

Chapitre 4

Sécurité avancée

4-1

Version – 11/2017

Objectifs du chapitre

Dans ce chapitre, nous allons

- ➲ Configurer le filtrage par adresses MAC
- ➲ Analyser d'autres menaces sur la sécurité
- ➲ Voir des protocoles d'authentification et de chiffrement avancés : 802.1X, TKIP, CCMP, EAP et WPA
- ➲ Voir le mécanisme d'authentification EAP avec RADIUS
- ➲ Voir la faille récente de la norme WPA (octobre 2017)

4-2

Sécurité avancée



Authentification par adresses MAC

Autres menaces sur la sécurité

Authentification avancée

Chiffrement avancé

EAP et RADIUS

Menace sur WPA

Résumé du chapitre

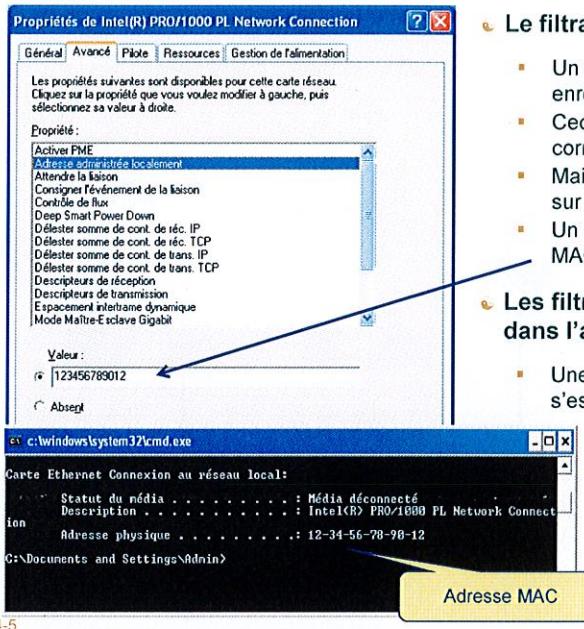
4-3

Contrôle d'accès avec les adresses MAC

- ◉ Chaque équipement sans-fil a une adresse MAC (Media Access Control) sur six octets
- ◉ Les points d'accès peuvent filtrer en fonction des adresses MAC des stations clientes
 - L'authentification par adresse MAC est un processus interne de l'AP
 - L'AP a une table interne d'adresses à autoriser ou interdire
- ◉ Un administrateur réseau peut enregistrer la liste des adresses MAC
 - Pour les équipements autorisés dans son entreprise
 - Il peut utiliser des serveurs RADIUS pour gérer la liste d'adresses MAC
- ◉ L'authentification par adresse MAC n'est pas un standard 802.11
 - L'implémentation peut varier d'un constructeur à l'autre
 - Certain bloque l'association, d'autre bloque simplement le trafic
 - On peut utiliser l'authentification Mac avec l'algorithme Open ou shared-key

4-4

Problèmes du filtrage MAC



Le filtrage s'applique au domaine sans fil

- Un équipement dont l'adresse MAC n'est pas enregistrée est bloqué
- Ceci suppose que la bonne adresse correspond à la bonne machine
- Mais un pirate peut dérober une carte légitime sur un portable de l'entreprise
- Un pirate expert peut sniffer des adresses MAC légitimes puis les réutiliser plus tard

Les filtres MAC peuvent aussi fonctionner dans l'autre sens

- Une carte volée ou celle d'un employé dont on s'est séparé peut être bloquée explicitement

Obtenir l'adresse MAC :

- Sous Windows, ipconfig /ALL
- Sous UNIX/Linux, utiliser ifconfig

Activer le filtrage MAC

Option MAC dans la configuration de votre AP

- EX : Onglets Advanced Security
- Définir "Deny all access" et "Permit only listed MAC addresses"

Selon BOX : entrer manuellement toutes les adresses MAC

- La taille de la liste varie d'un produit à l'autre

The image shows two screenshots of the Cisco Aironet 1200 Series Access Point configuration interface. The left screenshot shows the 'MAC ADDRESS AUTHENTICATION' page where 'Local List Only' is selected. The right screenshot shows the 'Wireless' tab's 'Access Restrictions' section, specifically the 'Wireless Client List' table. This table lists 40 MAC addresses, each with a status column indicating whether it is allowed or denied access. The table includes columns for MAC address, status, and a small icon representing the access level.

