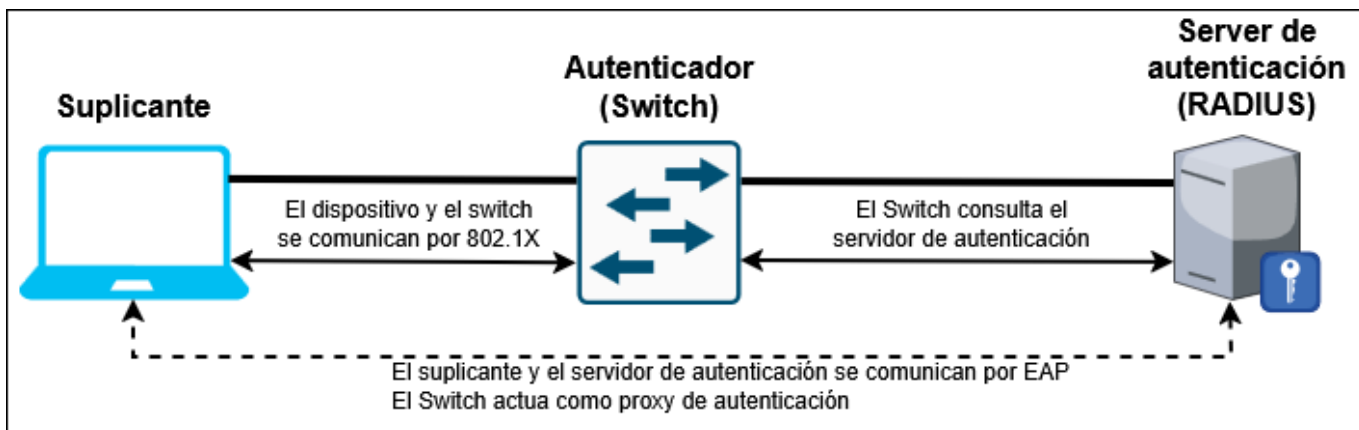


Seguridad a Nivel de Enlace [L2]

PBNAC en IEEE 802 Local Area Networks

802.1X es un estándar IEEE para control de acceso basado en puertos (PBNAC). Forma parte del grupo IEEE 802.1 de protocolos de red. Provee mecanismos de autenticación para dispositivos que se quieren conectar a una LAN o una WLAN. Los puertos del switch están bloqueados por defecto hasta que el dispositivo conectado sea autenticado correctamente en alguna entidad de seguridad de la infraestructura. La autenticación 802.1X involucra 3 partes:

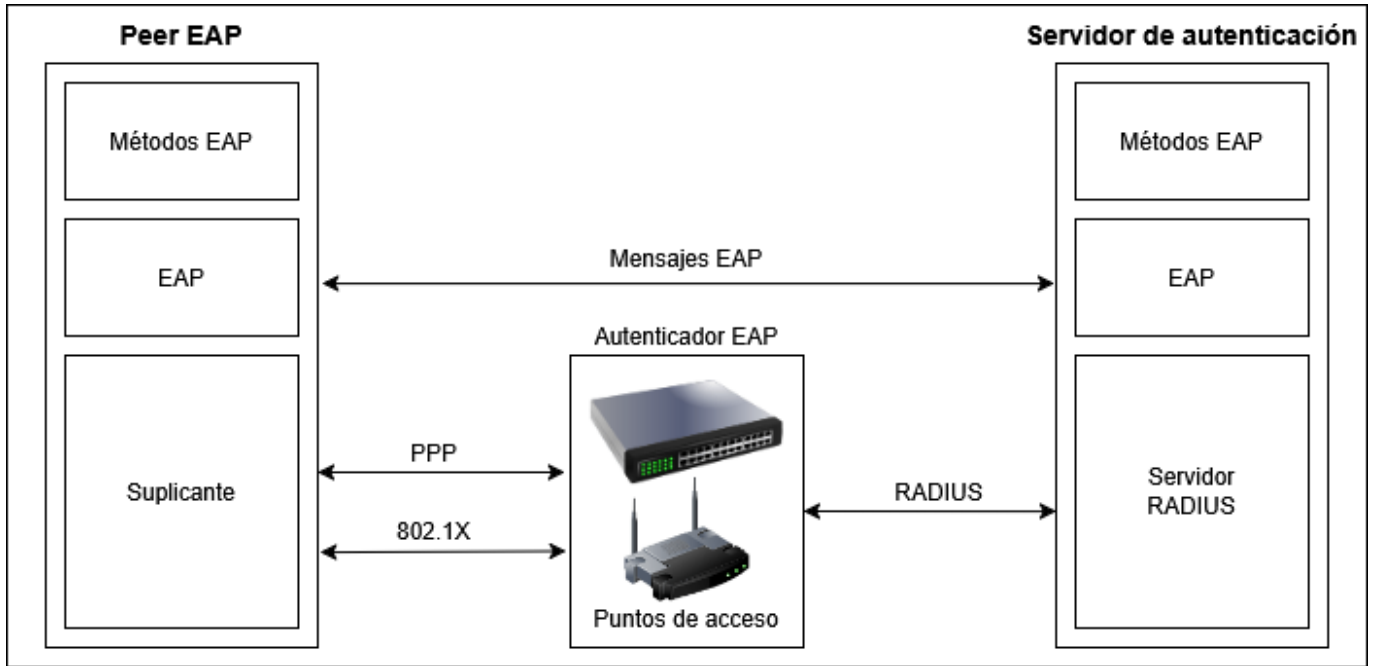
- Suplicante: Dispositivo cliente
- Autenticador: Switch o Punto de acceso
- Servidor de autenticación



Extensible Authentication Protocol (EAP)

Es un framework de autenticación de capa 2, no es un mecanismo de autenticación. Provee algunas funciones comunes y metodos de negociación de autenticación llamaods métodos EAP.

- La autenticación es proveida por el protocolo interno dentro de EAP, no por EAP
- Se usa en 802.1X entre el suplicante y el servidor de autenticación
- En EAP al suplicante se le llama peer, reflejando la idea general de que EAP podría ser usado para autenticación mutua entre entidades equivalentes.
- Facilita la implementación de entidades de autentiación intermedia o autenticadores en redes donde la gestión de usuarios está centralizada.



