WPA vs WPA2

Ana Hernández Rabal

21-12-2007

Índice

- Introducción
- WPA vs WPA2
- Autenticación
  - PSK
  - 802.1x
    - EAP
    - EAPOL
    - RADIUS
- Generación e intercambio de llaves
- Vulnerabilidades WPA
- Ataques WPA / WPA2-PSK
- Líneas futuras

Introducción

- WEP presenta grandes debilidades de seguridad
- Mejoras WPA
  - Claves de 128 bit (48bits de IV)
  - Cambio dinámico de claves
  - Evita ataques estadísticos
- WPA2, separación de la autenticación de usuario de la integridad y privacidad

WPA vs WPA2

- WPA medida intermedia hasta WPA2 o 802.11i (2004)

		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

Autenticación

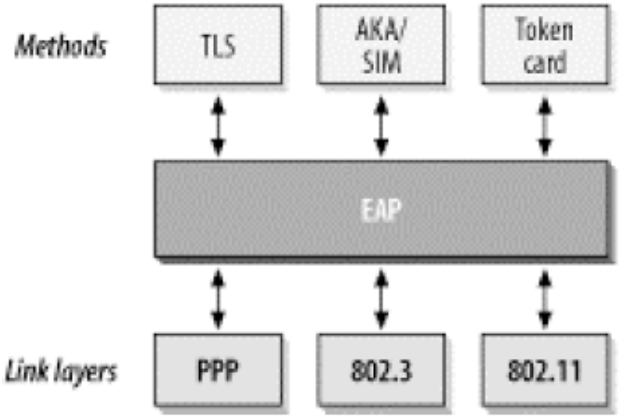
- Dos modos:
  - Modo Personal / PSK (PreShared Key)
  - Modo Empresarial / 802.1x

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
- Usuarios domésticos o pequeñas redes:
  - Configuración simple
  - Seguridad aceptable
  - Sin componentes adicionales: Servidor

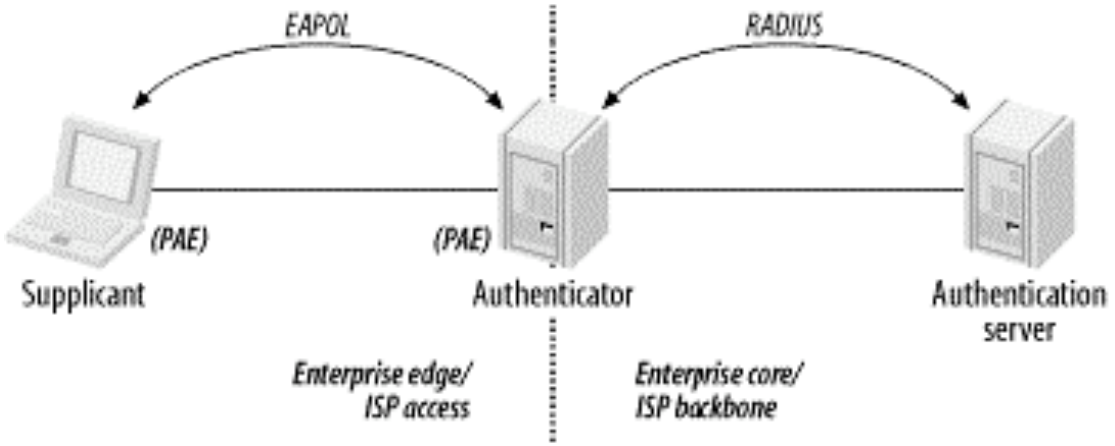
Autenticación: 802.1x (1)

- También implementación en redes cableadas
- Adecuado para empresas
  - 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)



