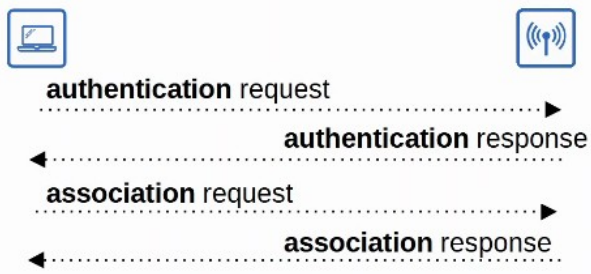
Cours 57 : Sécurité Sans Fil

Dans cette vidéo nous verrons la sécurité sans fil.
Nous verrons de nouveaux concepts en sécurité informatique en donnant d'abord une introduction à la sécurité dans le réseau sans fil puis des différentes méthodes d'authentification.
Nous verrons aussi les différentes méthodes de cryptage et de l'intégrité des données puis nous verrons le fonctionnement de WPA (Wifi Protected Access).

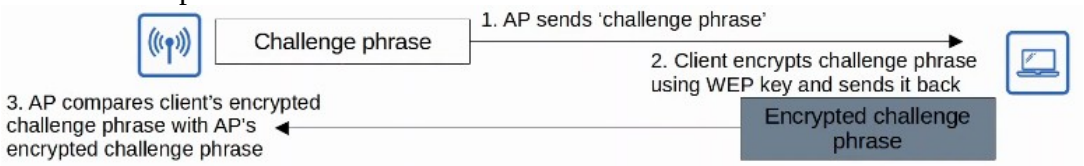
La sécurité est importante dans tous les réseaux et même encore plus essentiel dans les réseaux sans fil. La raison principale est que les signaux sans fil ne sont pas contenu dans des câbles, n'importe quelle appareil avec une certaine plage de signal peut recevoir ce trafique.
Dans des réseaux câblés, le trafique est souvent seulement crypté lorsqu'il est envoyé à travers un réseau qui n'est pas de confiance comme Internet. Dans les réseaux sans fil il est très important de crypté le trafique envoyé entre des appareils clients sans fil et un point d'accès car n'importe quelle appareil peut le réceptionner.
Nous verrons 3 concepts pour mieux comprendre cela :
- Authentification : Tous les clients doivent être authentifiés avant d'être associé avec le point d'accès. Dans un paramétrage d'entreprise, seulement les appareils et utilisateurs doivent aveoir accès au réseau. Un SSID séparé qui n'a pas accès au réseau de l'entreprise peut aussi être mis en place pour les invités. Ces invités ont moins de restrictions d'accès et ont un accès uniquement à Internet et non pas aux ressources internes de l'entreprise. De manière idéal les clients devraient aussi authentifier le point d'accès afin d'éviter de s'associer avec un point d'accès frauduleux.
Il y a plusieurs manière pour s'authentifier : Mot de passe, NomUtilisateur/MotDePasse, Certificats.
L'authentification se fais comme suit :



- Cryptage : Le trafique envoyé par les clients et les points d'accès doivent être cryptés afin qu'il ne soit pas lu par quelqu'un d'autre à l'exception du point d'accès du client.
Il y a plusieurs protocoles qui peuvent être utilisé afin de crypter le trafique.
Tous les appareils sur le WLAN utiliseront le même protocole, seulement chaque client utilisera une clé unique de cryptage/décryptage donc les autres appareils ne pourront pas lire son trafique.
Un « groupe de clé » est utilisé par le point d'accès pour crypter le trafique qu'il veut pour l'envoyer à tous ses clients. Tous les clients associés avec le point d'accès garderont cette clé donc ils pourront décrypter le trafique.
- Intégrité : Comme expliqué auparavant, l'intégrité s'assure que le message n'est pas modifié par un tiers partie. Le message qui est envoyé par l'hôte source devrait être le même que le message reçu par l'hôte de destination. Un MIC (Message Integrity Check) est ajouté aux messages pour aider à protéger leurs intégrité.
L'envoyeur calcule le MIC pour le message et l'attache au message, puis il crypte et envoie la trame. Le récepteur reçoit le message et décrypte le message, le récepteur calcul indépendamment un MIC pour le message (en utilisant le même protocole que l'envoyeur).
Si les deux MIC sont les mêmes le récepteur en déduit que le message n'a pas été altéré.