EAP define formatos de mensajes de autenticación genéricos

- Request
- Response
- Success
- Failure

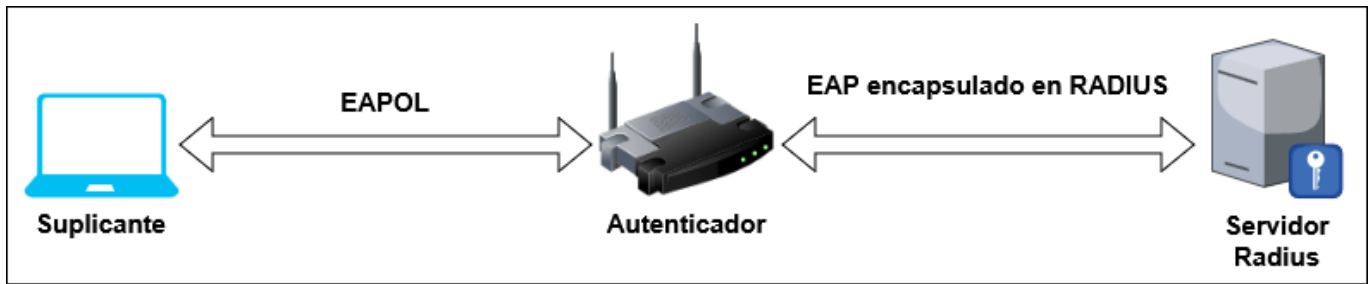
El campo "Tipo de autenticación EAP" especifica el mecanismo de autenticación elegido, el tipo de credenciales y como usarlas para realizar la autenticación mutua de forma segura. Hay tres tipos especiales de EAP:

- Identidad
- Notificación
- Nak

EAPOL y RADIUS

EAP normalmente funciona a nivel de enlace como Point-to-Point Protocol (PPP) o IEEE802 sin requerir una IP. 802.1X define la encapsulación de EAP sobre medios IEEE802 cableados, conocidos como EAP Over LAN (EAPOL). Si el autenticador y el servidor de autenticación no están ubicados conjuntamente, los mensajes EAP deben encapsulados en otro protocolo para ser entregados al servidor de autenticación, ocurriendo lo opuesto en una dirección inversa.

RADIUS (Remote Access Dial-In User Service) define sus propios protocolos de transporte para comunicación entre un Autenticador y un servidor RADIUS AAA. EAP se encapsula en atributos de RADIUS.



RADIUS

Define mensajes entre el El Servidor de Acceso a la Red (NAS) y el servidor de autenticación:

- el NAS envía un Access-Request
- El server de Autenticación responde con Access-Challenge, Access-Accept o Access-Reject

Se encapsula EAP en el Access-Request y Access-Challenge de RADIUS todas las veces que sea necesario.

- EAP-Message-attribute
- El Message-Authenticator Attribute es obligatorio para paquetes RADIUS transportando EAP-message Attributes.

Radius tiene su propio protocolo de seguridad basado en una clave compartida entre los endpoints (NAS y Server RADIUS)

Seguridad de RADIUS

Las respuestas del servidor de autenticación contienen un autenticador, las peticiones genéricas de los clientes no son autenticadas

- Authenticator = (code|id|length|requestAuth|Attributes|Shared Secret)
- RequestAuth es un nonce del NAS.

Si un paquete RADIUS transporta mensajes EAP, debe usar el atributo "Message-Authenticator" (Shared Secret, Code|ID|Length|RequestAuth|Attributes). Radius tiene su propia función key wrap para ocultar atributos confidenciales usando la clave compartida. Si un método EAP de autenticación genera material de clave (Master Session Key), el Pairwise Master Key (PMK) derivado de MSK es enviado en un paquete Access-Accept RADIUS del server al NAS cifrado con la clave compartida.

Seguridad EAP-RADIUS

- Radius es vulnerable a ataques de diccionario.
 - Las claves compartidas tienen un tiempo de vida muy largo, muchos mensajes van en texto plano con su respectivo autenticador.
 - Se usa MD5, que es altamente vulnerable
- Otros problemas están relacionados con privacidad, spoofing, hijacking, ataques replay, ataques de negociación, ataques de suplantación, Man in the middle...
- RADIUS recomienda usar un mecanismo de autenticación bidireccional y tecnología IPSEC para

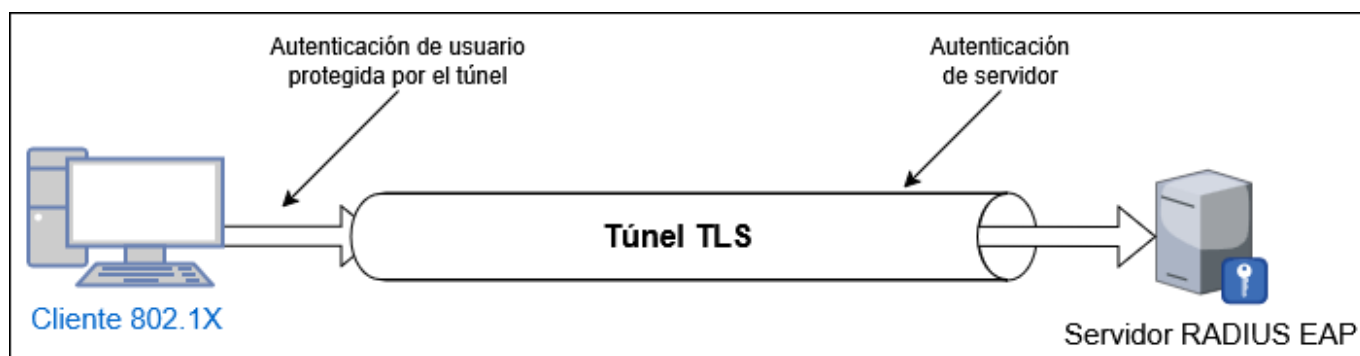
proteger la comunicación entre el NAS y el autenticador.