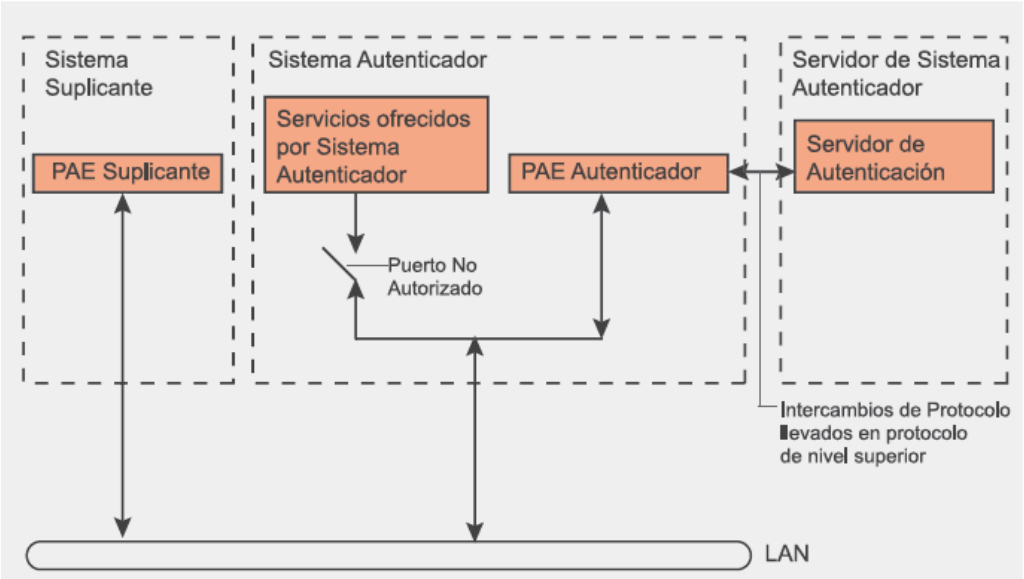
Autenticación: 802.1x (2)

- 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 (Remote Authentication Dial In User Service)



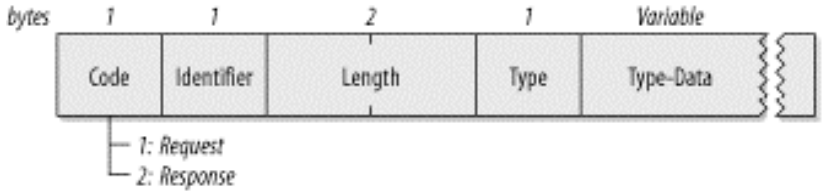
Autenticación: 802.1x (3)

- Cada puerto físico, dos puertos lógicos
  - PAE (Port Access Entity) de autenticación abierta siempre y permite el paso de procesos de autenticación
  - PAE de servicio sólo se abre tras una autenticación exitosa por un tiempo limitado (3600 segundos por defecto).



EAP (Extensible Authentication Protocol) (1)

- Tipos de mensaje:
  - Request: Mensajes desde el AP al cliente.
  - Response: Mensajes desde el cliente al AP.



  - Success: Enviado por el AP a la STA, significa que el acceso está permitido.
  - Failure: Enviado por el AP a la STA, indica que se deniega la conexión.

EAP (Extensible Authentication Protocol) (2)

- Mensajes Request / Response
  - Type: tipo de solicitud o respuesta.
    - Mayores que 4 métodos de autenticación.
    - Por parejas, excepción de cuando una solicitud no es aceptada, entonces el par debe enviar un NAK indicando un tipo alternativo.
    - Tipo1: Identity. Normalmente es la primera solicitud del autenticador.
    - Tipo2: Notification. Notificaciones del sistema de autenticación. y el campo TypeData es de longitud cero.
    - Tipo3: NAK. Indica un nuevo método de autenticación.
    - Tipo4: MD-5 Challange
    - Tipo5: One-time pasword (OTP)
    - Tipo6:Generic Token Card
    - Tipo13:TLS

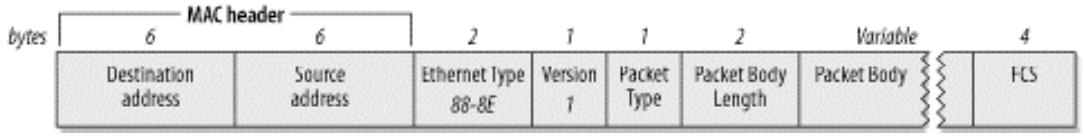
EAP (Extensible Authentication Protocol) (3)

- EAP-MD5
  - Función hash MD5
  - Vulnerable ataques de diccionario, desuso
- LEAP (Lightweight Extensible Authentication Protocol)
  - Desarrollado por Cisco
  - Versión modifcada de MS-CHAP
  - No hay protección, en desuso
- EAP-TLS (EAP-Transport Layer Security)
  - Basado en certificados digitales, tanto del cliente como del servidor
  - Proceso de autenticación
    - Envío de identificación (nombre de usuario) del solicitante al servidor de autenticación
    - El servidor envía su certificado
    - Lo valida y responde con el suyo propio
    - Si el certificado del solicitante es válido, el servidor responde con el nombre de usuario antes enviado y se comienza la generación de la clave de cifrado
    - Será enviada al AP por el servidor de autenticación

