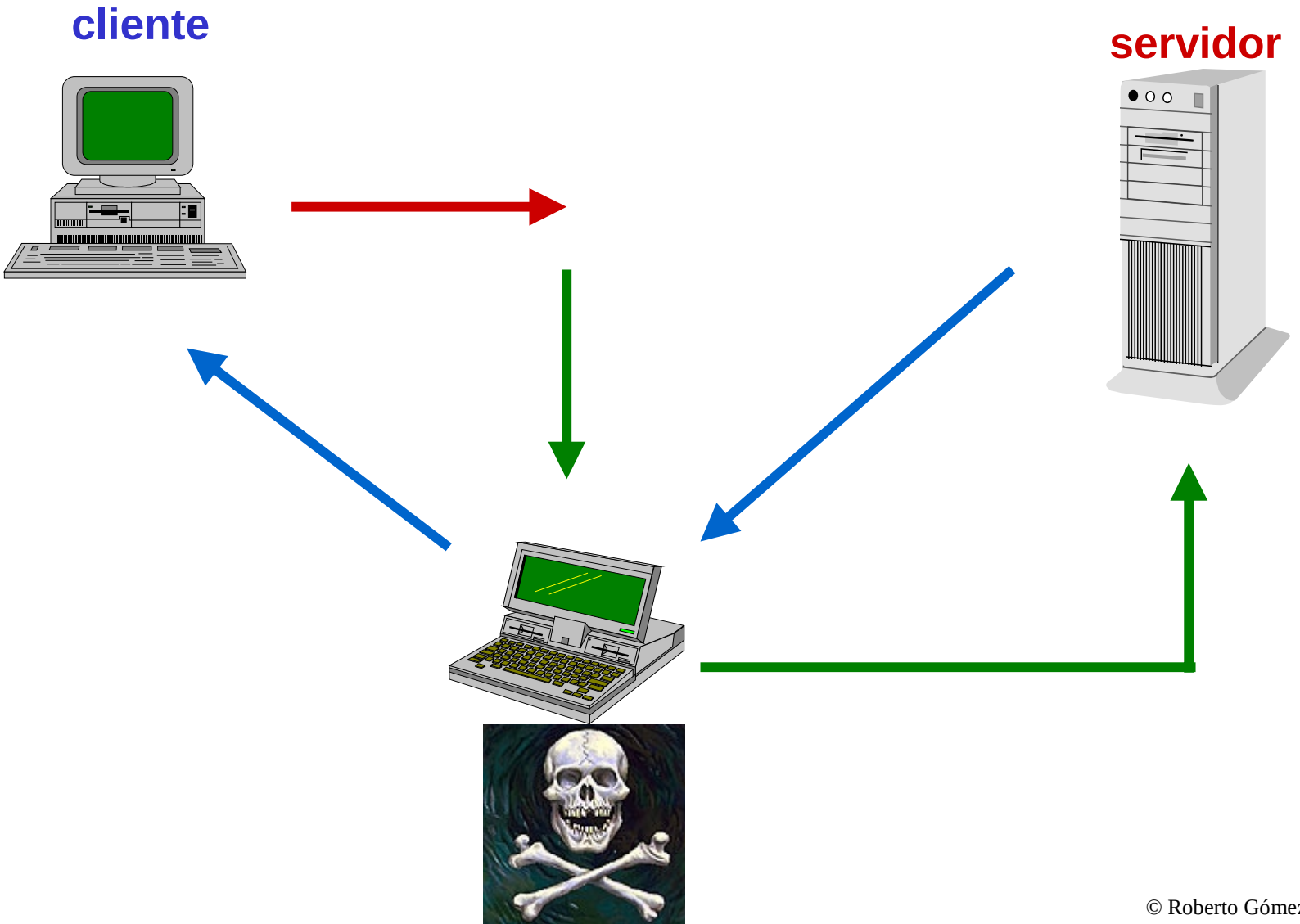
snifeando (husmeando)

