Seguridad en UDCWIFI

Índice

- Introducción
- Seguridad en redes inalámbricas WIFI
- WEP, WPA Y 802,11i: Descripción, Debilidades y Ataques
- Caso concreto: UDCWIFI

Introducción

Hablar de seguridad en redes inalámbricas, es como hacerlo sobre paracaidismo – si quieres seguridad, no lo practiques.

No existe ningún sistema 100% seguro, tan sólo hay que analizar la relación coste/beneficio de hacerlo razonablemente seguro según la disponibilidad tecnológica.

Seguridad en Redes Inalámbricas

El interfaz aire es una banda libre de acceso público, con lo que, la única forma de asegurar las comunicaciones es combinando **Encriptación y Autenticación**

Veremos de forma resumida los distintos algoritmos de seguridad, con sus debilidades, para así explicar por qué se han adoptado las actuales medidas de seguridad en la red inalámbrica de la UDC

Seguridad en Redes Inalámbricas

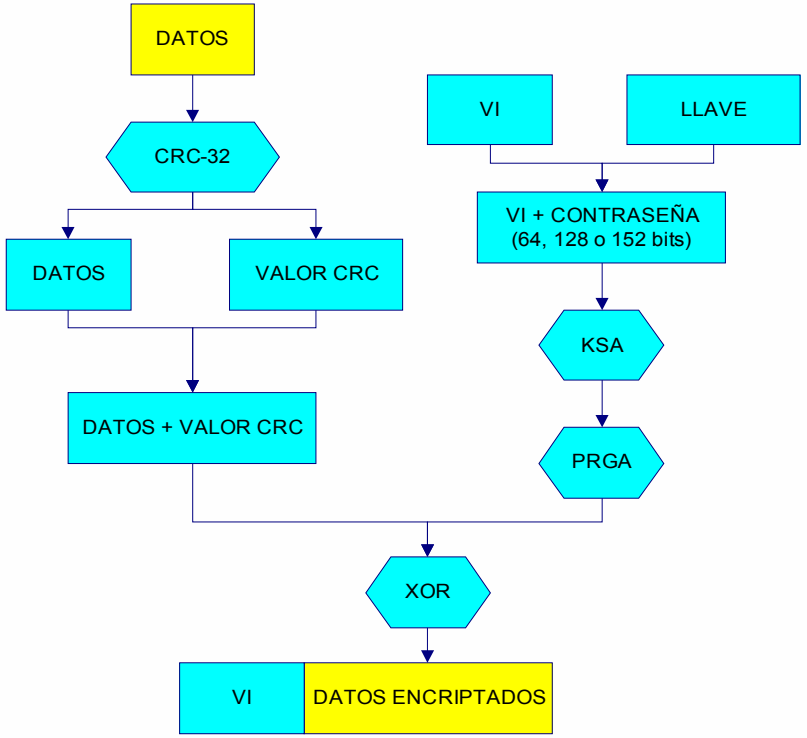
Los ataques a las redes inalámbricas se basan en:

- Ataques de fuerza bruta para averiguar contraseñas
- Debilidades de los algoritmos de encriptación
- Errores de configuración: configuración por defecto, SSID no ocultado y sin encriptación ni autenticación, ...

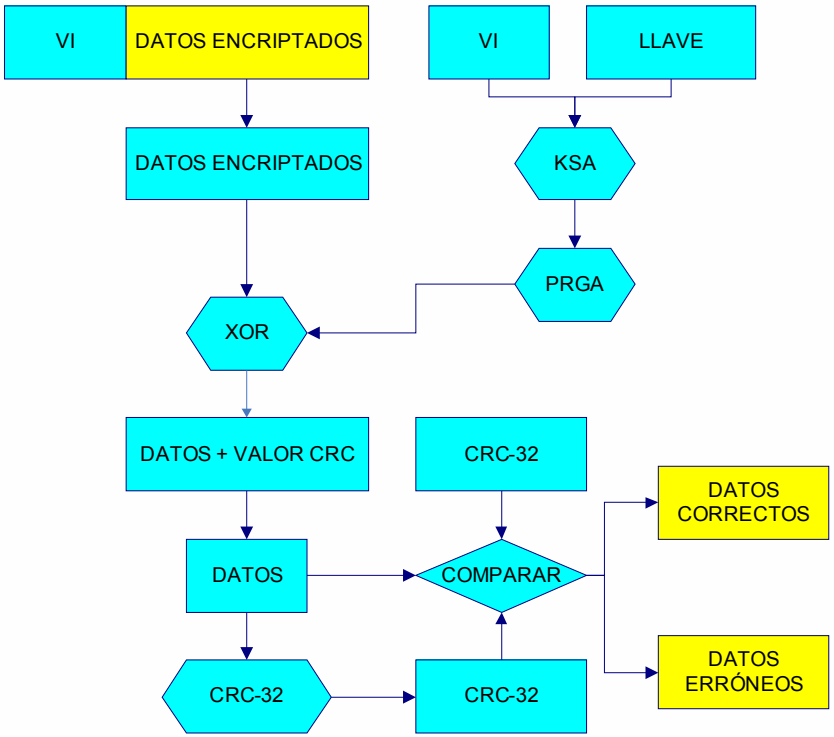
WEP (Wired Equivalent Privacy)

