Seguridad en Red

Javier Sánchez-Arévalo Díaz <arevalo@gul.uc3m.es>

7 de Abril de 2006

Grupo de Usuarios de Linux de la Universidad Carlos III de Madrid

Presentación

...

- ¿Quien soy?
- ¿De que va este curso/**charla**?
- Objetivos:
  - Poner de manifiesto la importancia de la seguridad de las redes de comunicaciones
  - Conocer algunas de las debilidades de los protocolos más frecuentemente utilizados, las herramientas y técnicas para atacarlos, y los medios de que disponemos para protegernos.

Índice (I)

Índice (II)

- Técnicas avanzadas
- Recomendaciones generales
  - Actualización del sistema
  - Sentido común
- Conclusiones
- Bibliografía/Referencias

Introducción

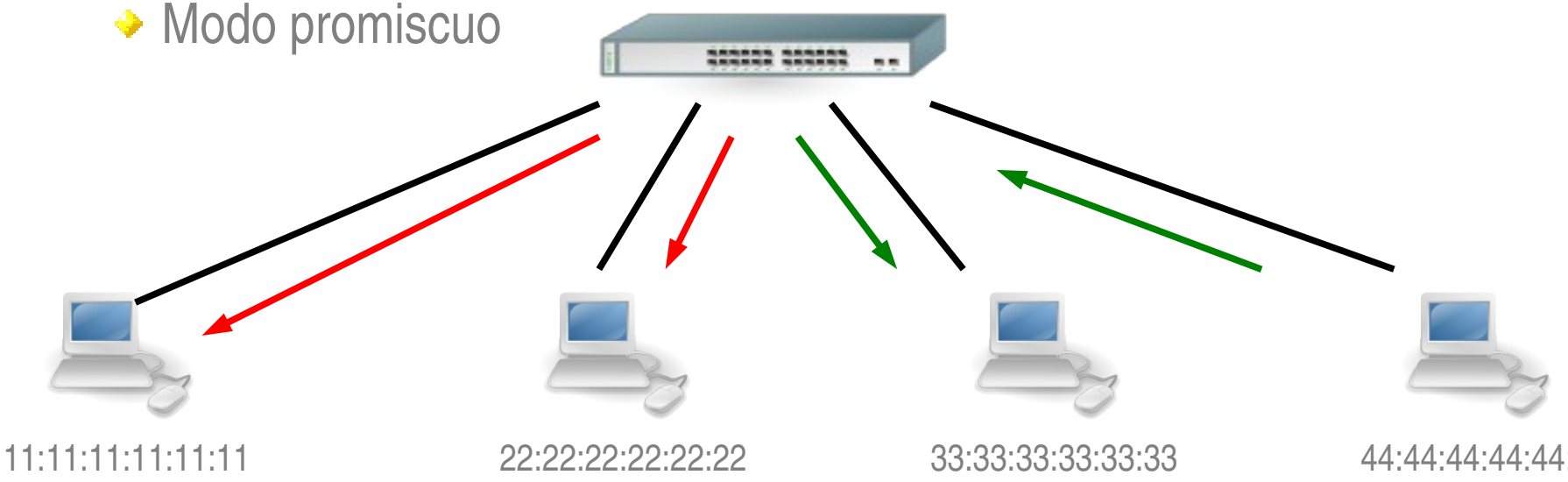
- Torre de protocolos

Niveles superiores (N5-N7)	HTTP, FTP, Telnet, SSH.
Nivel del transporte (N4)	TCP/UDP
Nivel de red (N3)	IP
Nivel de enlace (N2)	Ethernet
Nivel físico (N1)	100BASET, DSL, ISDN

Seguridad a Nivel 2

- Hubs
  - Que es. Como funciona
  - Problemas de seguridad
    - Escuchado de tráfico ajeno
  - Técnica
    - Modo promiscuo

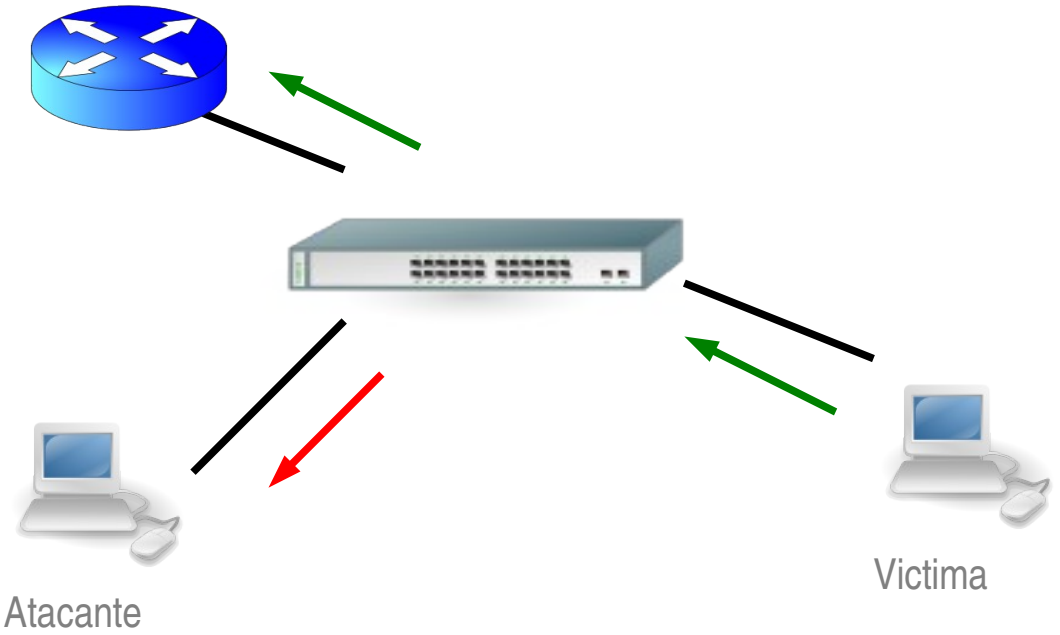
Eth src: 44:44:44:44:44:44
Eth dst: 33:33:33:33:33:33