Protocolos transmisión encriptados

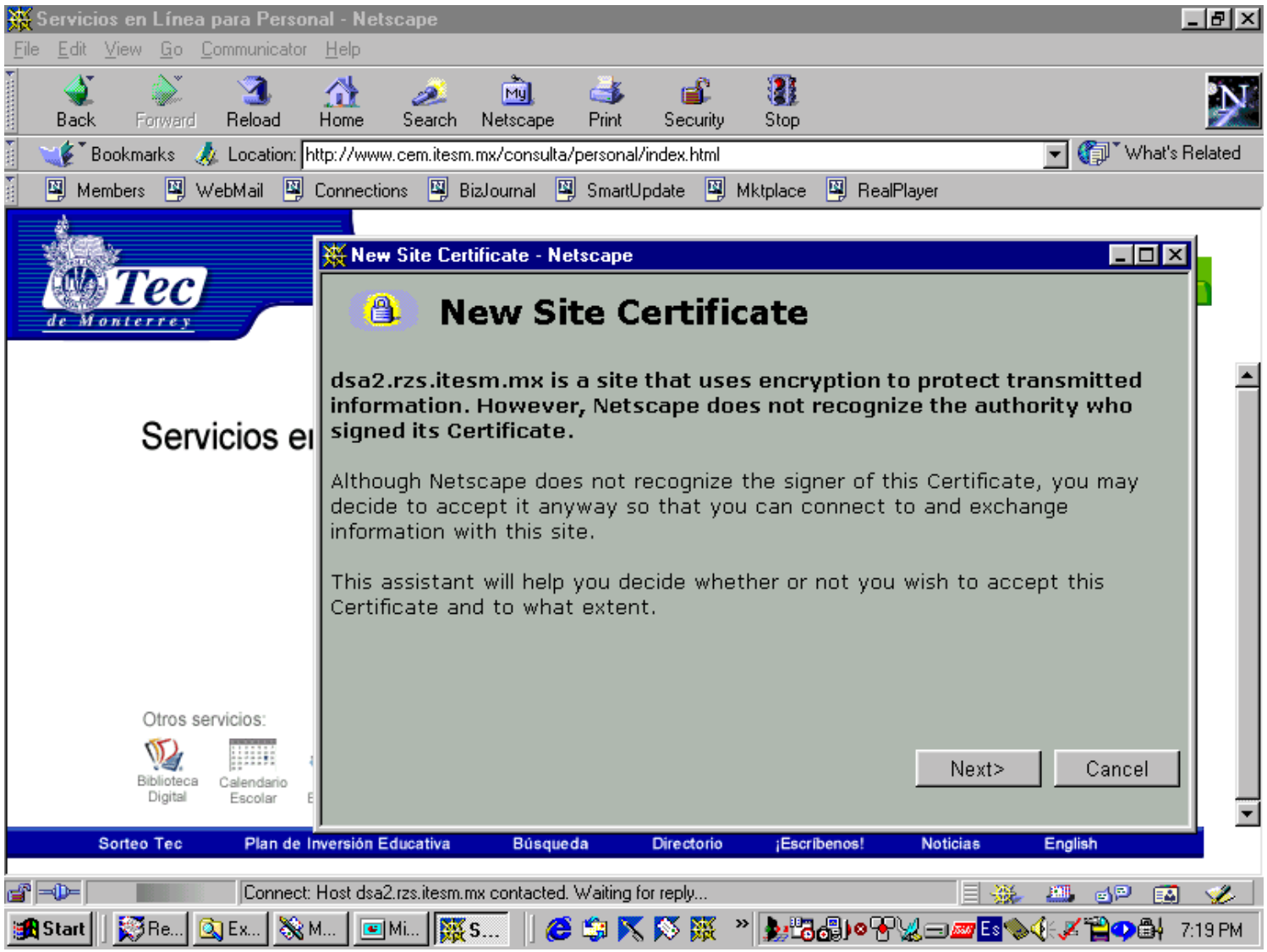
Protocolos transmisión encriptados



Spoofing



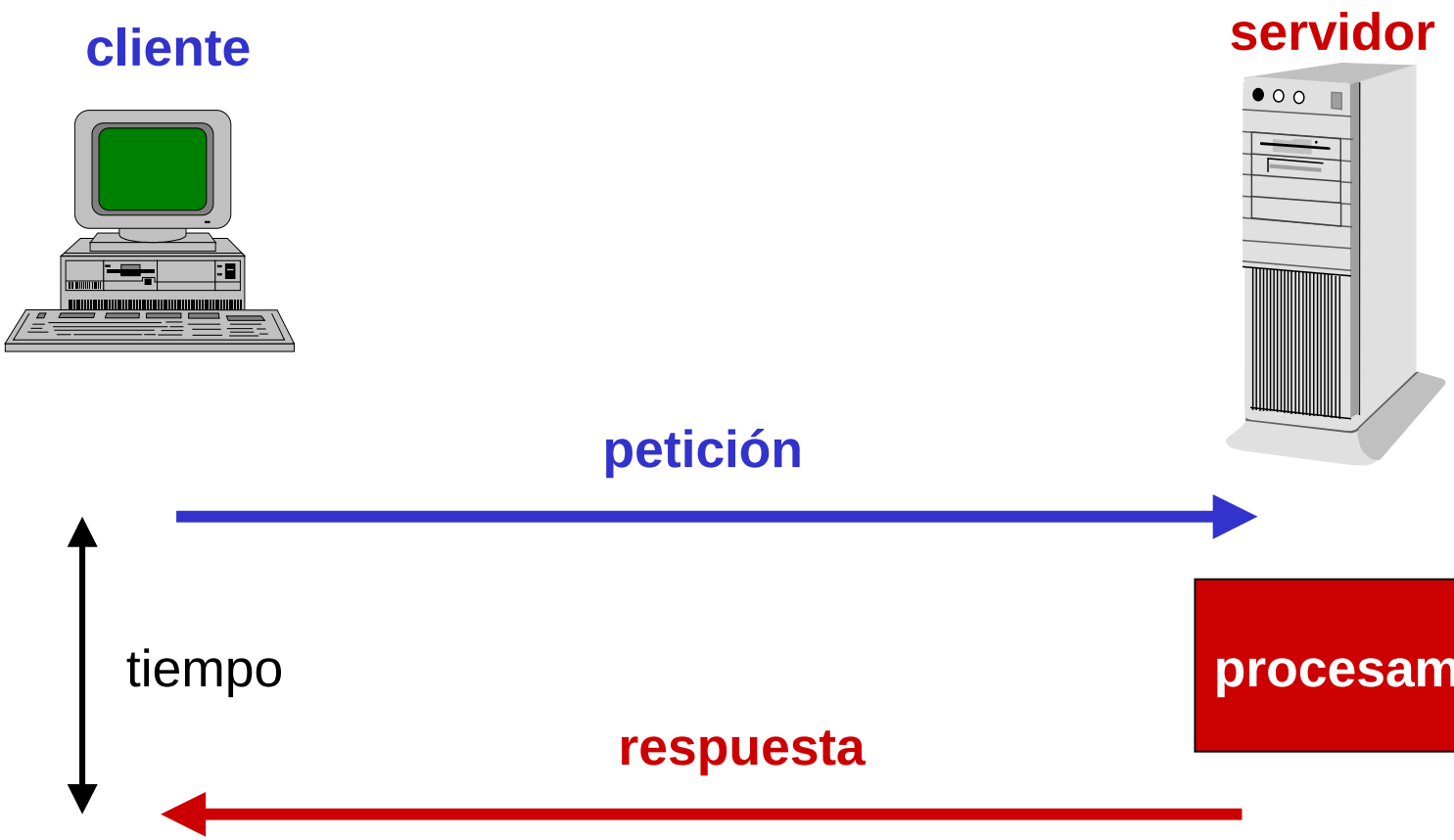
Los certificados



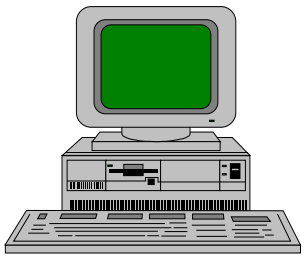
El código móvil

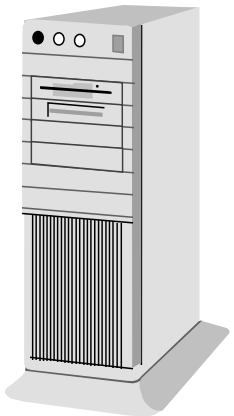
- Los *browsers* son la herramienta que usan los usuarios para nevegar por internet.
- Dos elementos fundamentales en internet:
  - cliente: el que realiza la busqueda de información
  - servidor: el que coloca la información en algun servidor
- Cuando la aplicación en el servidor es muy pesada
  - preferible realizar el trabajo en el cliente
  - desempeño (tiempo respuesta) mejora bastante
- Dos técnologias:
  - active x
  - los applets de java

El esquema cliente/servidor



¿Y si el procesamiento es grande?





