CURSO DE HACKING ÉTICO

REDES INHALÁMBRICAS – TEORÍA II

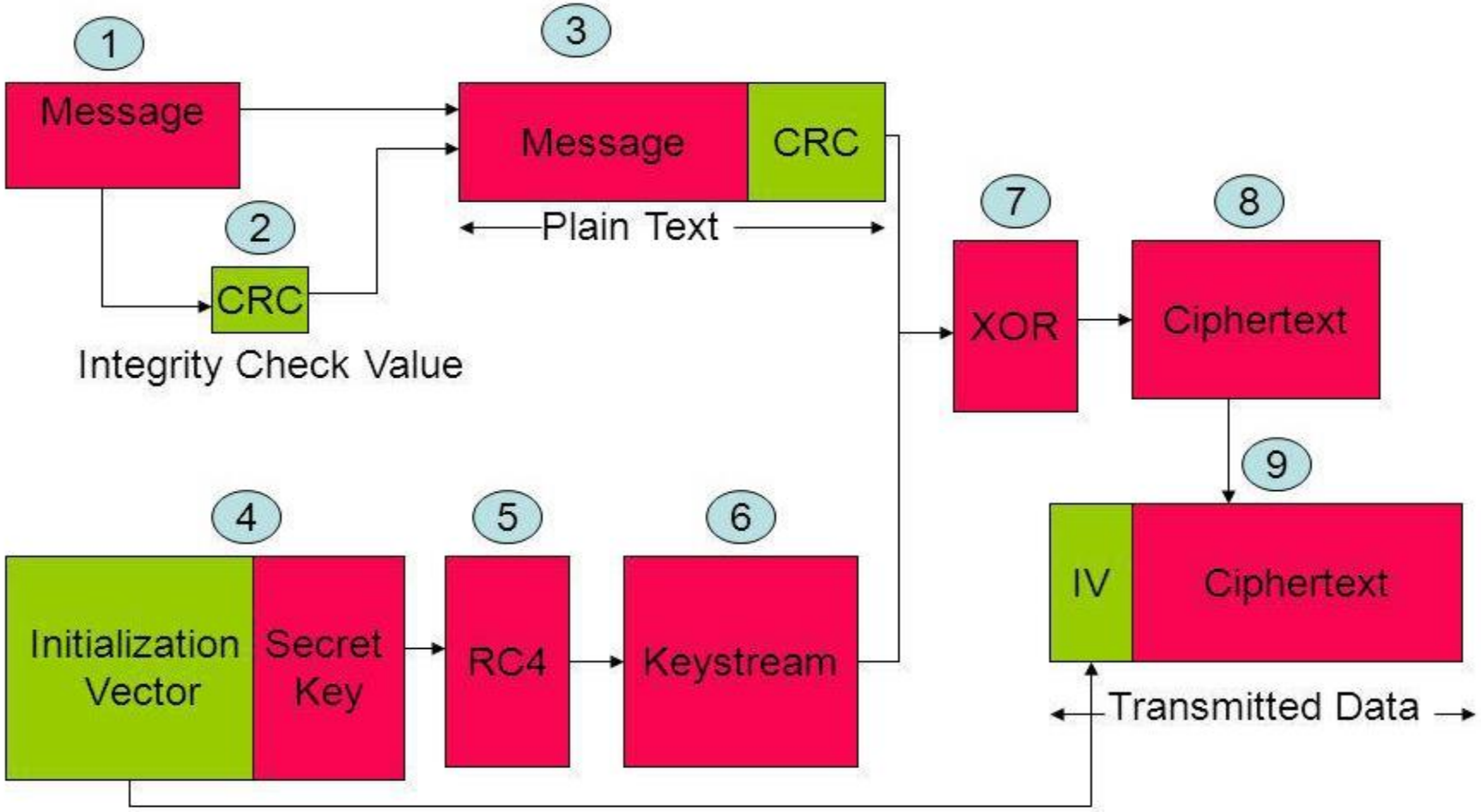
WEP (Wired Equivalent Privacy)

- WEP, es un protocolo de seguridad definido en el estándar 802,111b; que fue diseñado para proporcionar a las redes WIFI con un nivel de seguridad y privacidad comparable a las redes cableadas LAN.
- WEP usa un Vector de Inicializacion (IV) de 24 bits, para formar una trama cifrada RC4 para la confidenciabilidad de la información, y una verificación CRC-32 para verificar la integridad de los datos.
- Se han descubierto múltiples vulnerabilidades del cifrado RC4, siendo totalmente inseguro a día de hoy.
- Esto implica que puede ser fácilmente crackeado.

