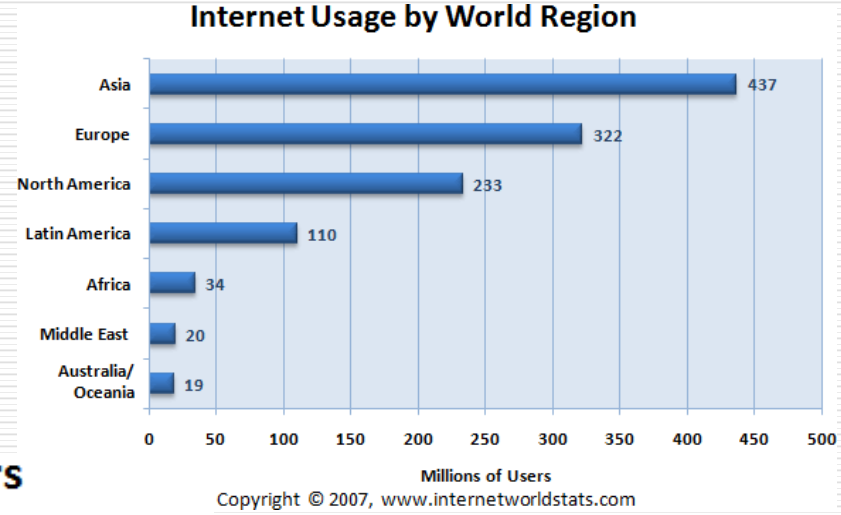
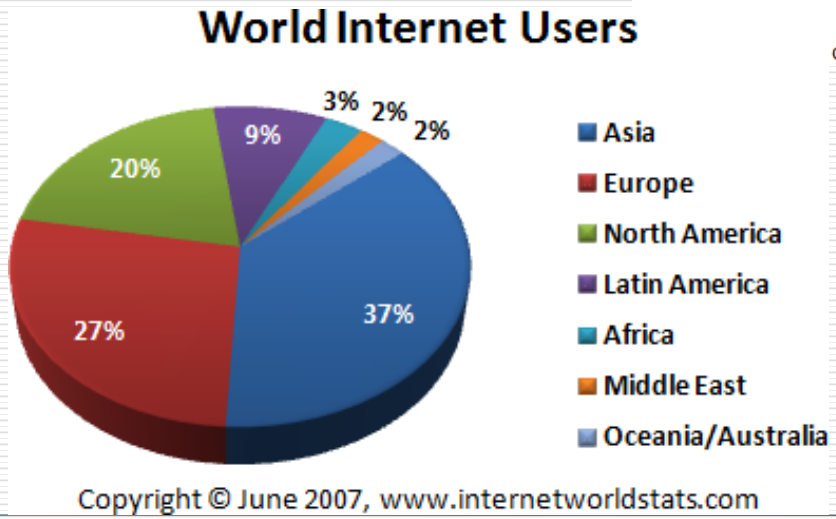
Seguridad en Redes Inalámbricas

Adrián Puente Z.
Security Project Leader
adrian@sm4rt.com
Twitter: @ch0ks
Tikkia: adrianpuente
www.hackarandas.com

Internet en el Mundo

- Latinoamérica como el 4 lugar en el mundo con 110 millones de usuarios





Internet en México

- Según la AMIPCI:
  - 55% son hogares
  - 3.9 Millones de cuentas de banda ancha
  - El 56% usa Wi-Fi

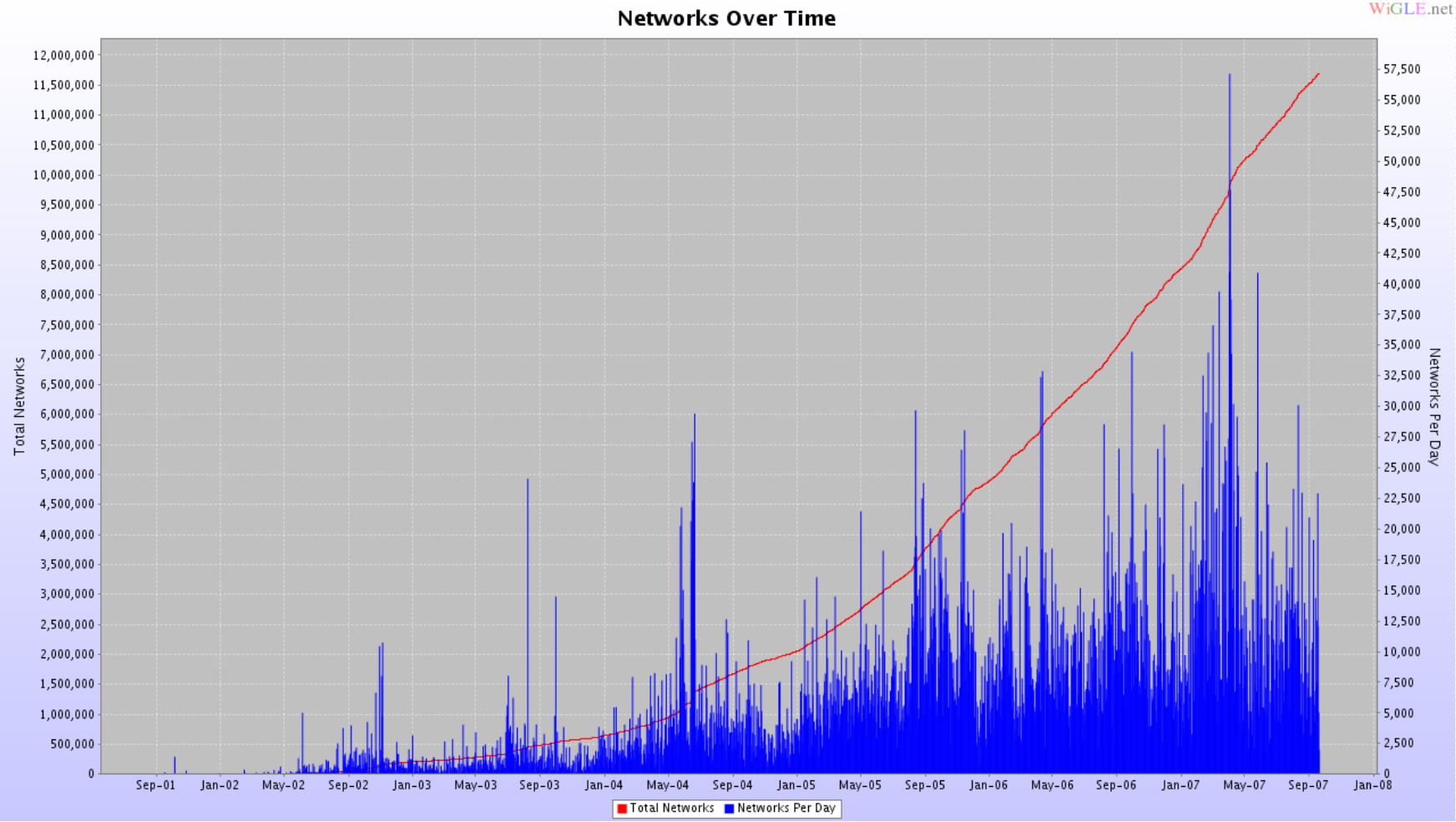
Año	Usuarios	Población	% Pen.	Fuente
2000	2,712,400	98,991,200	2.74%	ITU
2004	14,901,687	102,797,200	14.50%	AMIPCI
2005	17,100,000	103,872,328	16.46%	AMIPCI
2006	20,200,000	105,149,952	19.21%	AMIPCI
2007	22,700,000	106,457,446	21.32%	AMIPCI

