(IN)SEGURIDAD EN REDES WI-FI

Madrid, 14 de diciembre de 2010

FORO: IV Jornada STIC CCN-CERT

SESIÓN: (In)Seguridad en redes Wi-Fi

OBJETIVO:

¿Cuál es el estado real de la seguridad de las redes Wi-Fi al finalizar el año 2010?

"Desde hace tiempo ya se dispone de seguridad mediante WPA2, así que son seguras, ¿no?"

PONENTE:

- Sr. Raúl Siles (Taddong – www.taddong.com)

FECHA: 14 de diciembre de 2010

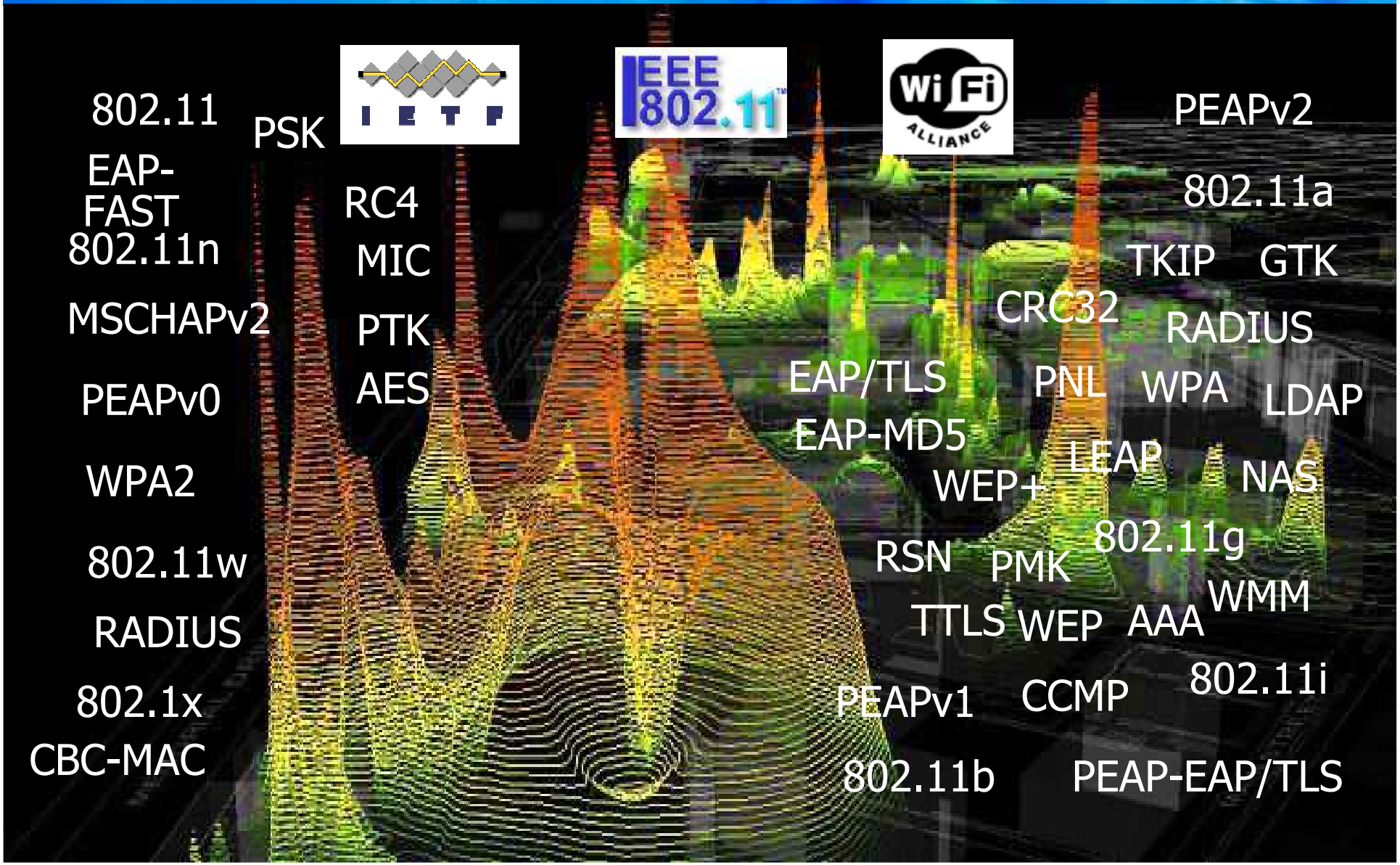
Titulo Transparencia

- ¿Cómo son las redes Wi-Fi para los usuarios… y para los técnicos?
- “¡Nosotros no tenemos wireless!”
- ¿Dónde llega la señal de mi red Wi-Fi?
- Hotspots Wi-Fi
- Tecnlogías de seguridad Wi-Fi
  - WEP, WPA(2)-PSK, WPA(2)-Enterprise & el futuro de las redes Wi-Fi
- Clientes Wi-Fi
  - Deficiencias, ataques contra la PNL, TAD-2010-003 y ¿dónde está mi PNL?
- Defensas
- Referencias

Wi-Fi para los usuarios

IV Jornada STIC CCN-CERT

Wi-Fi para los técnicos



"¡Nosotros no tenemos wireless!"

- "¿Estas seguro?"
- Política de seguridad vs realidad
- Dispositivos "autorizados"
  - Equipos de escritorio, portátiles, dispositivos móbiles
  - Puntos de acceso y controladores mal configurados
- Auditorías de seguridad y señales Wi-Fi
  - PCI DSS Wireless Guidelines (trimestral)
- Clientes Wi-Fi actuando como APs
  - Windows 7: Wireless Hosted Net (WPA2-PSK/AES)

    ```
    netsh wlan set hostednetwork mode=allow ssid=linksys key=…
    ```
  - Nueva percepción de seguridad

Mismo escenario: "No te preocupes, sólo tenemos WPA2-Enterprise…"

¿Dónde llega la señal de mi red Wi-Fi?

