XII CONGRESO NACIONAL DE ESTUDIANTES INGENIERIA DE SISTEMAS

XIICNEIS USACA – 2.003

Seguridad en la infraestructura de redes inalámbricas

Roberto Gómez Cárdenas

rogomez@itesm.mx

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

Las redes

- RED
  - unión de dos o más computadoras, para crear una comunicación entre ellas que les permita compartir información y recursos.
- Para realizar esta conexión se requiere de un medio físico, en el cual viajará la información.

Haciendo cuentas ...

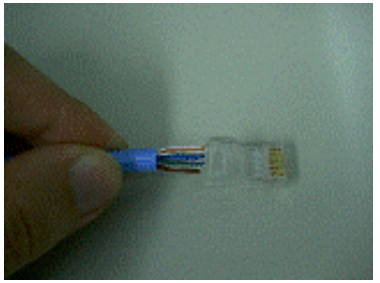
- Computación electrónica 60 años !
- Redes sólo tienen 40 años de vida !
- Seguridad 27 años !
- Internet 25 años !
- Web 12 años !
- Intranets 10 años...
- Extranets 8 años...

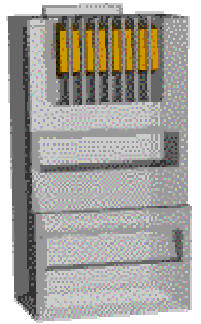
Conectividad

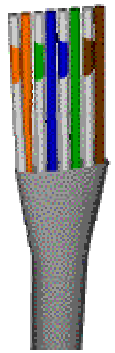
- ¿Cómo se conecta nuestro usuario a la red?
  - Narrowband
    - Dial-Up
      - 56Kbps (con suerte…)
  - Broadband
    - Ds0/E1…
      - Enlaces dedicados.
      - Oficinas / Escuelas
    - DSL
      - 128Kbps – 2Mbps
      - Requiere cobertura por el ISP

El Spaghetti

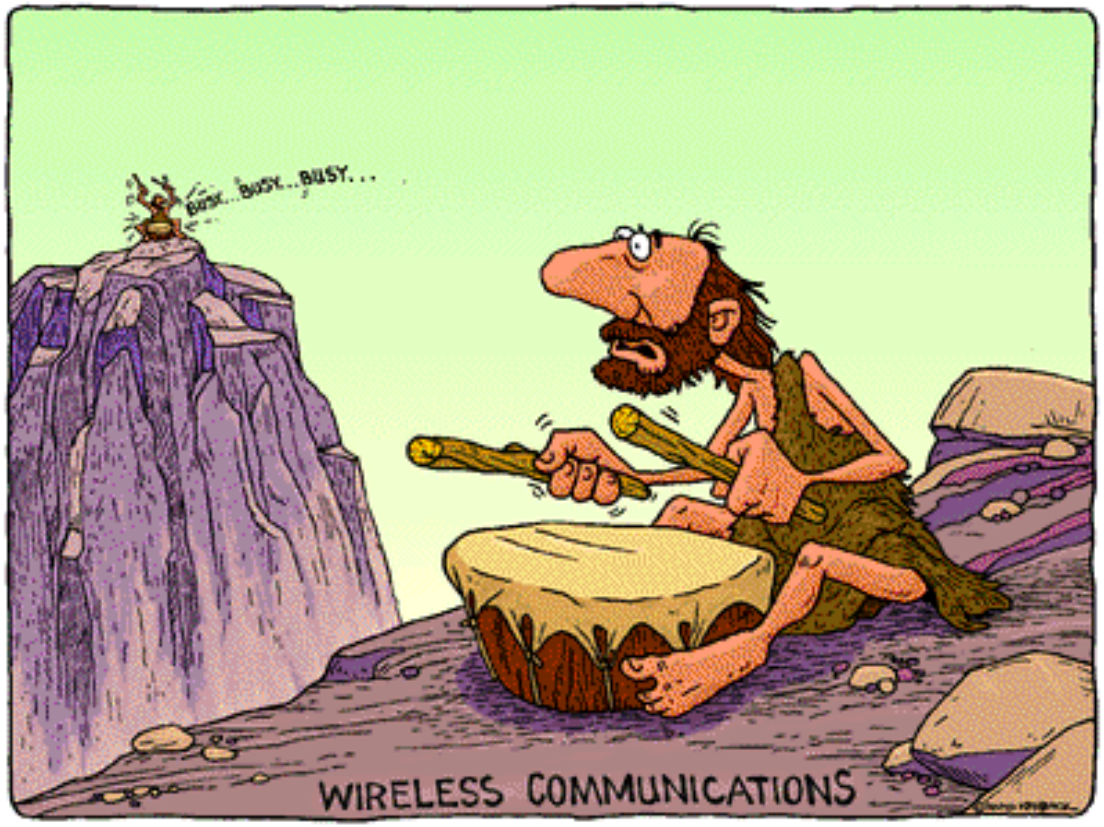
- Los datos requieren de un medio de transmisión
- Evolución de los cables
  - Coaxial
  - UTP
  - Fibra
- Problemas
  - Aumentar velocidad
  - Crecer la red
  - Costo







¿Alternativas?



¿Qué es una red inalámbrica o WLAN?

- El medio de transmisión más utilizado es el cable, pero para el caso de una red inalámbrica ese medio físico es el aire.
- WLAN: Siglas en inglés de Wireless Local Area Network.

¿Por qué Wireless LAN?

- Ausencia de cableado.
  - Bajo costo (cuidado con el TCO)
  - Liberación rápida.
- Movilidad del usuario.
- Interactividad
- Comunicación bidireccional
- Tecnología broadcast

¿Por qué no Wireless LAN?

- Ausencia de seguridad física.
- Baja tasa de flujo de datos.
- Espectro ruidoso y sin regulación.

¿Qué va a pasar con el cableado de red?

- Una red inalámbrica NO va a desplazar a una red por medio de cable.
- La red inalámbrica complementa a la red cableada en situaciones como
  - difícil montar una red,
  - realizar más conexiones
  - se requiere estar moviéndose de un área a otra sin necesidad de desconectarse de la red (computo móbil)