El Internet en México

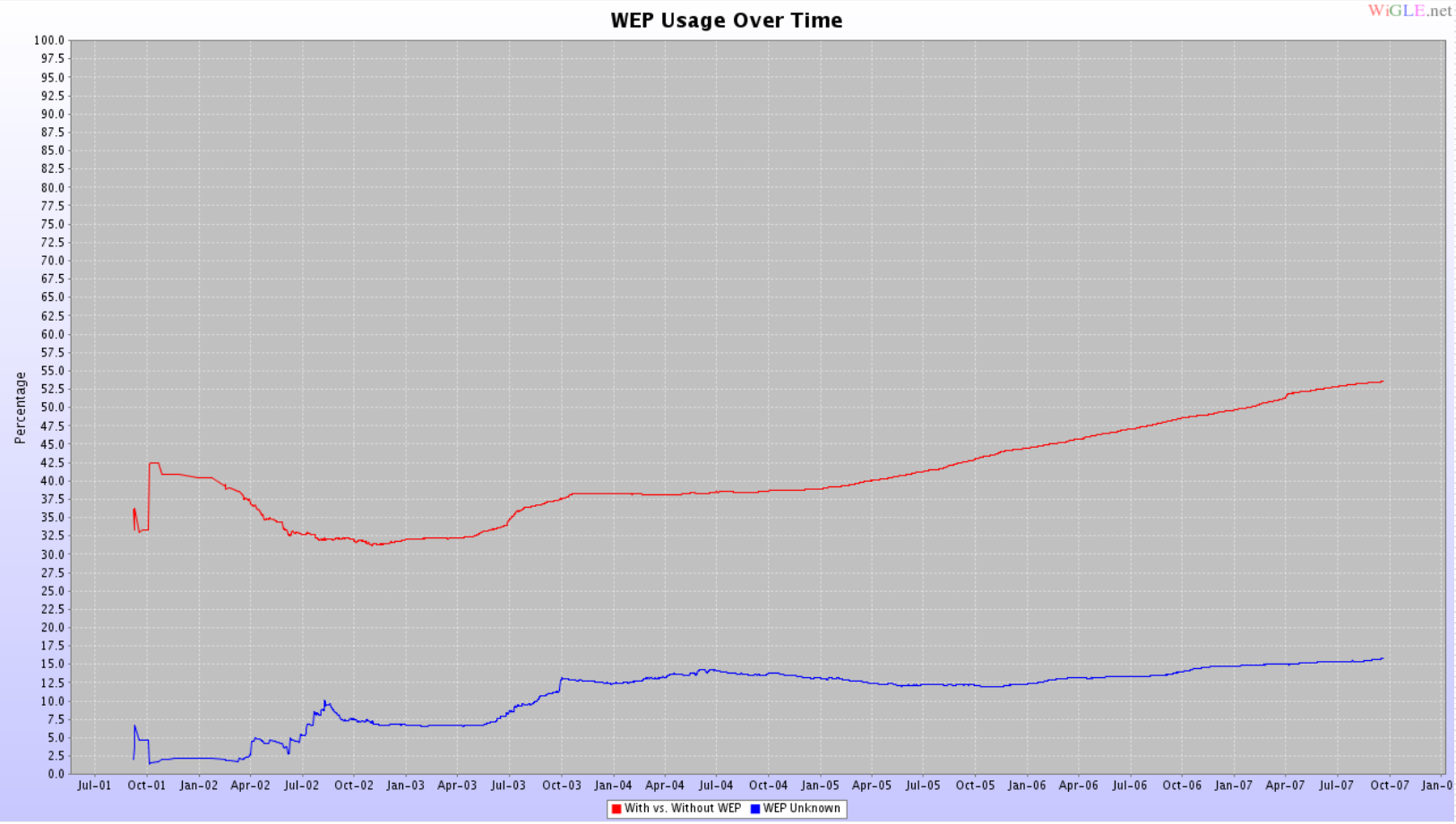
Tipo de uso	2001 a		2002 a		2004 b		2005 b		2006 c	
	Absolutos	Por ciento	Absolutos	Por ciento	Absolutos	Por ciento	Absolutos	Por ciento	Absolutos	Por ciento
Usuarios de Internet	**7 047 172**	**100**	**10 764 715**	**100**	**12 945 888**	**100**	**16 492 454**	**100**	**18 746 353**	**100**
Para obtener cualquier tipo de información general	4 251 094	60.3	5 797 991	53.9	5 433 471	42	10 112 004	61.3	7 773 638	41.5
Correo Electrónico	4 262 301	60.5	5 198 439	48.3	5 548 242	42.9	6 826 347	41.4	6 644 801	35.4
Educación	2 334 371	33.1	2 668 644	24.8	3 503 814	27.1	5 027 819	30.5	6 628 513	35.4
Chat	2 888 374	41	3 909 513	36.3	4 493 476	34.7	2 560 654	15.5	3 617 764	19.3
Para obtener información de bienes y servicios	328 398	4.7	850 955	7.9	1 057 775	8.2	1 482 048	9	1 466 434	7.8
Para jugar o descargar videos	ND	NA	ND	NA	ND	NA	1 200 995	7.3	1 844 664	9.8
Para obtener información de las organizaciones gubernamentales	ND	NA	ND	NA	ND	NA	917 040	5.6	1 113 740	5.9
Para realizar servicios bancarios o financieros	ND	NA	ND	NA	ND	NA	262 784	1.6	400 658	2.1
Para llenar formatos oficiales en los sitios de organizaciones gubernamentales	ND	NA	ND	NA	ND	NA	142 110	0.9	299 265	1.6
No especificado	72 536	1	22 892	0.2	204 444	1.6	95 702	0.6	63 156	0.3

NOTA:	Se refiere a la población de seis o más años. La suma de los parciales no corresponde con el total por ser una pregunta de opción múltiple.
a	Cifras correspondientes al mes de diciembre.
b	Cifras correspondientes al mes de junio.
c	Cifras preliminares correspondientes al mes de abril.
NA	No aplicable.
ND	No disponible.
FUENTE:	**INEGI. Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares.**

Uso de Redes Inalámbricas



Uso de WEP en Redes Inalámbricas



Costo / Funcionalidad / Seguridad

sm4rt securityservices

- El costo de la tenología disminuye
- La funcionalidad aumenta
- La cultura permanece

\- Costo
\+ funcionalidad
* cultura

H4ckersPl4yground XD

Wireless

- ¿Qué es Wireless?
  - Es la referencia de cualquier operación eléctrica o electrónica que no involucre cables
    - IrDa
    - Wi-Fi
    - Bluetooth
    - ZigBee
    - Telefonía celular digital y analógica
    - Comunicaciones satelitales
      - Radio FM y AM
      - Televisión
      - Internet Satelital