Seguridad a Nivel 2

- Hubs
  - Herramientas: sniffit, dnsiff, webspy, urlsnarf,...
  - Detección de interfaces en modo promiscuo

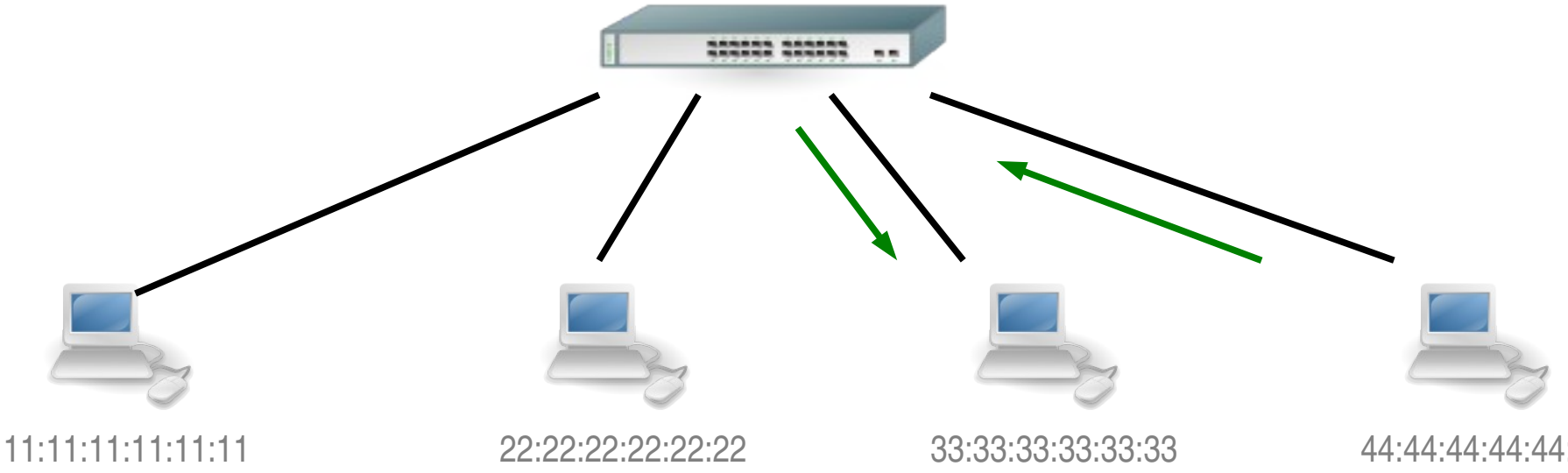
DEMO



Seguridad a Nivel 2

- Switchs
  - Que es. Como funciona
  - Problemas de seguridad
    - Falsa sensación de seguridad

Eth src: 44:44:44:44:44:44
Eth dst: 33:33:33:33:33:33



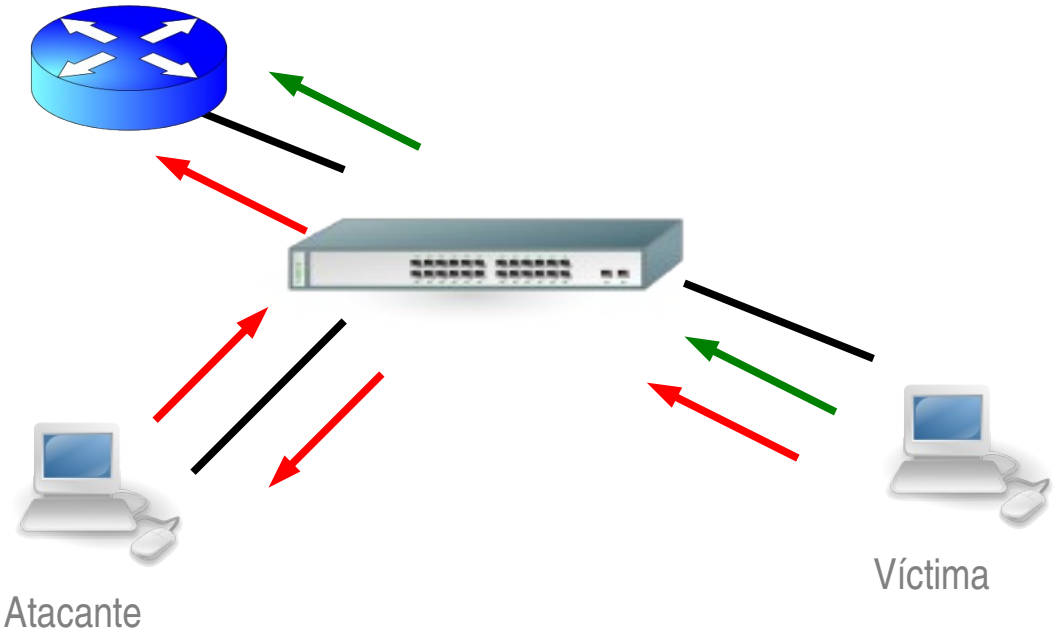
Seguridad a Nivel 2

- Switchs
  - Posibles ataques
    - Engaño a la víctima (Envenenamiento de tabla ARP)
    - Saturación del switch
  - Posibles soluciones
    - Fijado de direcciones MAC en puertos (PortSecurity)
    - Sólo una MAC por puerto
    - Uso de private VLANs (Protected ports)
    - Uso de 802.1x