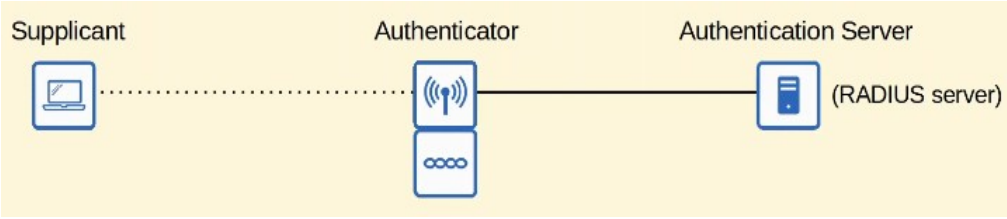
Voyons à présent différentes méthodes d'authentifications qui sont :
- Open Authentification
- WEP (Wired Equivalent Privacy)
- EAP (Extensible Authentication Protocol)
- LEAP (Lightweight EAP)
- EAP-FAST (EAP Flexible Authentication via Secure Tunneling)
- PEAP (Protected EAP)
- EAP-TLS (EAP Transport Layer Security)

Voyons chacune de ces méthodes plus en détail.
Le standard original 802.11 inclus deux options pour l'authentification :
- Open Authentication : Le client envoie une requête d'authentification et le point d'accès l'accepte. Sans questions. Il ne s'agit pas d'une méthode d'authentification sécurisé. Après que le client est authentifié et associé avec le point d'accès, il est possible que cela requière pour l'utilisateur de s'authentifier par une autre méthode avant que l'accès au réseau soit autorisé. (Par exemple un point d'accès Wifi).
- WEP (Wired Equivalent Privacy) : WEP est utilisé pour fournir les deux authentifications et cryptage du trafique sans fil. Pour le cryptage, WEP utilise l'algorithme RC4.
WEP est un protocol « clef partagé », qui requière à l'envoyeur et récepteur d'avoir la même clef. Ces clefs WEP peuvent être de 40bits ou 104bits de longueur. Les clefs peuvent être combinés avec un 24-bit 'IV' (Initialization Vector) pour apporter la longueur totale de 64 bits ou 128 bits.
Le cryptage WEP n'est pas sécurisé et peut être facilement cracké.
WEP peut être utilisé pour une authentification comme suit :



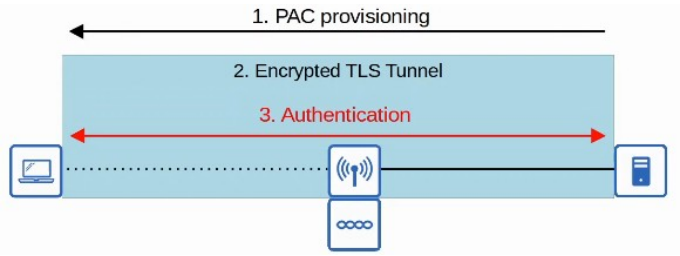
Le point d'accès envoie une phrase challenge. Le client crypte la phrase challenge en utilisant une clef WEP et la renvoie. Le point d'accès compare les phrase cryptés avec sa phrase crypté challenge. Si elles correspondent cela signifie que les deux appareils utilisent la même clef donc l'authentification fonctionne.

- EAP (Extensible Authentication Protocol) : EAP est un cadre dans l'authentification. Il définit un standard placé de fonctions d'authentifications qui sont utilisés par des méthodes EAP variés.
Nous verrons ces 4 méthodes EAP : LEAP, EAP-FAST, PEAP et EAP-TLS.
EAP est intégré avec 802.1X qui fournit un contrôle du réseau basé sur le s ports.
802.1x est utilisé pour limiter l'accès aux clients connectés à un LAN ou un WLAN jusqu'à se qu'il s'authentifient. Il y a 3 principale entités dans 802.1X :
1. Le demandeur est l'appareil qui veut se connecter au réseau.
2. L'authenticator est l'appareil qui fournit l'accès au réseau.
3. L'authenticator Server (AS) est l'appareil qui reçoit les informations d'identification et permet ou bloque l'accès.