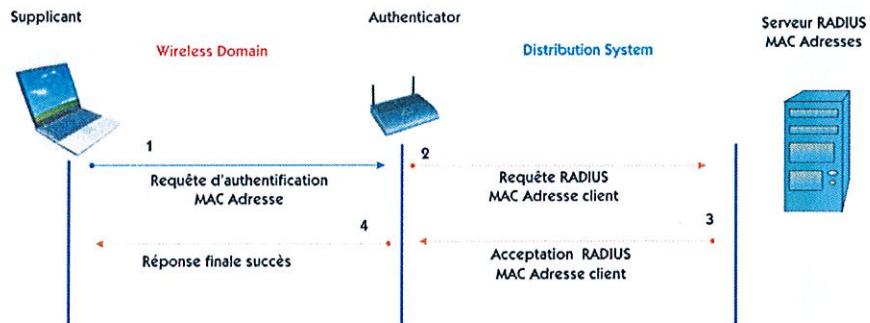
MAC Address	Status
MAC 01	Enabled
MAC 02	Enabled
MAC 03	Enabled
MAC 04	Enabled
MAC 05	Enabled
MAC 06	Enabled
MAC 07	Enabled
MAC 08	Enabled
MAC 09	Enabled
MAC 10	Enabled
MAC 11	Enabled
MAC 12	Enabled
MAC 13	Enabled
MAC 14	Enabled
MAC 15	Enabled
MAC 16	Enabled
MAC 17	Enabled
MAC 18	Enabled
MAC 19	Enabled
MAC 20	Enabled
MAC 21	Enabled
MAC 22	Enabled
MAC 23	Enabled
MAC 24	Enabled
MAC 25	Enabled
MAC 26	Enabled
MAC 27	Enabled
MAC 28	Enabled
MAC 29	Enabled
MAC 30	Enabled
MAC 31	Enabled
MAC 32	Enabled
MAC 33	Enabled
MAC 34	Enabled
MAC 35	Enabled
MAC 36	Enabled
MAC 37	Enabled
MAC 38	Enabled
MAC 39	Enabled
MAC 40	Enabled

4-6

Serveur d'adresses MAC

- Les produits d'entreprise prennent en charge une base de données d'adresses MAC via un serveur RADIUS

- EX : Cisco AiroNet



4-7

Sécurité avancée

Authentification par adresses MAC



Autres menaces sur la sécurité

Authentification avancée

Chiffrement avancé

EAP et RADIUS

Menace sur WPA

Résumé du chapitre

4-8

Autres menaces

- Les réseaux sans-fil ne sont pas seulement vulnérables aux écoutes
 - Ou aux accès dus aux faiblesses/attaques de la clé partagée WEP
- Il existe de nombreuses sortes de failles de sécurité
 - Équipements pirates
 - Attaques d'égal à égal
 - Changements de configuration
- Ainsi que les attaques DoS (Denial of Service)
 - Brouillage des fréquences radio
 - Inondation de données
 - Attaques de détournement : *Man-in-the-middle*

4-9

Points d'accès pirates

- Points d'accès pirates placés dans vos locaux
 - Par des employés mal intentionnés, des visiteurs ou des intrus professionnels
 - Permettent de se connecter au réseau câblé de l'extérieur de vos locaux
- Le pirate place l'AP comme si c'était son emplacement normal
 - Dans un coin, connecté au réseau câblé
 - Près du mur, pour lui permettre de sniffer de l'extérieur
 - Il utilise sa propre clé WEP/WPA pour éviter d'être intercepté par l'administrateur du réseau
 - Le SSID est défini pour correspondre à celui du WLAN existant, mais sur un canal différent
 - La diffusion du SSID est désactivée pour éviter que NetStumbler ne le détecte
- Ponts sans-fil placés dans la portée d'un réseau existant
 - Pour intercepter le trafic existant
 - Peut usurper l'adresse MAC d'un pont autorisé