Como funciona WEP

1. Un código de verificación CRC-32 es utilizado para añadir a los datos que queremos enviar, un Integrity Check Value (ICV), que es añadido a dichos datos.
2. Un número aleatorio de 24 bits, conocido como Vector de Inicialización (IV) es añadido a la clave WEP. Los dos datos juntos son conocidos como WEP Seed.
3. La combinación del IV y la clave WEB (60, 128 o 256 bits), sirve de entrada al algoritmo RC4 para generar lo que se llama Key Stream.
4. El sistema hace una operación lógica XOR del Key Stream con la combinación de los datos y del ICV para producir la trama de datos encriptados.
5. El sistema envía dicha trama junto con el Vector de Inicialización

Como funciona WEP



WAP/WPA2 (WIFI Protected Access)

- WPA es un protocolo de seguridad definido en el estándar 802,11i. Usa TKIP, Protocolo de Integridad de Clave Temporal, que usa el protocolo de cifrado RC4 de 128 bits y 64 bits para Comprobar la Integridad del Mensaje (MIC).
- El proceso de encriptación es similar al realizado en WEP, pero con varias diferencias. Para empezar, si bien TKIP usa el algoritmo RC4 proporcionado por RSA Security para encriptar el cuerpo del frame así como el CRC antes de la transmisión, en este caso se utilizan IV de 48 bits, lo que reduce significativamente la reutilización y por tanto la posibilidad de que un hacker recoja suficiente información para romper la encriptación. Por otro lado y a diferencia de WEP, WPA automáticamente genera nuevas llaves de encriptación únicas para cada uno de los clientes lo que evita que la misma clave se utilice durante semanas, meses o incluso años, como pasaba con WEP.

WAP/WPA2 (WIFI Protected Access)

- WPA implementa lo que se conoce como MIC o message integrity code, es decir código de integridad del mensaje. Recordemos que WEP introduce unos bits de comprobación de integridad o ICV en el payload del paquete. Desgraciadamente es relativamente fácil, a pesar de que los bits de ICV también se encriptan, de modificarlos sin que el receptor lo detecte. Para evitarlo se hace uso del MIC (8 bytes, Message Integrity Check), un sistema de comprobación de la integridad de los mensajes, que se instala justo antes del ICV. Para ello se emplea el algoritmo Michael.
- Para el proceso de autentificación WPA y WPA2 usan una combinación de sistemas abiertos y 802.1x. Inicialmente el cliente se autentifica con el punto de acceso , el cual le autoriza a enviarle paquetes. Acto seguido WPA realiza la autentificación a nivel de usuario haciendo uso de 801.1x. WPA sirve de interfaz para un servidor de autentificación como WPA/WPA2 (Wireless Protected Access).

WAP/WPA2 (WIFI Protected Access)

