Implementación de una red Wi-Fi segura mediante WPA y 802.11i

Sara Rincón Nicolás
María Unda Sada

Director: Pablo Garaizar Sagarminaga

Universidad de Deusto, 14 de Junio 2005

Contenidos

1. Motivación del proyecto
2. Nuevas soluciones de seguridad Wi-Fi
3. Implementación de una solución Wi-Fi segura
4. Explicación práctica
5. Conclusiones
6. Ruegos y preguntas

Motivación del proyecto

- Gran auge de las redes Wi-Fi
- Desarrollo de una solución bajo GNU/Linux
- Inseguridad intrínseca a las redes Wi-Fi
- Soluciones de seguridad obsoletas:

NOMBRE	DESCRIPCIÓN	HERRAMIENTAS DE ATAQUE
WEP	Wired Equivalent Privacy	WepLab, Wepcrack, Aircrack, etc.
Filtros	Acceder acceso según IP o MAC	`ifconfig eth1 hw ether` *MAC*- GNU/ Linux smac.exe - Windows
ESSID	Ocultación del ESSID de la red	Sniffer en Sistemas GNU/Linux Kismet

Nuevas soluciones de Seguridad Wi-Fi (1/2)

1. Estándar IEEE 802.11i:

- 802.1x.
  - Protocolo de autenticación basada en puerto
  - 3 entidades: cliente o suplicante, autenticador, servidor de autenticación
- EAP. Protocolo para el intercambio de mensajes entre cliente y servidor (Tabla)
- RADIUS. Servidor de autenticación centralizada de usuarios
- Cifrado: TKIP y AES-CCMP

2. Estándares de la Wi-Fi Alliance:

- WPA
  - Enterprise: RADIUS + EAP + 802.1x + TKIP
  - PSK o Personal: 802.1x + EAP+ TKIP
- WPA2 802.1x + AES-CCMP

Nuevas soluciones de Seguridad Wi-Fi (2/2)

TIPO EAP	DESCRIPCIÓN
EAP-MD5	Método de autenticación básico.
EAP-TLS	**Transport Layer Security.** Utiliza certificados para el cliente y el servidor.
EAP-TTLS	**Tunneled Transport Layer Security**. Extensión de TLS. No es necesario poseer un certificado por cliente.
EAP-PEAP	**Protected Extensible Authentication Protocol.** EAP a través del túnel. No soporta otros métodos para la negociación de la autenticación del cliente.
EAP-LEAP	**Light Extensible Authentication Protocol**. Ataques de diccionario. Autenticación mutua, distribución de clave de sesión segura y dinámica
EAP-SIM EAP-AKA	**Subscriber Identity Module** y **Authentication and Key Agreement** Se emplean en redes celulares, no en redes 802.11.

Implementación de una solución Wi-Fi segura: 802.11i

¿Por qué es menos recomendable el uso de WPA/WPA2?