4-10

Attaques d'égal à égal

- ❖ WEP/WPA ne sert à rien si tous les utilisateurs/invités connaissent la clé
- ❖ Un pirate peut facilement attaquer d'autres clients depuis un point Wi-Fi public (non configuré en hotspot)
 - Assis dans un coin confortable devant une bonne tasse de café !
 - Le pirate est *dans* le réseau !
- ❖ Un pirate peut utiliser des analyseurs de réseau sans-fil pour capturer des données
 - Intercepter mots de passe et données de tout le trafic Internet : FTP, POP, SMTP
 - Scanner les ports et exploiter les bogues de sécurité pour accéder aux PC et serveurs
- ❖ Si vous utilisez un point public ou si vous visitez un site, soyez vigilant, rien ne prouve que c'est bien un hotspot
 - Ne pas utiliser le client de courrier ordinaire avec POP
 - Utiliser un système Web-mail avec HTTPS pour récupérer le courrier
 - Ne pas utiliser FTP pour envoyer des fichiers — n'utiliser que le téléchargement anonyme
 - Utiliser des *sites de messagerie* qui ont des clients avec chiffrement ([https](https://)) ou utiliser un VPN

4-11

Changements de configuration

- ❖ Configurer un mot de passe d'administration solide, pas le mot de passe par défaut
 - Sinon, un pirate peut se connecter à l'AP et modifier sa configuration
 - Ex : ajouter des règles de pare-feu, ajouter des adresses MAC, lire des clés WEP
- ❖ L'accès à la page Web d'administration est souvent bloqué aux utilisateurs d'Internet
 - Mais les utilisateurs sans-fil peuvent toujours se connecter
- ❖ Interdire l'accès physique aux pirates ou aux employés non autorisés
 - AP et ponts montés à l'extérieur des bâtiments sont vulnérables
 - Ainsi que les zones communes dépourvues de sécurité physique
 - Les points d'accès ont un bouton Reset pour réinitialiser la configuration par défaut
 - Un pirate peut ressaisir le SSID et les paramètres de base, permettre l'administration via le Web
 - Il peut aussi se connecter au port console pour changer la configuration

4-12

Brouillage de la fréquence radio (*RF Jamming*)

- ◉ Un puissant signal RF peut arrêter un réseau sans-fil
 - Intentionnellement ou non
- ◉ Un pirate peut, intentionnellement, utiliser un générateur de signal RF très puissant
 - Une source mobile et une antenne directionnelle à l'extérieur de vos locaux
 - Relativement coûteux et donc pas très courant
- ◉ Les interférences involontaires sont courantes
 - Wi-Fi utilise les fréquences ISM (Instrumentation, Scientifique, Médical)
 - Téléphones sans-fil, baby-phones, fours micro-ondes
- ◉ Un point d'accès à proximité d'un autre sur le même canal
 - Les AP nouvellement installés, non configurés, utilisent souvent le canal 6
- ◉ Utiliser un analyseur de réseau sans-fil ou un analyseur de spectre RF
 - Triangulation et repérage de la source à l'aide d'une antenne directionnelle

4-13

Inondation de données

- ◉ On épouse le point d'accès avec trop de trafic
- ◉ Historiquement, les points d'accès saturent à moins de 5 Mbps
 - Un gros téléchargement pouvait facilement ralentir tout le monde
 - Les connexions DSL ascendantes, peu coûteuses, étaient plus lentes
 - Le débit d'une connexion DSL classique est inférieur à 1 ou 2 Mbps
 - Les entreprises peuvent avoir des connexions plus rapides, autorisant la saturation du WLAN
- ◉ Un générateur de paquets peut provoquer une inondation de données mal intentionnée
 - Même un simple "flood-ping" sous UNIX/Linux peut suffire
 - ping -f <ip du point d'accès>
- ◉ Atténuer l'effet de l'inondation en augmentant la bande passante disponible
 - Passer à un standard plus rapide : 802.11a ou 802.11g/n
 - Augmenter la vitesse de la connexion ascendante
- ◉ Identifier la source des attaques avec un analyseur de paquets
 - Les éliminer ou les bloquer : pare-feu ou outils de détection des intrusions

4-14

Attaques de détournement : Man-in-the-Middle

• Le pirate utilise un AP pirate pour détourner les clients

- En envoyant un signal plus fort que l'AP légitime
- D'une altitude plus élevée — au sommet d'un bâtiment
- Il peut augmenter la force du signal avec des amplificateurs ou une antenne à gain élevé
- Les deux AP doivent avoir le même SSID et la même clé WEP