EAP (Extensible Authentication Protocol) (4)

- EAP-TTLS (EAP-Tunnelled Transport Layer Security)
  - Túnel mediante TLS para transmitir el nombre de usuario y la contraseña
  - Requiere sólo certificado de servidor
- PEAP (Protected EAP)
  - Similar a EAP-TTLS
  - Basado en usuario y contraseña también protegidos.

EAPOL (EAP over LAN)



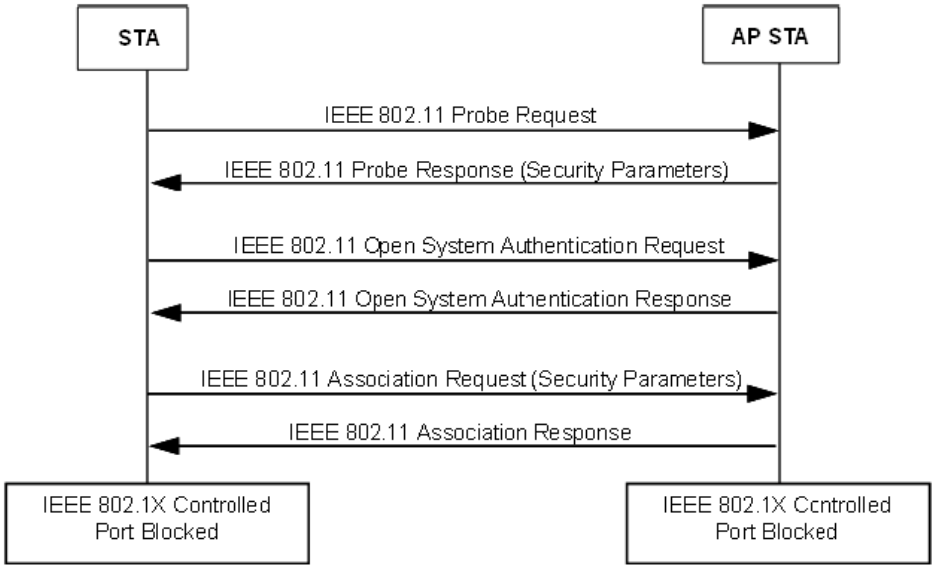
- Tipos de mensaje:
  - EAP-Packet: contenedores de mensajes EAP.
  - EAPOL-Start: El suplicante informa al autenticador que quiere autenticarse.
  - EAPOL-Logoff: Informa al autenticador que el cliente quiere desconectarse (convertirá el puerto en no autorizado).
  - EAPOL-Key: Soporte para de información claves.

RADIUS

- Tipos de mensaje:
  - Access-request: Mensajes desde el AP al servidor de autenticación.
  - Access-challange: Respuestas del servidor de autenticación al AP.
  - Access-accept: Enviado por el servidor de autenticación para indicar éxito en la autenticación
  - Access-reject: Enviado por el servidor de autenticación para indicar fracaso en la autenticación