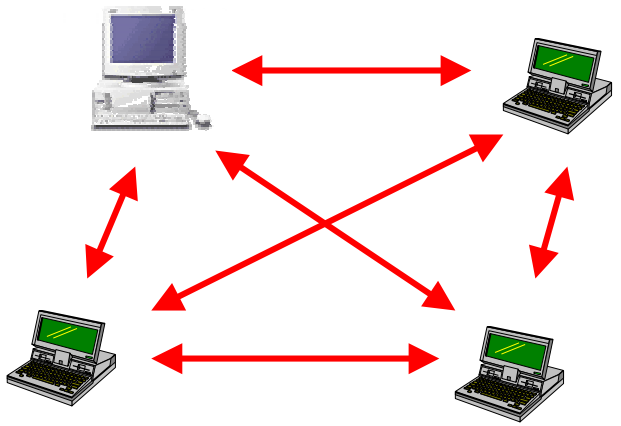
Tipos WLANS

- Ad-hoc

- Infraestructura permanente

WLAN Ad hoc

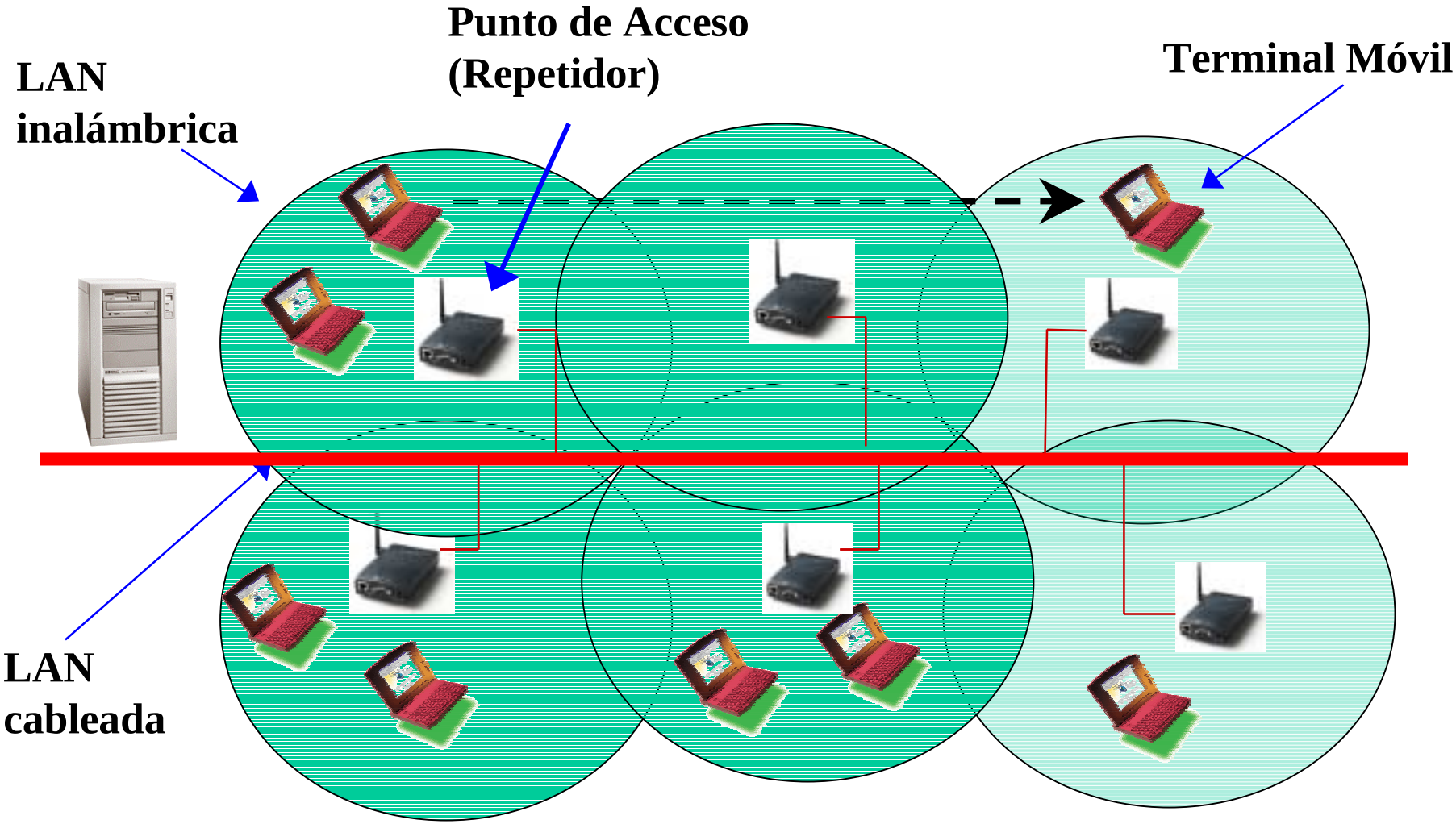
- Se juntan varios nodos móviles en una área reducida
- Se establece una comunicación entre ellos sin la ayuda de ningún tipo de columna (backbone).
- Para implementar redes ad hoc se tienen dos maneras:
  - Broadcasting/flooding
  - Infraestructura temporal



WLAN con infraestructura permanente

- Regularmente la infraestructura principal es una columna vertebral cableada (backbone).
- Esta estructura tiene puntos de contacto (puntos de acceso) con el medio inalámbrico.
  - estos pueden ser estaciones base o repetidores
- A partir del backbone existen dos tipos de comunicación
  - subida
  - bajada.

Ejemplo estructura WLAN



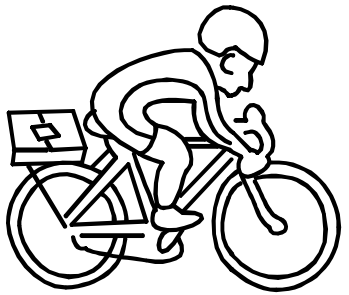
Elementos de una WLAN

IEEE 802.11

- Estándar transmisión de datos a través señales de radio
- Capa MAC semejante a Ethernet
- Soporta el stack de protocolos de TCP/IP y otros.
- Basado en
  - Direct Sequence Spread Spectrum (DSSS),
  - Frequency Hoping Spread Spectrum (FHSS),
  - Orthogonal Frequency Division Multiplexing (OFDM)
- Tipos
  - 802.11a (Wi-Fi-5)
  - 802.11b (Wi-Fi)
  - 802.11g

Riesgos de una WLAN

- Monitoreo de tráfico inalambrico
  - datos de usuarios
  - localización de usuarios
  - identidad de usuarios
  - análisis de tráfico
- Acceso no autorizado a una red a través de un enlace inalambrico
  - persona pasaendose en una bicicleta
- Corrupción de servicios inalambricos



Los actores principales

- Hackers
- Crackers
- Script Kidies

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 realiz 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.

Los phreakers

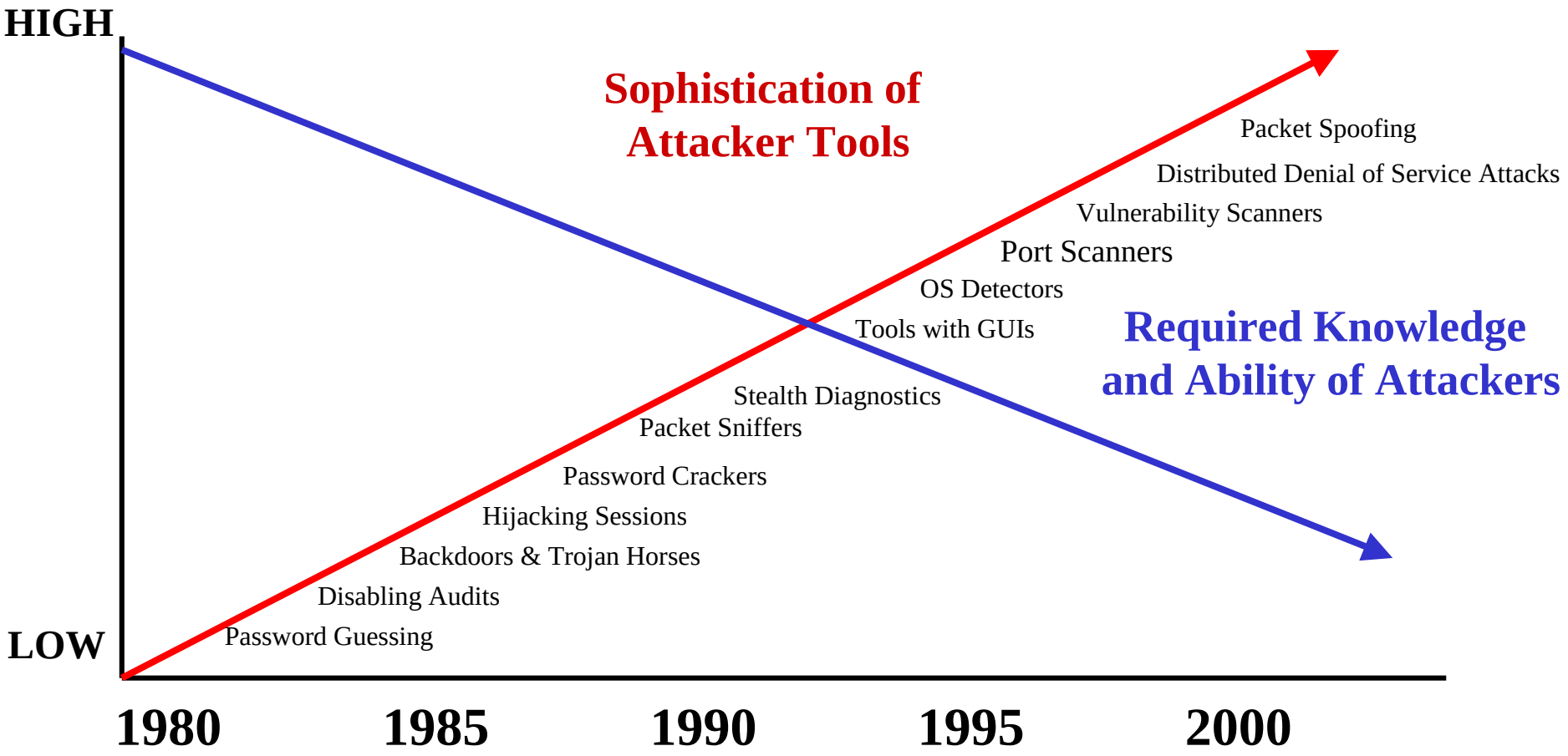
- Aquella persona que en forma persistente realiza intentos hasta obtener acceso a sistemas telefónicos privados.
- Una vez logrado el produce daños recursos del atacado, o se mismo.

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¨.

External Threats: Hacker Tool Explosion

Recent Web Search for “Hacker Tools” returned over 2100 hits



I get scanned dozens of times everyday. Less than 20% of those scans are US based

ISS User

> displaying from 1 to 138 of 138 defacement(s) found.