Mecanismos de autenticación basados en EAP

- EAP-TLS: Autenticación mutua durante el handshake inicial que establece el tunel tls. se requieren certificados X509 en ambos lados
- EAP-TTLS (EAP Tunneled TLS): Autenticación mutua, solo el server AAA necesita certificado X509. Normalmente la autenticación del cliente se hace usando contraseñas compartidas. .
- PEAP (Protected EAP): Similars a EAP-TTLS. El mecanismo de autenticación del suplicante usa EAP para transportar las credenciales del cliente.
- EAP-FAST (EAP Flexible Authentication via Secure Tunneling): No es necesario el uso de clientes o certificados de servidor. Usa PAC (Protected Access Credentials) para establecer el tunel TLS. Tiene 3 fases, PAC Provisioning, TLS Tunnel stablishment y Authentication.

Autenticación a través de un túnel TLS

Los credenciales de usuario son vulnerables a ataques de diccionario. Transimir infomración dentro de un tunel TLS previene que un atacante puede acceder a dichos credenciales. El túnel TLS se establece utilizando el certificado del servidor, autenticando en un primer momento el final de la conexión. Tras eso, se usa el tunel cifrado para enviar las credenciales del cliente de forma segura.



Secure Association Protocol

El acceso puede ser denegado para un peer autenticado debido a la ausencia de autorización u otras razones. Un peer sin credenciales de acceso o que ha fallado el proceso de autenticación puede tener acceso a la red para un servicio o para una VLAN de invitados. El completar la autenticación por parte de un perr y un server eap no significa que tenga acceso inmediato a la red, una Security Association entre el EAP per y el Authenticator debe ser establecida con el Secure Association Protocol.

MACsec

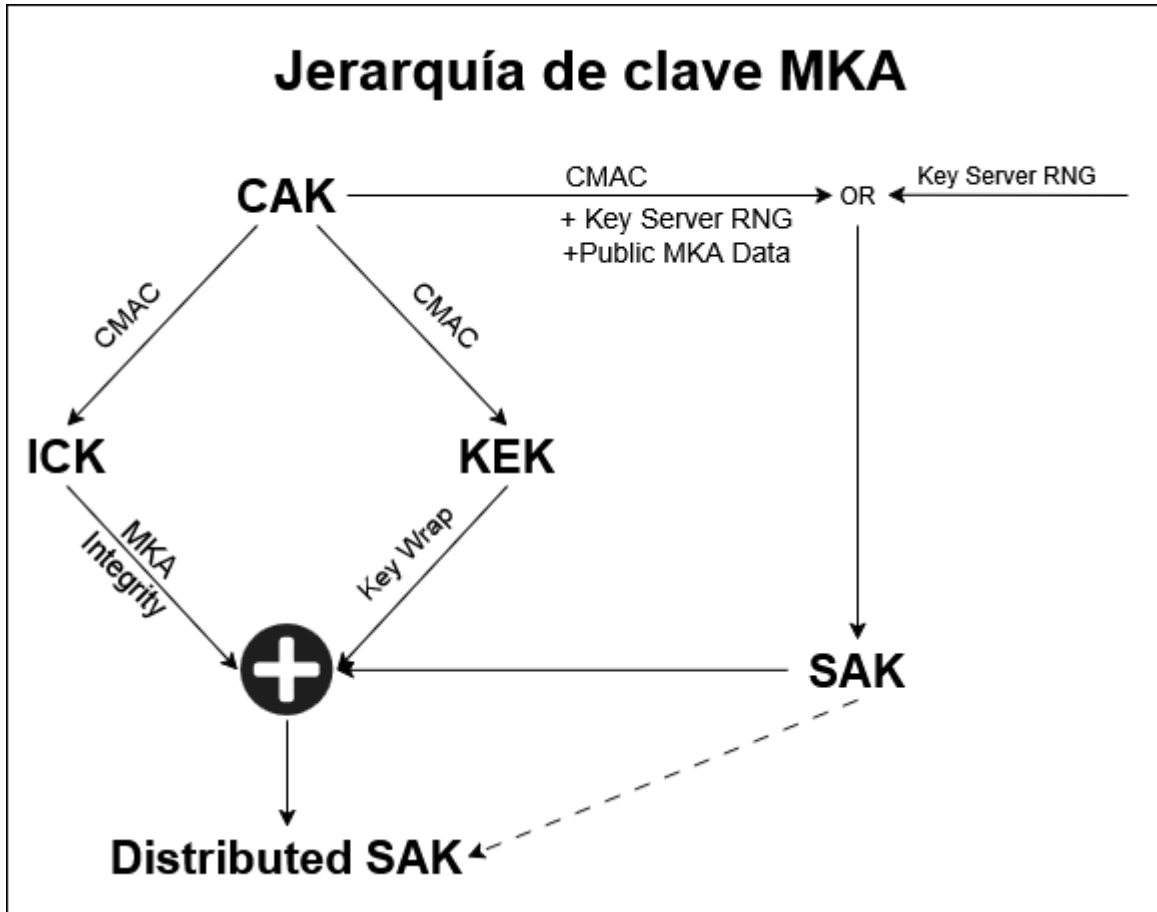
Es el cifrado de conexiones ethernet cableadas (IEEE 802.1AE). Cifrado en la capa MAC, cifrado a la velocidad del cable. MACsec garantiza lo siguiente:

- Integridad de los datos sin conexión
- Autenticidad de los datos de origen
- Confidencialidad

- Protección contra replay
- Limita la naturaleza y extensión de los ataques de denegación de servicio.

Definiciones MACsec

- Secure Connectivity Association (CA): Relación de seguridad establecida y mantenida por protocolos clave de acuerdo (MKA), que compone un subconjunto de puntos de acceso a servicio completamente conectados en estaciones conectadas a una sola LAN.
 - Secure Connectivity Association Key (CAK): Clave secreta poseída por los miembros de la CA
 - Secure Connectivity Association Key Name (CKN): Texto que identifica un CAK
 - CAK y CKN son derivados del material de clave del keyring que el método EAP inyectó en el solicitante y autenticador.
 - Cada CA tiene un key server elegido dinámicamente.
 - Un key server perteneciente a varias CA con peers en el mismo segmento puede crear un grupo CA.
- Secure Association (SA): Relación de seguridad que provee garantías de seguridad para los marcos transmitidos de un miembro de la CA a otro.
 - Cada SA está soportado por una sola secret key o un solo set de claves donde la operación utilizada para proteger un marco necesita más de una clave.
 - SA es unidireccional.
- Secure Association Key (SAK): La clave secreta usada por una SA.
- Secure channel (SC): Un SC es soportado por una secuencia de SAs, permitiendo el uso periódico de claves nuevas sin terminar la relación.
- MACsec Key Agreement (MKA): Protocolo IEEE802.1X. Puede descubrir miembros ya autenticados en una CA conectadas a la misma LAN. Puede confirmar la posesión mutua de CAK para probar autenticación mutua pasada. Asegura que los datos protegidos por MACsec no tienen retraso.
 - Usa marcos EAPOL-MKA para el intercambio de información
 - Asegura transporte multipoint-to-multipoint completamente distribuido.
 - Si no se implementa un MKA, MACsec puede seguir siendo usado para cifrar datos si los peers finales están configurados de forma estática.