- ¿Desde dónde podría un atacante conectarse a la red Wi-Fi, inyectar tráfico o capturar el tráfico?
  - "Desde el aparcamiento cercano"
- Edificios de oficinas compartidos en el centro de la ciudad
- Ajustar la potencia de transmisión y las antenas
- ¿Cuál es la máxima distancia de conexión de una red Wi-Fi?
  - Record mundial (nuevos records posteriores en 2007+)
  - Defcon 13:WiFi Shootout 2005: www.wifi-shootout.com
  - 200,96 Km
  - ¿Problema?
  - La curbatura de la tierra

HotSpots Wi-Fi

- No podemos vivir sin conexión a Internet
- Aunque no se dispone de una red Wi-Fi abierta y sin seguridad en la organización… ¿qué ocurre con los usuarios?
  - ¿Red de invitados?
- Ataques:
  - Captura de tráfico (confidencialidad)
    - "Sólo accedo a información pública…"
  - Manipulación del tráfico

game over!

- VPNs
  - En manos del usuario (establecimiento, DoS…)
  - ¿Protección a nivel 2?
  - HotSpots: portal cautivo vía web ☺
- HotSpots en el futuro: WPA2-Enterprise (== ó != usuarios)

Firesheep

- Secuestro de sesiones web
- Add-on para Firefox + Winpcap
  - Eric Butler & Ian Gallagher en octubre de 2010 - ToorCon 12
- No es un ataque nuevo, pero ahora cualquiera puede ejecutarlo
- Cifrado en sesiones web: autentificación vs sesión completa

facebook

YAHOO!

twitter

Google

amazon.com

http://codebutler.com/firesheep & Airpwn-MSF

Tecnologías de seguridad Wi-Fi

WEP

WPA(2)-PSK

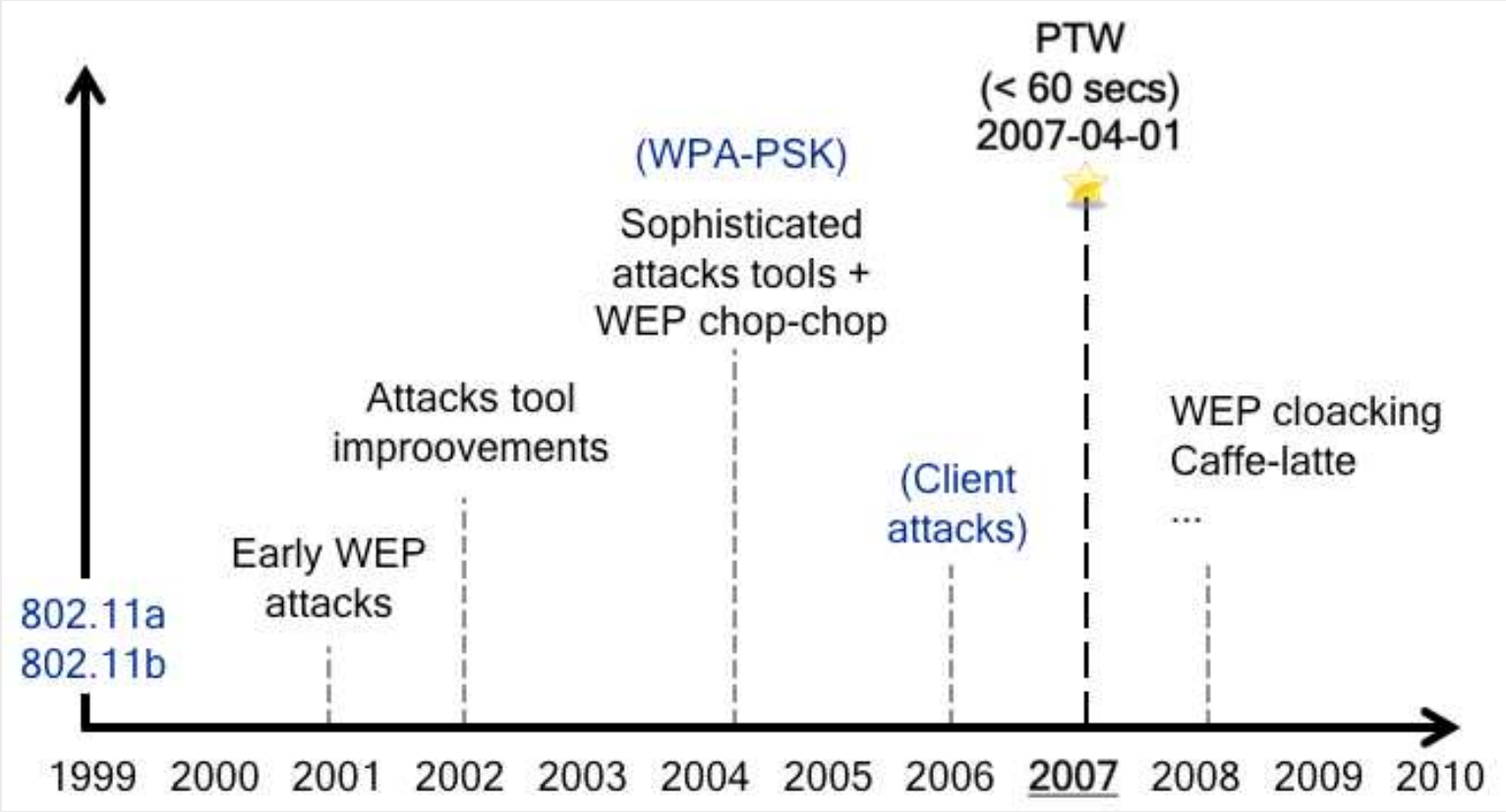
WPA(2)-Enterprise

El futuro de las redes Wi-Fi

DoS & Capacidades de detección (WIDS)