> date	> original site	> archive	> attacked by	> OS	> comments	> nmap	> class-C
23/01/2002	www.republicain-niger.com	mirror	S4t4n1c_S0uls	Solaris	none	view	history
22/01/2002	www.megaplus.ch	mirror	S4t4n1c_S0uls	Unknown	none	view	history
22/01/2002	www.colbayns.org.uk	mirror	S4t4n1c_S0uls	Windows	none	view	history
22/01/2002	www.traumgirl.ch	mirror	S4t4n1c_S0uls	Unknown	none	view	history
20/01/2002	www.onix.de	mirror	S4t4n1c_S0uls	Linux	none	view	none
20/01/2002	www.globo-insurance.com	mirror	S4t4n1c_S0uls	Windows	none	view	none
20/01/2002	www.atleticaitaliana.it	mirror	S4t4n1c_S0uls	Windows	none	view	none
20/01/2002	www.jacksonholebuilder.com	mirror	S4t4n1c_S0uls	Linux	none	view	none
19/01/2002	www.cdt.br	mirror	S4t4n1c_S0uls	Windows	none	view	none
15/01/2002	www.brainchainfreedom.com	mirror	S4t4n1c_S0uls	Windows	none	view	none
15/01/2002	www.co.macon.nc.us	mirror	S4t4n1c_S0uls	Windows	Redefacement	view	history
12/01/2002	www.rottenpeaches.com	mirror	S4t4n1c_S0uls	Windows	none	view	none
12/01/2002	www.forumsec.org.fj	mirror	S4t4n1c_S0uls	Windows	Redefacement	view	history
11/01/2002	eisenpower.com	mirror	S4t4n1c_S0uls	Windows	none	view	none
11/01/2002	www.thedqa.com	mirror	S4t4n1c_S0uls	Windows	none	view	history
11/01/2002	merchantsofsouthgaylord.com	mirror	S4t4n1c_S0uls	Windows	none	view	none
10/01/2002	lewisandroth.org	mirror	S4t4n1c_S0uls	Windows	none	view	none
10/01/2002	www.cbbound.com	mirror	S4t4n1c_S0uls	Windows	none	view	none
07/01/2002	www.melissa.org	mirror	S4t4n1c_S0uls	Windows	none	view	none
07/01/2002	www.cpinyc.com	mirror	S4t4n1c_S0uls	FreeBSD	none	view	history
07/01/2002	www.mmitech.com	mirror	S4t4n1c_S0uls	FreeBSD	none	view	history
07/01/2002	www.fgi.org	mirror	S4t4n1c_S0uls	FreeBSD	none	view	history
06/01/2002	www.efashionjewelry.com	mirror	S4t4n1c_S0uls	Windows	none	view	none
04/01/2002	www.honda.com.sg	mirror	S4t4n1c_s0uls	Windows	Redefacement	view	history
04/01/2002	www.lasvegaseventphoto.com	mirror	S4t4n1c_S0uls	Windows	none	view	none
04/01/2002	www.lasvegas2000.com	mirror	S4t4n1c_S0uls	Windows	none	view	history
04/01/2002	www.haquewater-lasvegas.com	mirror	S4t4n1c_S0uls	Solaris	none	view	none
03/01/2002	www.harmonyproperties.com	mirror	S4t4n1c_S0uls	Windows	none	view	none
03/01/2002	www.svuc.se	mirror	S4t4n1c_S0uls	Windows	none	view	none
01/01/2002	www.consiglio.regione.tos.it	mirror	S4t4n1c_S0uls	Windows	none	view	none
01/01/2002	www.hdc.ru	mirror	S4t4n1c_S0uls	Windows	none	view	none
30/12/2001	www.bibc.de	mirror	S4t4n1c_S0uls	Windows	none	view	none
30/12/2001	www.optimeq.com	mirror	S4t4n1c_S0uls	FreeBSD	none	view	none

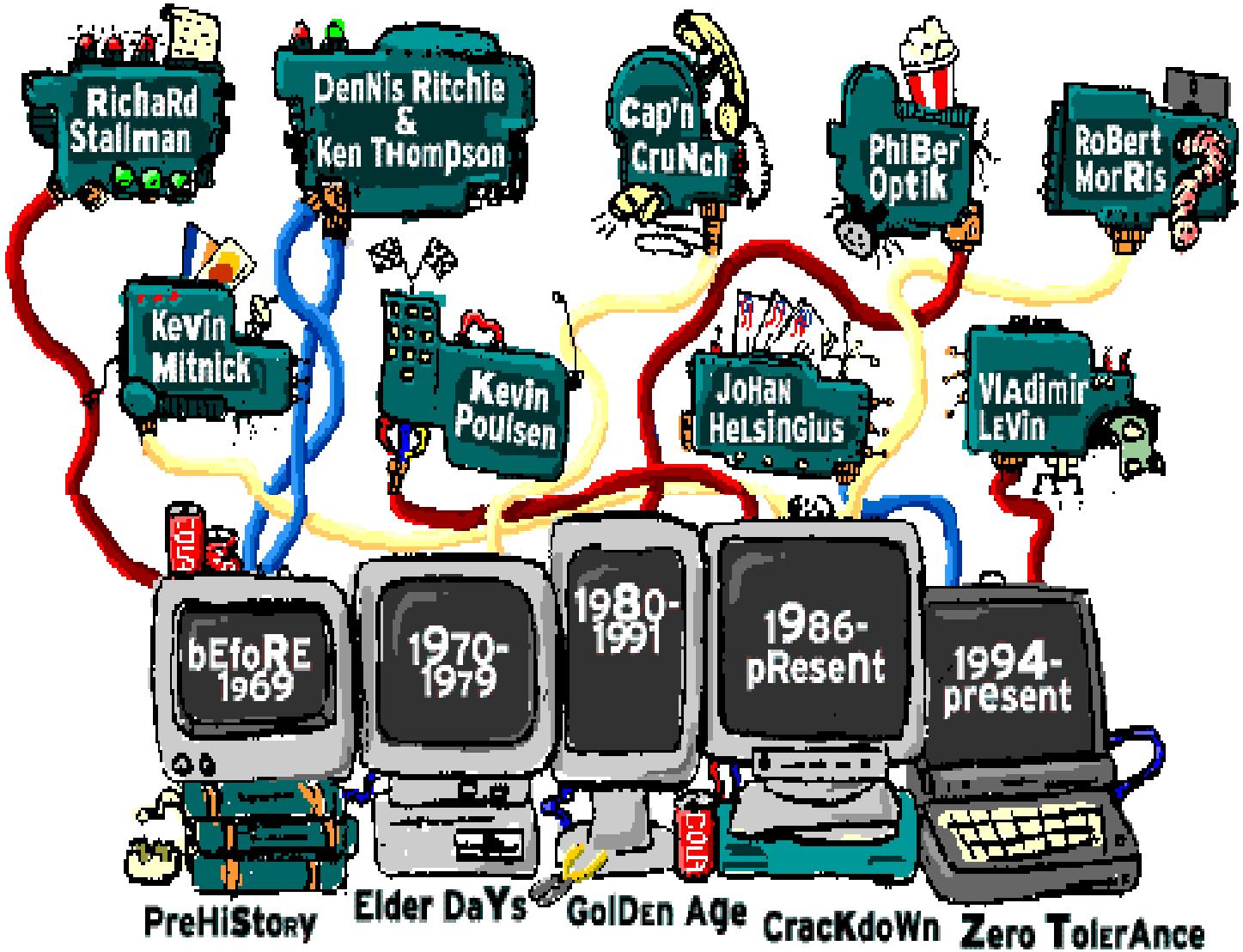
El Hacker: ¿cómo lo ven el resto de los usuarios?

- ¿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.

Hackers más Famosos.