Wi-Fi

- ¿Qué es Wi-Fi?
  - Es una rama de la Wi-Fi Alliance que busca mejorar la interoperabilidad de las redes inalámbricas locales con productos basados en el IEEE 802.11
- Modos de conexión
  - Ad-Hoc, Infraestructura, Master, Monitor.
- Tipos de conexión
  - Abierto (sin cifrado), WEP, WPA, WPA.
- Algortitmos
  - WEP, TKIP, 802.1X, AES-CCMP

WEP (Wired Equivalent Privacy)

- Implementacion de cifrado para mejorar el esquema de abierto
- Implementaciones
  - 64 = llave de 40 bits con 24 bits de vector de inicialización
  - 128 bits = llave de 104 bits con 24 bits de vector de inicialización
  - Existe de 256 bits para algunos dispositivos

WEP (Wired Equivalent Privacy)

- Usa el algoritmo de cifrado RC4 para la confidencialidad mientras que el CRC-32 proporciona la integridad.
- El RC4 funciona expandiendo una semilla para generar una secuencia pseudoaleatoria de mayor tamaño.
- Especifica un vector de iniciación (IV) de 24 bits que se modifica regularmente y se concatena a la contraseña para generar la llave

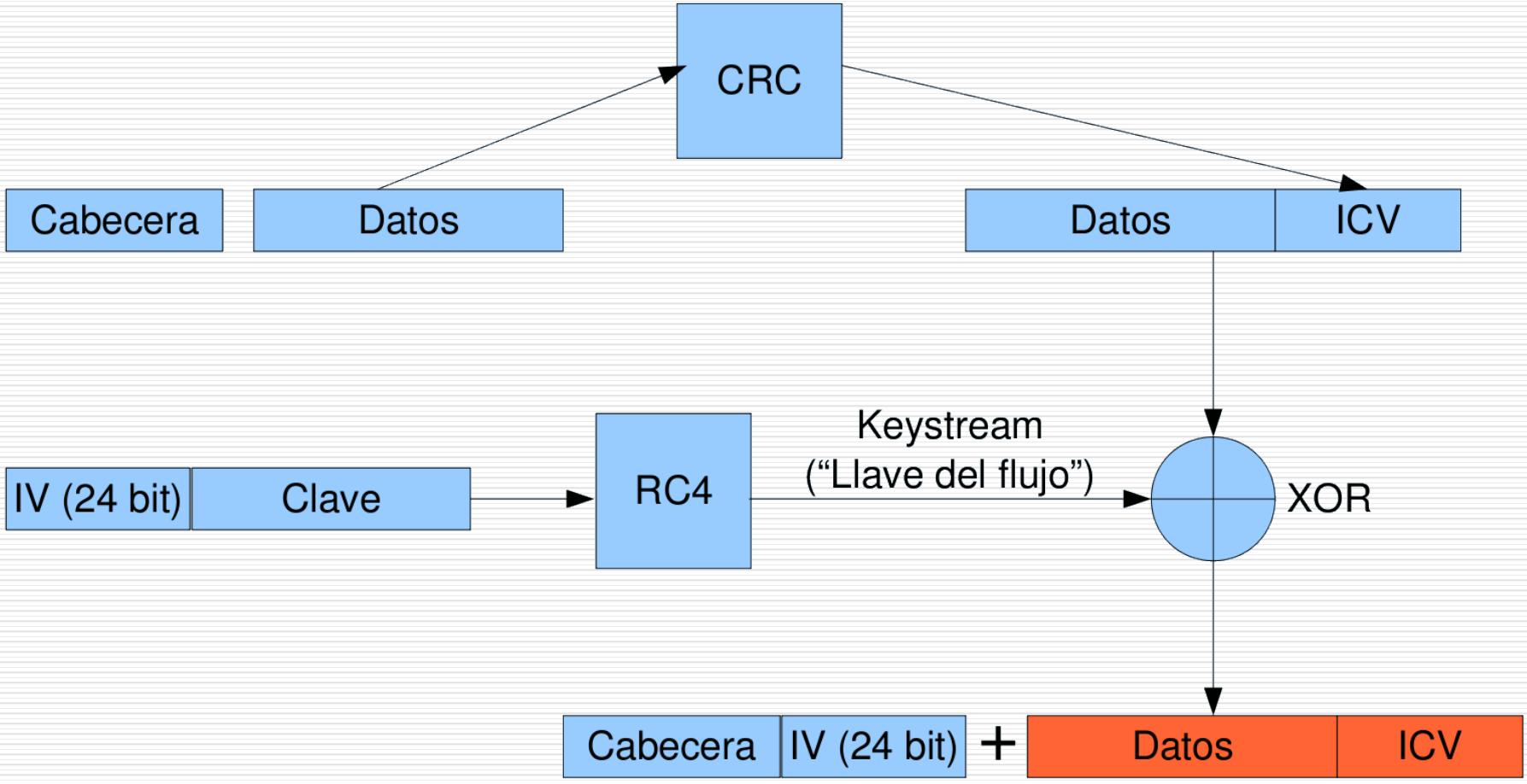
WEP - Mecanismos de Autenticación

- Open System Authetication
  - No provee autenticación, sino identificación usando la dirección MAC del dispositivo.
  - El cliente envía un bloque de administración de autenticación IEEE 802.11 que contiene su identidad.
  - El AP checa la inicialización de autenticación de identidad y devuelve un bloque de verificación de autenticación.
  - El cliente se conecta a la red.