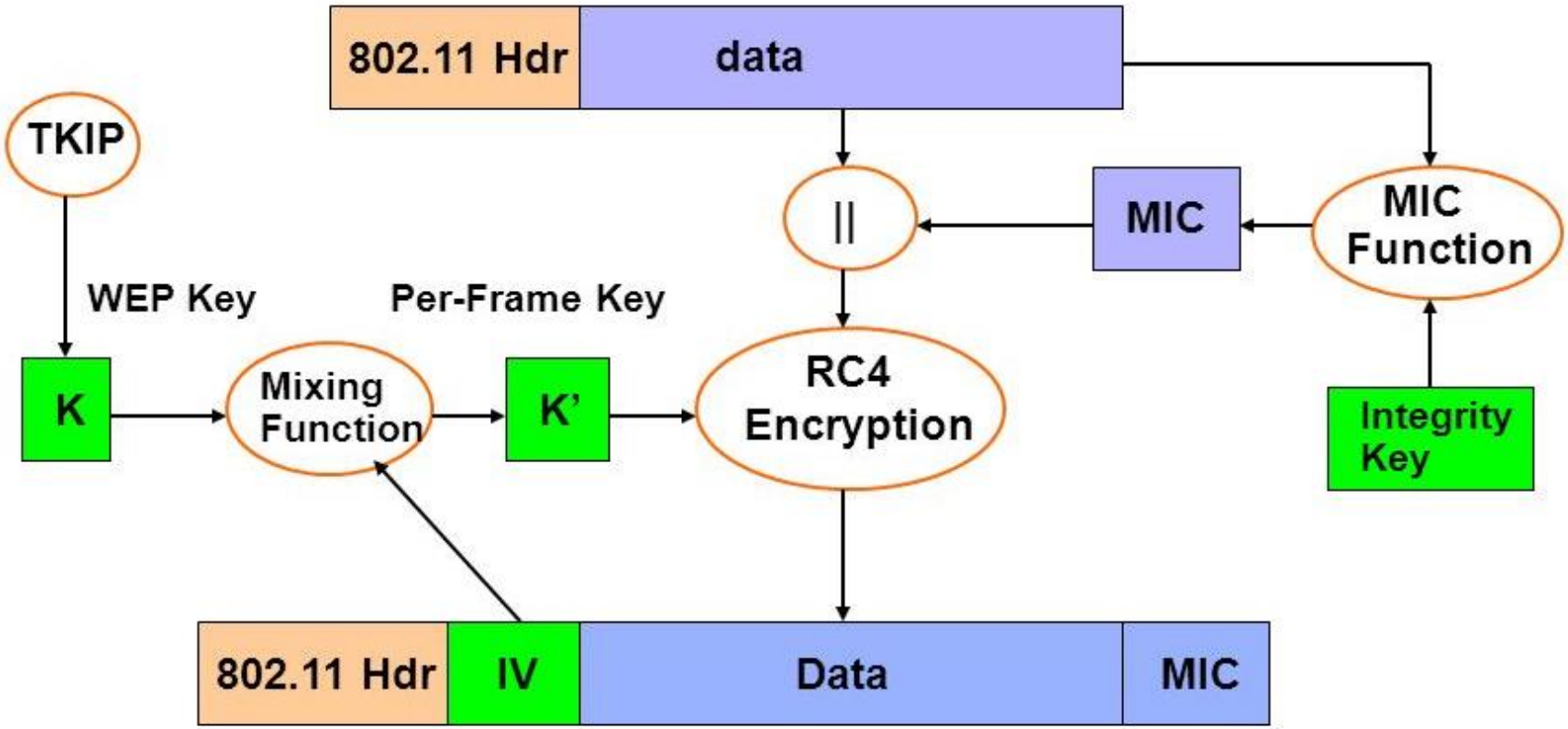
- En caso de que no se disponga de un servidor de autentificación se puede usar el modo con PSK. Una vez se ha verificado la autenticidad del usuario el servidor de autentificación crea una pareja de claves maestras (PMK) que se distribuyen entre el punto de acceso y el cliente y que se utilizarán durante la sesión del usuario. La distribución de las claves se realizará mediante los algoritmos de encriptación correspondientes TKIP o AES con las que se protegerá el tráfico entre el cliente y el punto de acceso.
- WPA2 fue lazada en septiembre de 2004 por la Wi-Fi Alliance. WPA2 es la versión certificada que cumple completamente el estándar 802.11i ratificado en junio de 2004.
- Análogamente a WPA, WPA2 presenta dos vertientes: la autentificación y la encriptación de datos. Para el primer elemento utiliza 802.1x / EAP o bien PSK. Para la encriptación se utiliza un algoritmo mejor que el TKIP, concretamente el AES.