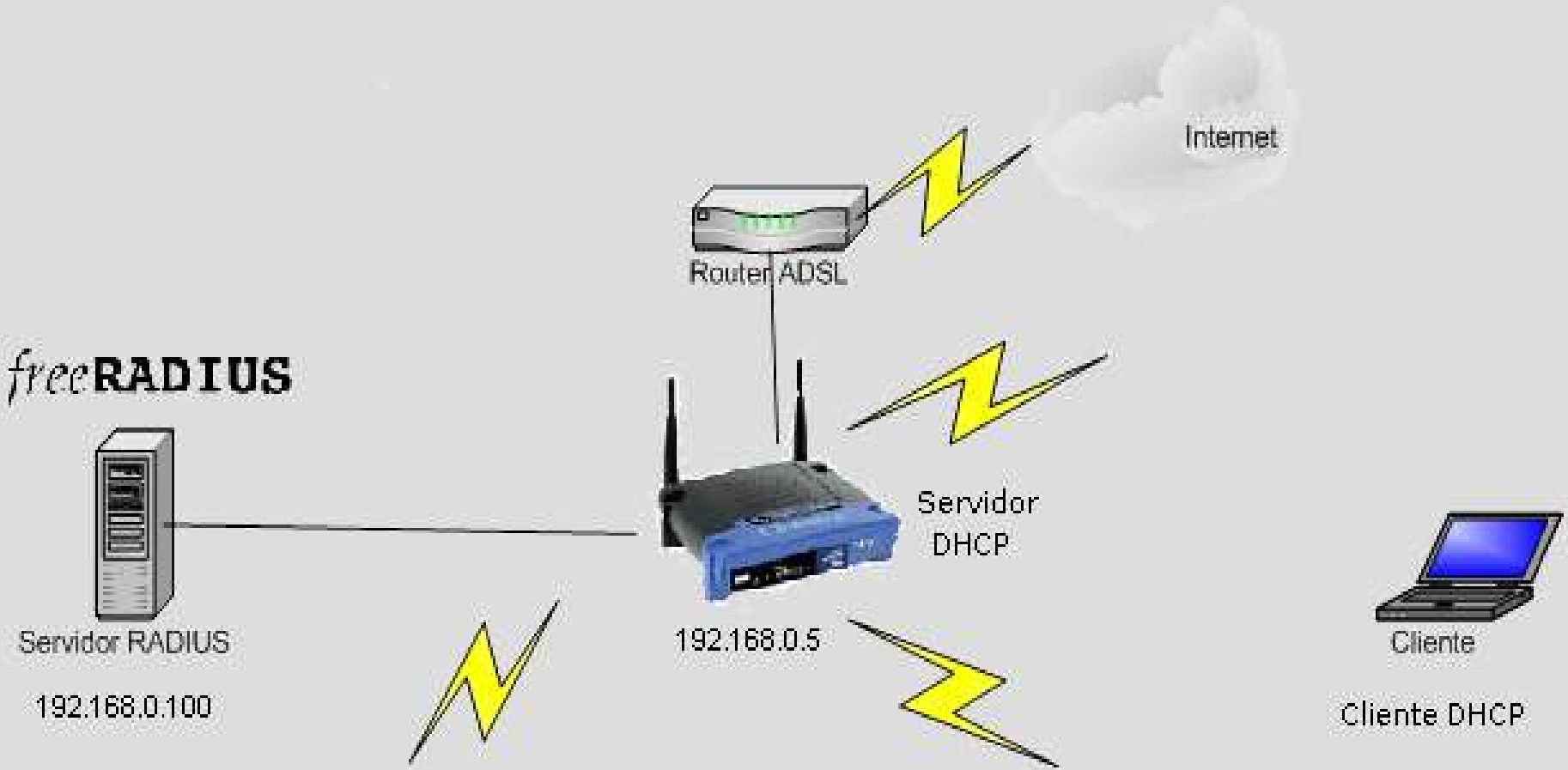
- WPA:
  - Actualizaciones de firmware
  - Vulnerabilidades explotables muy fácilmente

- WPA2:
  - Soluciona vulnerabilidades WPA
  - Estándar demasiado reciente – Incompatibilidad hw

Explicación práctica (1/2)

- Suplicante: Centrino 2100 (ipw2100)
  - Windows XP SP2
    - Simplicidad de configuración
    - Amplio soporte de estándares y tarjetas Wi-Fi
  - GNU/Linux 2.6.11: Xsupplicant 1.0.1-4
    - Ventajas de 802.1x: compatibilidad hw
    - Herramienta Open Source
- Autenticador: Linksys WRT54G
  - Facilidad de administración
  - Compatible con WPA / WPA2
- Servidor de autenticación: freeRadius 1.0.2
  - Implementación del protocolo RADIUS
  - Herramienta Open Source para GNU/Linux

Explicación práctica (2/2)



ConclusionesPOSIBLESAMP

- Desarrollo de una solución segura: Cumplido.
- Satisfacción personal por la implementación de un proyecto con una visión de futuro.
- Posibilidad de implantación real tanto a nivel doméstico como empresarial.
- Dificultades añadidas:
  - Uso de estándares Wi-Fi muy recientes
  - Incompatibilidades hardware
  - Escasa e incompleta documentación

Implementación de una red Wi-Fi segura mediante WPA y 802.11i

Ruegos y preguntas

Sara Rincón Nicolás
María Unda Sada