- Mensaje de Código de autenticación con cifrado basado en ASES (CMAC)
- CAK es el PMK que el Server de Autenticación entrega al Autenticador en RADIUS Access-Accept.
- Durante el diálogo EAP entre métodos equivalentes en el server de autenticación y el suplicante, este último obtiene el MSK y deriva el PMK (CAK)
- Es estándar también considera la posibilidad de la configuración manual de CAK y CKN en ambos extremos del enlace.

Seguridad de LAN Inalámbricas IEEE 802.11i

El estándar 802.11 describe las funciones y servicios que un dispositivo debe implementar para ser integrados en una red 802.11 centrándose en la capa física (PHY) y la capa de enlace de datos (DLL).

- Servicios: Soporta transferencias de datos asíncronas que se refieren al tráfico que es relativamente insensible a demoras temporales como el email o las transferencias de archivos. Opcionalmente también puede soportar tráfico que debe tener una demora específica para alcanzar una calidad de servicio QoS) aceptable. Incluye procedimientos para autenticación y cifrado de comunicaciones para asegurar la privacidad.
- Arquitectura:
 - Infraestructure Network
 - Point to point network
- Medium Access Control (MAC)
 - Mecanismo de acceso, fragmentación, cifrado
 - Gestion MAC: Sincronización, roaming entre APs, gestión de energía

- Capa física
 - Selección de canal, modulación, coding.

Las aplicaciones no deberían ser conscientes de la existencia de una red inalámbrica.

Arquitectura IEEE 802.11

1. Infrastructure Network: La tecnología basada en APs usa puntos de acceso para conectar el tráfico a una red troncal cableada o inalámbrica. Los puntos de acceso permiten a un dispositivo cliente inalámbrico comunicarse con otros dispositivos cableados o inalámbricos de la red. Cada AP gestiona comunicaciones en su rango. (Funciones MAC, funciones de gestión de movilidad, funciones de autenticación...)
 1. Elementos de una infrastructure network:
 1. Station (STA): Ordenador con mecanismos de acceso al medio inalámbrico y conexión por radio al AP
 2. Access Point (AP): Estación integradas con la radio y la red cableada (sistema de distribución)
 3. Basic Service Set (BSS): Grupo de estaciones, incluyendo el AP, dentro del rango de transmisión del AP
 4. Portal: Gateway a otra red.
 5. Distribution System: Conexión en diferentes áreas AP a la red lógica (EES: Extended Service Set)
 2. El rango de un AP es de entre 20 y 500 metros, soportando entre 15 y 250 usuarios dependiendo de la tecnología. Múltiples AP pueden soportar la transferencia de un AP a otro según el usuario se mueve de un área a otra. Un AP inalámbrico puede monitorizar el movimiento de un cliente a través de su dominio y permitir o denegar tráfico o clientes.
 3. Puentes LAN en exteriores: Point-to-multipoint bridge, conecta lans en diferentes edificios. Alternativa económica a comprar cables de fibra óptica.
2. Red Point-to-Point (ad hoc): Una WLAN puede ser utilizada como una red stand-alone en cualquier lugar para enlazar varios equipos si tener que contruir o extender redes cableadas. En topología Point to Point, los dispositivos cliente dentro de una celda se comunican directamente entre ellos, no hay AP, los nodos deben estar en el mismo rango de transmisión.
 1. Redes Inalámbricas multisalto:
 1. Mobile ad hoc network (MANET): Propone una arquitectura plana donde cada nodo inalámbrico tiene capacidades de enrutado, extendiendo el rango de sus transmisiones más allá de su propio rango de cobertura. Enrutado en capa de red
 2. Mesh Wireless Network (IEEE 802.11s): Introduce una jerarquía en la arquitectura de red inalámbrica con la implementación de nodos mesh, routers troncales estacionarios, operando puentes en una red switched, pero enrutando en el nivel de enlace/MAC

Seguridad WLAN

- Amenazas de seguridad:
 - Interferencia en el medio inalámbrico: Ataques DoS aprovechando el espacio libre para comunicación
 - Escucha de comunicaciones: Limitar el acceso a la red es difícil.
 - Uso de recursos no autorizados
 - Ataques de engaño: Robo de credenciales fingiendo ser un AP, redes abiertas sin

seguridad.

- Técnicas de ataque en WLANs
 - Ataques con marcos de gestión: Si los marcos de gestión no están ni cifrados ni tienen protección de integridad, cualquiera puede falsificarlos. Esto puede ser usado para implementar ataques MitM o DoS.
 - Ataques Replay: Se captura un marco y se reenvía tal como es. Puede ser usado para ganar acceso no autorizado a la red
 - MAC spoofing: Se cambia la dirección MAC del atacante para hacerse pasar por un punto de acceso autorizado o un STA.
 - Denegación de servicio: Para prevenir que los usuarios autorizados puedan acceder a los recursos de red.
 - Crackeo offline de claves de cifrado o contraseñas: usando fuerza bruta o ataques de diccionario.
 - Man in the Middle: Se introduce una estación malintencionada entre otras 2, interceptando el tráfico entre estas sin interrumpir la comunicación, actuando como repetidor.