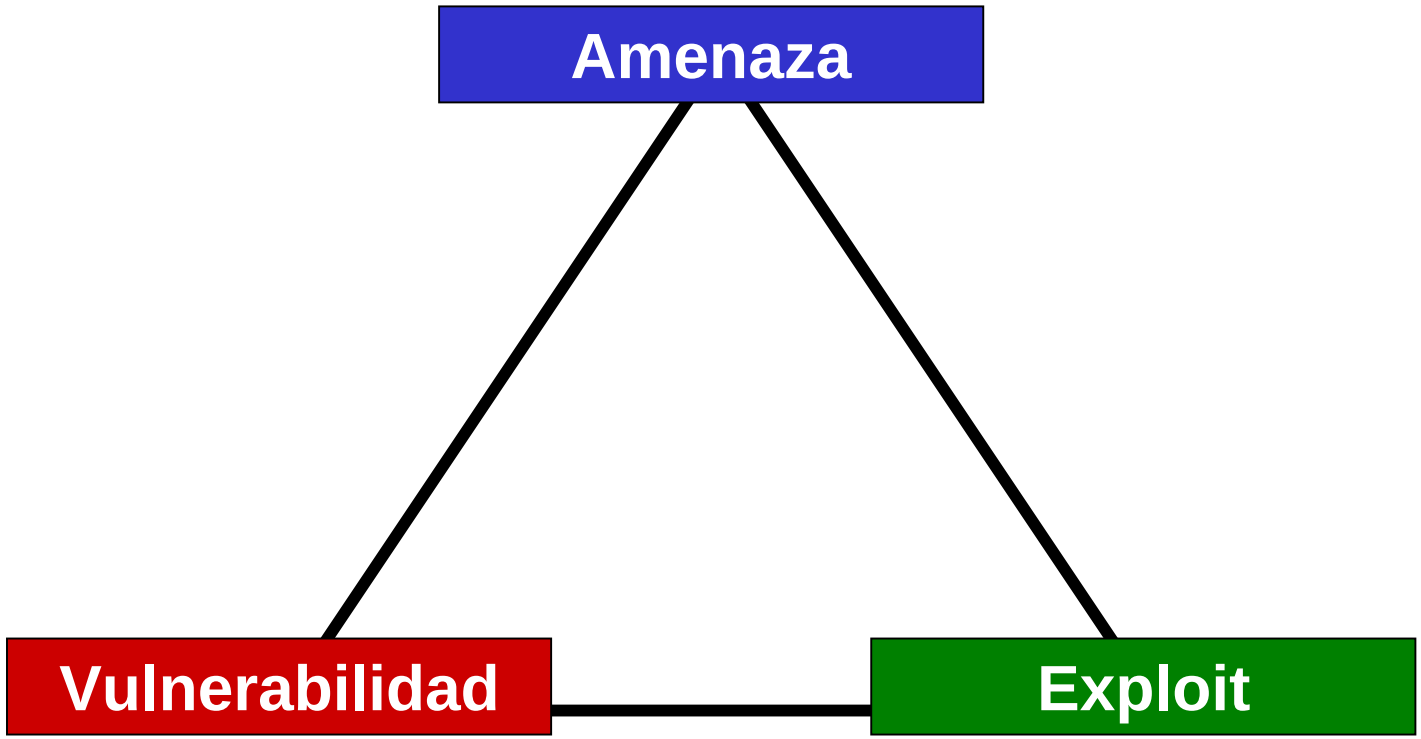
Algunos grupos

- Chaos Computer Club
- Cult of the Dead Cow
- DC2600.org
- AntiOffline removing the Dot in Dot.com
- The gethohackers
- DARK CLAW
- LoD

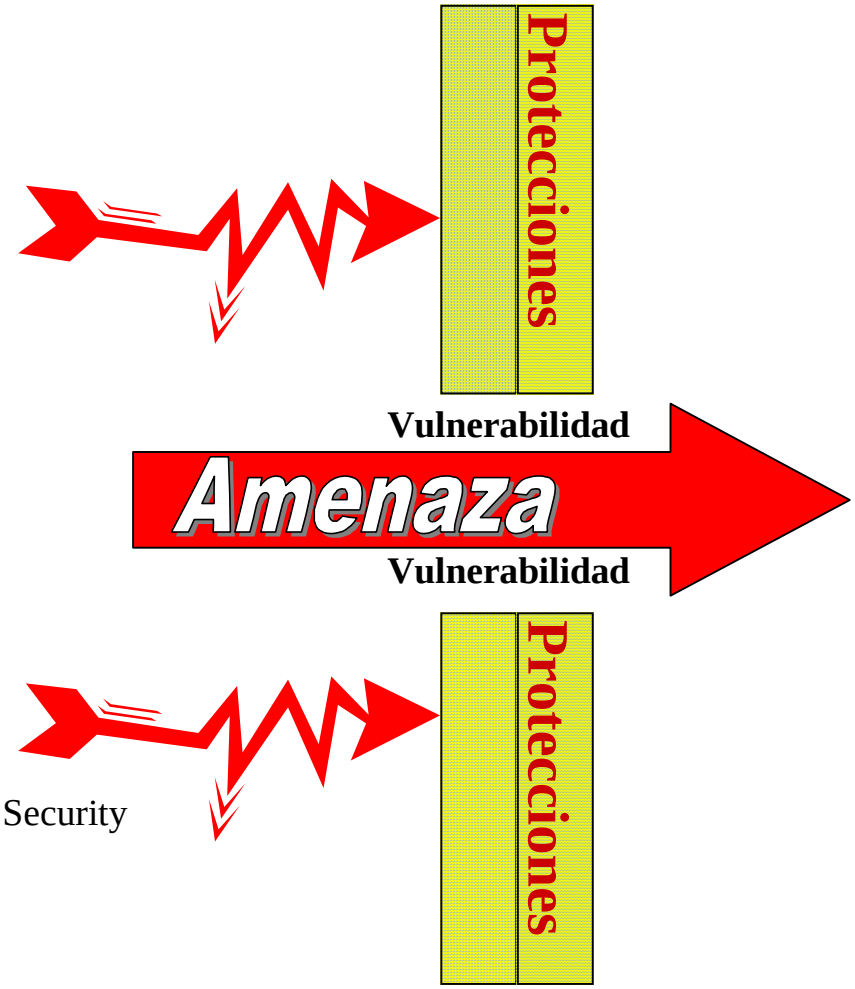
Otros actores

- Lammer
- Newbie
- Rider
- Sneaker
- Carding 

El triangulo del peligro



Vulnerabilidad vs amenaza

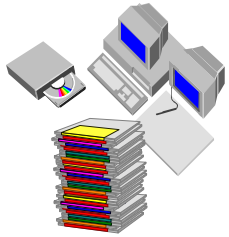


Activos

Datos

Instalaciones

Hardware/Software



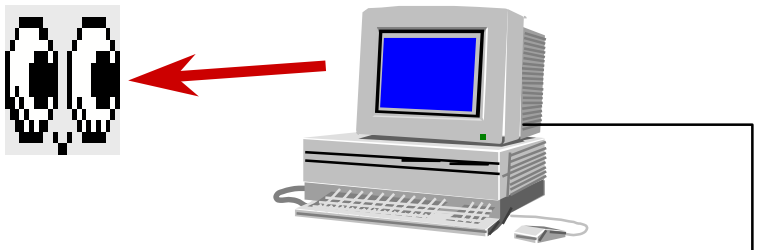
Source:
An Introduction to Computer Security
The NIST Handbook
NIST- Serial
Publication 800-12

¿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.
- Esto incluye cualquier acción que causa la destrucción, modificación o retraso del servicio no autorizado.

Tipos de Ataques

Ataques Pasivos.



Ataques Activos.

Principales Ataques

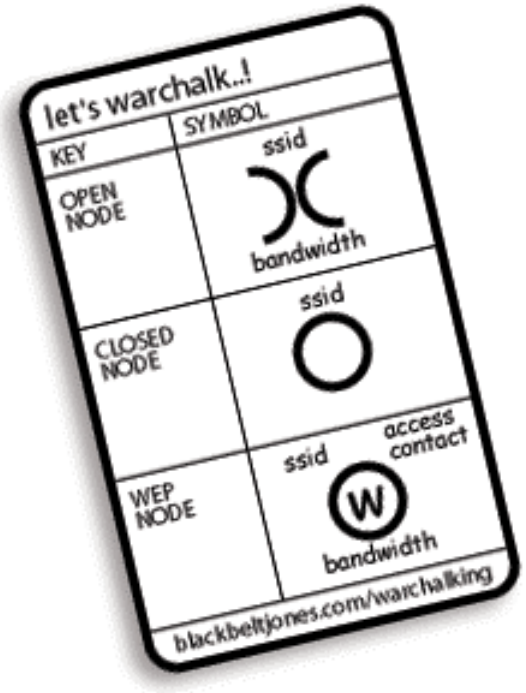
- Virus
- Caballo de Troya
- Gusanos (Worms)
- Bugs
- Trapdoors
- Stack overflow
- Pepena
- Bombas lógicas
- Dedos inexpertos
- Falsificación
- Usurpación
- Sniffers
- Spoofing
- Spam
- Grafiti
- Ingeniería Social
- Negación de servicio

Descubrimiento

- El SSID (Service-Set Identifiers) es esencialmente el nombre de una red inalámbrica.
- La mayoría de los Access Points envían vía broadcast el SSID, esta situación permite el descubrir APs de manera sencilla.
  - probar a FF:FF:FF:FF:FF:FF con SSID nulo o “any”
  - AP envía su SSID)
- El SSID se incluye en cada uno de los paquetes que no se cifran (sniffing del SSID a pesar de que el AP no los envíe por broadcast).