WAP vs WAP2

	WPA	WPA2
Modo Enterprise	Autentificación: 802.1x / EAP	Autentificación: 802.1x / EAP
	Encriptación: TKIP/ MIC	Encriptación: AES-CCMP
Modo Personal	Autentificación: PSK	Autentificación: PSK
	Encriptación: TKIP/ MIC	Encriptación: AES-CCMP

En el modo Enterprise el sistema trabaja gestionada mente asignando a cada usuario una única clave de identificación, lo que proporciona un alto nivel de seguridad. Para la autentificación el sistema utiliza el ya comentado 802.1x y para la encriptación un algoritmo de cifrado mejor que el TKIP, el AES. Para el caso de funcionamiento en la versión personal, se utiliza una clave compartida (PSK) que es manualmente introducida por el usuario tanto en el punto de acceso como en las máquinas cliente, utilizando para la encriptación o bien TKIP o AES. En este sentido las diferencias con WEP se basan en el algoritmo de cifrado de los datos.

Cómo funciona WAP



Problemas

- **DoS** - Desgraciadamente WPA no está exento de problemas. Uno de los más importantes sigue siendo los DoS o ataques de denegación de servicio. Si alguien envía dos paquetes consecutivos en el mismo intervalo de tiempo usando una clave incorrecta el punto de acceso elimina todas las conexiones de los usuarios durante un minuto. Este mecanismo de defensa utilizado para evitar accesos no autorizados a la red puede ser un grave problema.
- **Deautenticación** - el objetivo es forzar al cliente a reautenticarse, lo que unido a la falta de deautenticación para las tramas de control que se utilizan para la autenticación y asociación hacen posible que la atacante la suplantación de direcciones MAC (ARP Spoofing)
- Podemos establecer ciertas medidas
  - Filtrado de direcciones MAC
  - Ocultacón del nombre dela RED SSID

Debilidades WPA/WPA2

- La vulnerabilidad más práctica es el ataque contra la clave PSK de WPA/WPA2. La PSK proporciona una alternativa a la generación de 802.1X PMK usando un servidor de autenticación. Es una cadena de 256 bits o una frase de 8 a 63 caracteres, usada para generar una cadena utilizando un algoritmo conocido: PSK = 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. La PTK es derivada de la PMK utilizando el 4-Way Handshake y toda la información utilizada para calcular su valor se transmite en formato de texto.

Debilidades WPA/WPA2

- La fuerza de PTK radica en el valor de PMK, que para PSK significa exactamente la solidez de la frase. Como indica Robert Moskowitz, el segundo mensaje del 4-Way Handshake podría verse sometido a ataques de diccionario o ataques offline de fuerza bruta. La utilidad cowpatty se creó para aprovechar este error, y su código fuente fue usado y mejorado por Christophe Devine en **Aircrack** para permitir este tipo de ataques sobre WPA. El diseño del protocolo (4096 para cada intento de frase) significa que el método de la fuerza bruta es muy lento (unos centenares de frases por segundo con el último procesador simple). La PMK no puede ser pre-calculada (y guardada en tablas) porque la frase de acceso está codificada adicionalmente según la ESSID. ***Una buena frase que no esté en un diccionario (de unos 20 caracteres) debe ser escogida para protegerse eficazmente de esta debilidad***.

Amenazas WIFI

Los riesgos en las redes inalámbricas los podemos clasificar en función del tipo de ataque:

- Ataques de control de acceso. Intento de entrar en una red evadiendo las medidas de contro., tal como MAC filter, etc.
- Ataques de integridad. Intentan cambiar o alterar los datos durante la transmisión. El atacante envía tramas de gestión, control, etc sobre la red WIFI
- Ataques de confidenciabilidad. El atacante intenta interceptar información confidencial rompiendo la encriptación.
- Ataques de disponibilidad (DoS). El atacante intenta deliberadamente obstruir el acceso al servicio WIFI de los clientes.
- Ataques de autenticación. Robo de la identidad de los clientes WIFI.