Seguridad a Nivel 2

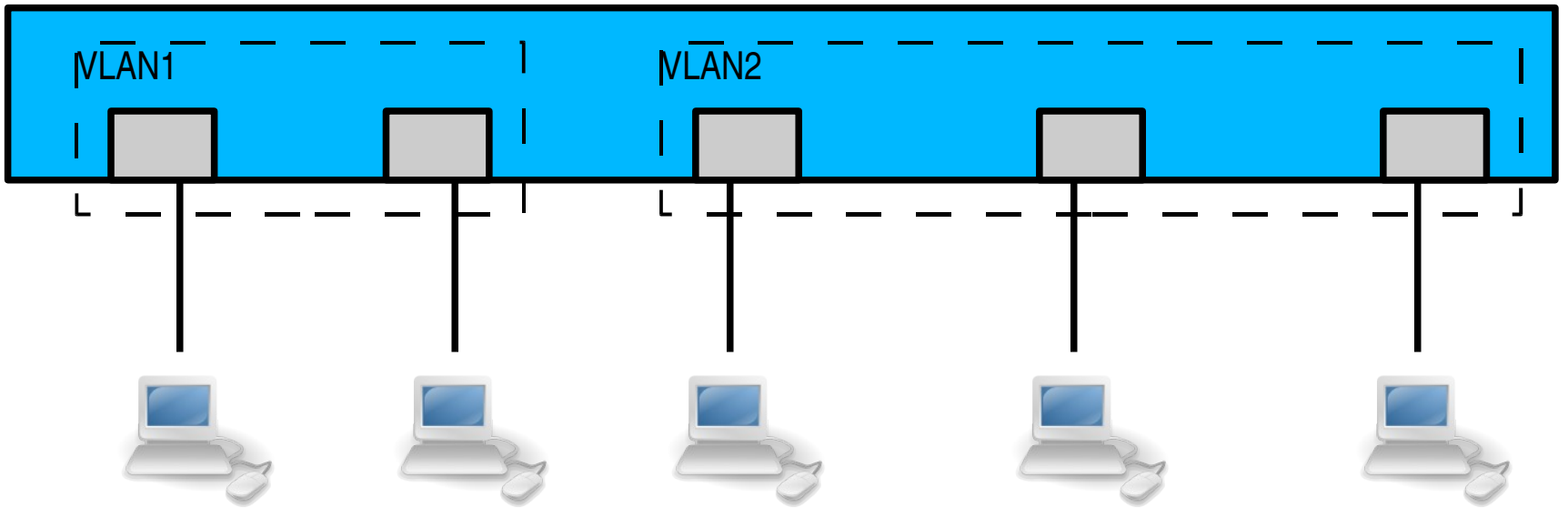
- Switchs
  - Técnica: Envenenamiento de tablas ARP
  - Herramienta: ettercap

DEMO



Seguridad a Nivel 2

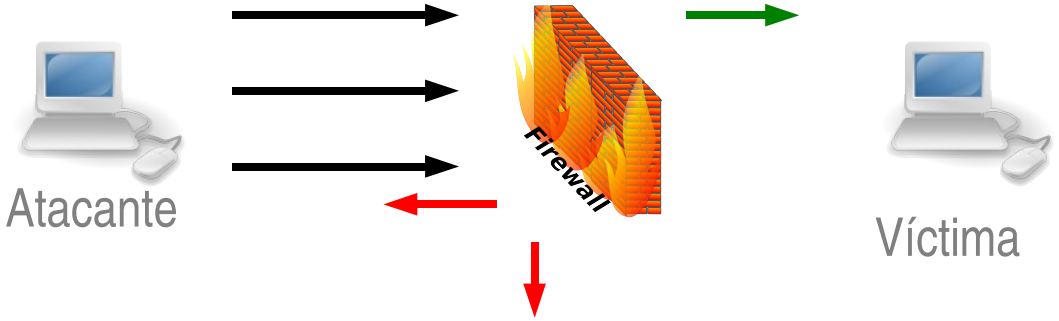
- VLANs
  - Que es. Como funciona
  - Ventajas
    - Aislamiento de redes
    - Agrupamiento de usuarios dispersos



Seguridad a Nivel 3

- Cortafuegos
  - Que son. Como funcionan
    - Reacciones posibles
      - Accept, Reject, Drop
  - Escaneos de puertos
    - Tipos
    - Técnicas de evasión
    - IDS
  - Herramientas
    - netstat
    - nmap, amap, vmap
  - Moraleja: “Si dejas pasar algo, potencialmente lo dejas pasar todo”