Ataque Man in the Middle en WLANs

- El MitM trata de pasar desapercibido. Este ataque se puede utilizar para esichar, recolectar credenciales, manipular marcos, romper conexiones TLS... Dependiendo de la situación del intruso, su conocimiento de credenciales de acceso o los objetivos, hay diferentes estrategias y técnicas:
 - Si el atacante está conectado a la misma wifi en la que se encuentra la víctima, puede simplemente impersonar algunos servicios.
 - Si un atacante, sin credenciales de acceso, está conectado via ethernet al sistema de distribución detrás del AP, puede usar varias técnicas antes mencionadas.
 - Otra técnica es suplantar el AP original o tratar de tumbar el AP original e impersonarlo en un canal diferente (Evil Twin)
- Contramedidas:
 - Si el atacante está dentro de la red es difícil de detectar, se puede usar un IDS o IPS.
 - No usar redes abiertas
 - Evitar conexiones automáticas a redes inalámbricas
 - Usar métodos de autenticación robustos como WPA-Enterprise
 - Usar sistema secundario de autenticación y tecnología de cifrado siempre que sea posible.

Contramedidas Oficiales

- Wired Equivalent Privacy (WEP): De las peores soluciones de seguridad que existen
- Wi-Fi Protected Access (WPA): Solución temporal para parchear el desastre que fue WEP.
- IEEE 802.11i y WPA2: Estandar actual
- WPA3: Oficialmente lanzado en 2018

Contramedidas específicas

- Control de acceso
 - Deshabilitar SSID

- Filtrar direcciones MAC
- Autenticación usando una clave común (WPA/2/3)
 - PSK: Pre Shared Key (WPA/2)
 - SAE: Simultaneous Authentication of Equals (WPA/3-Enterprise)
- dot1x: Autenticación usando un servidor AAA (WPA/2/3-enterprise)
- Autenticación usando portal captivo
- Deshabilitar WPS PIN mode en el AP
- Comunicaciones de datos con confidencialidad y autenticación
 - Temporal key Integrity Protocol (TKIP) y “Michael” MIC
 - AES-CCMP: AES (Advanced Encryption Standard) CTR (Counter mode) con CBC-MAC (Cipher Block Chaining Message Authentication Code) Protocol (IEEE 802.11i y WPA2)

Robust Security Network Association (RSNA)

El estándar IEEE 802.11i introduce este concepto como el tipo de asociación usada por un apr de estaciones si el proceso para establecer autenticación o asociación entre ellos incluye el 4-Way Handshake o Fast Transition Protocol. Durante el 4-way handshake ambas estaciones se demuestran la una a la otra que han sido configuradas con la misma Pair Master Key (PMK) la cual es material criptográfico primordial del cual las claves de cifrado se van a derivar.

Pre-RSNA

- Autenticación de la estación
 - Sistema abierto: No hay autenticación, solo filtrado de MAC
 - Clave compartida:
 - El AP envía un mensaje en plano (Challenge) que es cifrado por STA usando la clave wep compartida. Tras recibir el challenge cifrado, el AP cifra el original una vez y lo compara.
 - No hay autenticación del dispositivo, solo prueba de que se conoce la clave WEP.
 - Cifrado WEB
 - RC4 Stream Cipher

RSNA

- Autenticación:
 - 802.1x usando EAP y un servidor de autenciación, proveyendo autenticación mutua (WPA/2-enterprise)
 - PSK (PreShared Key): 4-way handshake que solo prueba que se conoce el PSK (WPA/2-Personal)
- Integridad y mecanismos de cifrado
 - mandatorio: CMP/AES y MIC
 - AES require hardware especial ausente en tarjetas de red antiguas
 - Opcioinal: TKIP y “michael” MIC
 - Solo recomendado para parchear equipamiento pre-RSNA
- Procedimientos para el establecimiento y gestión de claves dinamicas temporales.
 - El 4-way handshake provee de:
 - Nuevo integridad temporal y claves de cifrado cada vez que una estación se conecta a la red. Las claves temporales deben ser renovadas cada poco

- Diferentes claves de intergridad/cifrado parta cada estación, proveyendo algo de confidencialidad/protección interna contra dispositivos conectados a la misma WLAN.
 - El AP gestiona una clave de cifrado temporal y una clave de integridad temporal por estación, para tráfico unicast y un grupo de claves temporales para transmisiones broadcast/multicast. Si la funcionalidad marcos de gestión robistos es activada, una clave de grupo temporal (IGTK) para hacer broadcast de frames será definida.
 - Todas las calves son definidas del PMK
- si la autenticación 802.1X es activada, el la fase de 4-way handshake también es ejecutada inmediatamente después del diálogo entre el suplicante y el servidor de autenticación

Jerarí de claves

- Pairwise Master Key (PMK): La clave es derivada de un metodo EAP o obtenida directamente de una PSK (PreSharedKey)
- Pairwise Transient Key (PTK): Concatenación de claves de sesión derivadas de la PMK. sus componentes son:
 - Clave de confirmación (KCK)
 - Clave de cifrado de clave (KEK)
 - Clave Temporal (TK)

Portal Captivo

El objetivo es localizar una web de autenticación entre el punto de acceso y el resto de recursos.
Pasos:

1. Tras asociarse con el Ap y obtener su configuración de web, el dispositivo cliente no podría acceder ningún otro recurso al estar el AP haciendo filtrado de MAC/IP
2. Cuando el usuario trata de acceder un recurso es automaticamente redirigido a un sitio de autentiación usando el cliente web
3. El usuario debe proveer login/contraseña
4. Si la autenticación es exitosa, entonces el resto de recursos se vuelven disponibles.

Normalmente es usado por ISPs para proveer acceso a internet a través de puntos de acceso conocidos como hotspots. Tiene los siguientes problemas:

- Normalmente el resto de la comunicación no va cifrada
- Se puede realizar IP/MAC spoofing de un dispositivo ya autenticado.
- Enmascaramiento de varios dispositivos detrás de uno con capacidad de reenvio.
- Si el AP solo redirecciona pticiones iniciales http al sitio de autenticación y no filtra otros puertos, la autenticación puede ser saltada usando servidores externos.

Cifrado

El criptoanálisis es el estudio de los textos cifrados en un intento por restaurar el mensaje original o recuperar la clave de cifrado:

- Ciphertext-only attack

- Known-plaintext attack
- Chosen-plaintext attack
- Chosen-Ciphertext attack (El más difícil)

En un caso ideal, todos los mensajes han sido cifrados con la misma clave. Para implementar esta estrategia con solo una clave, la clave conocida y el vector de inicialización deben ser combinados en origen y destino para generar una contraseña de un solo uso. El vector de inicialización debe viajar en texto plano dentro del mensaje cifrado. Si el Vector de inicialización increse en 1 monotonamente, puede ser usado como un numero de paquete contra un ataque de replay.