Amenanas WIFI

Ataques de Control de Acceso

El atacante intenta acceder a la red evadiendo las medidas de control de acceso como puede ser filtrado MAC, etc.

- War Driving
- Rogue Acces Points
- MAC Spoofing
- AP Misconfiguration
- Ad Hoc Associations
- Promiscous Client
- Unauthorized Association

Amenanas WIFI

Ataques de Integridad

Este tipo de ataque implica cambiar o alterar los datos durante la transmisión, enviando tramas de control, gestión o datos sobre la red para engañar a los dispositivos WIFI para poder realizar otro tipo de ataque (p.e. Dos)

- Data Frame Injection
- WEP injection
- Data Replay
- IV Replay Attacks
- RADIUS Replay
- Bit-Flipping Attacks

Amenanas WIFI

Ataques de confidenciabilidad

Este tipo de ataque intercepta la información confidencial enviada sobre una red inalámbrica, tanto si está o no encriptada. En caso que lo esté intentará romper la encriptación para acceder a la información.

- Eavesdropping: Ethereal, Ettercap, Kismet
- Traffic Analysis
- Cracking WEP KEY: Aircrack, AirSnort, …
- Evit Twin AP: HostAP, OpenAP
- Session Hijacking
- MITM attack: dsniff, Ettercap

Amenanas WIFI

Ataques de disponibilidad

En este tipo de ataque se intenta de forma deliberada obstruir el acceso al servicio WIFI a los dispositivos (DoS)

- Robo del AP
- Disassociation Attacks
- EAP-Failure: File2air
- Beacon Flood: FakeAP
- DoS
- De-authenticate Flood: Airjack, Omerta
- Routing Attacks: RIP protocol

Amenanas WIFI

Ataques de autenticación

Este tipo de ataca intenta hacerse con la identidad de los clientes WIFI, tal como su información personal, credenciales de acceso, etc.

- PSK Cracking: KisMAC
- LEAP Cracking: Anwrap, Asleap
- Domain Login Cracking: John the Ripper, L0phtCrack, Cain & Abel
- Identity Theft: Wireshark
- Application Login Theft: Password Sniffer, dsniff

Metodología de ataque a redes WIFI

El objetivo final de un ataque a una red WIFI (o cableada), es obtener acceso no autorizado a la red para obtener acceso a sus recursos.

El ataque normalmente sigue una secuencia de acciones para encontrar cada posible punto de entrada a la red destino, para poder entrar aplicando las técnicas enumeradas anteriormente.

El atacante usa diferentes metodologías como pueden ser:

- Descubrimiento WIFI
- Análisis del tráfico WIFI
- Probar diversos vectores de ataques
- Romper la encriptación de los algoritmos de cifrado
- Comprometer la red WIFI

Metodología de ataque a redes WIFI

Descubrimiento de redes WIFI

Tenemos múltiples herramientas que nos permiten detectar posibles objetivos:

- inSSIDer, https://www.metageek.com
- Kismet, https://www.kismetwireless.net
- NetStumbler, http://www.stumbler.net
- AirRadar4, https://www.koingow.com
- WifiExplorer (Móviles) , http://nutsaboutnets.com
- Analizador de WIFI, de Abdelrahman M.Sid, Play Store

Metodología de ataque a redes WIFI

Análisis del tráfico WIFI

El análisis de tráfico permite al atacante identificar posibles vulnerabilidades y posibles “víctimas” de una red WIFI

- WireShark/AirPcap, https://www.wireshark.org
- SteelCentral Packet Analyzer, https://www.riverbed.com
- OmniPeek Enterprise, https://www.savvius.com
- CommView for WIFI, http://www.tamos.com
- AirMagned WIFI Analyzer, http://enterprise.netscout.com

Metodología de ataque a redes WIFI

Lanzar ataques contra una red WIFI

Una vez hemos descubierto y analizado la red objetivo por parte del atacante, este está en disposición de lanzar diversos ataques sobre la red destino según metodologías vistas anteriormente.

- Aircrack-ng Suite, https://www.aircrack-ng.org