- Desarrollado en 1999 por la IEEE como parte del estándar 802.11
- Aún a sabiendas de sus debilidades, fue considerada la mejor opción, y muchos siguen creyendo que una red inalámbrica protegida con WEP es 100% segura
- Incluye dos métodos de autenticación: **Open Key y Shared Key**

WEP-Mecanismo de encriptación



Proceso Encriptación



Proceso Desencriptación

WEP-Deficiencias de encriptación

- El VI es demasiado corto (24 bits) y además aparece en claro
- El VI es normalmente estático (cambiarlo en cada paquete es opcional según estándar)
- CRC lineal
- Chequeo de integridad independiente de la llave

WEP-Deficiencias de autenticación

- **Open System**: No hay autenticación
- **Shared Key** : Capturando el segundo (desafío en claro) y tercer mensaje (texto del desafío con la clave compartida) => WEP = Datos encriptados **XOR** Datos. Todos los datos, excepto el texto del desafío, son iguales para todas las respuestas de autenticación. Un atacante tiene entonces todos los elementos para conseguir autenticarse (para conectarse a la red, necesita atacar romper WEP)

WEP- Ataques

- **Ataques de fuerza bruta** : clave semilla obtenida a partir de una passphrase ASCII y PRGA generador lineal
- **Ataques con diccionario**
- **Ataque inductivo Airbaugh** : desencripta el tráfico en tiempo real basándose en que el CRC es lineal y el chequeo de integridad independiente de la llave. Tabla < VI – keystream> => el atacante recibe un paquete y mira en la tabla a qué keystream está asociado el VI recibido => keystream **XOR** datos encriptados = datos

WEP- Ataques

- **Debilidades del algoritmo de distribución de claves** : Se adivina la clave mediante monitorización pasiva (2 a 10 millones de paquetes). Es posible adivinar la clave utilizada para la encriptación VI's débiles

WEP- Soluciones propietarias

- **Clave WEP extendida** : Agere y US Robotics. Sólo consigue que se tarde más en romper la clave
- **Clave WEP dinámica** : Cisco, Microsoft, ... Cambio de claves dinámico en los AP
- **Cisco LEAP**: Cisco

Ataques a redes WiFi

- **WEP Cracking** : Aprovechando las debilidades de WEP
- **Ataques a la dirección MAC** : La MAC viaja plana por el interfaz aire, y una vez capturada una válida el atacante suplanta la identidad del usuario. También permite hacer ataques DoS
- **ESSID ocultado** : Esnifar esperando conexión de un cliente (ESSID en la trama PROBE REQUEST). Desconexión del cliente configurando la dirección MAC del AP y enviando tramas DISASSOC al cliente forzando reconexión para ver el ESSID

Ataques a redes WiFi

- **Man-in-the-Middle** : Interceptar el tráfico entre el AP y el cliente y dejar un “rogue access point” cerca de él para forzar reasociación con él. El atacante usa la MAC de la víctima para asociarse al AP real
- **Denegación de Servicio (Denial of Service)** : Esnifar para ver la MAC de AP y hacerse pasar por él y mandar “management frames” al cliente o a broadcast

WPA (WiFi Protected Access)

- En el 2003 se desarrolla 802.11i por presiones de la WiFi Alliance y para solucionar las debilidades de WEP
- WPA es un subconjunto de 802.11i que sólo requiere actualización de firmware
- Encriptación: TKIP (Temporal Key Integrity Protocol)
- Usa MIC (Message Integrity Check) para verificar la integridad del mensaje
- Implementa autenticación basada en 802.1X EAP