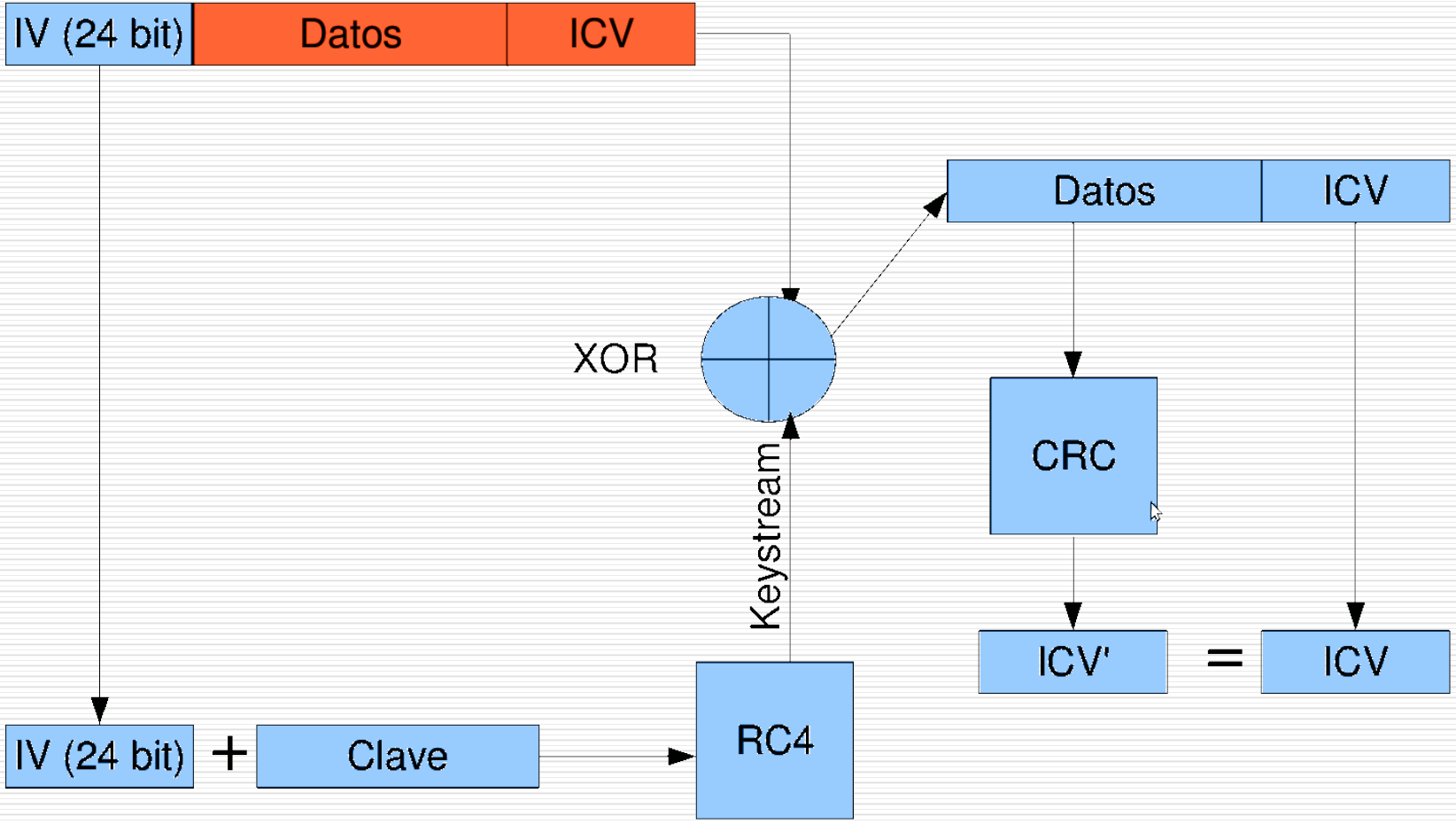
WEP - Mecanismos de Autenticación

- Shared Key Authentication
  - Es muy insegura y no se recomienda usar. Sólo verifica que la estación tiene conocimiento de la clave precompartida.
  - El cliente manda una solicitud de autenticación al AP
  - El AP devuelve un reto de autenticación
  - El cliente emplea la llave compartida de 64 o 128 bits para cifrar la el reto y devolverlo al AP
  - El AP descifra el reto con la llave compartida y si esta corresponde a la enviada autentica al cliente y le da acceso a la red

WEP – Esquema de Cifrado



WEP – Esquema de Descifrado



WEP - Vulnerabilidades

- No se implementa adecuadamente el vector de iniciación del algoritmo RC4
- Utiliza un enfoque directo y predecible para incrementar el vector de un paquete a otro.
- Además existe un problema con el tamaño de los vectores de iniciación
- Los IV's se transmiten en plaintext
- Vulnerabilidad Shared Key Authentication

WEP – Herramientas de Cracking

- Herramientas de cracking
  - Wep0ff
  - aircrack-ng
  - aircrack-ptw
  - AirSnort
  - WEPCrack
  - Weplab
  - Kismet, KisMAC, and KisWin

WEP – Alternativas Comerciales

- Para el 2004 el WEP fue revocado y sustituido por el WPA.
- WEP2 usa cifrado y vector de iniciación de 128-bits. aun mantiene las mismas vulnerabilidades del WEP.
- WEP+ por Agere Systems. Evita IV’s débiles. Eficaz cuando WEP+ es usado a ambos extremos y no previene los ataques de Replay.
- Wep Dinámico cambia las claves WEP de forma dinámica.

Cracking WEP – Video Demo

- http://is.gd/rP5k

WPA (Wi-Fi Protected Access)

- Una enorme mejoría sobre WEP
- WPA adopta la autentificación de usuarios mediante el uso de un servidor, donde se almacenan las credenciales y contraseñas de los usuarios de la red.
- Permite la autentificación mediante clave compartida ([PSK], Pre-Shared Key), que de un modo similar al WEP, requiere introducir la misma clave en todos los equipos de la red.
- Implementación del TKIP (Temporal Key Integrity Protocol)

Wi-Fi Protected Access WPA

- Medida intermedia hasta WPA2 o 802.11i (2004)
- Autenticación
  - Modo Personal / PSK (PreShared Key)
  - Modo Empresarial / 802.1x

		WPA	WPA2
Modo Personal	Autenticación	PSK	PSK
	Cifrado	TKIP (RC4) / MIC	CCMP (AES) / CBC-MAC
Modo Empresarial	Autenticación	802.1x / EAP	802.1x / EAP
	Cifrado	TKIP (RC4) / MIC	CCMP (AES) / CBC-MAC

TKIP (Temporal Key Integrity Protocol)

- Cambia claves dinámicamente a medida que el sistema es utilizado.
- Mejora la integridad de la información cifrada. La CRC (Cyclic Redundancy Check)
- Implementa el MIC (Message Integrity Code), también conocido como "Michael"
- Incluye protección contra ataques de "repetición"

WPA – Autenticación PSK

- Clave compartida previamente
- Se introduce la contraseña en cada estación para acceder a la red
- Son de 8 a 63 caracteres (pasphrase) o una cadena de 256 bits
- Clave para iniciar la autenticación, no para el cifrado
- Nada garantiza que la clave sea compleja
- Al final los caracteres ASCII se les hace un hash reduciendolo de un máximo de 504 a 256 bits
- El ataque consiste en capturar el intercambio de llave cifrada y realizar un criptoanálisis