Cifrado WEP (Wired Equivalency Privacy)

- Basado en cifrado RC4 usando claves de 64/128/256 bits.

$$C = P \oplus K_{iv}, \quad K_{iv} = \text{PRNG}(IV \mid \text{WEP key})$$

- El vector de inicialización es de solo 24 bits, es cuestión de tiempo que sea reutilizado.
- La clave (WEP Key) es una clave de larga duración compartida entre todos los STA y AP
- El reuso de Vector de Inicialización por parte de los STA no está prohibido.
- Si sabes P y C puedes obtener directamente K_{iv}

$$P \oplus C = P \oplus P \oplus K_{iv} = K_{iv}$$

- Algunos vectores de inicialización son peligrosos ya que permiten saber algunos bytes de la clave WEP fácilmente.
- La comprobación de redundancia física usada en WEP como comprobador de integridad de valor es insegura debido a su linealidad, permite cambiar datos y actualizar el CRC sin saber la clave WEP.
- WEP NO DEBE SER USADO POR RAZONES DE SEGURIDAD.

Protocolo de integridad de clave temporal (TKIP)

Incluido como una opción por la wifi alliance en WPA y en el estándar IEEE 802.11i y correspondientes programas de certificación WPA2. Solo debe ser usado en dispositivos cuya tarjeta de red no soporta AES. TKIP depende de la presencia del mecanismo de 4-way handshake. Los datos son cifrados usando el algoritmo RC4 con una clave temporal de 128 bits como entrada. En cada STA, el TKIP sequence Counter (TSC) es incrementado en uno cada vez que cada tecto cifrado transmitido, de forma que los mensajes recibidos con TSC menor al anterior serán descartados, esto evita ataques de replay. Se incorpora un valor de comprobación de integridad más fuerte: "Michael" Message Integrity Code (MIC).

- Funciones hash no lineales usando clave de integridad temporal diferente a la clave de cifrado TK.
- Como contramedida, si ocurren 2 errores MIC en 1 minuto, se renuevan las claves temporales

TKIP para todos los STA conectados al AP.

- Vulnerable a ataques DoS
- Mejor que WEP, pero no mucho mejor.

AES-CTR con Protocolo CBC-MAC

WPA2 es una mejora de WPA implementando gran parte del estándar 802.11i, tiene una filosofía similar a TKIP:

- La clave temporal (TK) se obtiene durante el 4-way handshake y se renueva cada cierto tiempo.
- Número de paquetes (PN) de 48 bits, usados para el vector de inicialización y para prevenir ataques replay
- Si se llega al límite de la secuencia de PN, se renueva la TK.

La principal mejora consiste en el cambio de cifrado de RC4 a AES block Cipher y una integridad MIC también basada en AES (CBC-MAC MIC). WPA2 puede funcionar con WPA bajo el mismo SSID. Para hacer esto, los APs funcionan en WPA2 Mixed Mode, ofreciendo métodos de cifrado TKIP y CMP.

Vulnerabilidades en el 4-way Handshake

Los mensajes del 4-way hadnshake son emitidos en texto plano. Aun atacante puede obtener el Anonce Snonce, AA, y SPA simplemente escuchando.

- Si el atacante están dentro de la red y conoce el PMK, puede derivar el PTK negociado entre el AP y la víctima y, por lo tanto, descifrar cualquier mensaje que la víctima envíe o reciba.
- Si el atacante no tiene acceso a la red, puede tratar de realizar ataques offline de diccionario. Se pueden aplicar las siguientes contramedidas:
 - Con autenticación PSK, usar una secuencia aleatoria hexadecimal larga como contraseña
 - No usar el SSID por defecto, se recomienda cambiarlo para evitar tablas rainbow precomputadas que pueden ser usadas en la red wifi.
- Con WPA2-Enterprise, el PMK es comigurado de forma segura por el servidor AAA, dificultando los ataques de fuerza bruta.
 - Un ataque MitM suplantando el AP y el server AAA puede llevar al robo de credenciales si el suplicante está mal configurado.

Si el atacante no llegó a tiempo, puede provvocar una deautenticación para forzar a la STA a repetir la asociación y completar un nuevo 4-way handshake.

Otros problemas pueden ser ataques:

- KRACK (Key Reinstallation Attack): un ataque de replay durante el 4-way handshake para reinstalar una clave ya en uso usando un ataque MitM Evil Twin. lo que afecta tanto a WPA-personal como a WPA-Enterprise, aunque algunos parches de software pueden solucionar el problema.
- PMKID attack: efectivo con WPA-PSK, capturar uno de los mensajes del 4-way handshake es suficiente si contiene el valor PMKID en el elemento RSN IE enviado por el AP en los mensajes clave EAPOL.

Wireless Protected Setup (WPS)

WPS se encarga de la experiencia de usuario de la configuración wifi automatizada, tiene 3 entradas lógicas:

- Registrar: entidad con la autoridad para emitir o revocar credenciales de dominio, puede ser implementado en el AP si es internal o en un dispositivo externo si es external.
- Enrollee: Dispositivo que quiere unirse al dominio WLAN.
- AP

Wireless Protected Setup tiene varias vulnerabilidades:

- PBC (Push Button Configuration), NFC o Código QR
- PIN: Contraseña de dispositivo obtenida por el Enrollee que debe ser introducida en el Registrar para autenticar mutuamente ambos extremos antes de transmitir la configuración wifi
- Se recomienda NO usar WPS con PIN