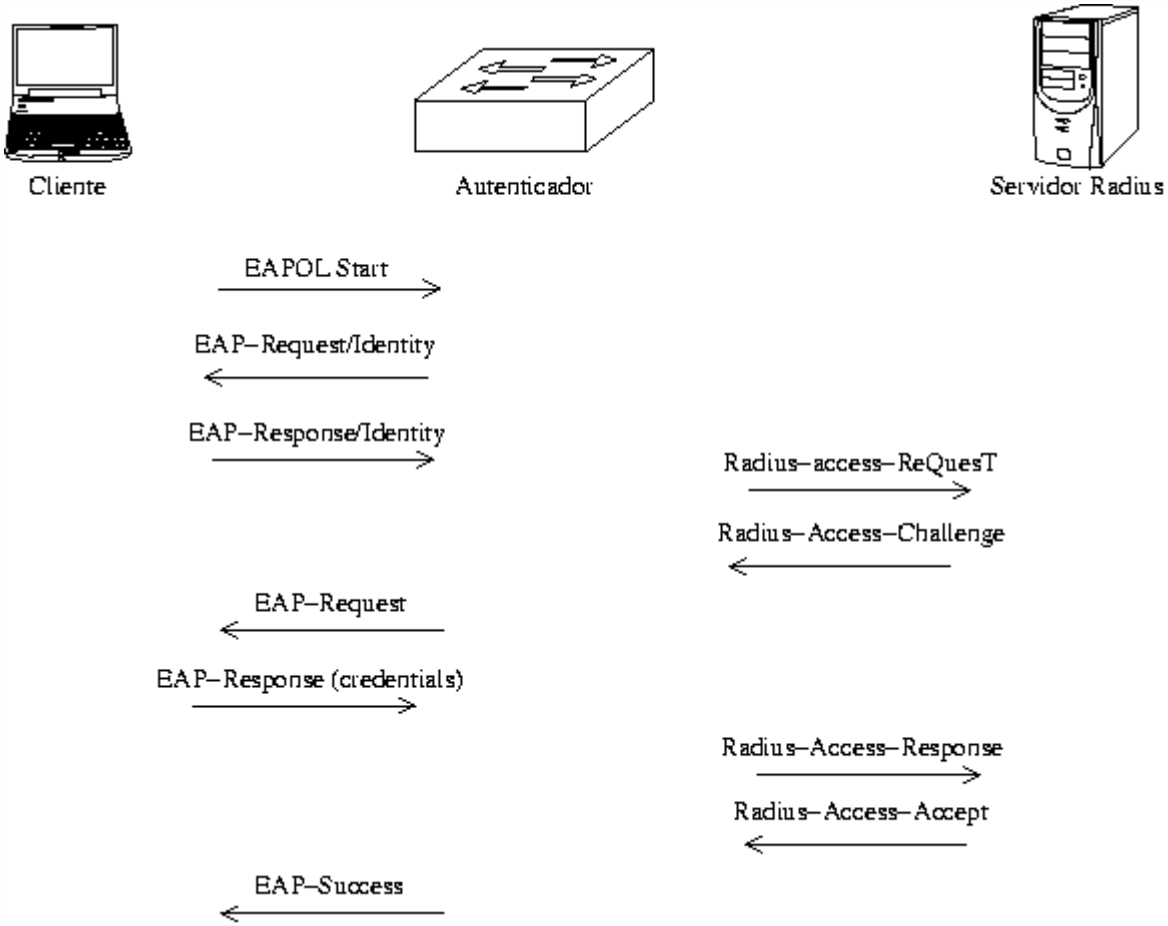
WPA - Autenticación

- En el estándar 802.1X se definen los siguientes elementos: suplicante, servidor de autenticación y autenticador
- **Método de clave pre-compartida (PSK)** : Destinado a entornos SOHO donde puede no existir un servidor de autenticación. La autenticación es similar a WEP clave compartida

WPA - Autenticación

UDCWIFI

- **EAP (Extensible Authentication Protocol)**



WPA - Autenticación (Variantes EAP)

- **EAP – LEAP** (Cisco). Emplea usuario/contraseña
- **EAP – TLS** (RFC 2716). Emplea certificados X.509
- **EAP – TTLS** (Funk Software). Certificado sólo en el autenticador
- **EAP – PEAP** (Protected EAP)

WPA - Encriptación

- **Encriptación TKIP (Temporal Key Integrity Protocol)**: Cambio automático de claves temporales cada 10000 paquetes. Una clave temporal de 128 bits es compartida entre clientes y AP, se combina con la dirección MAC del cliente y se añade un VI de 48 bits para marcar el número de secuencia de paquetes (garantía de diferentes claves para diferentes clientes)

WPA – Verificación de integridad

- **Michael Message Integrity Check** : Refuerza la verificación de la integridad de los datos. Es un mensaje (MIC) de 64 bits calculado usando el algoritmo de Michael (www.deadhat.com/wlancrypto). El mensaje MIC se inserta en el paquete TKIP

WPA – DEBILIDADES PSK
ATAQUES PSK

Cuando se usa PSK en lugar de 802.1X, la PSK es la clave (PMK) usada para la autenticación mutua y la generación de claves temporales (PTK)

Ataque INTRA-PSK

- Conociendo la PSK, la generación dinámica de claves temporales cae en manos de cualquier atacante, ya que es posible conocer el resto de información
- Todos los datos, a excepción de la PSK están disponibles en el proceso inicial de autenticación que puede ser esnifado por cualquier cliente

WPA – DEBILIDADES PSK
ATAQUES PSK

Ataques Diccionario

Una estación que no conoce la PSK puede usar un ataque diccionario offline para romperla

Caso concreto: UDCWIFI

- Opción adoptada: WPA + 802.1X
- ¿Por qué EAP-TTLS?. Solución transitoria hasta resolver el modo de distribución de certificados
- EAP-TTLS: Autenticación fuerte del servidor por parte del cliente => se establece una sesión TLS (Transparent Layer Substrate) => autenticación del cliente por parte del servidor usando otro método (EAP-MD5)

Caso concreto: UDCWIFI

- Servidor RADIUS: FreeRadius
- Almacenamiento de claves: OpenLDAP
- Certificado: Se ha montado una CA propia usando OpenSSL
- Los equipos seleccionados para el despliegue, soportan WPA-TKIP

MUCHAS GRACIAS