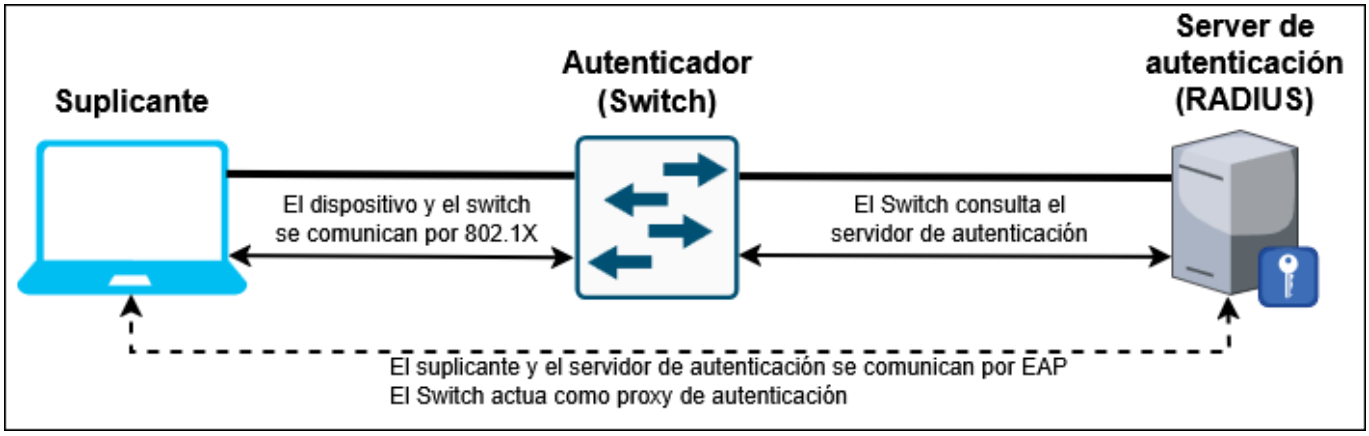
Seguridad a Nivel de Enlace

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:

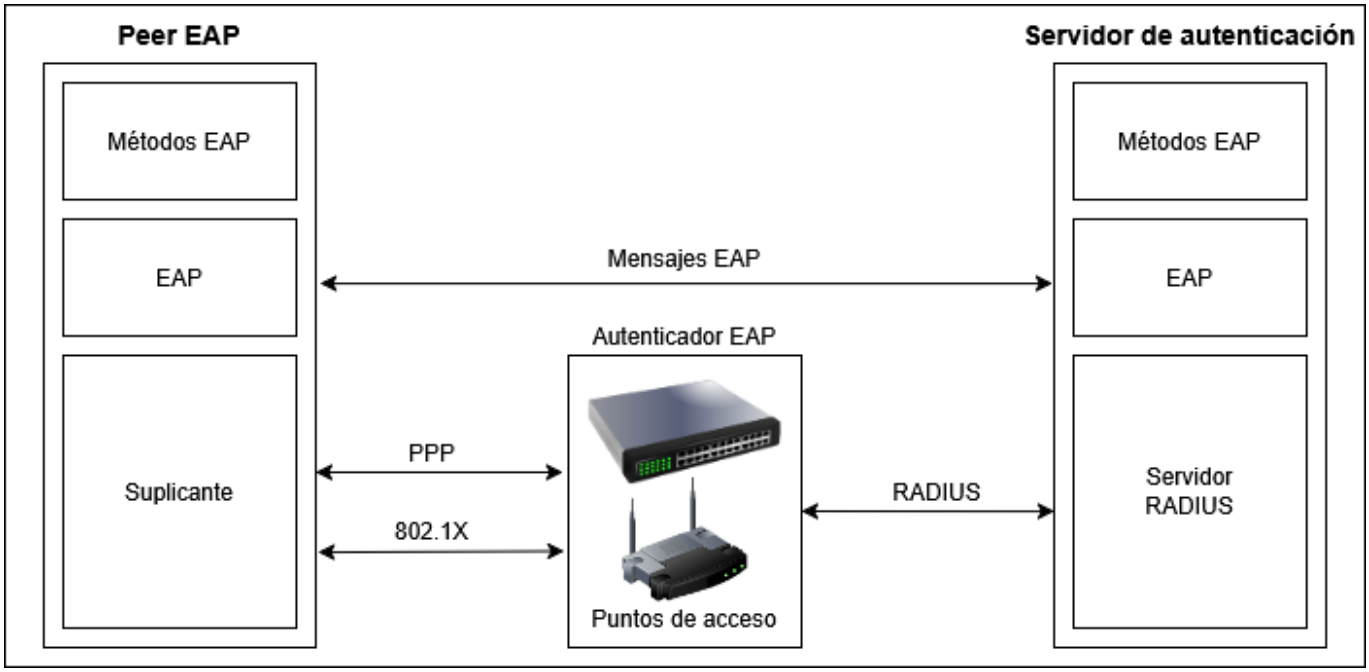
- Suplicante: Dispositivo cliente
- Autenticador: Switch o Punto de acceso
- Servidor de autenticación