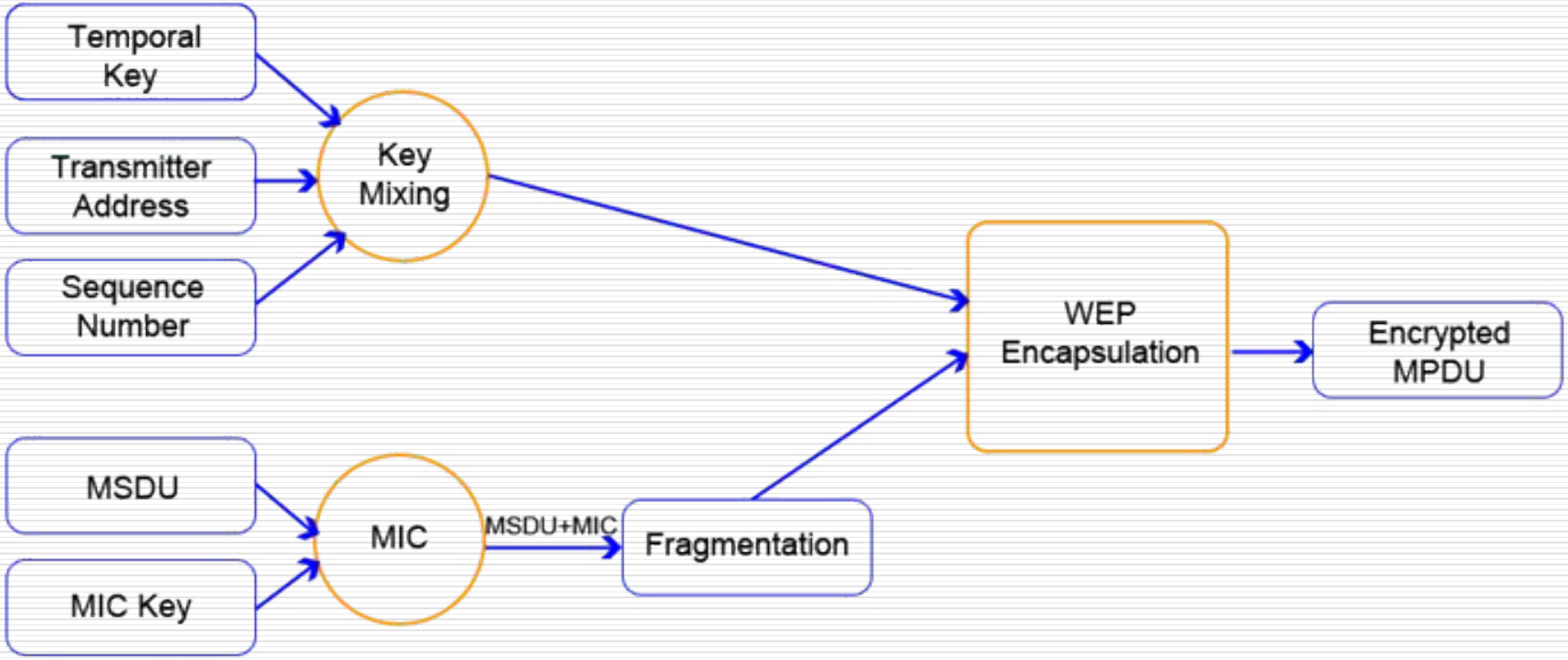
WPA – PSK - TKIP

- Creado para sustituir WEP
- Clave temporal de 128 bits Compartida entre los clientes y los puntos de acceso.
- Combina la clave temporal con la dirección MAC del cliente y agrega un vector de inicialización de 16 octetos para la clave que cifrará los datos.
- Cada estación utiliza diferentes streams claves para cifrar los datos.

WPA – PSK - TKIP

- El hashing de clave WEP protege a los vectores de inicialización (IVs) débiles para que no sean expuestos haciendo hashing del IV por cada paquete
- Utiliza el RC4 para el cifrado,igual que WEP
- Cambia las claves temporales cada 10.000 paquetes
- Utiliza el algorimo MIC para la integridad

WPA – PSK - TKIP


Temporal Key
Transmitter Address
Sequence Number
Key Mixing
MSDU
MIC Key
MIC
MSDU+MIC
Fragmentation
WEP Encapsulation
Encrypted MPDU

WPA - Vulnerabilidad

- Debilidad algoritmo Michael
  - Es invertible
- Debilidad TKIP
- Ataque de diccionario offline contra PSK (passphrase)
  - Capturar 2 primeros paquetes del 4-Way Handshake
  - Diferencias WPA y WPA2, la función para calcular el MIC
  - Aircrack, genpmk, cowpatty

Cracking WPA con TKIP – Video Demo

- http://is.gd/rPbt

WPA2

- Conocido como RSN (Robust Security Network). Es la implementación del 802.11i
- Emplea el AES donde el WPA y el WEP usan RC4
- 802.1X para Autenticación
- RSN para administrar las asociaciones
- Un Algoritmo CCMP basado en AES para tener privacidad, integridad y autenticación del origen
- Implementa el Four-Way Handshake

WPA2 – CCMP

- Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
- Parte obligada del WPA2 y opcional del WPA.
- Reemplaza el TKIP del WPA y al WEP
- Emplea AES y a diferencia del TKIP
- La administración de la llave y la integridad del mensaje es manepor un solo componente alrededor del AES.

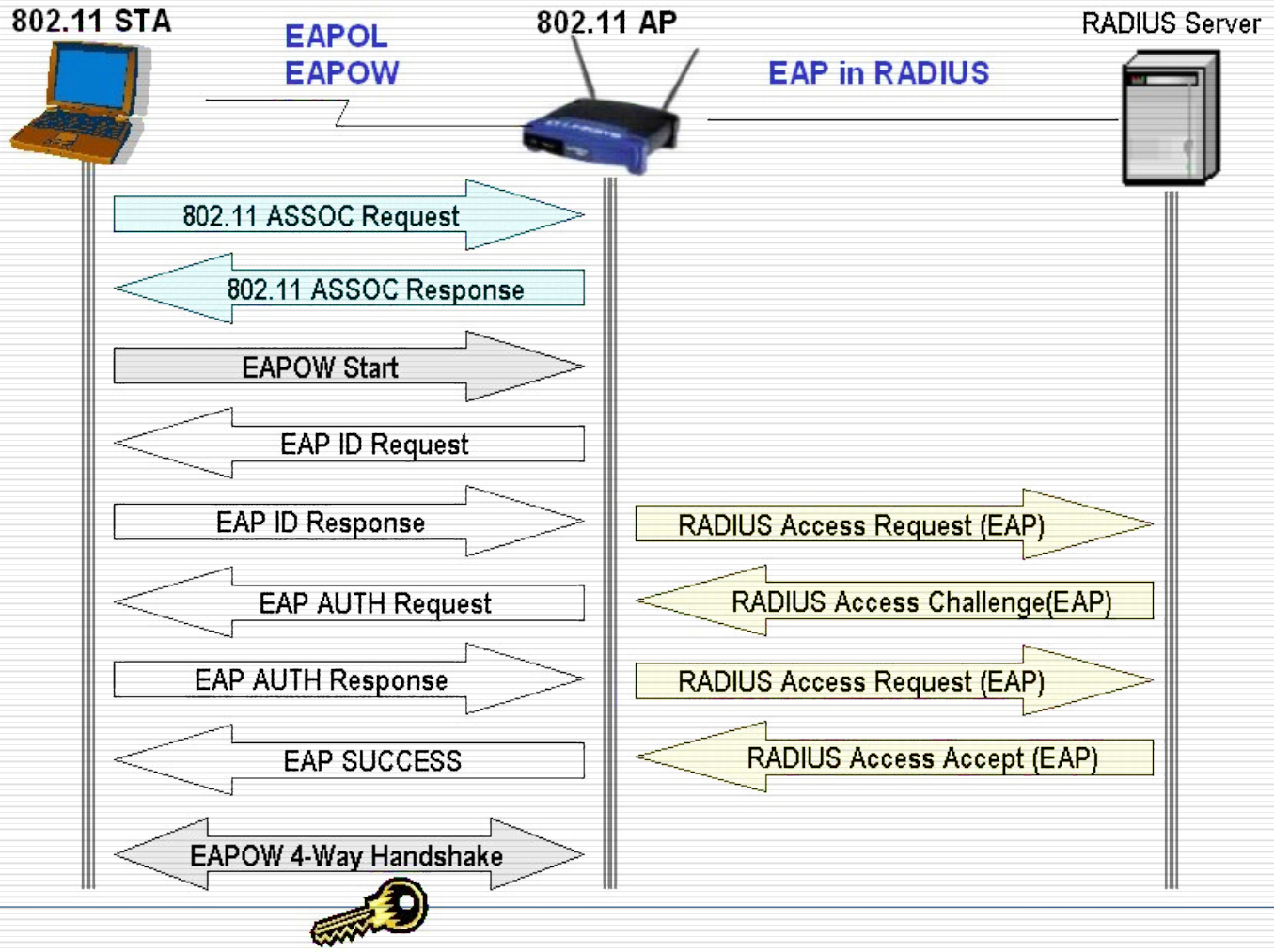
WPA/WPA2 – Autenticación 802.1x

- También implementación en redes cableadas
- Requiere servidor configurado (RADIUS)
- Se basa en puertos: Un puerto por cliente
- Para el control de admisión utiliza EAP (Extensible Authentication Protocol),
- Hace posible la comunicación entre clientes (solicitantes) y servidores de autenticación (ej. RADIUS)