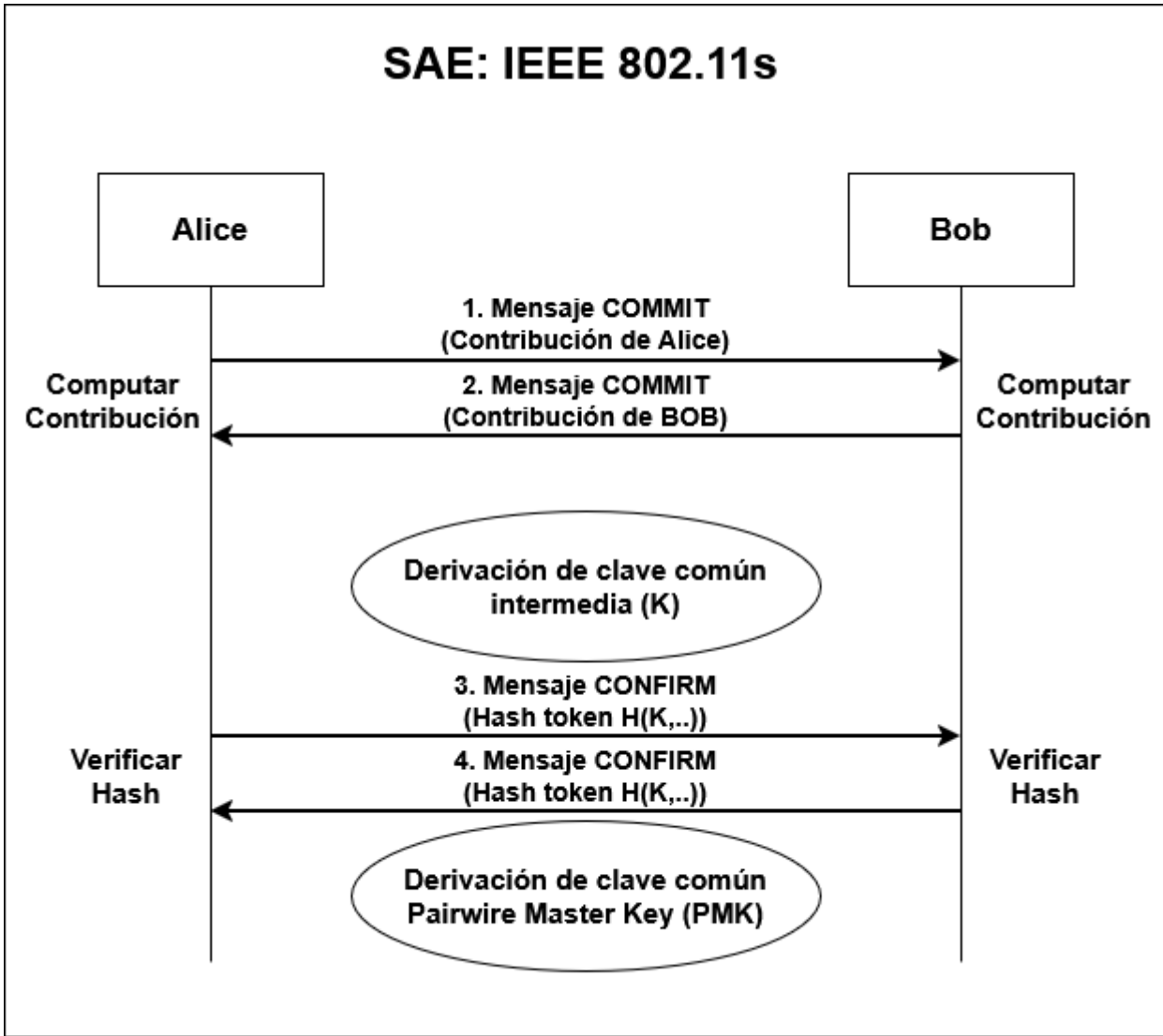
Robust Management Frames

Introducidos en el IEEE 802.11W. Antes de establecimiento PTK, los marcos de control necesitaban comenzar la asociación de red no podían estar ni cifrados ni con protección de integridad, por lo que un atacante podía fácilmente falsificarlos. Los marcos especialmente importantes son "Deauthentication" y "Disassociation" ya que podrían ser falsificados para implementar ataques DoS o forzar a la víctima a volver a hacer el 4-way handshake. Con Robust Management Frames, dichos marcos están cifrados y con protección de integridad con cada Clave temporal (TK) que cada STA negoció con el AP en el momento de la conexión, por lo que no pueden ser fácilmente falsificados. La nueva Integrity Group Temporal Key (IGTK) es establecida durante el 4-way handshake para proteger la integridad de algunas emisiones broadcast y multicast del AP.

WPA3

El PMF (Protected Management Frames) es obligatorio. En vez de PSK se usa SAE (Simultaneous Authentication of Equals) para WPA-Personal.

- Autenticación SAE en vez de Open Authentication en la primera fase de la conexión de una STA
- PMK diferente para cada asociación entre AP y STA, establecido con privacidad.
- Resistencia a ataques de diccionario online.
- La contraseña inicial no se usa para derivar las claves.
- Modo de transición WPA3-SAE



Sae usa el protocolo DragonFly:

```


$$\begin{array}{|c|c|} \hline \textbf{Alice} & \textbf{Bob} \\ \hline \begin{array}{l} \text{Computar} \\ \text{Contribución} \end{array} & \begin{array}{l} \text{Computar} \\ \text{Contribución} \end{array} \\ \hline \begin{array}{l} \text{Verificar} \\ \text{Hash} \end{array} & \begin{array}{l} \text{Verificar} \\ \text{Hash} \end{array} \\ \hline \end{array}$$


$$\begin{array}{l}
 1. \ r_A, m_A \in \{1, \dots, q\} \quad 2. \ s_A = r_A + m_A \quad 3. \ E_A = P^{-m_A} \\
 \begin{array}{l} P \in Q \\ 1. \ r_B, m_B \in \{1, \dots, q\} \quad 2. \ s_B = r_B + m_B \quad 3. \ E_B = P^{-m_B} \end{array} \\
 s_A, E_A \rightarrow \quad \leftarrow s_B, E_B \\
 5. \ ss = (P^{s_B} E_B)^{r_A} \quad \text{Verify } B \\
 \begin{array}{l} A = H(ss \mid E_A \mid s_A \mid E_B \mid s_B) \\ \text{Verify } A \\ ss = (P^{s_A} E_A)^{r_B} \quad \text{Verify } A \\ B = H(ss \mid E_B \mid s_B \mid E_A \mid s_A) \end{array} \\
 \hline K = H(ss \mid E_{AE_B} \mid (s_A + s_B) \bmod q) \quad \hline \end{array}$$


```

WPA3 también incorpora OWE (Opportunistic Wireless Encryption), similar a Open Networks, pero con cifrado. En WPA-Enterprise, para el cifrado de autenticación se usa Galois/counter Mode Protocolo de 256 bits (AES-GCMP-256). Para sustituir WPS se hace uso de DPP (Wi-Fi Device Provisioning Protocol), que es más simple y permite una configuración segura para dispositivos sin pantalla.