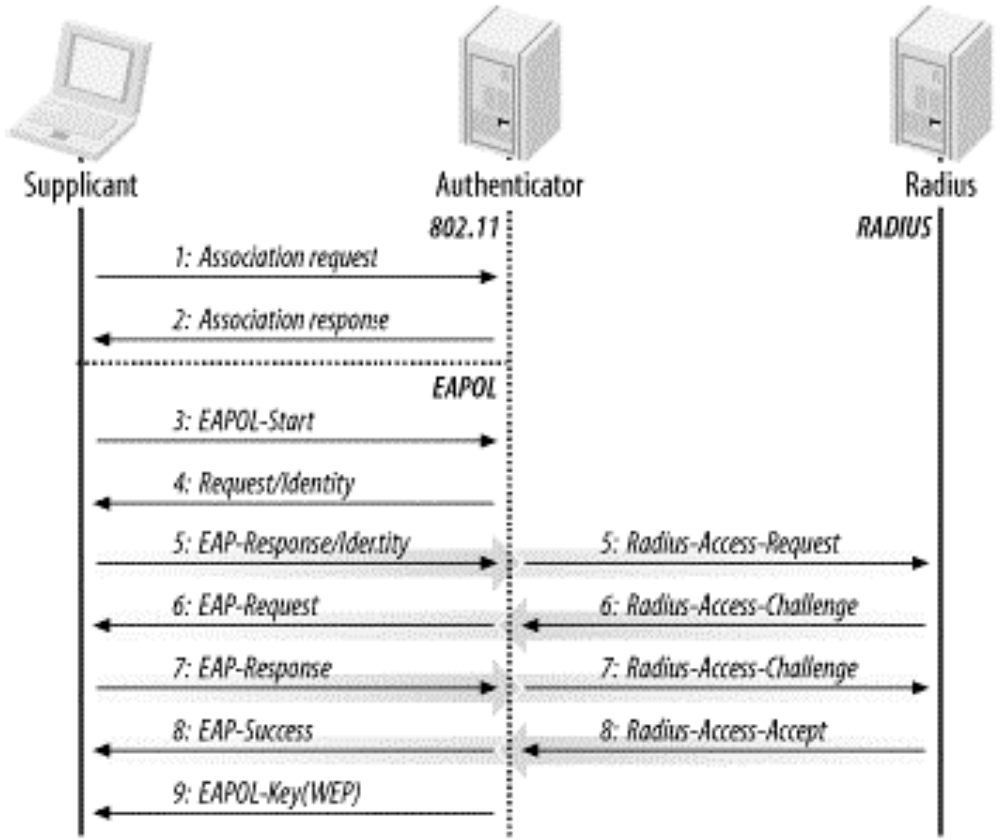
802.1x (1)

- Intercambio tramas gestión 802.11 entre STA y AP



802.1x (2)

- Tras la asociación de la STA: autenticación 802.1x



802.1x (3)

- La autenticación 802.1X inicio: el AP pide datos de identidad del cliente.
- Respuesta del cliente con el método de autenticación preferido.
- Intercambio mensajes entre el cliente y el servidor de autenticación para generar una clave maestra común (MK).
- Al final, el servidor de autenticación envía al AP un mensaje Radius Accept, con la MK y un mensaje final EAP Success para el cliente.

Generación e intercambio de llaves (1)

- Partimos de la PMK (Pairwise Master Key)
  - Para PSK (generada desde una passphrase (de 8 a 63 caracteres) o una cadena de 256-bit), PMK = PSK
  - Para 802.1X, PMK es derivada de la MK de autenticación
  - No se usa nunca para la encriptación o la comprobación de integridad
  - Generar una clave de encriptación temporal de sesión: PTK (Pairwise Transient Key)
- Derivación de la clave: dos handshake
  - 4-Way Handshake: derivación de la PTK (Pairwise Transient Key) y GTK (Group Transiet Key)
  - Group Key handshake: renovación de GTK

Generación e intercambio de llaves (2)

- PTK se deriva de la PMK, MAC del AP, MAC del cliente y dos nº aleatorios (ANonce y SNonce, generados por el autenticador y el suplicante)
- PTK, longitud depende el protocolo de encriptación: 512 bits para TKIP y 384 bits para CCMP. Son varias claves temporales dedicadas:
  - KCK (Key Confirmation Key 128 bits): Clave para la autenticación de mensajes (MIC) durante el 4-Way Handshake y el Group Key Handshake
  - KEK (Key Encryption Key 128 bits): Clave para asegurar la confidencialidad de los datos durante el 4-Way Handshake y el Group Key Handshake
  - TK (Temporary Key 128 bits): Clave para encriptación de datos (usada por TKIP o CCMP)
  - TMK (Temporary MIC Key – 2x64 bits): Clave para la autenticación de datos (usada sólo por Michael con TKIP). Se usa una clave dedicada para cada lado de la comunicación