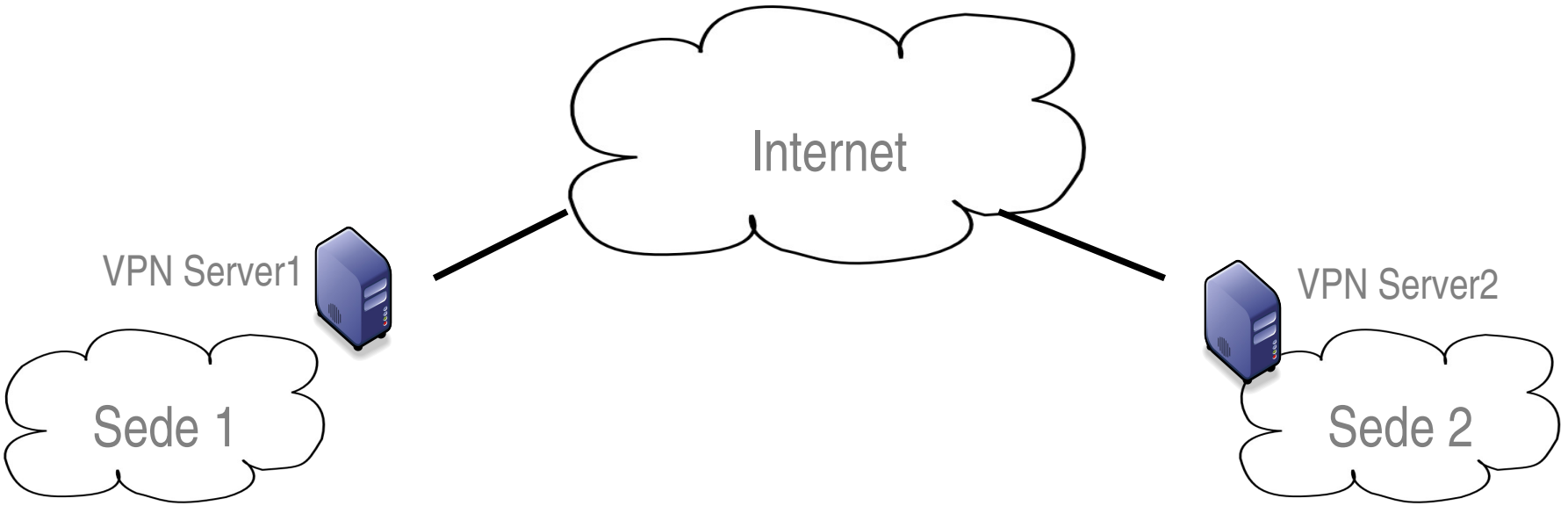
DEMO



Seguridad a Nivel 3

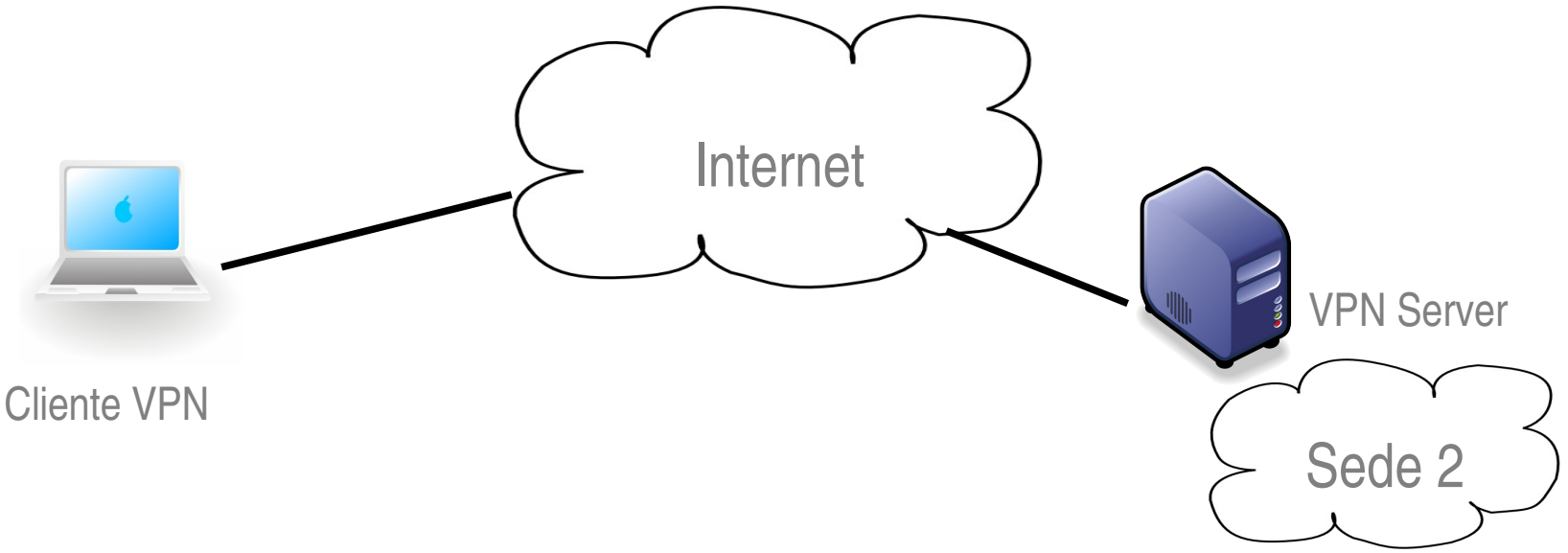
- Redes Privadas Virtuales (VPNs)
  - Que son. Como funcionan
    - Escenarios
  - Tipos
    - IPSec, SSLVPN, SSHVPN
  - Ventajas de proteger a Nivel3
  - Ventajas de IPSec
    - Standard (Ipv6), compatibilidad
    - Selección de:
      - Autenticación
      - Cifrado
  - Un ejemplo (Wifi UC3M)