Descubrimiento

- Netstumbler y amigos
- Wardriving
- Warchalking
- Sniffing – Ethereal/Airopeek
- Window XP y cierto software de tarjetas de red detectan AP's disponibles



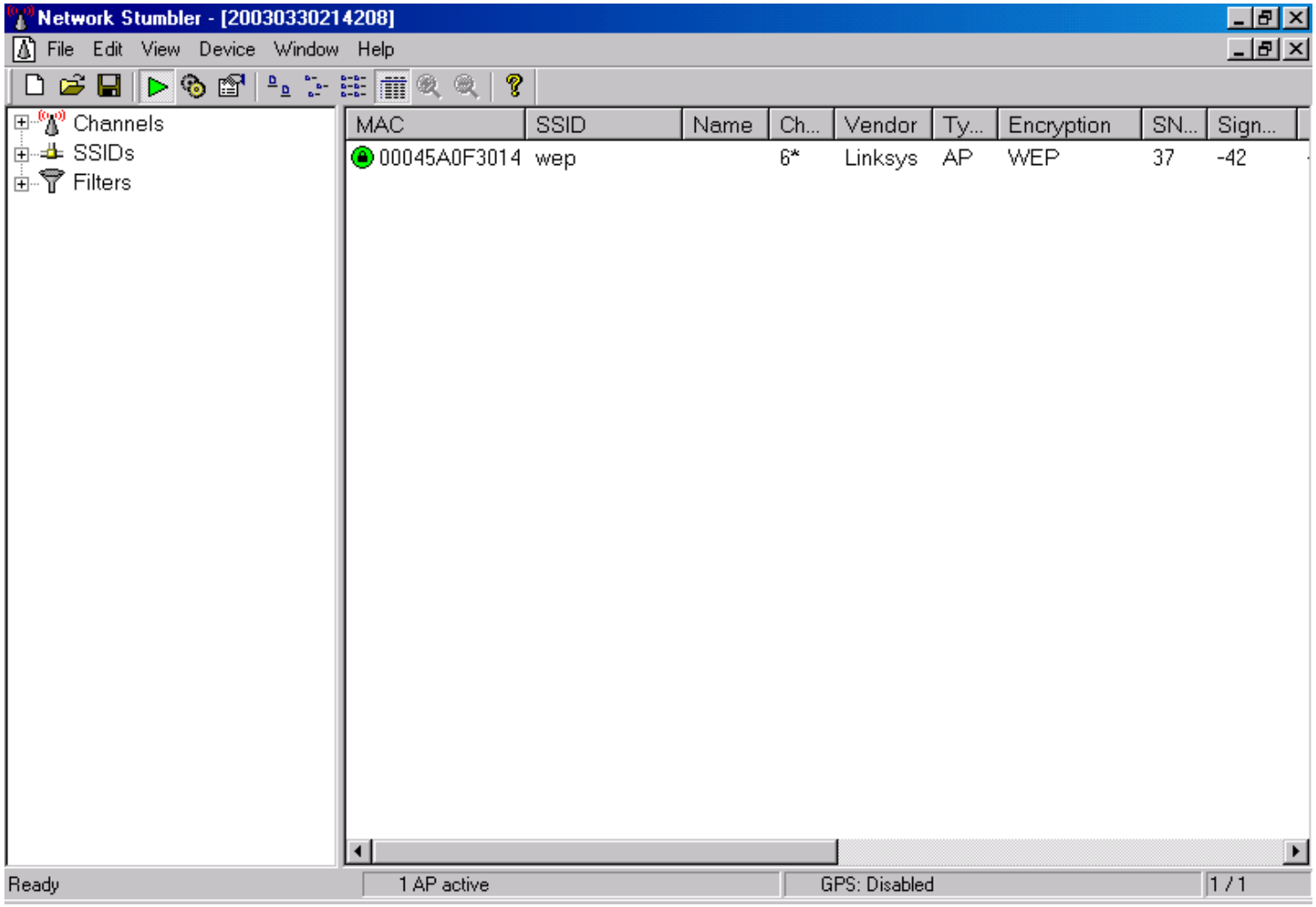
- Antennas
  - Omnidireccionales
  - Direccionales

Wardriving

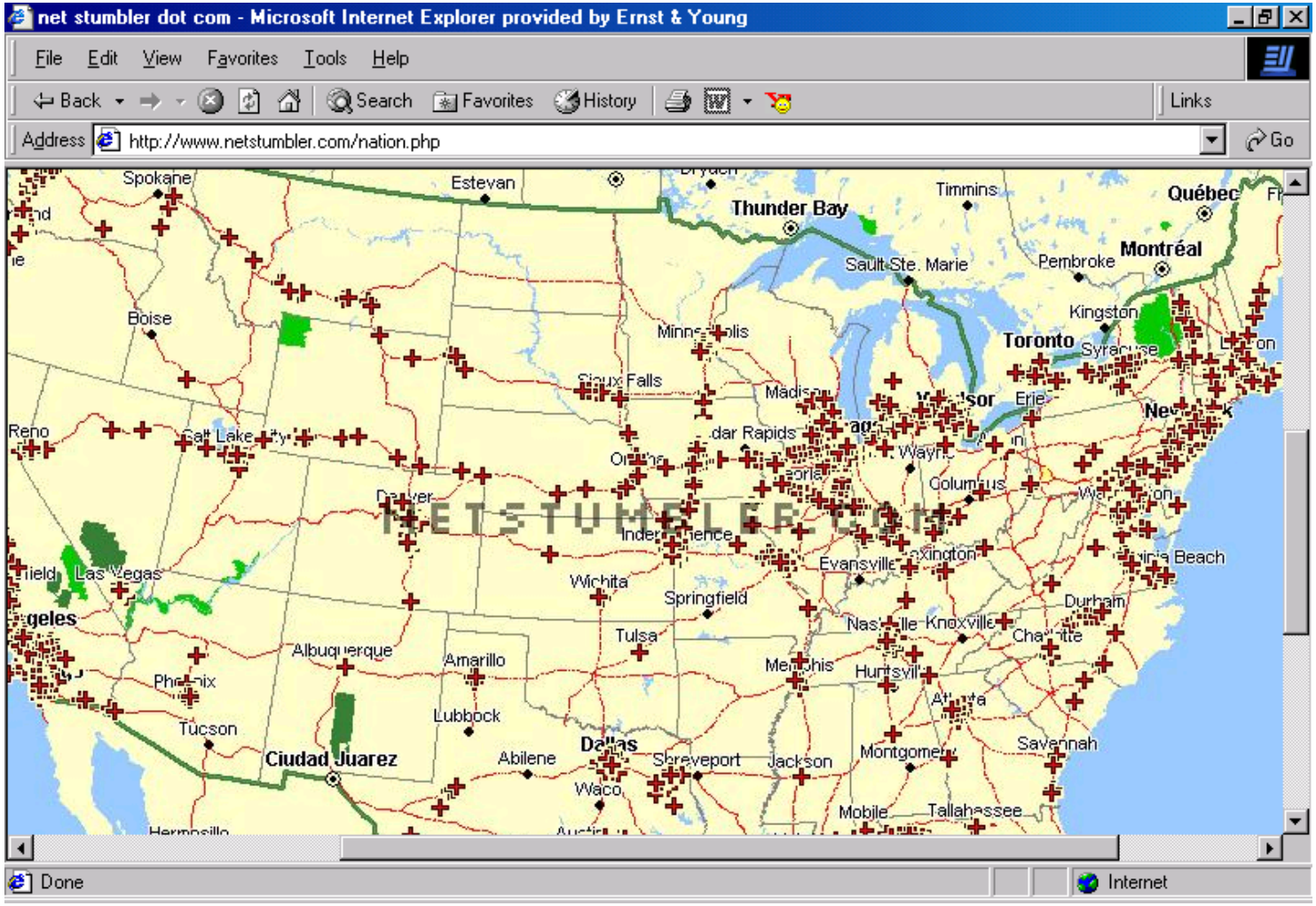
- Acto de descubrir redes inalámbricas en un área a través de conducir en esa área con el equipo necesario (laptop, tarjeta de red inalámbrica, software necesario, posiblemente antena externa).