• Le pirate génère une rafale d'interférences sur toutes les bandes ou des trames de déconnection en ciblant un client

- Les clients perdent le signal/la connexion et tentent de s'associer de nouveau

• Les clients s'associent à l'AP pirate

- Le pirate peut intercepter les données sensibles

• La connexion ascendante peut être établie vers le réseau légitime

- L'AP pirate est "l'homme au milieu", entre les clients et l'AP légitime

• Décourager ces attaques en renforçant la sécurité

- Filtrage par adresses MAC, authentification et chiffrement avancés

4-15

Sécurité avancée

Authentification par adresses MAC

Autres menaces sur la sécurité



Authentification avancée

Chiffrement avancé

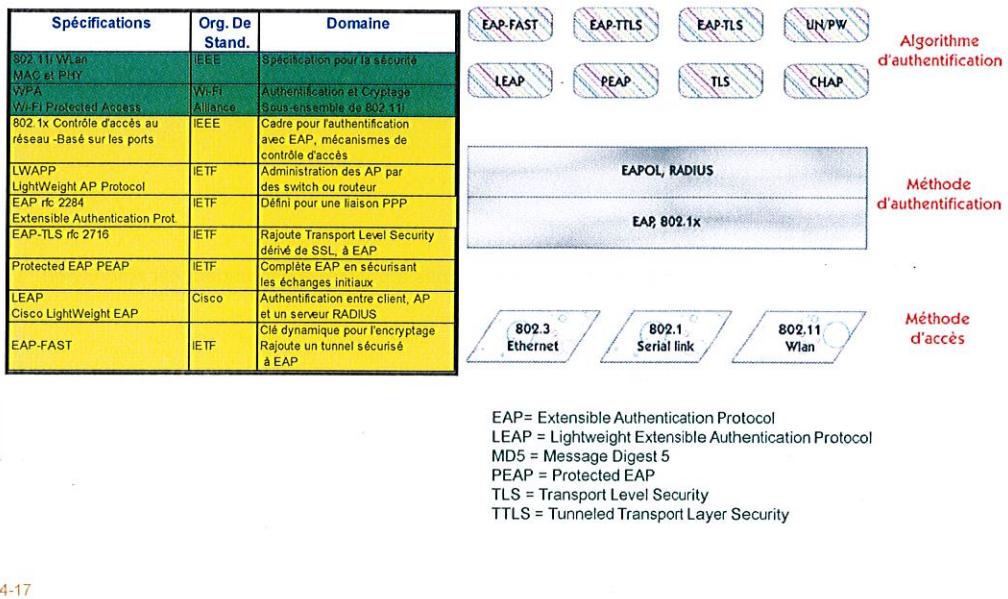
EAP et RADIUS

Menace sur WPA

Résumé du chapitre

4-16

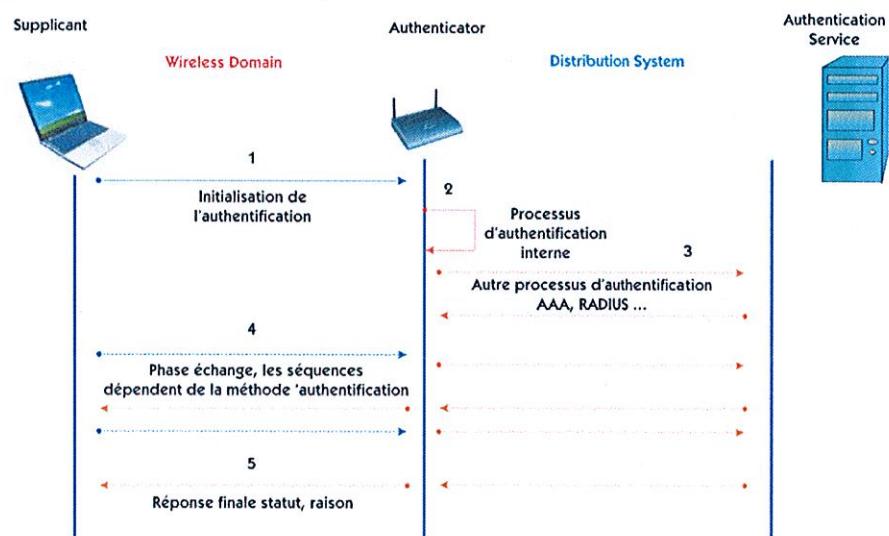
Les couches des protocoles d'authentification