WEP

- Wired Equivalent Privacy (WEP): no en la organización pero…



http://www.radajo.com/2007/04/what-else-do-you-need-not-to-use-wep.html

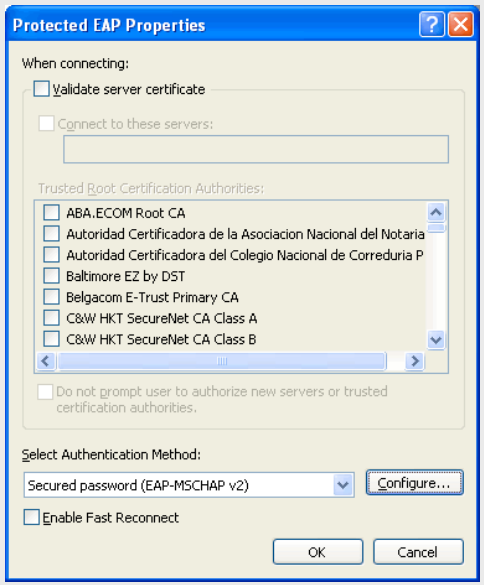
WPA(2)-PSK

- Clave pre-compartida
  - Cualquier usuario puede capurar el tráfico de otros usuarios
- Longitud de la clave
  - Mínimo de 8 caracteres, recomendado 20 caracteres, máximo de 64
- Debilidades en la asignación de la clave: proveedores de telco
- Ataques de rainbowtables
  - Múltiples rainbowtables disponibles (diccionario con 1 millón de palabras)
  - Ataques mediante las GPUs de las tarjetas gráficas (x 10K)
  - Ataques “en la nube” (diccionario con 284 millones de palabras)
    - Captura de tráfico (4 tramas)
    - SSID (nombre de la red Wi-Fi)
    - E-mail

Algo compartido… ¡no es secreto!

WPA(2)-Enterprise

- TKIP es una solución temporal: se debe usar AES
  - DoS en el diseño (WMM) y ataque chop-chop
- WPA2/AES-CCMP + 802.1x/EAP
  - Autentificación fuerte mediante credenciales de usuario y certificados digitales
  - Validación de los certificados digitales incorrecta
    - CA
    - Servidor de autentificación (RADIUS)
    - Acceso a las credenciales del usuario
- Hole 196
  - Clave de grupo (GTK)
  - Ataques internos menos detectables
- 802.11n: ¿Listo para detectar los ataques?



Algo compartido… ¡no es secreto!

El futuro de las redes Wi-Fi

- Historia de las tecnologías Wi-Fi:
  - WEP desde 1999 & TKIP desde 2003
- 2011: TKIP no permitido en APs sólo (…+AES) y WPA2/AES por defecto (vs. abierto)
- 2012: TKIP no permitido en STAs
- 2013: WEP no permitido en APs (… todavía PoS)
- 2014: TKIP+AES no permitido en APs (sólo WPA2/AES) y WEP no permitido en STAs
- En 2014 tendremos dos mundos Wi-Fi: seguro e inseguro
  - WPA2/AES por defecto: ¿Cuál es la clave? (WPS)
  - Redes Wi-Fi abiertas: ¡Todavía permitidas!

Clientes Wi-Fi

Deficiencias

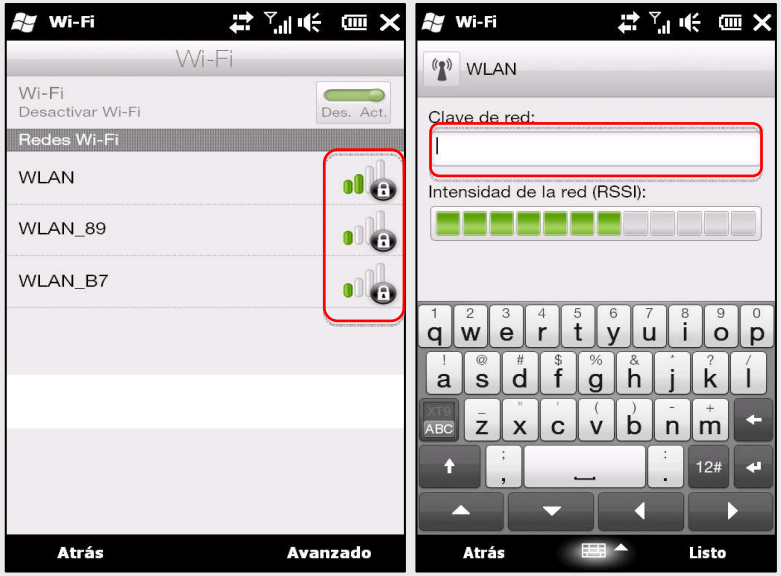
Ataques contra la PNL

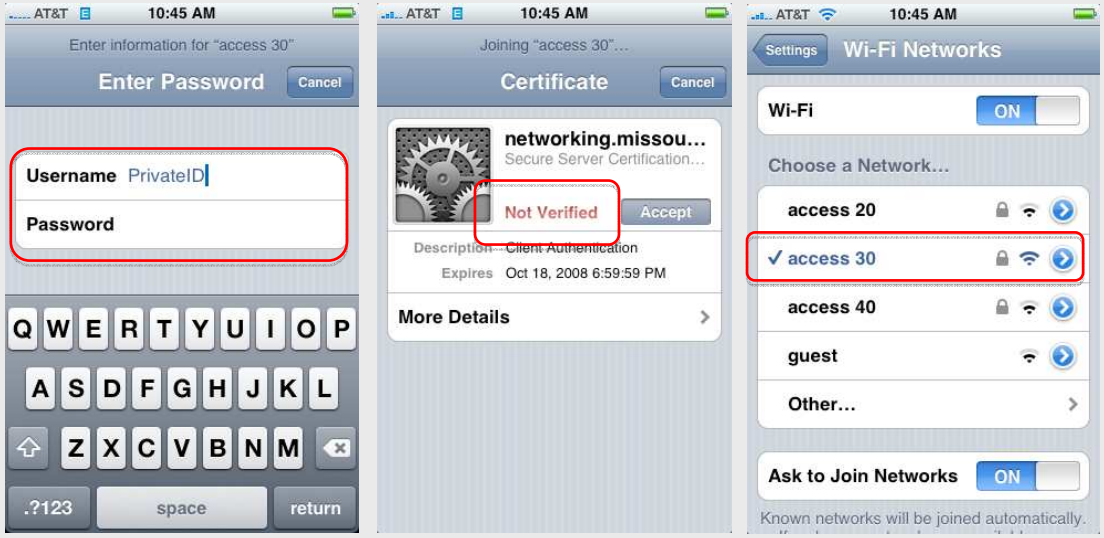
TAD-2010-003

¿Dónde está mi PNL?