WPA/WPA2 – Autenticación 802.1x

- Componentes:
  - Suplicante: estación inalámbrica que quiere acceder a la red.
  - Estación Autenticador: realiza el control de acceso, habilita el puerto tras la autenticación. Punto de acceso
  - Servidor de autenticación: comprueba si el cliente esta autorizado para acceder a la red. Servidor AAA (Authentication, Authorization, Accounting) como RADIUS

WPA/WPA2 – Autenticación 802.1x



WPA/WPA2 – Autenticación 802.1x

- Muchas variantes, algunas incluyen certificados digitales validados por PKI
  - EAP-TLS (previously tested)
  - EAP-TTLS/MSCHAPv2
  - PEAPv0/EAP-MSCHAPv2
  - PEAPv1/EAP-GTC
  - EAP-SIM
- ¿Invencible?

Hackers de Wi-Fi

- ¿Que busca un hacker de Wi-Fi?
  - Obtener información confidencial
  - Conseguir acceso a una zona restringida
  - Controlar un segmento
  - Reconocimiento o remuneración
- ¿Cómo lo consigue?
  - Ingeniería social
  - Critoanálisis
  - Error humano
    - mala implementación
    - post-it

Panorama Actual

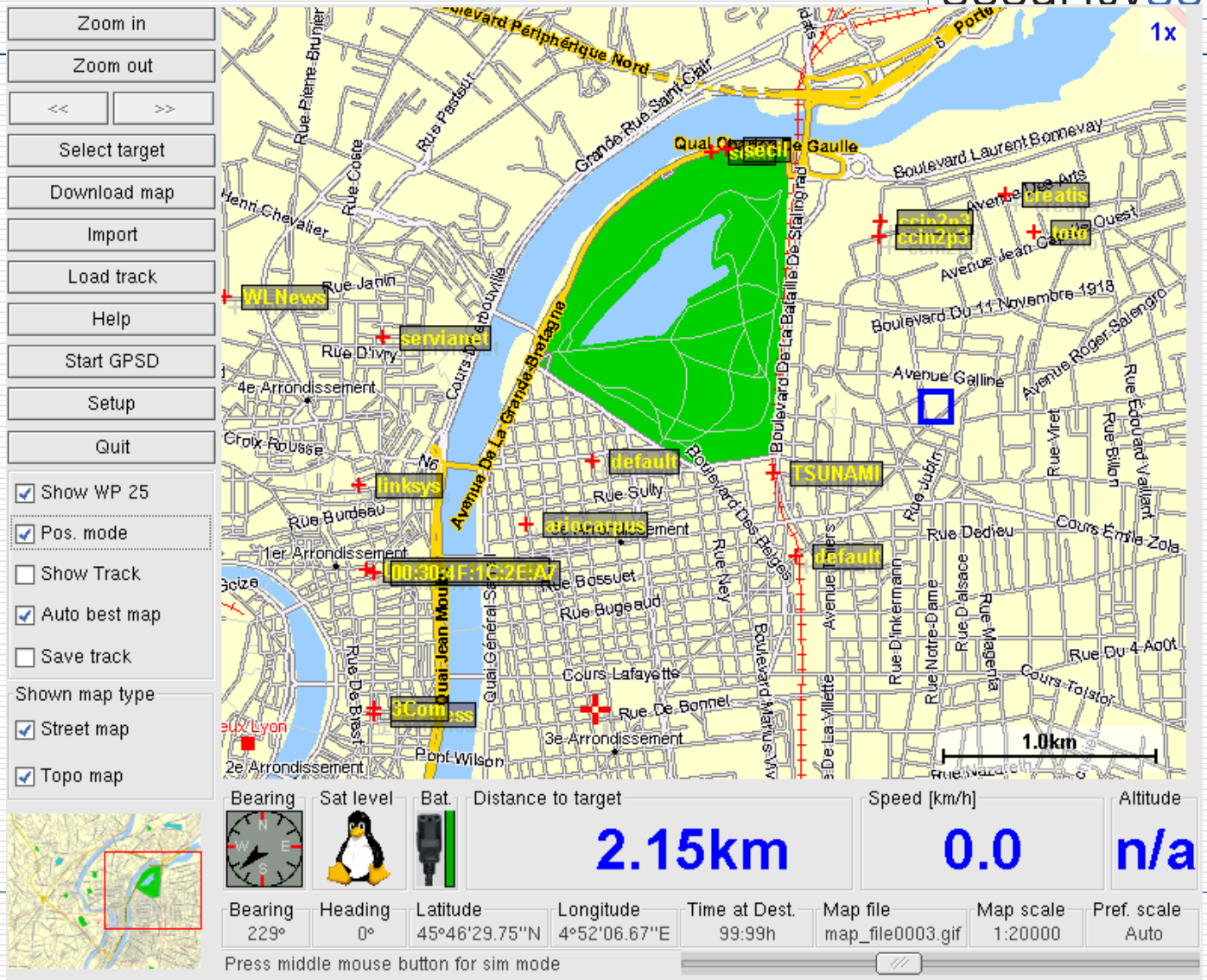
- Se crean nuevas tecnologías mucho mas rápido que nuevas leyes.
- Ignorancia de la víctima
- Poco seguimiento del ataque
- Ignorancia de las autoridades
- Diferencias entre las leyes entre países
- Anarquía

Wardriving

- Es la actividad de manejar mientras se detectan redes inalámbricas y se registran.
- Muchas veces se combina el GPS con el Wardrive para localizar la red en un mapa
- De esta actividad se derivan
  - Warwalking
  - Warflying
  - Walkchalking
  - ¿Warcycling?