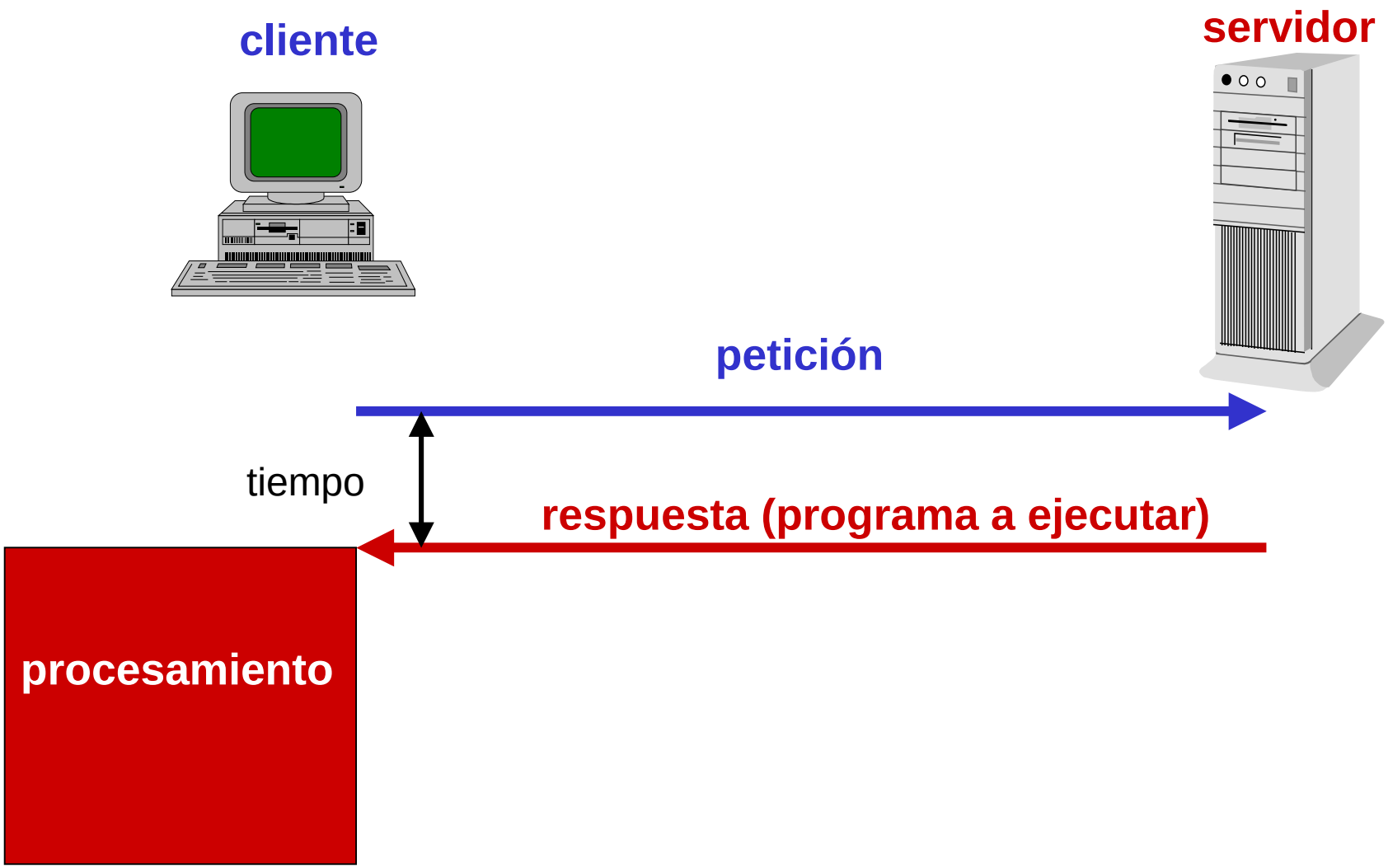
petición

tiempo

procesamiento

respuesta