4-17

Principe de l'authentification

Les éléments d'un modèle tri-partie



4-18

Le modèle tri-partie

• Supplicant

- Celui qui demande l'accès :
 - Identité et preuve que c'est bien lui
 - Connecté au réseau par l'intermédiaire du port de l'authentificateur dont l'accès est contrôlé
 - Notion de port qui permet le contrôle d'accès
 - Appelé *peer* dans les RFC de l'IETF

• Authenticator

- L'authentificateur : le point d'accès Wi-Fi, ne sait pas à priori si le demandeur est autorisé ou non
- Appelé *Network Access Server (NAS)* par l'IETF

• Le serveur d'authentification

- Choisit le protocole d'authentification
- Vérifie et accorde ou refuse la permission d'accéder au réseau et services
- AAA, RADIUS, TACACS+, ...

4-19

EAP (Extensible Authentication Protocol)

• EAP est un protocole flexible utilisé pour transporter des informations d'authentification

- RFC 2284 mis à jour par le RFC 3579
- Identifie l'utilisateur
- Les messages EAP fournissent la méthode d'authentification
- Le point d'accès bloque tout le trafic provenant du client sauf les paquets EAP jusqu'à ce que EAP réussisse

• Deux caractéristiques majeures

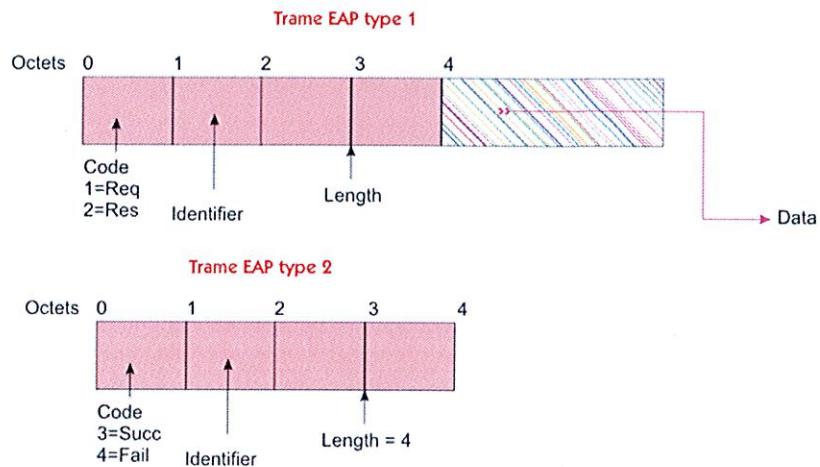
- Séparation des échanges de messages et du processus d'authentification proprement dit.
- D'où une extensibilité facilité, on peut modifier le processus d'authentification par des extensions sans affecter la couche EAP.

• Bases d'EAP

- 4 types de messages : request, response, failure, et success
- 2 formats de trame de message : request/response et success/failure
- Une chorégraphie extensible
- EAP définit également un paquet pour négocier la configuration du protocole EAP (C227)