- Redes Privadas Virtuales (VPNs)
  - Escenario I: Interconexión de sedes



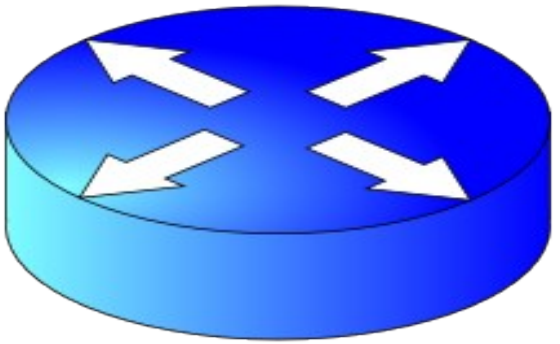
Seguridad a Nivel 3

- Redes Privadas Virtuales (VPNs)
  - Escenario II: Sistema de acceso remoto



Seguridad a Nivel 3

- Routers
  - Denegaciones de servicio
    - Encaminamiento dinámico: RIP, OSPF, BGP
    - Inundación SYN
    - DDoS
    - Ataques de magnificación (smurf, fraggle)



Seguridad a Nivel 5-7

- Servicios de consola remota
  - Telnet
    - Autenticación mediante usuario/password
    - Tanto la autenticación como la sesión van en claro
  - SSH
    - Alternativa segura a Telnet y FTP (Ojo con las prestaciones)
    - Posibilidades de autenticación
      - Usuario/password
      - Pareja clave Publica/privada (Tokens)
    - Uso de criptografía dura
    - Potente sistema de túneles
      - Redirección local o remota de puertos (-L, -R)
      - Servidor SOCKS (-D)

DEMO

~/.ssh/authorized_keys

Seguridad a Nivel 5-7

- Correo electrónico
  - Protocolo SMTP entre estafetas
    - No autenticado ni cifrado (en origen)
  - Protocolos como POP3 o IMAP entre estafeta y usuario final
    - Sistemas de autenticación débil y no cifrados (en origen)
  - Problemas de seguridad (I)
    - Usurpación de identidad de usuarios legítimos
    - Servidores que admiten *Relay*
      - Spam, usurpación de identidad,...
    - Imposibilidad de distinguir información legítima en los correos
      - Sólo podemos estar seguros del destinatario

DEMO

Seguridad a Nivel 5-7

- Correo electrónico (II)
  - Problemas de seguridad (II)
    - Trazado de comunicaciones
    - Ataques contra vulnerabilidades de lector de correo
    - Incitación a ejecución de adjuntos
      - Directa *".exe"*
      - Indirecta *"*.*"*
  - Solución de alguno de estos problemas
    - Uso de criptografía de clave asimétrica
      - PGP, GPG,...
      - Ofrece: Confidencialidad, integridad, autenticación, no repudio
    - Mantener actualizado el software
    - **Uso del sentido común**

Seguridad a Nivel 5-7

En que extensiones confías...?

DEMO

Adobe Reader

Seguridad a Nivel 5-7

- Servicios Web
  - Seguridad en el servidor
    - Vulnerabilidades del servidor HTTP o el S.O.
    - Errores de configuración del servidor
    - **Errores en las aplicaciones**
      - Campos ocultos
      - Cabeceras
      - Cookies o parámetros débiles
      - Traversal directory attack
      - Publicación de información indebida (Google Hacks)
      - Inyección SQL

DEMO

Seguridad a Nivel 5-7

- Servicios Web
  - Seguridad en el cliente
    - Robo de credenciales o datos sensibles directo
    - Suplantación SSL
    - XSS