Deficiencias en los clientes Wi-Fi

- ¿A qué tipo de red te estás conectando con tu dispositivo móvil?
  - iPhone, Windows Mobile, etc
  - Tiene un candado, así que debe ser muy segura ☺
  - Imposibilidad de deshabilitar la conexión automática a redes Wi-Fi conocidas
  - Solución: Configurar la red Wi-Fi manualmente



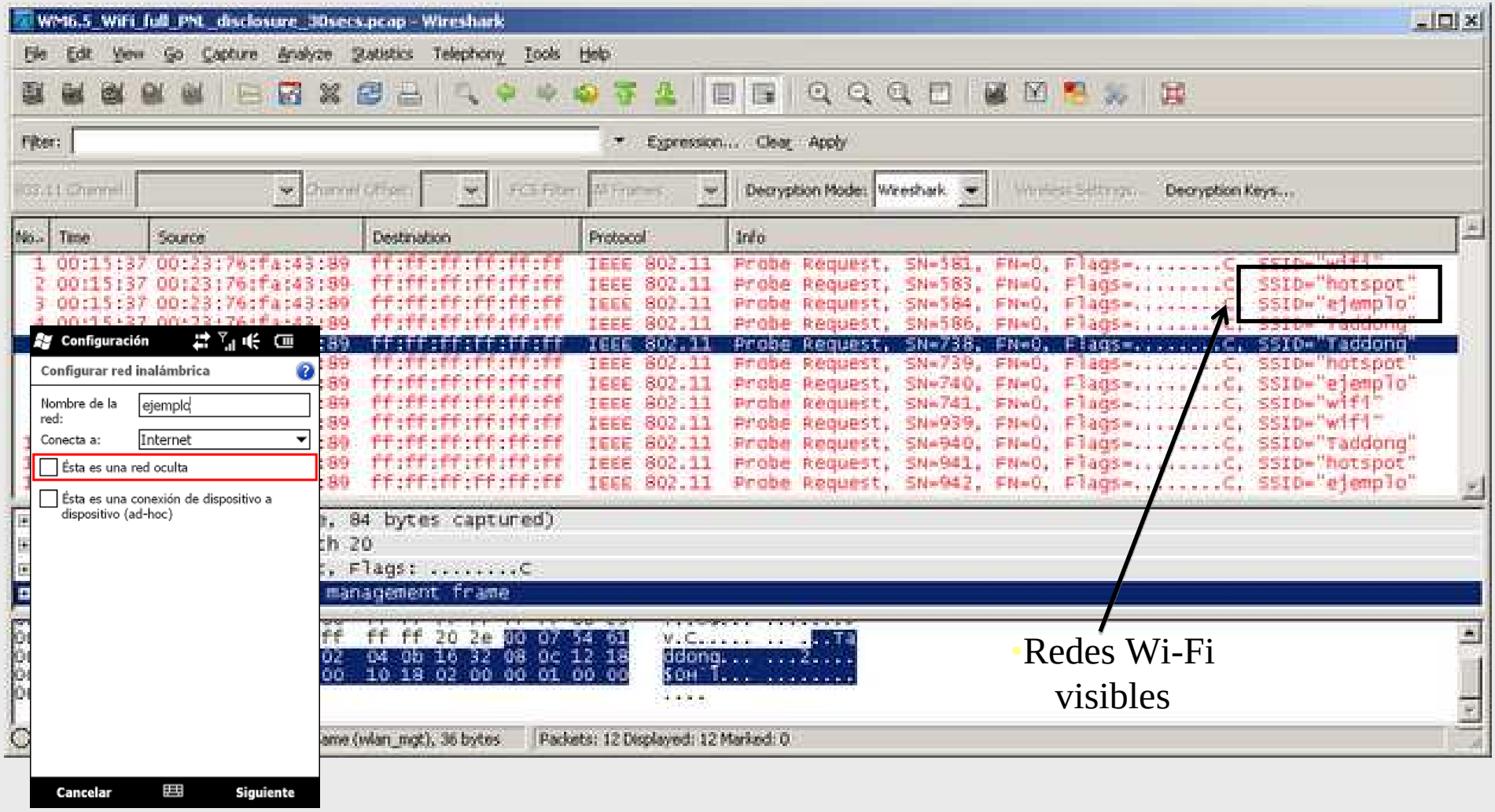


Ataques contra los clientes Wi-Fi (PNL)