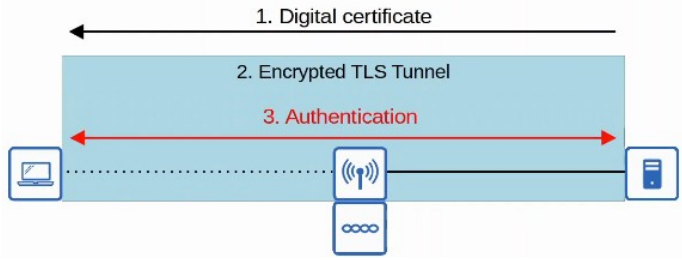


Voyons différentes méthodes d'authentifications EAP utilisés dans des LAN sans fil.
- LEAP (Lightweight EAP) : a été développé par Cisco pour une amélioration de WEP.
Les clients doivent fournir un nom d'utilisateur et un mot de passe pour s'authentifier.
En addition, une authentification mutuel est fournit par le client et le serveur qui envoie une phrase challenge entre chacun tout comme WEP.
Pour améliorer la sécurité des clefs Dynamic WEP sont utilisés, signifiant que les clés sont changés fréquemment. Tout comme WEP, LEAP est considéré comme vulnérable et ne devrait plus être utilisé.

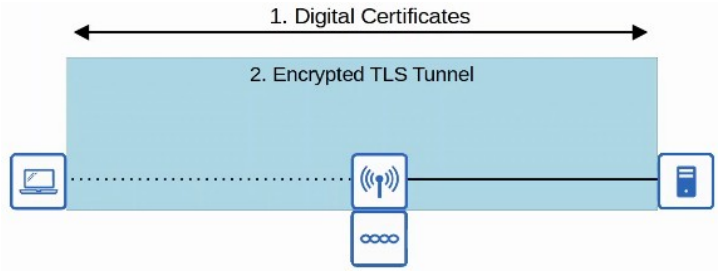
- EAP FAST (EAP Flexible Authentication via Secure Tunneling) : EAP FAST a aussi été conçu par Cisco. Cette méthode consiste en 3 phases :
1. Un PAC (Protected Access Credential) est généré et passé depuis le serveur vers le client.
2. un Tunnel sécurisé TLS est établi entre le client et le serveur d'authentification.
3. à l'intérieur du tunnel sécurisé (crypté), le client et le serveur communiquent pour authentifier/autoriser le client.



- PEAP (Protected EAP) : Tout comme EAP-FAST, PEAP implique d'établir un tunnel TLS sécurisé entre le client et le serveur. Au lieu d'utiliser PAC, le serveur a un certificat digital.
Il montre son certificat au client, le client utilise le certificat digital pour authentifier le serveur.
Puisque seulement le serveur fournit un certificat pour l'authentification, le client doit rester authentifié dans le tunnel sécurisé, par exemple en utilisant MS-CHAP (Microsoft Challenge-Handshake Authentication Protocol)



- EAP-TLS (EAP Transport Layer Security) : PEAP ne requière que le AS (Auithentification Serveur) pour avoir un certificat, EAP-TLS requière un certificat sur le AS et sur chacun des clients.
EAP-TLS est la méthode d'authentification sans fil la plus sécurisé, mais il est plus difficile de l'intégrer par rapport à PEAP car chaque appareil client a besoin d'un certificat.
Puisque le client et le serveur s'authentifient chacun avec un certificat digital il n'y a pas besoin pour authentifier le client dans un tunnel TLS.



Nous allons à présent voir les méthodes de cryptage et d'intégrité qui sont :
- TKIP (Temporal Key Integrity Protocol)
- CCMP (Counter/CBC-MAC Protocol)
- GCMP (Galois/Counter Mode Protocol)
Nous aurions pu ajouter WEP mais il a déjà été décrit auparavant.