Wardriving

Wardriving - Netstumbler

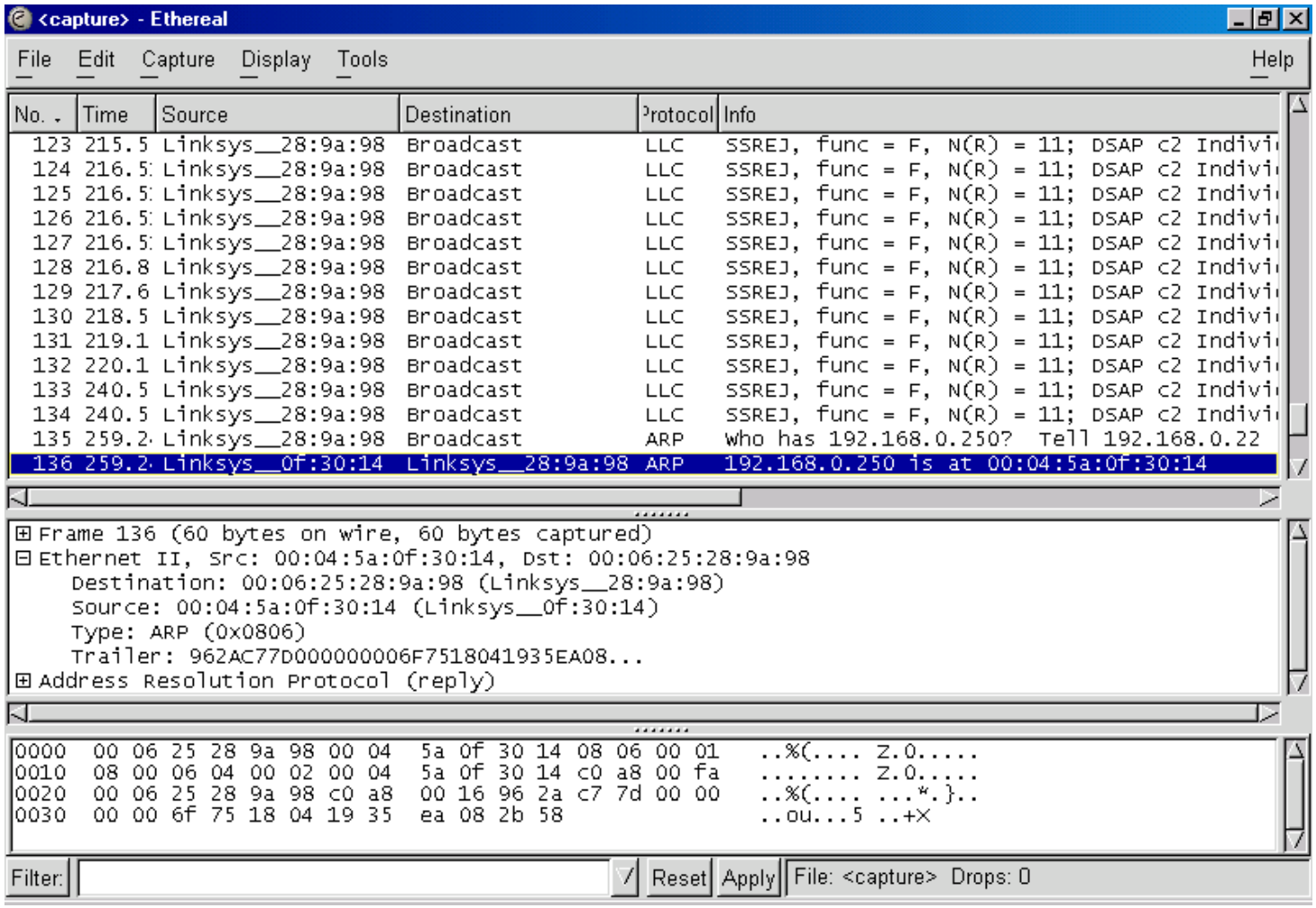


Wardriving - Netstumbler



Wardriving/Warchalking - Ministumbler

Descubrimiento - Sniffing



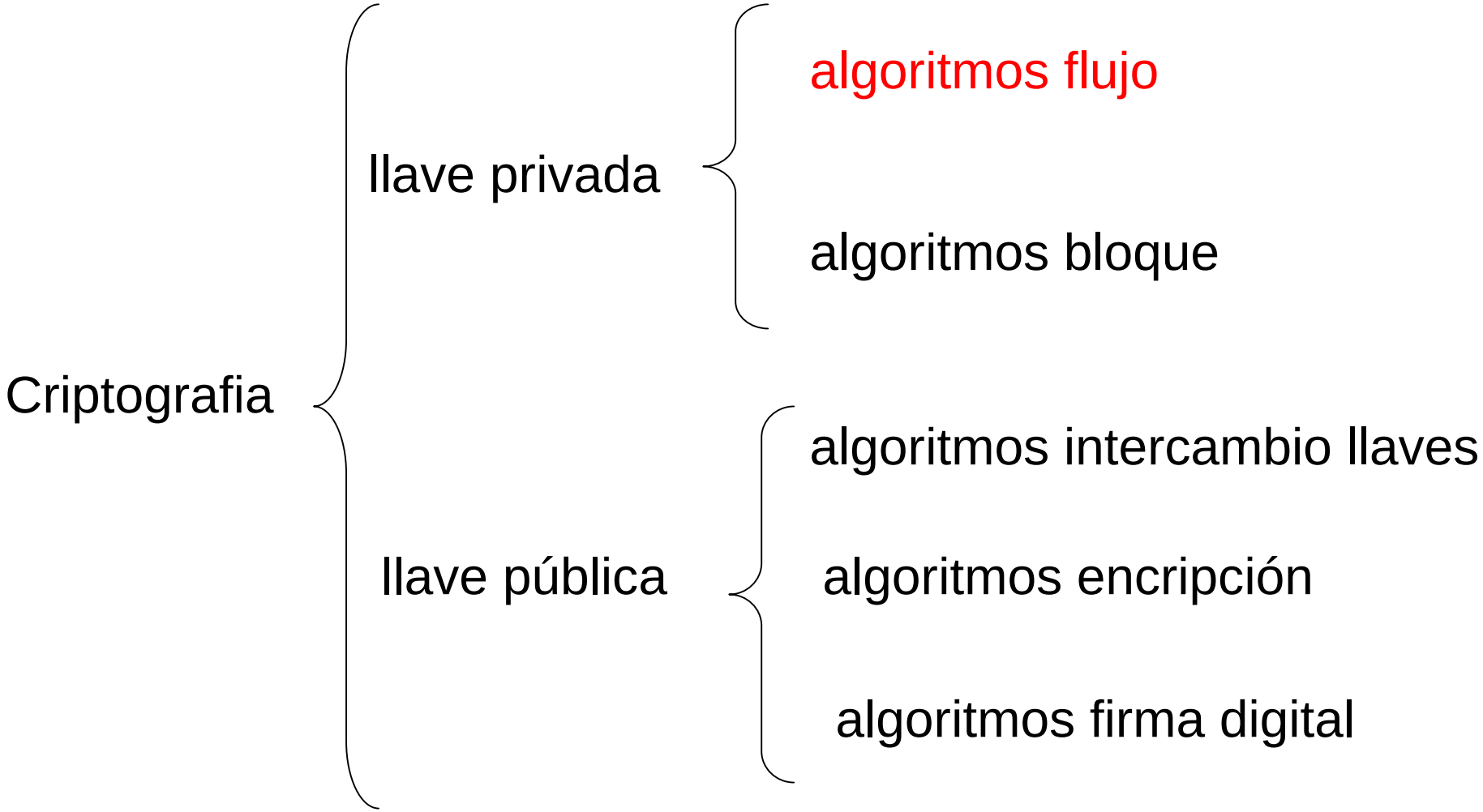
¿Pero que estamos buscando?

- Redes inalámbricas
  - Preferentemente con WEP deshabilitado
  - Preferentemente con DHCP habilitado

Servicio WAP de IEEE 802.11

- WAP: Wired Equivalency Privacy (WEP)
- Protección igual o mejor que las redes alambradas
- Uso de llaves para autenticar cada estación
- Puntos de acceso tambien requieren una llave para ser admitidos en la red
- Desarrollo de rotocolos de autenticación y de distribución de llaves se les deja a los vendedores
- Encripción opcional de datos entre estaciones usando algoritmo RC4

Un poco de cripto

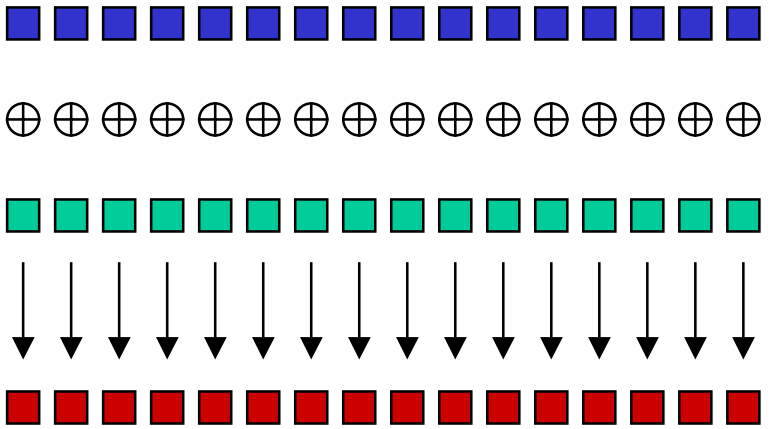


Encripción de criptosistemas de flujo

Texto Claro:

GNPA(semilla):

Criptograma:



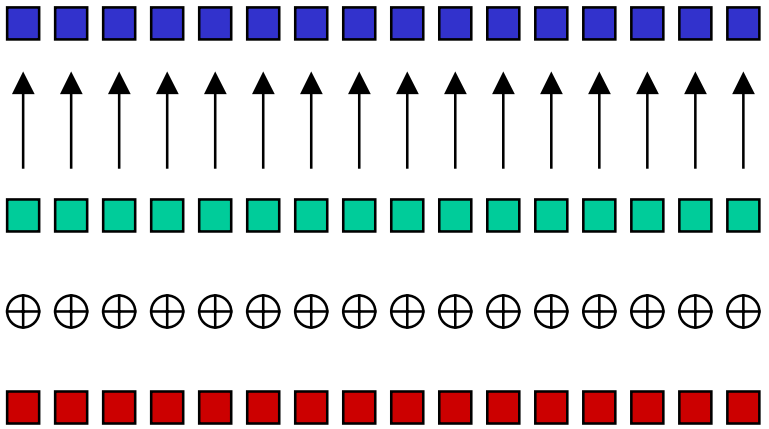
GNPA: Generador Números Pseudo-Aleatorios

Decripción de criptosistemas de flujo

Texto Claro:

GNPA(semilla):

Criptograma:



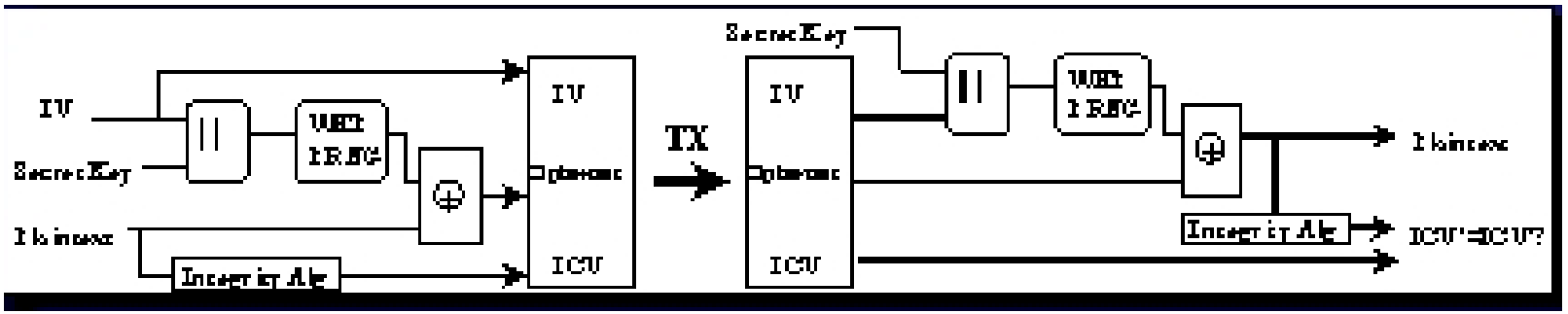
GNPA: Generador Números Pseudo-Aleatorios

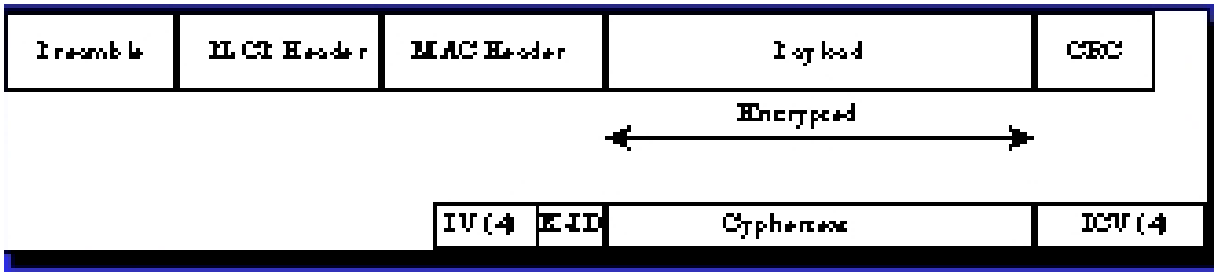
Algoritmo RC4

- Algoritmo propietario (RSA)
- Algoritmo de flujo
- Longitud llave variable (hasta 2048 bits)
- Algoritmo rápido
- Se dice que es un algoritmo muy fuerte
- Exportable fuera de US
- Algoritmo *dado a conocer* en internet en 1994

Encripción datos en IEEE 802.11

- La llave secreta es de 40 bits
- Se cuenta con un vector de inicalización de 24 bits





Comentarios sobre la seguridad IEEE 802.11

- Solo los datos de la estación estan encriptados
  - la identidad de la estación no se encripta
- El algoritmo se encuentra a nivel MAC (acceso) no actualizable
- Llaves de 40 bits
  - cortas para reducir overhead
  - ¿qué pasa con ataques de fuerza bruta?

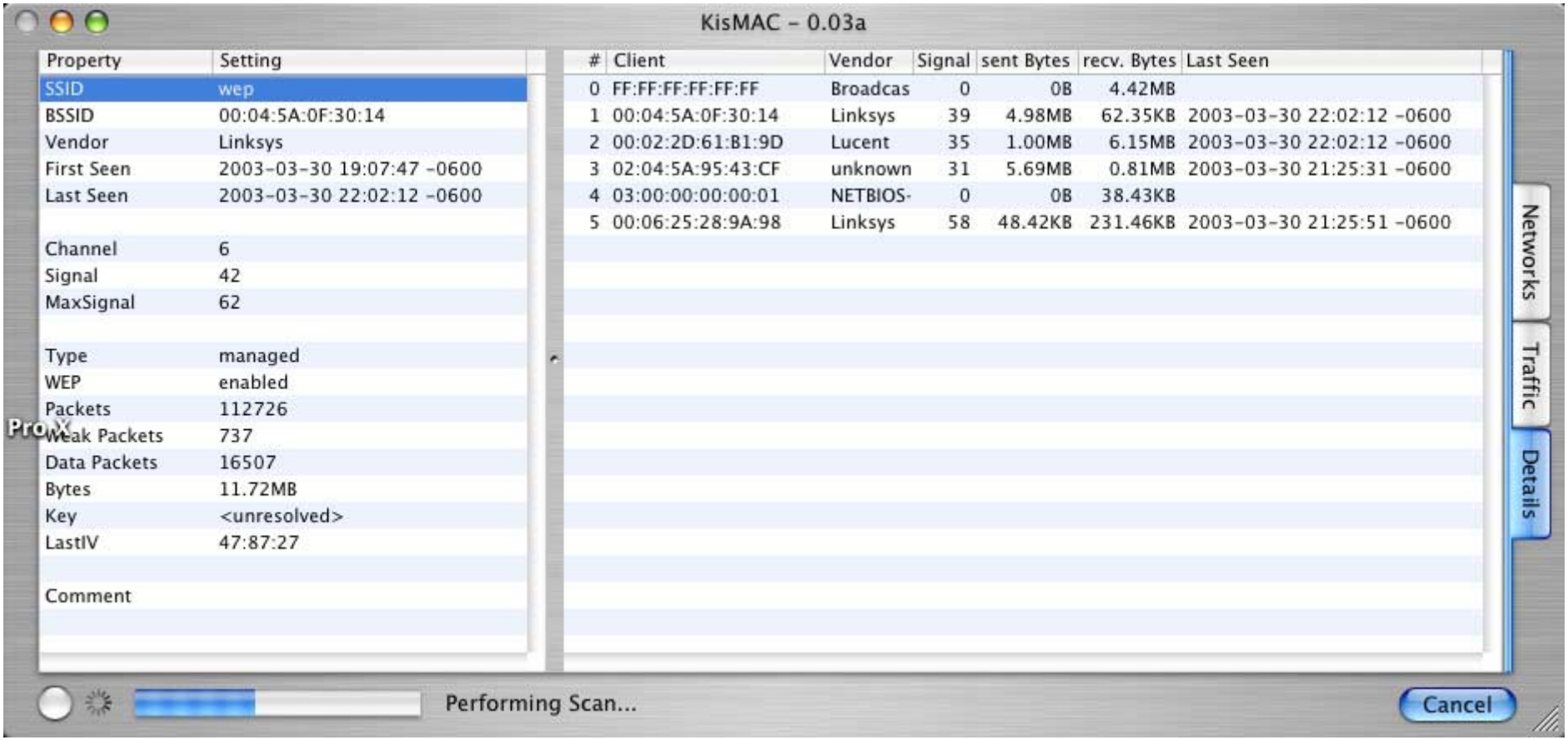
Atacando WEP

- Explotar las vulnerabilidades de la implementación de WEP en IEEE 802.11b:
  - Colisiones del vector de inicialización (“Weak Scheduling attack)
  - Brute-forcing (40 bits)
- Wired Equivalent Privacy
  - WEP utiliza un campo de 24 bits conocido como Vector de Inicialización (IV) que es utilizado como parte de la llave secreta compartida.
  - Sin embargo, el IV es incluido en el paquete en la porción de texto claro.
  - Debido a que el IV es solo de 24 bits (2^{24}=16,777,216)

Atacando WEP

- Un atacante lo que debe hacer es interceptar la cantidad de tráfico suficiente para capturar lo que se conoce como una colisión del IV, esencialmente la reutilización de un flujo de llave.
  - esta información puede ser utilizada para decifrar el tráfico.
- Se requiere entre 100MB y 1GB de información para que este ataque sea factible.
- Exiten herramientas que relizan esto:
  - KisMAC, AirSnort, WepCrack, Kismet.
- Adicionalmente,
  - JAMAS olvidar que es clásico usar contraseñas débiles ej: password, admin, wep, orinoco, nombre_compañía, etc.