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

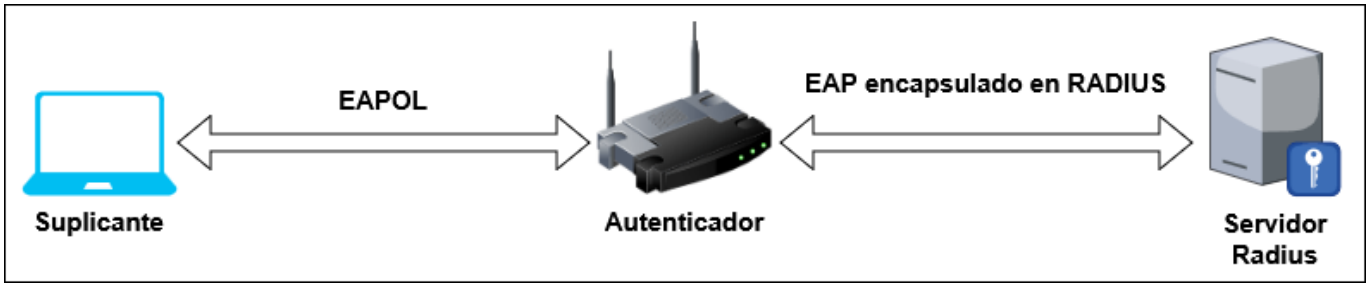
El campo “Tipo de autenticación EAP” esoecifica el mecanismo de autenticación elegido, el tipo de credenciales y como usarlas para realizar la autenticación mutua de forma segura. Hay tres tipos especiales de EAP:

- Identidad
- Notificación
- Nak

EAPOL y RADIUS

EAP normalmente funciona a nivel de enlace como Point-to-Point Protocol (PPP) o IEE802 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-Autenticator Atribute 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 respeustas del servidor de autenticación contienen un auntenticador, 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 métido EAP de autenticación genera mateial de clave (Master Session Key), el Pairwise Master Key (PMK) deruvadi 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, antaques de suplantación, Man in the middle…
- RADIUS recomienda usar un mecanismo de autenticación bidireccional y tencnología IPSEC para

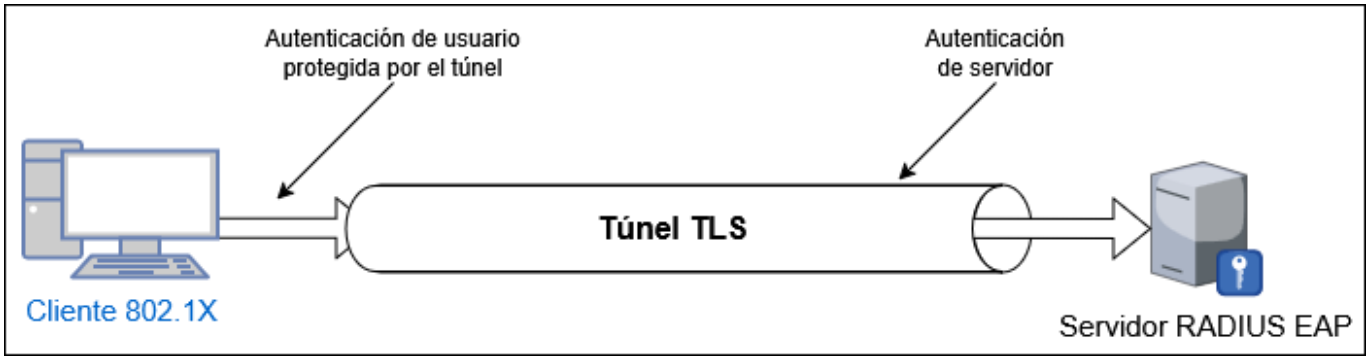
proteger la comunicación entre el NAS y el autenticador.

Mencanismos 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 antenticación del cliente se hace usando contraseñas compartidas. .
- PEAP (Protected EAP): Similasr 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 Asociation entre el EAP per y el Authenticator debe ser establecida con el Secure Association Protocol.