- Ataques dirigidos y contra la privacidad de los clientes Wi-Fi
- ¿Cómo funcionan los clientes Wi-Fi?
  - PNL: Preferred Network List
  - Búsquedas periódicas por nombre: revelando información y detalles
  - Un atacante puede capturar el tráfico y ver los nombres de las redes
- Los sistemas operativos “de verdad” evitan este comportamiento en la actualidad (!redes ocultas), pero… ¿y los dispositivos móviles?
- Vulnerabilidad TAD-2010-003
  - Windows Mobile 6.5 & PNL (redes ocultas y visibles)
  - Conocido desde 2005, corregido en Windows XP desde 2007
  - SSID (o conjuntos) únicos: identificación del usuario (privacidad)
  - El atacante “ayuda” al dispositivo a conectarse a su red (dirigido)

http://blog.taddong.com/2010/09/vulnerability-in-indiscreet-wi-fi.html

TAD-2010-003: Descubrimiento

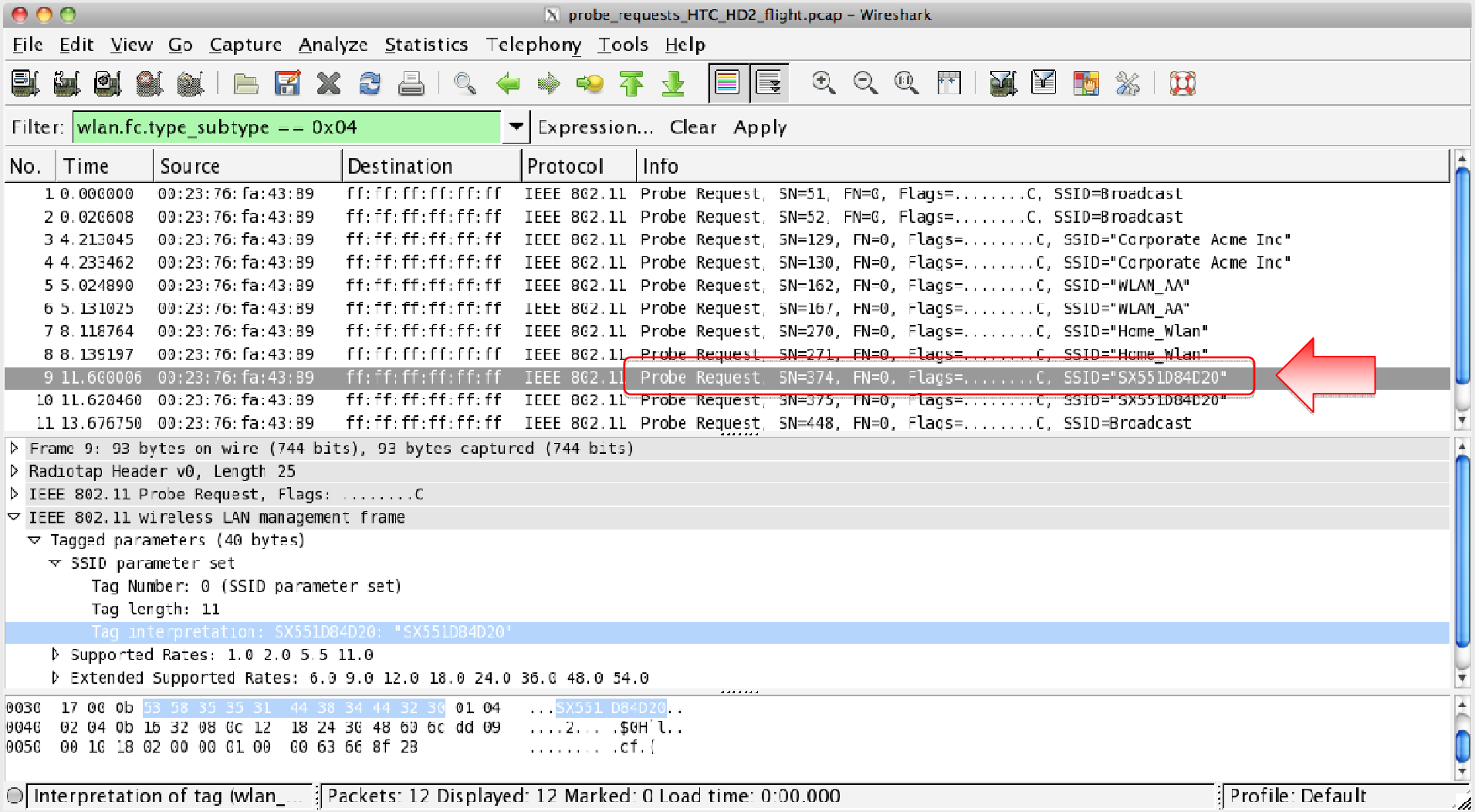


TAD-2010-003: Ataques

- Ataques tipo “Karma”
  - Los clientes Wi-Fi comprueban la presencia de sus redes preferidas
  - “¿Está mi <SSID> aquí?”…. ¡Por supuesto! ☺
  - Asociación y conexión automática desde los dispositivos móviles
  - El atacante ofrece todo: red Wi-Fi, servidores DHCP/DNS/correo & Internet
- Herramientas
  - Karma: http://theta44.org/karma/index.html
  - Airbase-ng (aircrack-ng.org) & Karmetasploit (MSF + Karma/Airbase)
  - Ataques sobre la contraseña WEP y WPA(2)-PSK
- Microsoft & TAD-2010-003: ¿baja severidad?, ¿forzar: ya lo hace el sólo?
  - “However, because of the low severity impact of the information disclosed combined with the fact that the attack would be untargeted (i.e. the attacker cannot force the mobile device to disclose the PNL), Microsoft would not issue a public security update to address this issue.”
  - Windows Phone 7