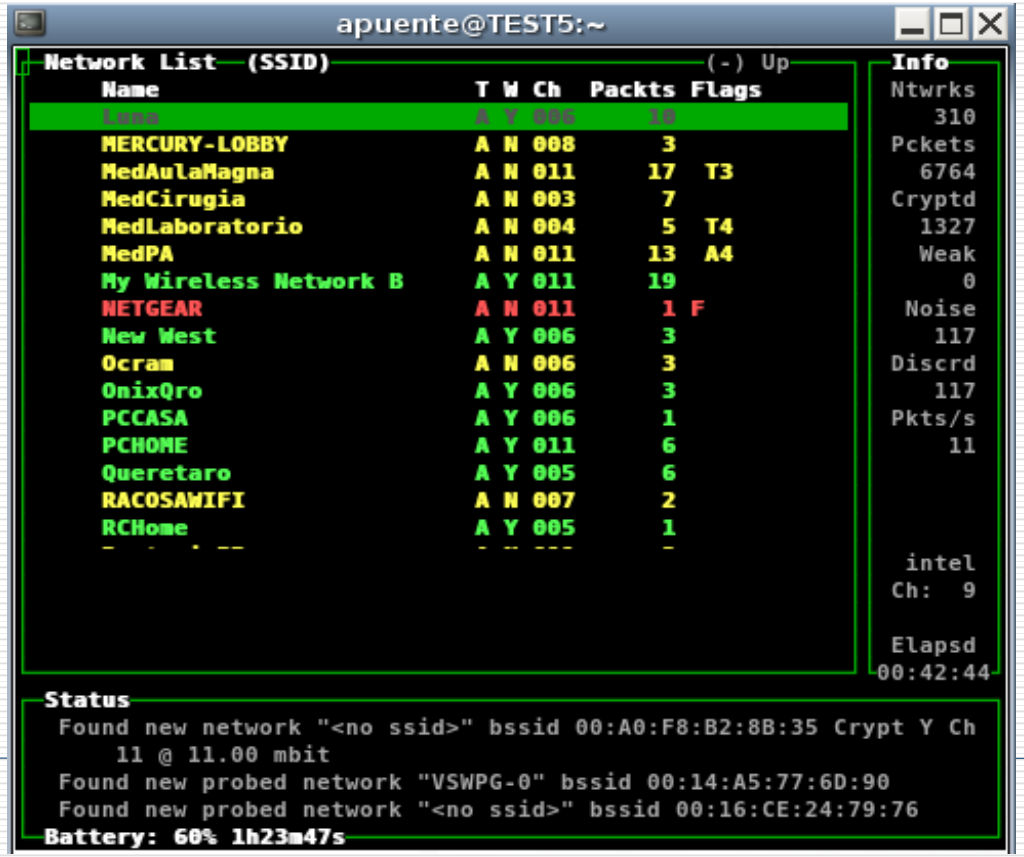
Wardriving

sm4rt securityservices



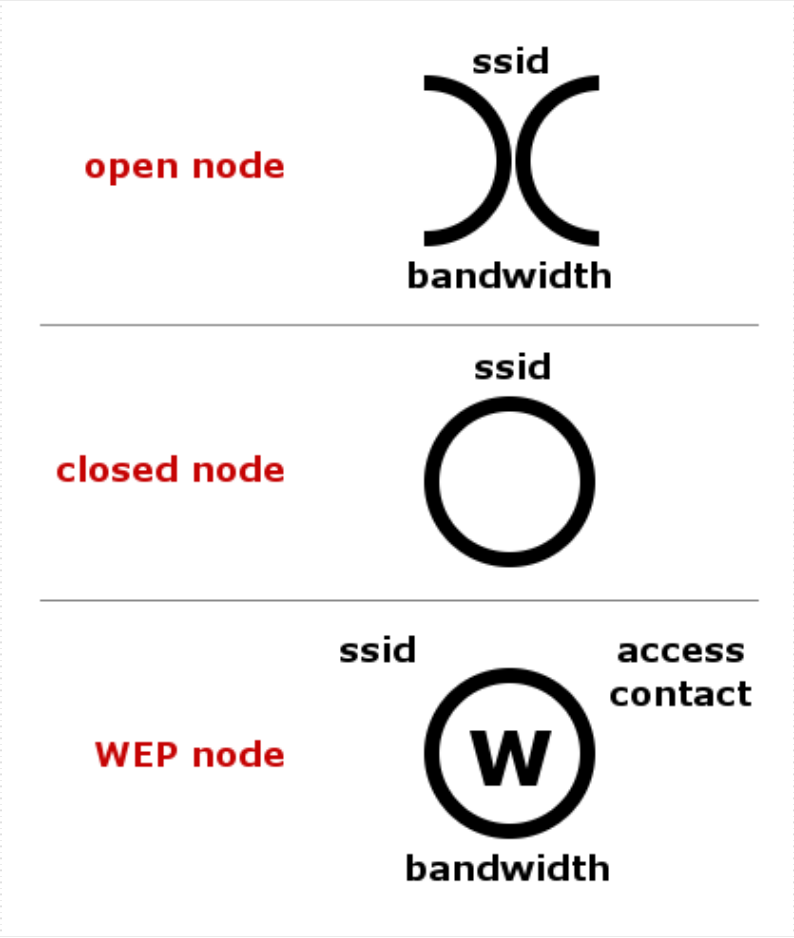
Wardriving

- De Querétaro a Celaya observé hasta 310 redes inalámbricas de diferentes tipos en 43 minutos.



Walkchalking

- Es ir caminando y marcar en la pared o suelo símbolos que describan la red localizada