MACsec

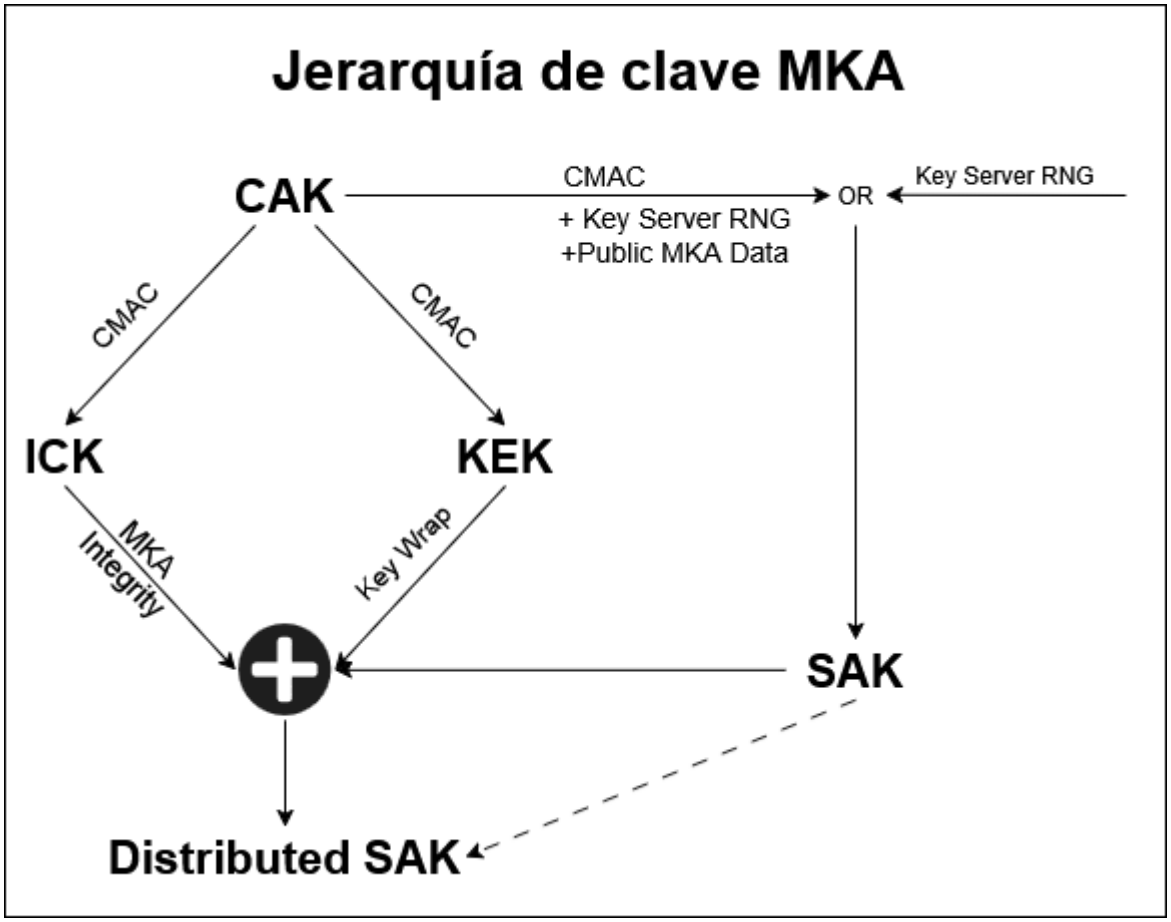
Es el cifrado de conexiones ethernet cableadas (IEEE 802.1AE). Cifrado en la capa MAC, cifrado a la velocidad del cable. MACsec garantiza lo siguiente:

- 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): Relacion de seguridad establecida y mantenida por protocolos clave de acuerdo (MKA), que compone un subset de puntos de awcceso a servicio completamente conectados en estaciones conectadas a una sola LAN.
    - Secure Connectivity Association Key (CAK): Clave secreta poseida por los miembros de la CA
    - Secure Connectivity Assiciation Key Name (CKN): Texto que identifica un CAK
    - CAK y CKN son derivados del material ram del keyring que el método EAP inyectó en el suplicante y auntenticador.
    - 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 peer finales estan configurados de forma estática.



- Mensaje de Codigo de autenticación con cibrado 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 tambien cosidera 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 demorras 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 ecifrado 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. Infraestructure 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 mobilidad, funciones de autenticación…)
    1. Elementos de una infraestructure 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: Conexion 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 trafico 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 arquitecutra plana donde cada nodo inalámbiroc 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 los marcos de gestión no están ni cifrados ni tienen protección de integridad, cualquiera puede falsificarlos. Esto puede ser usado para implementear 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 ce 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 coenctado a la misma wifi en la que se encuentra la víctima, puede simplemente impersonar algunos servicios.
    - Si un atacante, sin credenciales de acceso, esta conectado via ethernet al sistema de distribución detrás del AP, puede usar varias técnicas antes mecionadas.
    - 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 Proteccted Access (WPA): Solución tempora 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 estandar IEEE 802.11i intruduce 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 Protcol. 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 primodial del cual las claves de cifrado se van a derivar.

Pre-RSNA

- Autenticación de la estación
    - Sistema abierto: No hay auntenticación, 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 auntenticación del dispositivo, solo proeba 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
    - Opcioional: 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 depués del diálogo entre el suplicante y el servidor de autenticación

Jeraría 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 usandos 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 estategia con solo una clave, la clave conocida y el vector de inicialziación deben ser combinados en origen y destino para generar una contraseña de un solo uso. El vector de inicalización debe viajar ent exto plano dentro del mensaje cifrado. Si el Vector de inicialización increse en 1 monotonamente, puede ser usado como un nomero de paquete contra un ataque de replay.

Cifrado WEP (Wired Equivalency Privacy)

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

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

- 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 redundacia física usada en WEP como comprovador de integridad de valor es insegura debido a su linealidad, permite cambiar datos y actualizar el CRC sin saber la calve WEP.
- WEP NO DEBE SER USADO POR RAZONES DE SEGURIDAD.

Protocolo de integridad de clave temporal