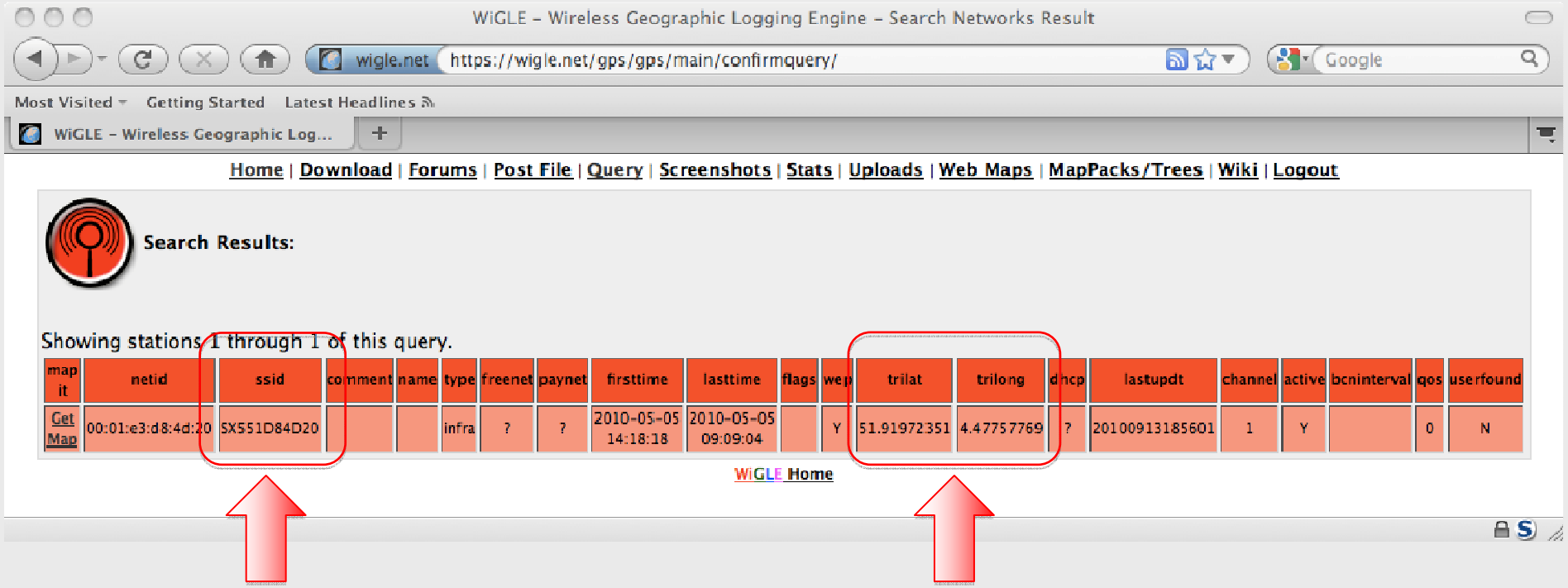
TAD-2010-003: Ataques dirigidos

- Tráfico capturado “durante un vuelo a Holanda” (HTC HD2, WM6.5):



TAD-2010-003: Geolocalización (Wigle & Google Street View)

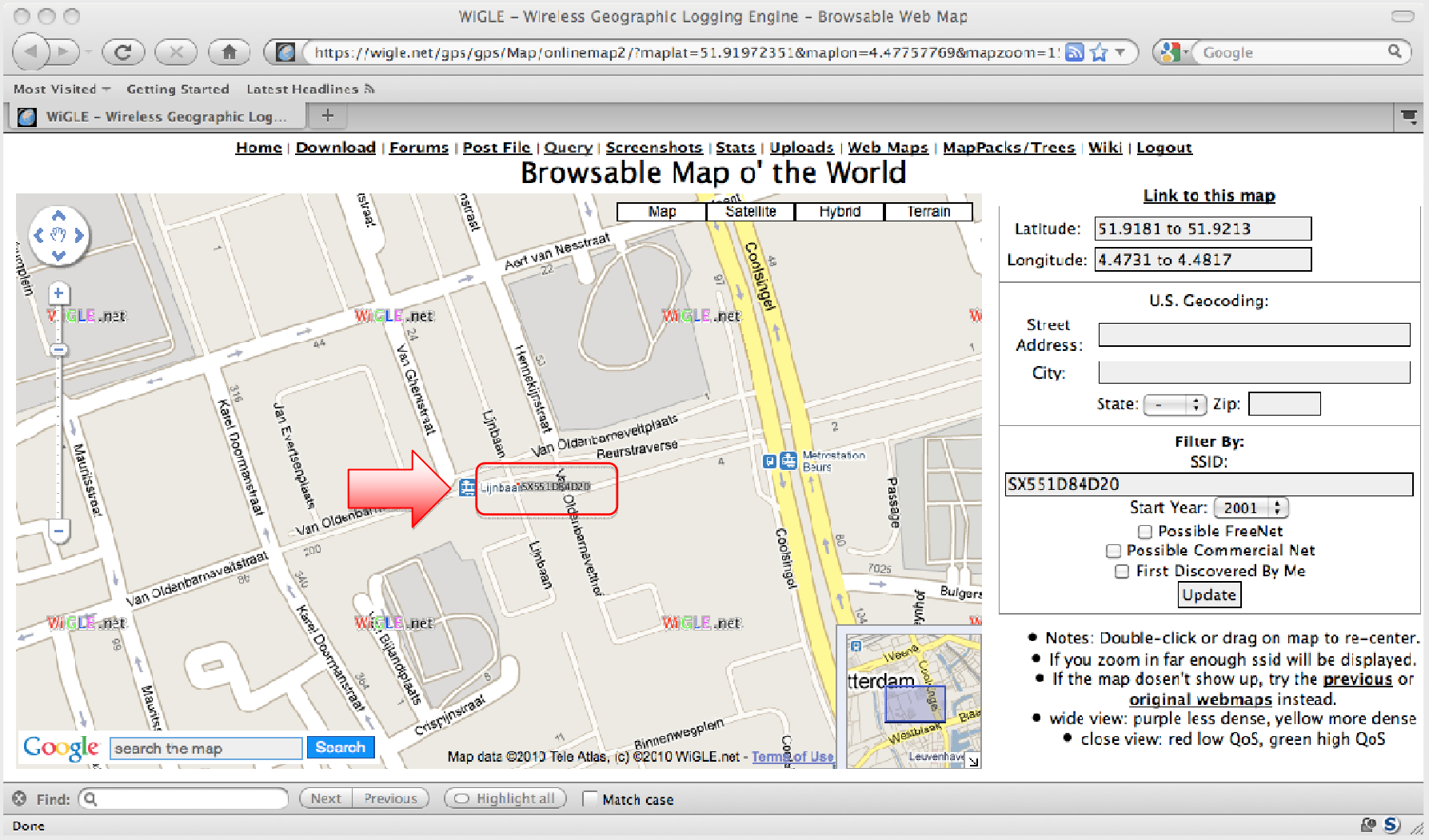
- SSID: “SX551D84D20”