Atacando WEP



Airsnort

- Herramienta para wireless LAN que recupera llaves de encriptación.
- Opera rastreando las transmisiones que pasan por la red inalámbrica.
- Una vez que han sido enviados suficientes bloques de información calcula la llave de encriptación utilizada.
- Todas las redes de 802.11b con 40/128 bit WEP (Wired Equivalent Protocol) son vulnerables, ya que tienen numerosas grietas de seguridad.

¿Cuanta información requiere?

- AirSnort, junto con WEPCrack son las primeras implementaciones públicas de este tipo de ataque.
- Requiere interceptar aproximadamente de 100MB a 1GB de datos, una vez que los tiene, AirSnort puede adivinar la llave de encriptación utilizada en menos de un segundo.

Prerequisitos de Airsnort

- Linux, wlan-ng drivers, 2.4 kernels.
- Para compilar AirSnort se requiere:
  - fuente del Kernel
  - paquete de PCMCIA CS.
  - paquete de wlan-ng
  - patch wlan-monitor-airsnort
- AirSnort requiere el juego de chips Prism2,
  - las tarjetas que lo poseen son las únicas capaces de llevar a cabo el sniffing necesario.

¿Es posible obtener tantos datos?

- Negocio con cuatro empleados que utilizan el mismo password.
- Estos empleados navegan por la red todo el día
  - generando alrededor de 1,000,000 de bloques de información al día,
  - de los cuales aproximadamente 120 de ellos son débiles.
- Después de 16 días es casi seguro que la red haya sido crackeada.
- En este ejemplo la red no esta saturada
  - en el caso de una red saturada generalmente este tiempo se reduciría a un solo día.

Algunas observaciones

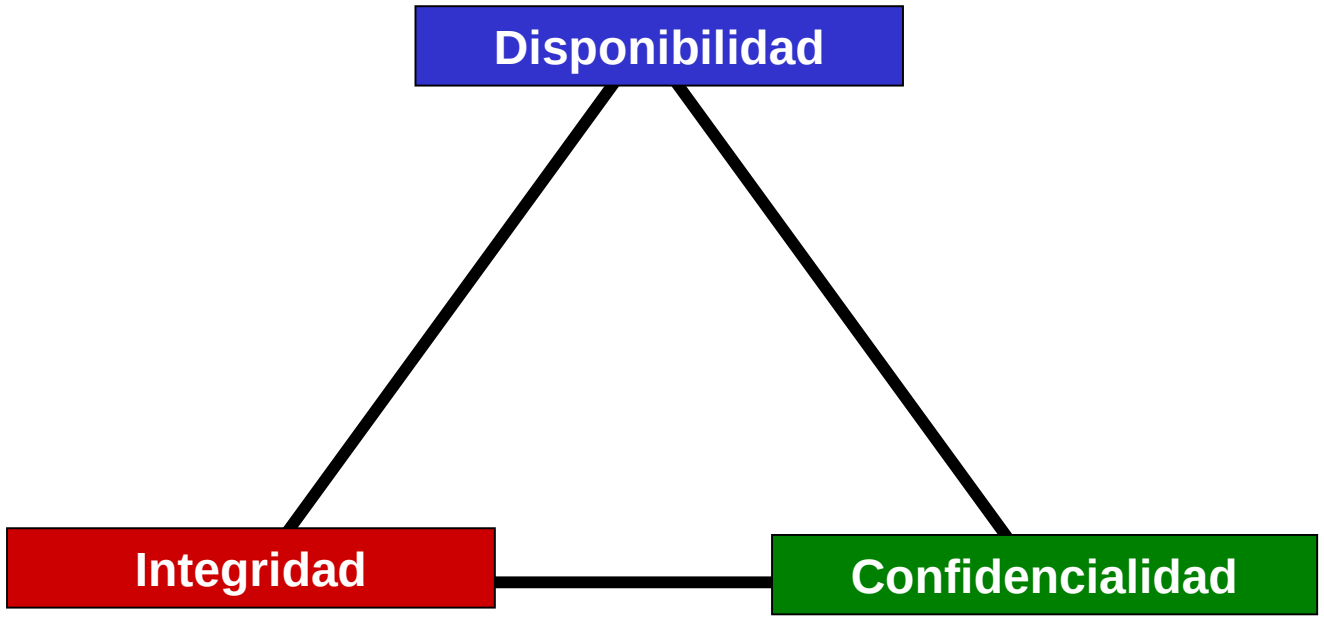
- Se esta atacando un *protocolo* que utiliza un *algoritmo de encripción*, no al algoritmo en si.
- Posibles acciones a tomar:
  - encriptar a niveles más altos del protocolo
  - actualizar a los estandares 802.11 cuando estos estén disponibles
  - tener cuidado con la generación de llaves
- RC4 es utilizado en otros protocolos “sin problemas”.

¿Y una vez conectado?

- Una vez que alguien ha logrado conectarse a una red inalámbrica todos los métodos de ataque en capa 2, capa 3, capa 4, ..., capa 7 son posibles:
  - Spoofing
  - Hijacking
  - Sniffing
  - DOS
  - Exploits
  - BruteForcing
  - Código Malicios (Worms)
  - ...

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.



La seguridad involucra 3 dimensiones (no sólo una)

Diseñar pensando en la seguridad

Roles y responsabilidades

Auditar dar seguimientos y rastrear

Mantenerse al día con el desarrollo de seguridad

Falta de conocimiento

Falta de comrpomiso

Falla humana

Los productos no cuentan con funciones de seguridad

Demasiado difícil mantenerse al día

Muchos problemas no se ven abordados por estándares técnicos (BS 7779)

Los productos tienen problemas

Asegurando el sistema

- Objetivo
  - minimizar los riesgos potenciales de seguridad
- Análisis de riesgos
  - análisis amenazas potenciales que se pueden sufrir,
  - las pérdidas que se pueden generar
  - y la probabilidad de su ocurrencia
- Diseño política de seguridad
  - definir responsabilidades y reglas a seguir para evitar tales amenazas o
  - minimizar sus efectos en caso de que se produzcan
- Implementación
  - usar mecanismos de seguridad para implementar lo anterior

Mecanismos de seguridad

- Son la parte más visible de un sistema de seguridad.
- Se convierten en la herramienta básica para garantizar la protección de los sistemas o de la propia red.
- Se dividen en:
  - prevención
  - detección
  - recuperación

Contramedidas – 802.11b

- Habilitar WEP con llave de 104 bits (128 bits)
- **Conectar los Access Points en una zona de seguridad "pública" (ó de bajo riesgo) posiblemente en una DMZ, jamás conectar la red inalámbrica a la red alámbrica de manera transparente.**
- Implementar un segundo nivel de seguridad:
  - VPN
  - IPSEC
  - SSL
  - SSH

Contramedidas 802.11b

- 802.11a promete ser más robusto en términos de seguridad (confidencialidad, integridad y autenticación), pero lo mismo se dijo cuando se diseñó y liberó 802.11b.
- Como siempre una de las mejores contramedida es el conocimiento profundo de la tecnología que se está utilizando/analizando.

Conclusiones

- No existe un 100% de seguridad.
- Tengo información sensible en mi institución/organismo
- Hay que definir políticas.
  - respetarlas y darle seguimiento
- Conforme la tecnología avanza se necesitan algoritmos más fuertes
- Sin embargo la tecnología de criptoanálisis también evoluciona.

Referencias

- Wireless Communications and Networks. William Stallings
- HackProofing Your Wireless Network. Varios.
- Wireless Maximum Security. Cyrus Peikari.
- www.netstumbler.com
- www.bitshift.org
- www.wirelesslanresource.com
- http://wlana.net

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"

XII CONGRESO NACIONAL DE ESTUDIANTES INGENIERIA DE SISTEMAS

XIICNEIS USACA – 2.003

Dr. Roberto Gómez Cárdenas

DCC del ITESM-CEM

rogomez@itesm.mx

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