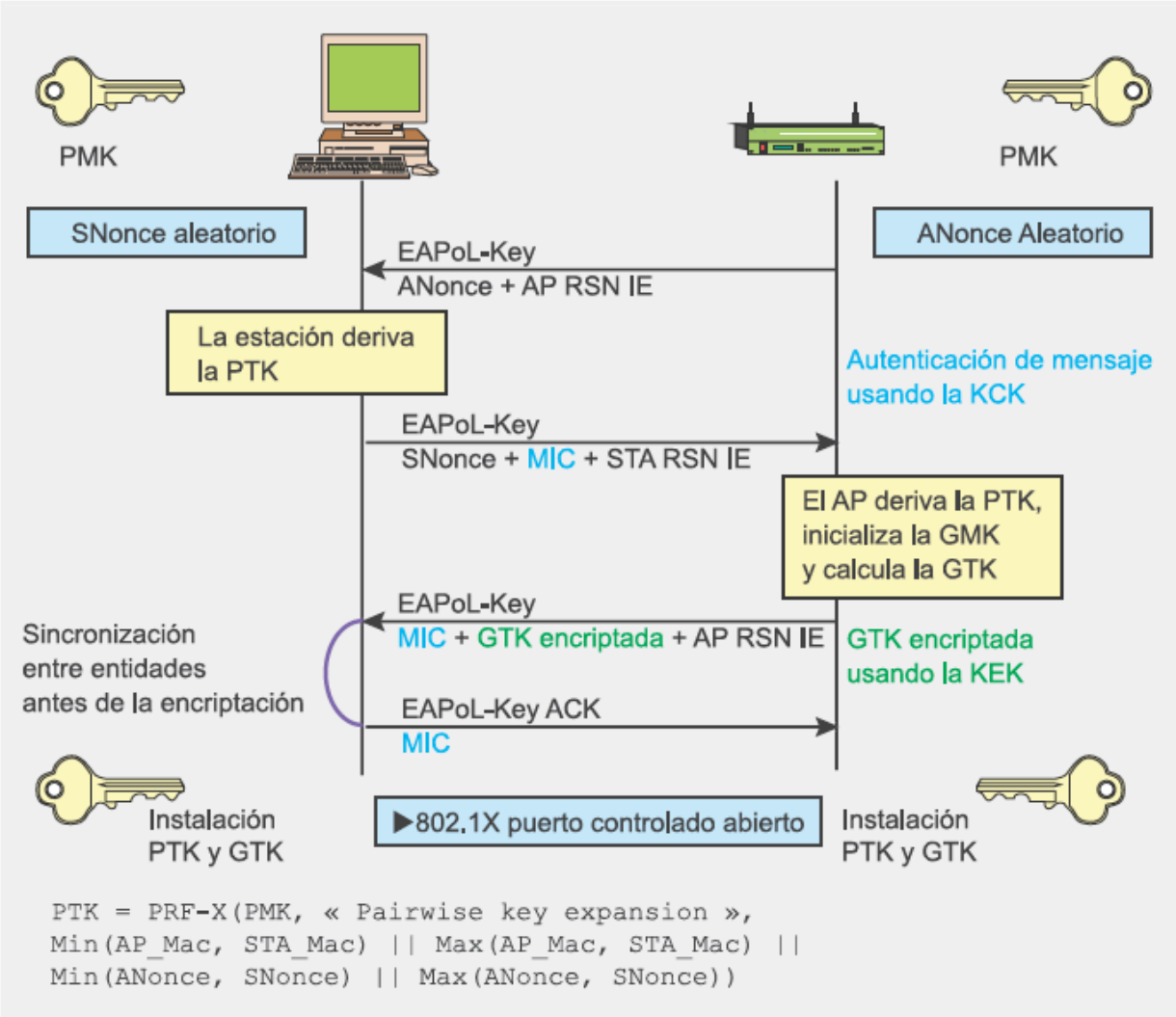
Generación intercambio de llaves (3)

- El tráfico multicast se protege con otra clave: GTK (Group Transient Key), generada de la clave maestra GMK (Group Master Key), MAC del AP y un nº aleatorio GNonce
- GTK, longitud depende del protocolo de encriptación 256 bits para TKIP y 128 bits para CCMP. Se divide en claves temporales dedicadas:
  - GEK (Group Encryption Key): Clave para encriptación de datos (usada por CCMP para la autenticación y para la encriptación, y por TKIP)
  - GIK (Group Integrity Key): Clave para la autenticación de datos (usada solamente por Michael con TKIP)