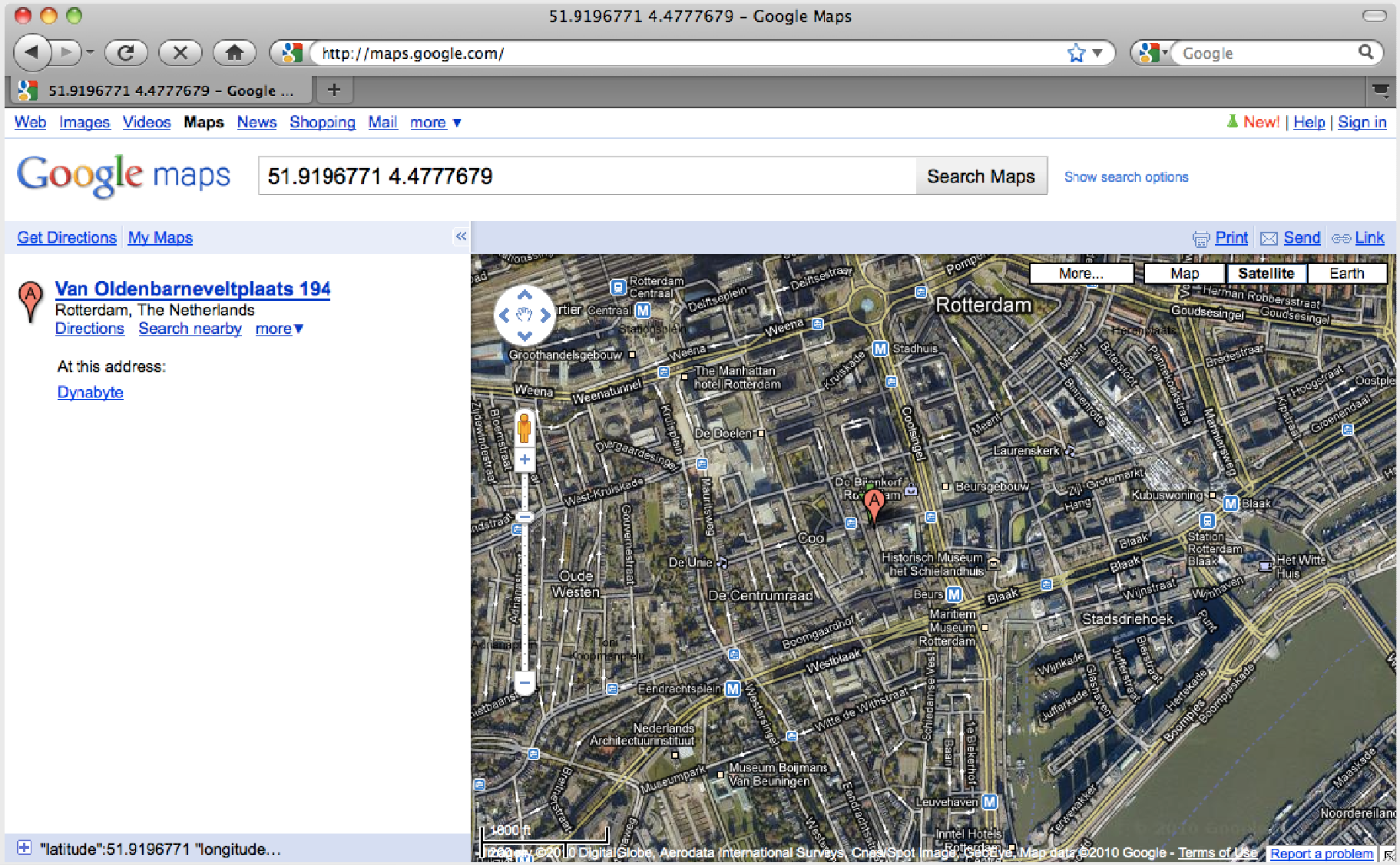
- Wigle: : http://wigle.net
- Google Geolocation API: HTTPS + JSON

TAD-2010-003: Geolocalización en el mapa (Wigle)

- ¿Dónde vives, trabajas, o quedas con los amigos…?



TAD-2010-003: Geolocalización en el mapa (Google)



Sr. iPhone… ¿dónde está mi PNL?

- Cuando el dispositivo se conecta a una red Wi-Fi, la almacena en la PNL
- Pero, ¿cuándo se elimina una red Wi-Fi de la PNL y cómo?
- La opción “Forget this Network” sólo está disponible cuando la red Wi-Fi está al alcance (en el rango) del dispositivo móvil
  - iPhone 2G, 3G y 4G
- Solución: Volver al lugar dónde está la red Wi-Fi…
- … o simularla (conociendo que existe)
- Gestión de PNLs