DEMO

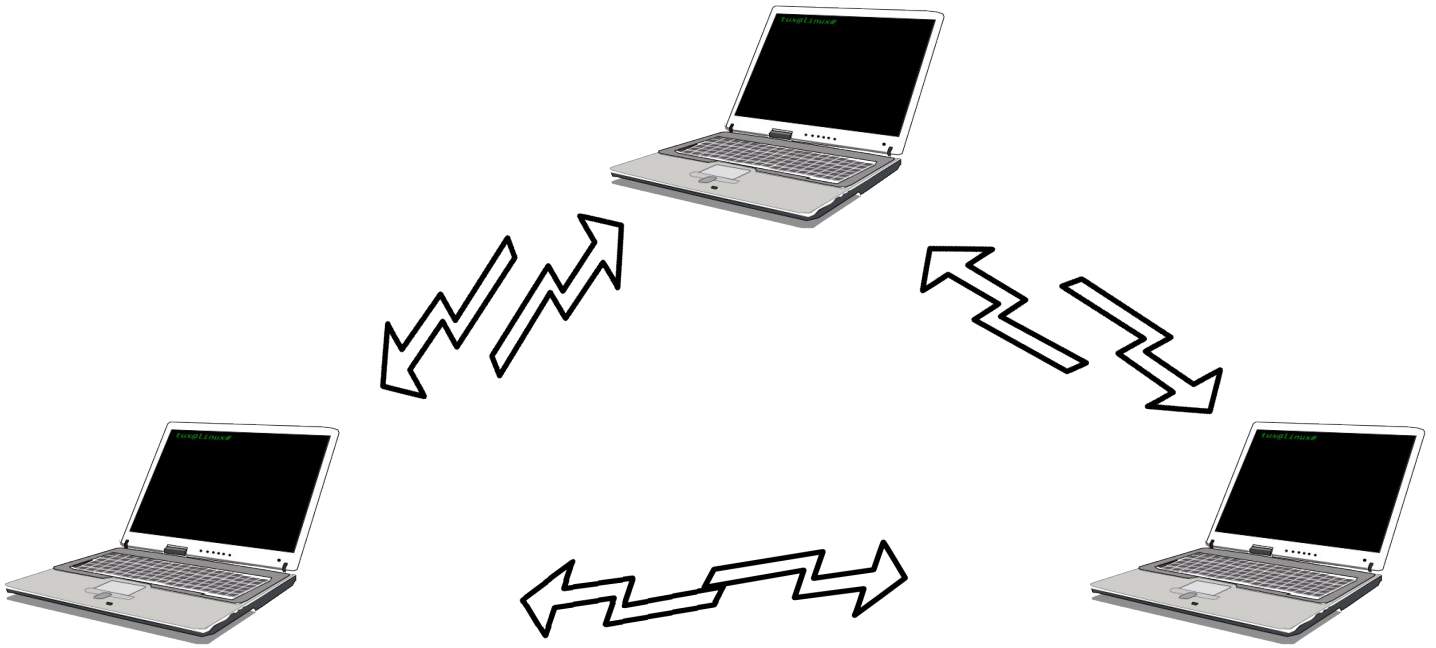
Seguridad en redes inalámbricas

- Redes inalámbricas
  - Que son. Como funcionan
  - Ámbito:
    - IEEE802.11 (a/b/g)
  - Modos de funcionamiento
    - ad-hoc
    - infraestructura
    - Otros: monitor, master, repetidor
  - Tipos de tramas:
    - Probe request/respond
    - Autentication request/respond
    - Beacon
    - datos

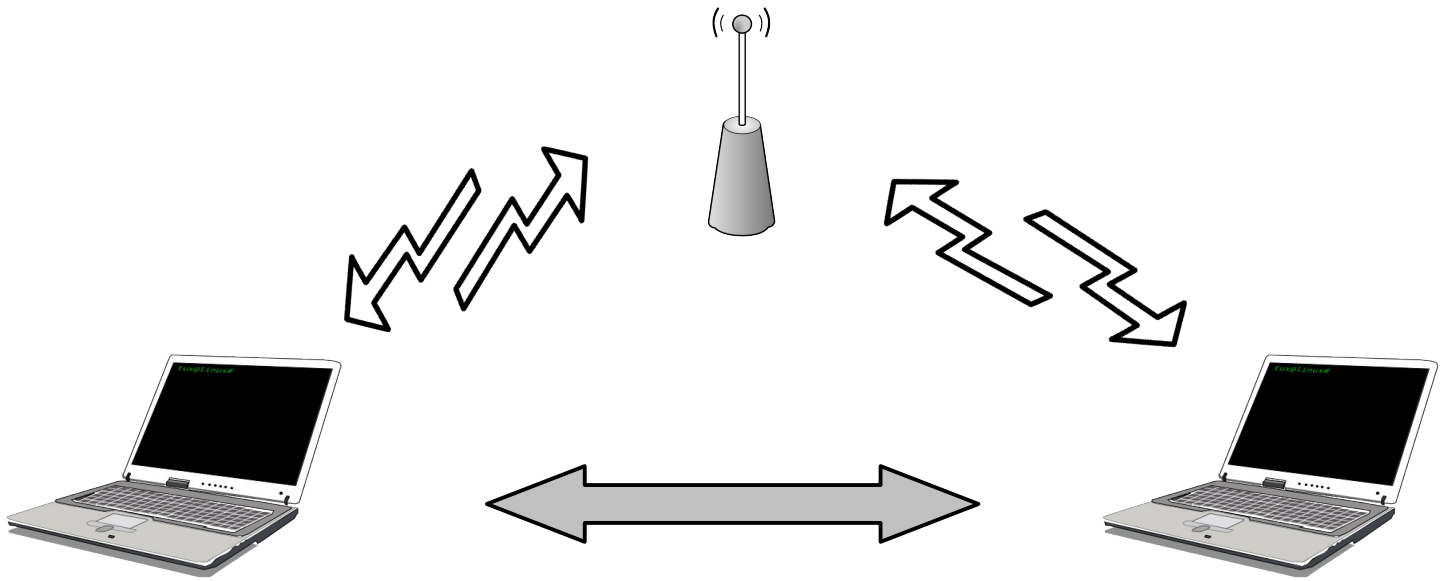
DEMO

Seguridad en redes inalámbricas

- Modo ad-hoc



- Modo infraestructura

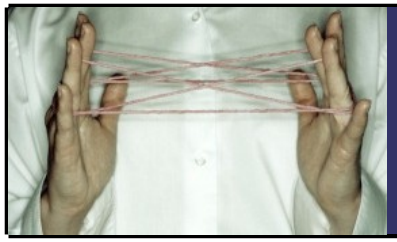


Seguridad en redes inalámbricas

- Sistemas de seguridad
  - Ocultamiento de ESSID
  - Filtrado MAC
  - Seguridad WEP
  - Seguridad WPA (1, TKIP)
    - Personal
    - Profesional
  - Seguridad WPA (2, AES)
    - Personal
    - Profesional
  - Otros
    - PEAP,LEAP,...

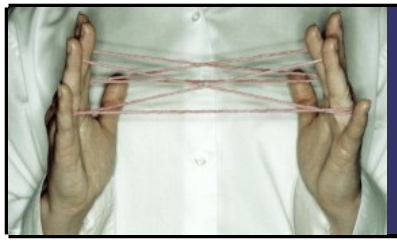
Seguridad en redes inalámbricas

- Conclusiones
  - Únicas configuraciones seguras (de menor a mayor)
    - WPA (1, TKIP)
      - Personal. Sólo con clave suficientemente robusta
      - Enterprise
    - WPA (2, AES)
      - Personal o enterprise
    - **VPNs**
  - Otros problemas de seguridad
    - Suplantación de punto de acceso
    - Desasociación de estaciones
    - Aseguramiento de HotSpots



Técnicas avanzadas

- Técnicas no recomendadas
  - Cambio de puertos de para los servicios
  - Enmascaramiento de servidores (Banners, errores,...)
- Técnicas sí recomendadas
  - Para evitar exploits
    - Aleatorización de punteros de pila
    - Separación eficaz de zonas de memoria
  - Para minimizar riesgos
    - Entornos enjaulados
    - UserModeLinux
    - VmWare



Técnicas avanzadas

- ...
  - Comprobación de firma de ficheros
    - Procedentes de paquetes de la distribución (debsums)
    - Cualquier fichero del sistema (tripwire)
  - Detección de rootkits (chkrootkit, rkhunter,...)
  - *Backup, discos cifrados, IDS, Antivirus, FW, VPN...*

Recomendaciones generales

...ya estoy asustado, ¿ahora que hago?