Técnicas de ataque en VLANS

Ataques de control de acceso

- War Driving: Descubrimiento de VLANS escuchando a los beacons o enviado probe request, provegendo puntos de lanzamiento para ataques. (Airmon-ng, DStumbler, KisMAC, MacStumbler, NetStumbler, Wellenreiter, WiFiFoFum)
- Rogue Access Point: Instalación de un AP no seguro dentro de un firewall, creando una backdoor a una red de confianza.
- Ad Hoc Associations: Conexión directa a una estación no securizada, circunvalando la seguridad de un AP.
- Mac Spoofing: Reconfiguración de la MAC del atacante para suplantar a un AP o Estación autorizados. (MacChanger, SirMacsAlot, SMAC, Wellenreiter, wicontrol)
- 802.1X RADIUS cracking: Recuperación de la clave RADIUS por fuerza bruta usando la solicitud de acceso 802.1X para uso con un AP Evil Twin.

Ataques de confidencialidad

- Eavesdropping: Captura y decodificación de tráfico de aplicaciones para obtener información potencialmente sensible. (bsd-airtools, Ettercap, Kismet, Wireshark...)
- WEP key Cracking: Captura de datos para recuperar la clave WEP usando métodos activos o pasivos. (Aircrack-ng, Airoway, Airsnort, chopchop, dwepcrack, WepAttack, WepDecrypt, WepLab, Wesside)
- Evil Twin AP: Enmascarandose como un AP autorizado para engañar a los usuarios. (cquireAP, D-Ling G200, HermesAP, Rogue Squadron, WifiBSD)
- AP Phising: Se corre un portal captivo o web falsa en un AP evil Twin para pescar credenciales y datos de los usuarios. (AirPWN, Airsnaf, Hotspotter, karma, RGlueAP).
- Man in the Middle: Se usan herramientas MitM para interceptar sesiones TCP o túneles SSL/SSH. (dsniff, Ettercap-GN, sshmitm)

Ataques de integridad

- 802.11 Frame injection: Creación y envío de marcos 802.11 falsificados. (Airpwn, File2air, libradiate, void11, WEPWedgie, wnet dinject/reinject)
- 802.11 Data Replay: Captura de marcos de datos 802.11 para posterior replay modificado
- 802.1x EAP Replay: Captura de EAP 802.1X
- 802.1X RADIUS Replay: Captura de mensajes Access-accept o Reject de RADIUS para posterior replay.

Ataques de autenticación

- Shared Key Guessing: Intento de autenticación con clave compartida 802.11 adivinando, con clave por defecto o con contraseñas WEP crackeada.
- PSK Cracking: Recuperación de un PSK WPA/WPA2 de un marco clave de handshake usando un ataque de diccionario. (coWPAtty, genpmk, kisMAC, wpa_crack)
- Application Login Theft: Captura de credenciales de usuario desde protocolos de aplicación en texto plano (Ace Password Sniffer, Dsniff, PHoss, WinSniffer)

- Domain Login Cracking: Recuperación de credenciales de usuario crackeando hases de contraseñas de NetBIOS usando ataques de fuerza bruta o diccionario. (Jonh the Ripper, L0pthCrack, Cain)
- VPN Login Cracking: Recuperación de credenciales de usuario mediante el uso de ataques de fuerza bruta contra el protocolo de autenticación VPN. (Ike_scan e ike_crack para IPSec y anger y THC-pptp-bruter para PPTP)
- 802.1X Identity theft: Captura de identidades de usuario desde el texto plano de los paquetes de respuesta de identidad de 802.1X
- 802.1X Password Guessing: Usando una identidad capturada, tratar de tantear la contraseña del usuario
- 802.1X LEAP Cracking: Recuperación de credenciales de usuario de paquetes Lightweight EAP 802.1X usando ataques de diccionario para crackear la el hash de la contraseña NT. (Anwrap, Asleep, THC-LEAPcracker)
- 802.1X EAP Downgrade: Se fuerza un servidor 802.1X a ofrecer un tipo de autenticación más debil usando paquetes EAP-Response/NAK falsificados (File2air, libradiate)

Ataques de disponibilidad

- AP-theft: Eliminar físicamente el AP del espacio público
- Queensland DoS: Explotación del Mecanismo CCSMA/CA Clear Channel Assesment (CCA) para hacer que el canal parezca ocupado.
- 802.11 Beacon Flood: Generación de cientos de beacons falsos para dificultar a las Stations la localización de un AP legítimo (FakeAP)
- 802.11 Associate / authenticate Flood: Envío de mensajes Authenticate o Associates falsos de MACs aleatorias para llenar la tabla de asociación del AP (FATA-Jack, Macfld)
- 802.11 TKIP MIC Exploit: Generación de datos TKIP inválidos para superar el límite de errores MIC del AP, provocando una suspensión del servicio WLAN (File2air, wnet dinject, LORCON)
- 802.11 deauthenticate flood: Inundación de las estaciones con mensajes Deauthenticates o Disassociates para desconectar usuarios del AP (AirePlay, Airforge, MDK, void11, Commercial WIPS)
- 802.1X EAP-Start Flood: Inundación de un AP con mensajes EAP-Start para consumir recursos o crashear el objetivo (QAcafe, File2Air, libradiate)
- 802.1X EAP-Failure: Observación de un intercambio EAP válido para después enviar mensajes falsificados de EAP failure (QAcafe, File2Air, libradiate)
- 802.1X EAP-of-Death: Envío de mensajes identity response EAP malformados que provocan crasheos en los AP (QAcafe, File2Air, libradiate)
- 802.1X EAP Length Attacks: Envío de Mensajes EAP type-specific con campos length incorrectos para intentar crashear un AP o un server radius (QAcafe, File2Air, libradiate)

From:

<https://www.knoppia.net/> - **Knoppia**

Permanent link:

https://www.knoppia.net/doku.php?id=master_cs:secom:tm2_v2

Last update: **2026/05/27 18:06**