Voyons chacune de ces méthodes plus en détail.
- TKIP (Temporal Key Integrity Protocol) : WEP a été trouvé trop vulnérable, mais le matériel sans fil de ce temps étaient conçus pour utiliser WEP. Une solution temporaire a été nécessaire jusqu'à ce qu'un nouveau standard soit crée et du nouveau matériel crée.
TKIP ajoute une grande variété de fonctionnalités de sécurité, par exemple :
Un MIC est ajouté pour protéger l'intégrité des messages. Un Algorithme de mélange des clef est utilisé pour créer une clef WEP unique pour toutes les trames.
Le vecteur d'initialisation est doublé en longueur de 24bits à 48bits, rendant l'attaque par brute force beaucoup plus difficile. Le MIC inclut l'adresse MAC de l'envoyeur pour identifier la trame de l'envoyeur. Un timestamp est ajouté au MIC pour éviter les attaques Replay (Attaque par réinsertion en Français). Les attaques Replay impliquent de ré-envoyer une trame qui a déjà été transmise. De plus une séquence de nombre TKIP est utilisé pour garder une trace de la trame envoyé depuis chaque adresse MAC source. Cela protège aussi contre les attaque Replay.

- CCMP (Counter/CBC-MAC Protocol) : CCMP a été développé après TKIP et est plus sécurisé. Il est utilisé dans WPA2. Pour utiliser CCMP il faut qu'il soit supporté par le matériel de l'appareil. De vieux matériaux construit uniquement pour utiliser WEP/TKIP ne peuvent pas utiliser CCMP.
CCMP consiste dans l'utilisation de deux différents algorithmes pour fournir le cryptage et MIC.
1. AES (Advanced Encryption Standard) counter mode encryption.
AES est le protocole de cryptage le plus sécurisé actuellement utilisé. Il est largement utilisé dans le monde. Il y a plusieurs modes pour l'opération de AES. CCMP utilise le « counter mode ».
2. CBC-MAC (Cipher Block Chaining Message Authentication Code) est utilisé comme MIC pour s'assurer de l'intégrité des messages.

- GCMP (Galoisμ/Counter Mode Protocol) : GCMP est plus sécurisé et efficace par rapport à CCMP. Il a augmenté son efficacité qui permet un haut transfert des données par rapport à CCMP. Il est utilisé dans WPA3. GCMP consiste lui en deux algorithmes :
1. Cryptage AES counter mode
2. GMAC (Galois Message Authentication Code) est utilisé comme MIC pour s'assurer de l'intégrité des messages.

Voyons le fonctionnement de WPA.
L'alliance Wi-Fi a développé 3 certifications WAP pour les appareils sans fil :
WPA, WPA2, WPA3

Pour être certifié WPA, l'équipement doit être testé dans le lab de test autorisé.
Toutes ces certifications supportent deux modes d'authentification :
- Mode Personnel : Un pre-shared key (PSK) ou clé pré-partagé est utilisé pour l'authentification. Lorsque l'on se connecte à un réseau de maison Wi-Fi, on entre le mot de passe et être authentifié, cela est le mode personnel. C'est le plus commun dans de petits réseaux. Le PSK n'est pas envoyé dans les airs. Un four-Way handshake est utilisé pour l'authentification, et le PSK est utilisé pour générer une clé de cryptage.
- Le mode Entreprise : 802.1X est utilisé avec un serveur d'authentification (Serveur RADIUS). Une méthode non spécifique EAP est spécifié, donc tous les autres méthodes d'authentifications sont supportés (PEAP, EAP-TLS, etc..)

La certification WPA a été développé après qu'il a été prouvé que WEP soit vulnérable et inclut les protocoles suivants :
- TKIP (Basé sur WEP) fournit le cryptage/MIC.
- authentification 802.1X (Mode Entreprise) ou PSK (Mode Personnel)

WPA2 a été publié en 2004 et inclut les protocoles suivant :
- CCMP qui fournit le cryptage/MIC
- authentification 802.1X (Mode Entreprise) ou PSK (Mode Personnel)

WPA3 a été publié en 2018 et inclut les protocoles suivant :
- GCMP fournit le cryptage/MIC
- authentification 802.1X (Mode Entreprise) ou PSK (Mode Personnel)
- WPA3 fournit aussi différentes fonctionnalités additionnel de sécurité comme par exemple :
- PMF (Protected Management Frames) qui protège la gestion des trames 802.11 de l'espionnage.
- SAE (Simultaneous Authentication of Equals) protège le four-way handshake lorsqu'il utilise le mode personnel d'authentification.
- Le partage de secret empêche les données d'être décryptés après avoir été transmises dans les airs. Donc un attaquant ne peut pas capturer la trame sans fil et donc essaie de les décrypter plus tard.