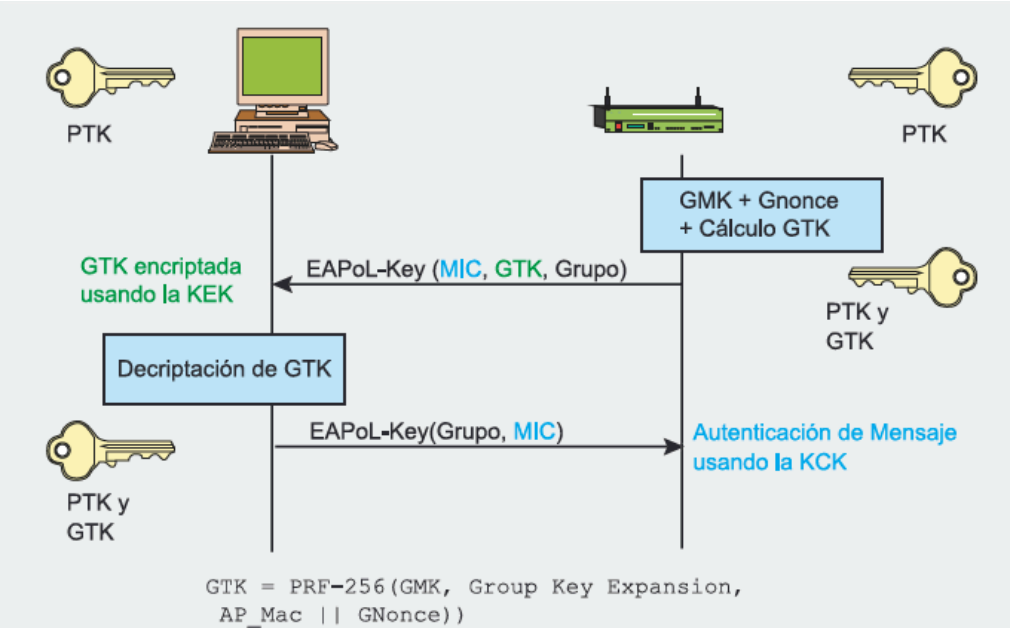
Generación intercambio de llaves (4)

- 4-Way-Handshake
  - Confirmar que el cliente conoce la PMK
  - Derivar una PTK nueva
  - Instalar claves de encriptación e integridad
  - Encriptar el transporte de la GTK
  - Confirmar la selección de la suite de cifrado
- Group Key Handshake
  - Disasociación de una estación o para renovar la GTK, a petición del cliente
- También existe un STAkey Handshake. Generación de una clave, STAkey, por el punto de acceso para conexiones ad-hoc

Generación intercambio de llaves (5): 4-Wav-Handshake



Generación intercambio de llaves (6): Group Key Handshake



Vulnerabilidades WPA

- Debilidad algoritmo Michael
  - Es invertible
- Debilidad TKIP

Ataque WPA / WPA2-PSK (1)

- Ataque de diccionario offline contra PSK (passphrase), recupera PMK
- Conocido el SSID del AP, tabla con hash del diccionario (PMK) para ese AP, reducimos tiempo (de chequear unas 50 passphrases/seg a unas 60000 passphrases/seg)
- PMK = PBKDF2(frase, SSID, SSID length, 4096, 256)donde,
  - PBKDF2 es un método utilizado en PKCS#5
  - 4096 es el número de hashes
  - y 256 la longitud del resultado
- Para conseguir PMK, capturar 2 primeros paquetes del 4-Way Handshake
  - PTK = PRF-X (PMK, Pairwise key expansion, Min(AP_Mac, STA_Mac) || Max(AP_Mac, STA_Mac) || Min(ANonce, SNonce) || Max(ANonce, Snonce))
  - Capturados intentar calcular el valor PSK=PMK para calcular PTK y derivar claves temporales

Ataque WPA / WPA2-PSK (2)

- Si adivinamos PSK, tenemos PTK, calculamos el MIC del segundo mensaje con la KCK y si es igual lo habremos adivinado la clave
- Cowpatty, Aircrack
- Diferencias WPA y WPA2, la función para calcular el MIC
- Conociendo PMK, puedes acceder a la red, pero no descifrar paquetes
  - Clave temporal por usuario y sesión
  - Capturar paquetes 4-Way-Handshake para conseguir PTK concreta
  - También se puede obtener GTK del tercer mensaje

Líneas futuras

- Cifrado
  - WPA: TKIP
  - WPA2:
    - TKIP
    - CCMP
    - WRAP
- Integridad
  - WPA: Michael
  - WPA2: CBC-MAC