Enchúlame la Tarjeta

- Hay modificaciones en hardware para mejorar sus ataques

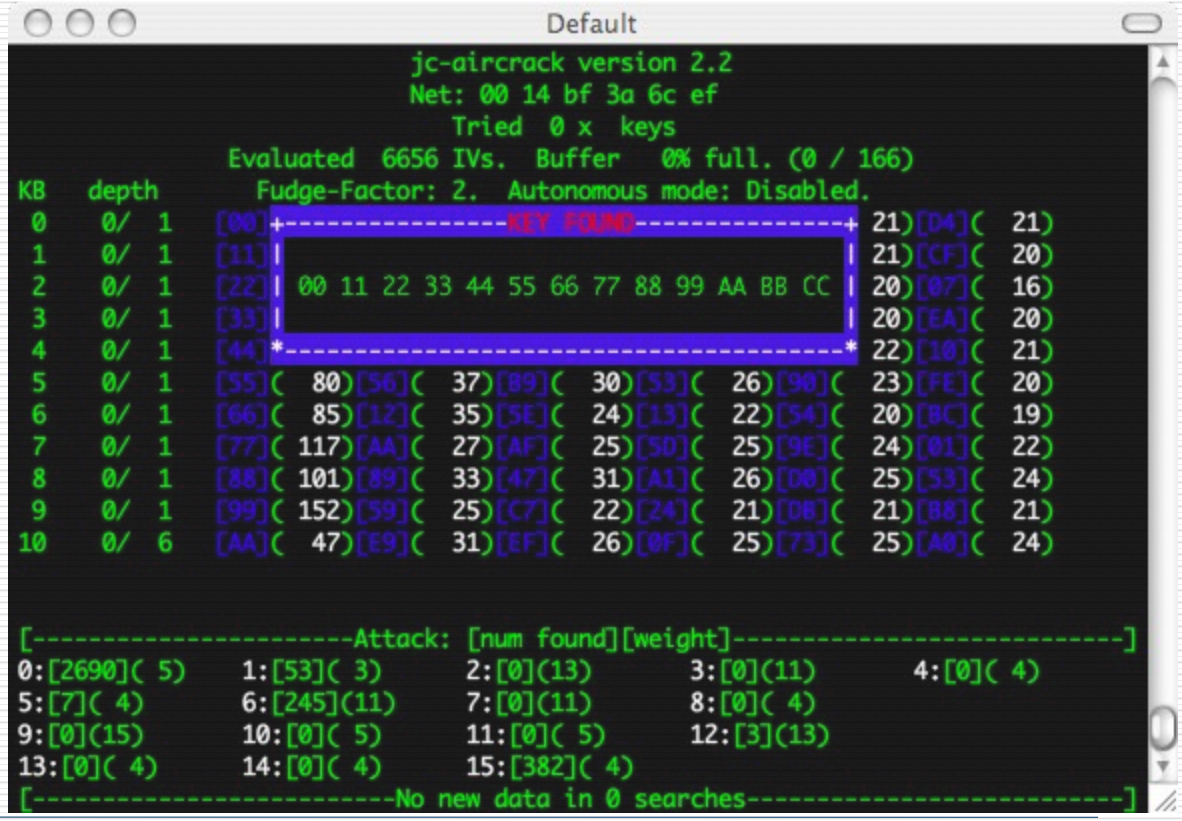
Enchúlame la Tarjeta

sm4rt securityservices

Enchúlame la Tarjeta

Mejora del Software

- Nuevos algoritmos de criptoanálisis
  - aircrack-ng
  - aircrack-ptw
  - airoscript
  - cowpatty
  - genpmk



Mejora del Software

- Distribuciones live CD expecializadas
  - Backtrack
  - Wifislax
  - Wifiway

Cómo Protegerme

- Si no requieres tener red inalámbrica no la pongas
- Asigna contraseña al Access Point.
- Esconde el ESSID que aún así se puede obtener y cámbiaselo a algo que no diga 2WIRE[HACKME]
- Usa al menos WEP de 128, sí puedes WPA aunque los dispositivos mas viejos no lo soportan

Cómo Protegerme

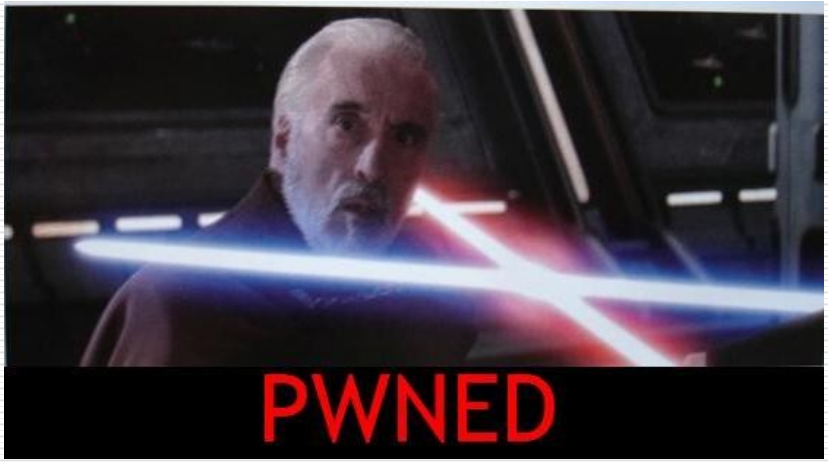
- Filtra las MACs de las máquinas si no tienes demasiadas aunque esto se puede hacer un infierno en grandes redes
- Cambia seguido la clave WEP y la contraseña del Access Point
- Revisa tu Access cada que puedas, este logea las máquinas que se han conectado, si ves alguna máquinas desconocida cambia las contraseñas

Cómo Protegerme

- Cambia el sistema operativo de tu Linksys por Tomato o DD-WRT o mantén actualizado tu firmware
- Asigna firewalls personales a tus máquinas y quita carpetas compartidas que no sean necesarias y las que si ponles permisos por grupos o usuarios.
- Ponle contraseñas a los usuarios de las máquinas, al menos al Administrador

Nada es Seguro

- Las medidas de seguridad mitigan los ataques
- Algo es mejor que nada
- Aún así... nada es seguro



La Tecnología Evoluciona – MIMO

- Multiple Input Multiple Output (MIMO) o Pre-N

- Es una técnica de antenas inteligentes que incrementan la velocidad, rango, confiabilidad y eficiencia espectral de los sistemas inalámbricos.

La Tecnología Evoluciona - 802.11n

- Propuesta de modificación al estándar IEEE 802.11-2007.
- Incremento significativo en la velocidad máxima de transmisión de 54 Mbps a un máximo de 600 Mbps.
- Utiliza MIMO generando canales de trafico simultáneos entre las diferentes antenas de los productos 802.11n
- Canales de 20 y 40 Hz (Lo que permite incrementar enormemente la velocidad)
- El uso de las bandas de 2,4 y 5 Ghz simultáneamente

La Tecnología Evoluciona - WiMax

- WIMAX son las siglas de Worldwide Interoperability for Microwave Access (interoperabilidad mundial para acceso por microondas).
- Es una norma de transmisión de datos usando ondas de radio.
- Permite la recepción de datos por microondas y retransmisión por ondas de radio. El protocolo que caracteriza esta tecnología es el 802.16.
- Permite velocidades de hasta 70 Mbps.

La Tecnología Evoluciona - WiMax

Estándar	Descripción
802.16	Utiliza espectro licenciado en el rango de 10 a 66 GHz, necesita línea de visión directa, con una capacidad de hasta 134 Mbps en celdas de 2 a 5 millas. Soporta calidad de servicio. Publicado en 2002.
802.16a	Ampliación del estándar 802.16 hacia bandas de 2 a 11 GHz, con sistemas NLOS y LOS, y protocolo PTP y PTMP. Publicado en abril de 2003
802.16c	Ampliación del estándar 802.16 para definir las características y especificaciones en la banda d 10-66 GHz. Publicado en enero de 2003
802.16d	Revisión del 802.16 y 802.16a para añadir los perfiles aprobados por el WiMAX Forum. Aprobado como 802.16-2004 en junio de 2004 (La última versión del estándar)
802.16e	Extensión del 802.16 que incluye la conexión de banda ancha nómada para elementos portables del estilo a notebooks. Publicado en diciembre de 2005

Los Hackers se Superan

- El reto intelectual y el reconocimiento es su motivación

Teddy-Net
the Wifi
Teddy Trojan

Slurpr – the
mother of all
wardrive
boxes

Referencias

- Seguridad Wireless, Foro, http://is.gd/4pek
- El Hacker, Foro, http://is.gd/s67X
- The Church of Wifi, Site, http://is.gd/s68n
- Remote Exploit, Site, http://is.gd/3Za5
- Slurpr Project, http://is.gd/4P2h
- Wireless Security Handbook, Aaron E. Earle, Auerbach Publications
- Extienda su Wi-Fi, http://is.gd/rPCL
- El 802.11n ya está aquí, http://is.gd/rPDl
- IEEE 802.11n, http://is.gd/agoZ

Referencias

- Arranca WIFI y WiMax DF !!, Arrancan dos programas piloto, http://is.gd/rQyJ
- Seguridad Wi-Fi – WEP, WPA y WPA2, Guillaume Lehembre, http://is.gd/rQzt
- Seguridad en redes inalámbricas, Vulnerabilidades del protocolo WEP, sin autor, http://is.gd/rQAB
- The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards, SANS Institute InfoSec Reading Room, http://is.gd/s60d
- WiMAX, http://is.gd/25fn

Gracias

sm4rt securityservices

www.hackarandas.com

Licenciado bajo CC
Algunos derechos reservados