Defensas

Tecnologías Wi-Fi

Clientes Wi-Fi

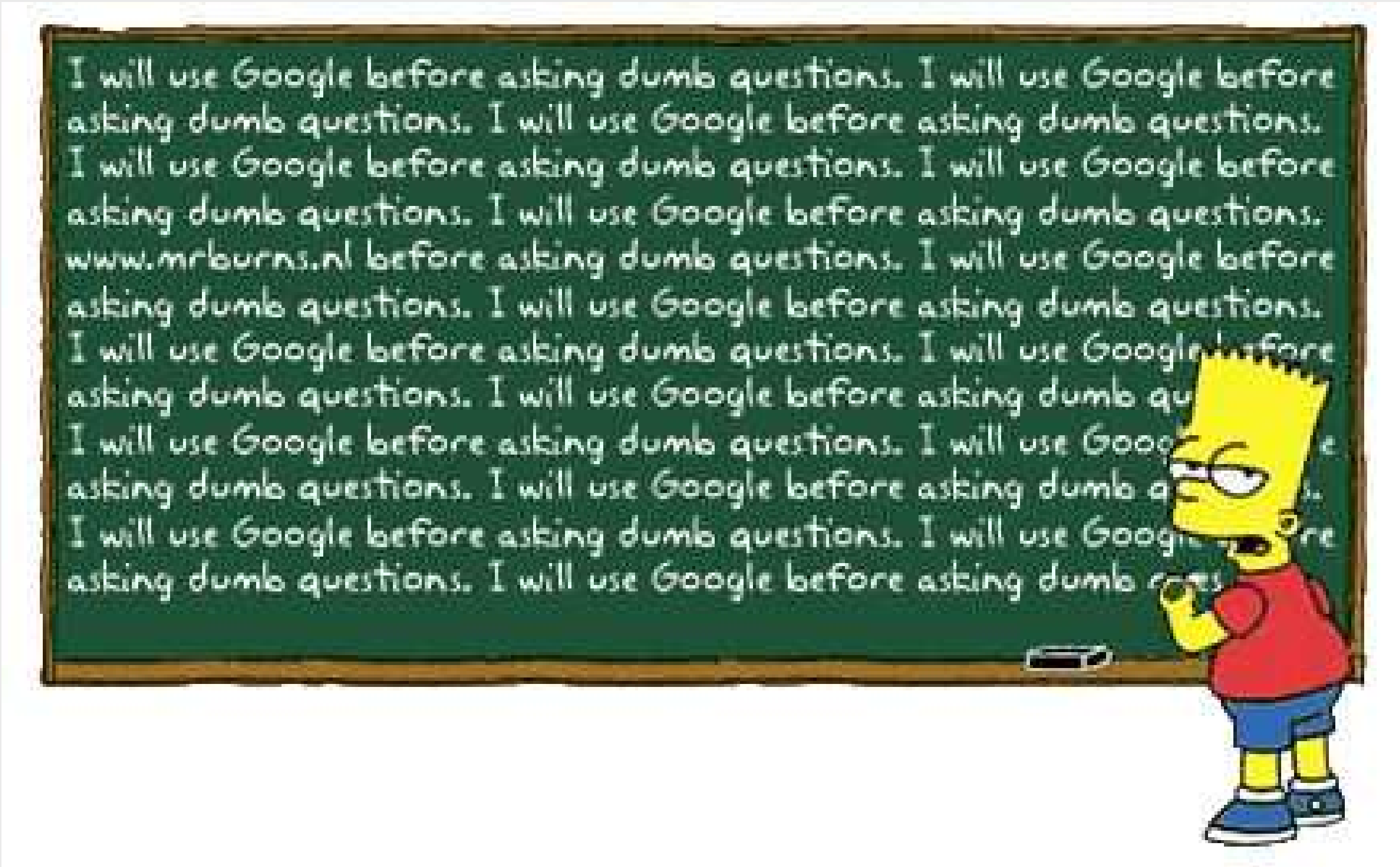
- Tecnologías Wi-Fi
  - Capacidades de detección de dispositivos no autorizados y ataques (WIDS)
  - Limitar el rango de las señales Wi-Fi
  - WPA2-Enterprise (AES-CCMP + EAP/TLS): !TKIP
  - Proteger el tráfico RADIUS (IPSec) y contraseñas distintas por dispositivo
  - Validación completa de los certificados digitales y no preguntar al usuario
  - DoS
- Clientes Wi-Fi
  - Deshabilitar el interfaz Wi-Fi si no se está usando
  - No conectarse a redes abiertas o WEP: VPN y clientes “100%” seguros ☹
  - Gestionar los clientes Wi-Fi en detalles
    - Evitar o controlar conexiones automáticas a redes Wi-Fi conocidas
    - Deshabilitar automáticamente el interfaz si no se conecta en X seguntos (móviles)
    - Evitar redes ad-hoc y redes “desconocidas”
  - Gestión avanzada de la PNL (GPO) y de los drivers, clientes Wi-Fi y SW

Referencias

- "Wi-Fi (In)Security - All Your Air Are Belong To…". Raul Siles. GOVCERT.NL Symposium 2010. Noviembre 2010.
  - http://www.taddong.com/en/lab.html
- Taddong's Blog (Wi-Fi posts)
  - http://blog.taddong.com/search/label/Wi-Fi
- RaDaJo Blog (Wireless posts)
  - http://www.radajo.com/search/label/Wireless
- Raul Siles' Wi-Fi webpage
  - http://www.raulsiles.com/resources/wifi.html
- E-mail: raul@taddong.com
- Twitter: @taddong

Taddong

www.taddong.com


I will use Google before asking dumb questions. I will use Google before
asking dumb questions. I will use Google before asking dumb questions.
I will use Google before asking dumb questions. I will use Google before
asking dumb questions. I will use Google before asking dumb questions.
www.mrburns.nl before asking dumb questions. I will use Google before
asking dumb questions. I will use Google before asking dumb questions.
I will use Google before asking dumb questions. I will use
asking dumb questions. I will use Google before asking dumb
I will use Google before asking dumb questions. I will use
asking dumb questions. I will use Google before asking dumb
I will use Google before asking dumb questions. I will use
asking dumb questions. I will use Google before asking dumb

Gracias

- Correos electrónicos
  - info@ccn-cert.cni.es
  - sondas@ccn-cert.cni.es
  - redsara@ccn-cert.cni.es
  - ens@ccn-cert.cni.es
  - ccn@cni.es
  - organismo.certificacion@cni.es
- Páginas Web:
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - www.oc.ccn.cni.es

Nuestro agradecimiento a:

Platino

tb·security

hp

Patrocinadores

amper Epicom

Check Point SOFTWARE TECHNOLOGIES LTD. We Secure the Internet.

dintel

Ironwall STRATEGIC SECURITY SYSTEMS

Microsoft

S21sec La seguridad digital del futuro, hoy

Revista SIC seguridad en informática y comunicaciones