Prefiero que se haga en el cliente



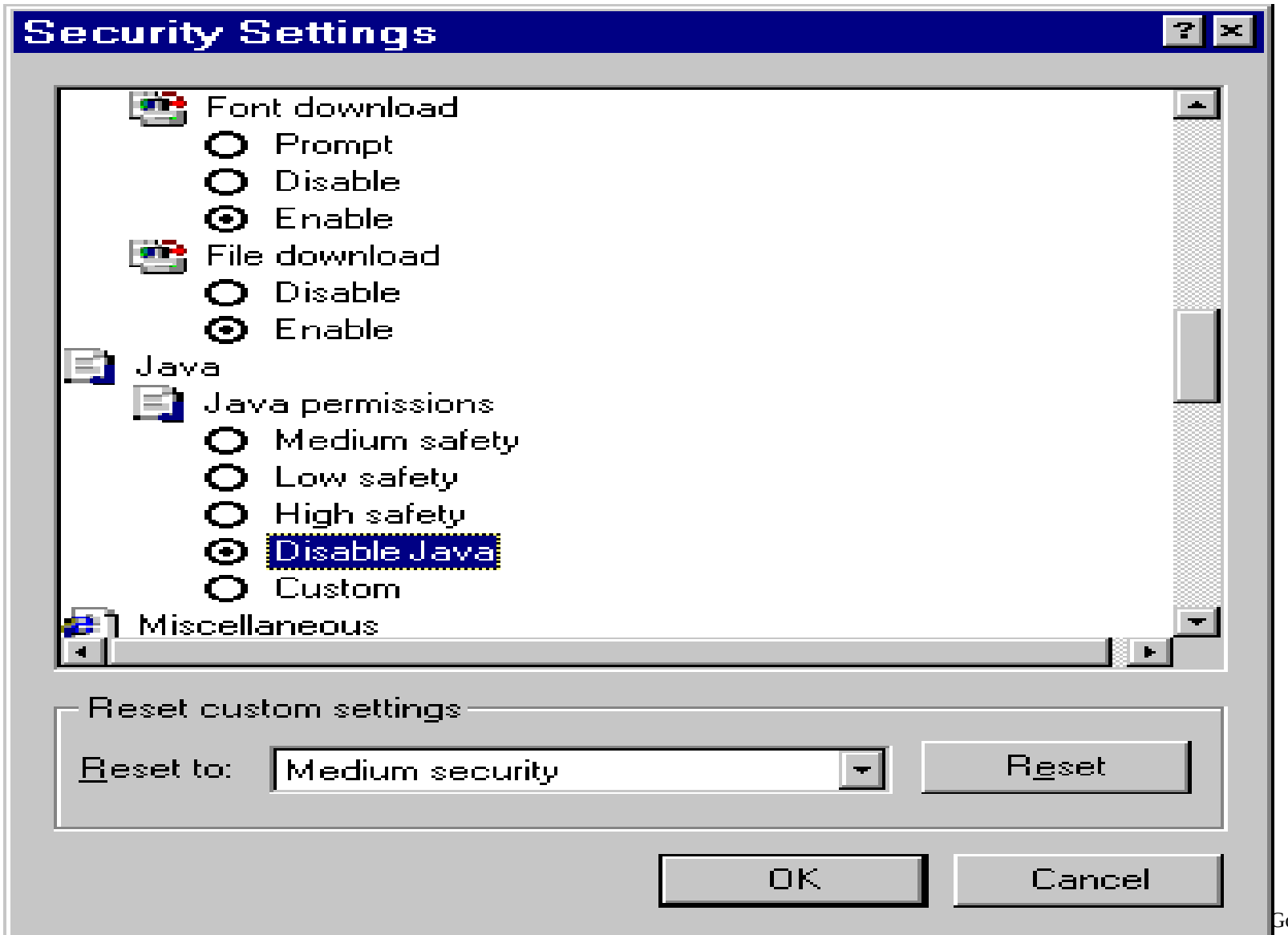
¿Qué pueden llegar a hacer?