- Actualización del sistema
  - ¿Por qué actualizar?
    - Nuevas funcionalidades
    - Corrección de vulnerabilidades
  - ¿Que actualizar?
    - Todo (Incluido el kernel)
  - ¿Como actualizar?
    - Manualmente (Inabordable)
    - Herramientas automáticas
      - Debian (APT + http://security.debian.org)
      - Gentoo (emerge)
      - Redhat (UP2DATE)

Recomendaciones generales

...ya estoy asustado, ¿ahora que hago?

- Exponer los menores servicios posibles
- Correr los servicios con los menores privilegios posibles
- Instalar la menor cantidad posible de software
- Prestar especial atención a la configuración de los servicios
  - Aplicar manuales de bastionado
- A la realizar desarrollos propios tener presente desde el momento inicial la seguridad. Esto requiere conocer técnicas de programación segura y los vectores más habituales de ataque por parte de los programadores.
- Realizar las labores de fortificación en todos los puntos y a todos los niveles posibles

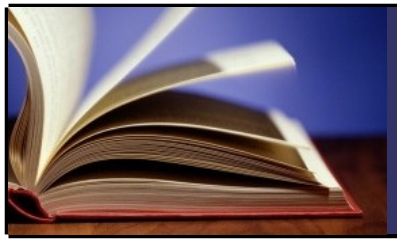
Recomendaciones generales

sed un poco paranoicos, sólo un poco.

Usa el sentido común.... Luke!

Conclusiones

- Ningún SO, servicio o hardware es seguro de por si
  - Un sistema es tan seguro como el esfuerzo que dediquemos a ello
- Amenazas inherentes a los protocolos y otras propias de productos o configuraciones
- ¿Cuanto me preocupo?
  - *¿Cuantos enemigos tienes?*
  - *¿Cuanto vale lo que estas protegiendo?*
  - *¿Cuanto estas dispuesto a invertir en seguridad?*

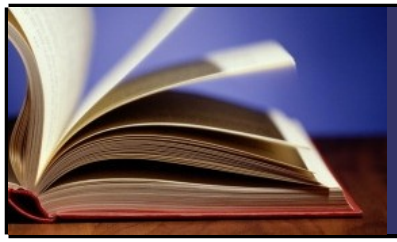


Bibliografía/Referencias

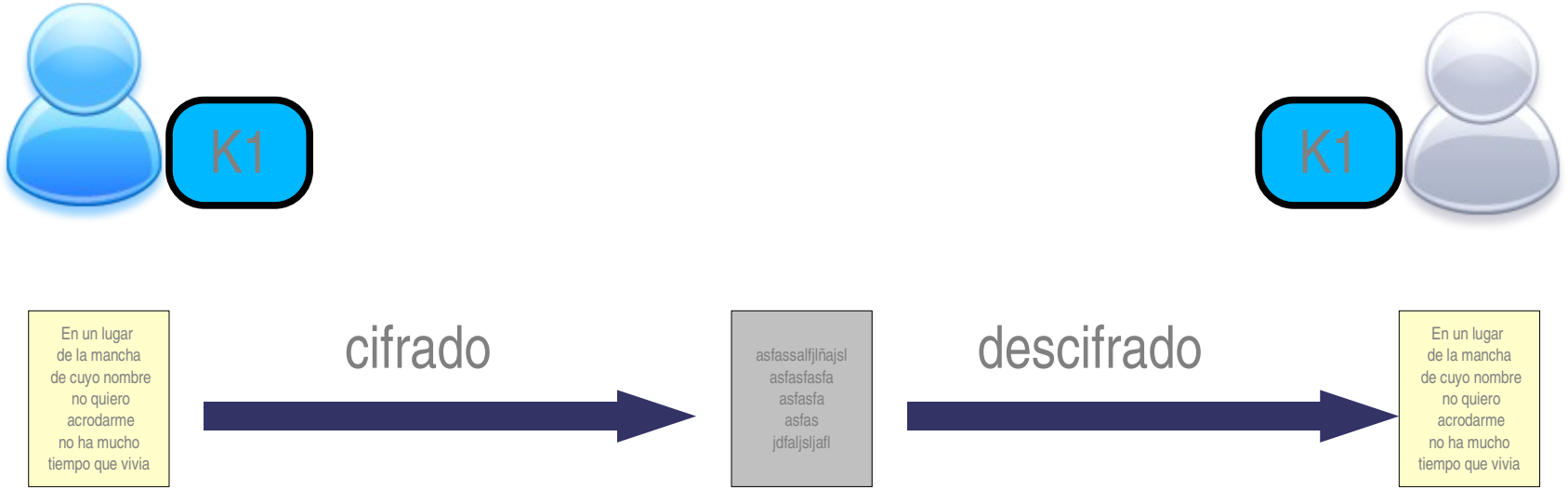
- http://www.google.com
- http://www.security-focus.com
- http://packetstormsecurity.nl