- Pueden leer o escribir en el sistema de archivos del cliente.
- Pueden realizar conexiones a red del host original.
- Pueden iniciar programas en el cliente.
- Pueden realizar llamadas a métodos definidos en el cliente.
- Recomendación: configuración del browser

Las cookies

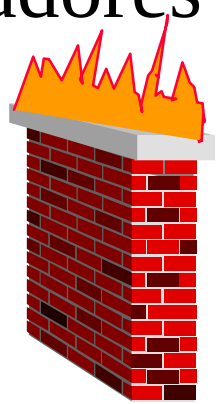
- Es información que un sitio Web escribe en el disco duro, de tal forma que pueda recordar algo acerca del usuario tiempo después.
- Tecnicamente:
  - información para uso futuro almacenada por el servidor en el cliente
- Su ubicación depende del browser.
- Permite al servidor almacenar información acerca del usuario en su propia máquina.
- Principal problema: privacidad

Configuración Microsoft Internet Explorer



Otros mecanismos

- Firewalls
- Proxies
- IDS
- Biométricos
- Tarjetas Inteligentes
- Analizadores de Vulnerabilidades



Referencias

- *Hacking Exposed*; McClure, Scambray y Kurtz, Mc. Graw Hill
- *Unix System Security*; D.A. Curry, Addison Wesley
- *Seguridad en Windows 2000*; Jeff Schmidt, Pearson Education
- *Network Intrusión Detection*; Northcutt, Ed. New Riders, 2da. edición
- *Network Security*; Kaufman, Perlman y Speciner, Ed. Prentice Hall

Referencias

- *Applied Cryptography Protocols, Algorithms and Source in C*; B. Schneier, John Wiley & Sons
- *Firewalls and Internet Security*,William R. Cheswick and Steven M. Bellovin, Addison Wesley Professional Computing Series, 1995, 5a, edición.
- *Practical Unix & Internet Security*, S. Garfinkel, G. Spafford, O'Reilly, 1996, 2da. edición
- Revista: Sys Admin Unix Journal
- Revista: Dr. Doob's

Algunas ligas interesantes

- http://www.securityfocus.com
- http://www.cert.org
- http://www.sans.org
- http://www.kriptograma.org
- http://www.packetstorm.com
- http://www.snort.org
- http://www.tripwire.com
- http://www.linux.org
- http://www.microsoft.com
- http://webdia.cem.itesm.mx/dia/ac/rogomez

Conclusiones

- Los ataques existen, no es ficción.
- La información corre peligro.
- Es importante estar consciente de lo anterior y tomar acciones al respecto.
- La seguridad al 100% no existe, todo es posible franquear.
  - se trata de dificultar la tarea del intruso

Más conclusiones

- La seguridad nunca es negra o blanca y el contexto cuenta más que la tecnología.
- No porque un sistema operativo no protega contra granadas de mano, este no sirve
  - solo implica que no podemos deshacernos de nuestras paredes, ventanas y puertas
- Diferentes tecnologías de seguridad tienen lugares importantes en una solución general de seguridad.

Más conclusiones

- El termino seguridad no tiene sentido fuera de contexto.
  - un sistema puede ser seguro mientras ciertos avances matemáticos no ocurran, o por un periodo de tiempo, o contra ciertos tipos de ataques.
  - un sistema puede ser seguro contra el criminal promedio, o contra cierto tipo de espionaje industrial, o contra una agencia nacional de inteligencia con un cierto conjunto de habilidades.

¡Gracias por su atención!

Panorama de la Seguridad en Redes

Roberto Gómez Cárdenas

rogomez@campus.cem.itesm.mx

http://webdia.cem.itesm.mx/dia/ac/rogomez

La invencibilidad depende de uno mismo; la vulnerabilidad del enemigo, de él.

La invencibilidad reside en la defensa; la posibilidad de la victoria en el ataque.

Sun Tzu, "El arte de la guerra"