- http://www.gul.uc3m.es
- ftp://ftp.gul.uc3m.es
- mailto://gul@gul.uc3m.es
- mailto://arevalo@gul.uc3m.es

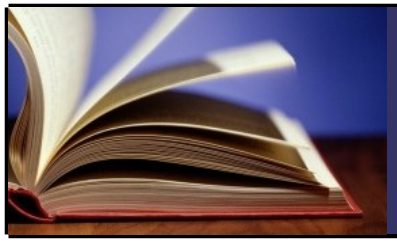
Anexos



Cifrado simétrico

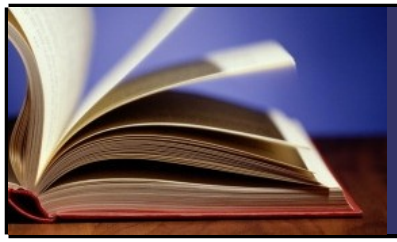


- Problemas
  - N claves distintas para N comunicaciones
  - Distribución de claves
  - ...

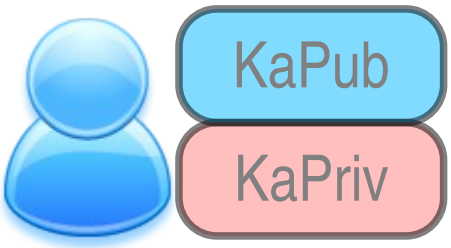


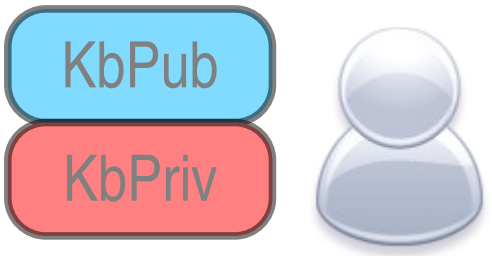
Funciones resumen

- Propiedades
  - Genera un número de tamaño fijo a partir de una entrada de cualquier tamaño
  - Computo directo sencillo
  - Computo inverso imposible
  - Probabilidad muy baja de colisión
  - Cambio mínimo en la entrada produce cambio total en la salida
  - ...

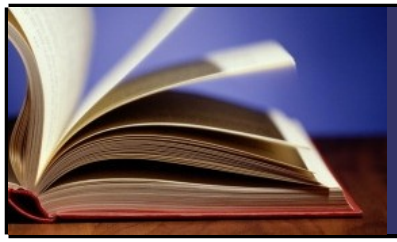


Cifrado asimétrico

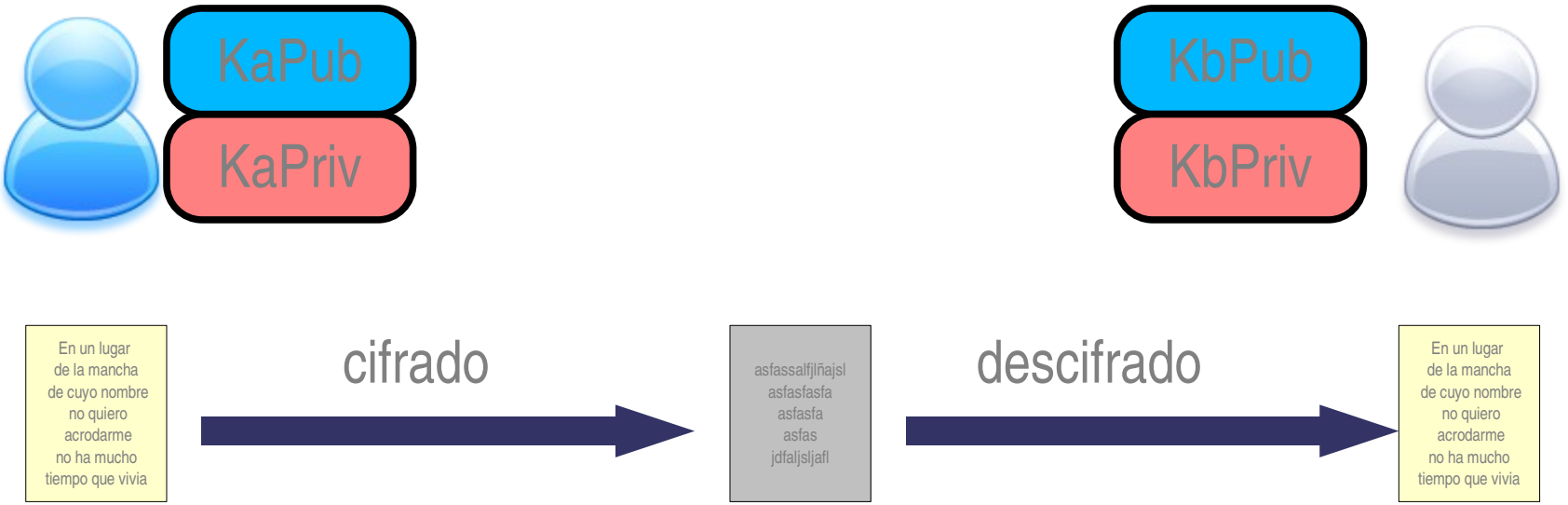




- Propiedades
  - Cada usuario sólo tiene 2 claves. Una pública y una privada
  - La clave pública se debe distribuir.
  - La clave privada se mantiene secreta
  - Se cifra con una u otra clave en función del objetivo que se persiga.



Cifrado asimétrico



- ¿Que logramos?
  - Confidencialidad
  - Integridad
  - Autenticación
  - No repudio