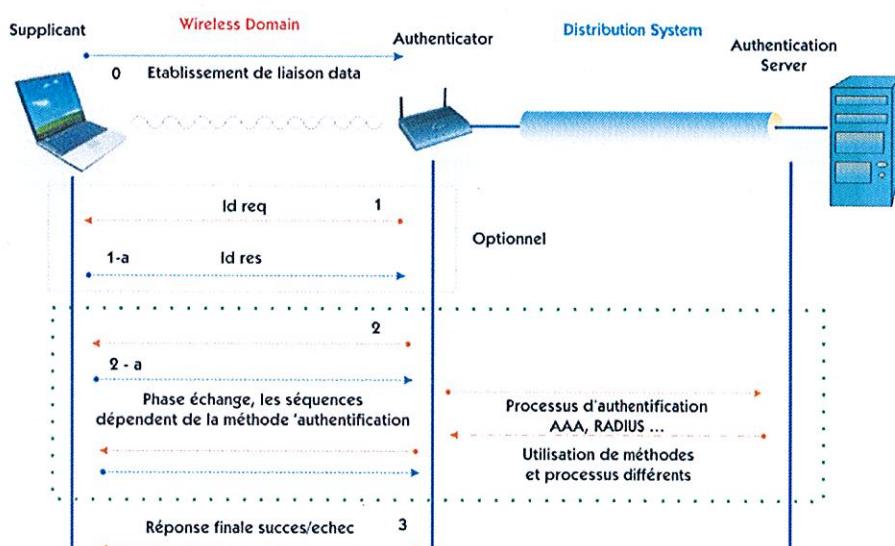
4-20

EAP – Format de trames



4-21

Échange EAP



4-22

Mécanismes d'authentification EAP

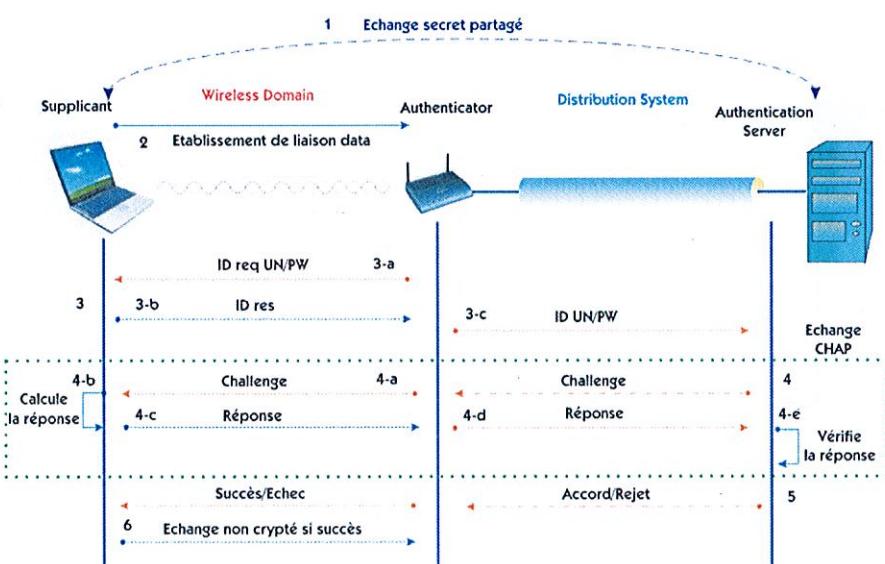
• EAP fournit la trame générale pour les mécanismes d'authentification

• Les différents mécanismes utilisant EAP over Lan (EAPoL) sont

- EAP-MD5
- EAP-OTP (One Time Password)
- EAP-TLS
- EAP-TTLS
- EAP-GTC (Generic Token Card)
- EAP-MSCHAPv2 (Microsoft CHAP)
- PEAP
- LEAP
- EAP-FAST

4-23

EAP-MD5



4-24

EAP-MD5

• EAP-MD5 - premier schéma d'authentification EAP

- C'est un protocole CHAP – Challenge Handshake Authentication Protocol – RFC 1994
- Le client et le serveur partagent une clé secrète – habituellement un couple UserName/Password - Ceci doit se faire en Out-of-band.
- Principe d'envoi d'un challenge au client, réponse du client en cryptant le challenge avec la clé commune, le serveur vérifie la réponse et accepte ou rejette l'authentification
- EAP-MD5 est un pur protocole d'authentification
 - Après l'authentification les messages sont transmis en clair.
 - C'est également une authentification du client uniquement.
 - L'authentificateur n'est pas contrôlé – on ne peut pas détecter les AP pirates.
 - C'est un processus assez léger, ne demande pas de hardware performant, pas d'infrastructure de distribution de certificat et de clé.
 - Assez vulnérable aux attaques par dictionnaire ou force brute.

• EAP-OTP (One Time Password)

- Similaire à MD5, mais utilise une passphrase pour générer la clé secrète de chiffrement
- Le changement de passphrase peuvent se faire en clair, un algorithme va générer la clé.
- Pour contrer les attaques par replay.

• EAP-GTC (Generic Token Card)

- 4-25
- Similaire à OTP, avec une carte hardware qui génère le flux pour chiffrer la réponse

Introduction à TLS (Transport Layer Security)

• RFC 2246 – TLS 1.0

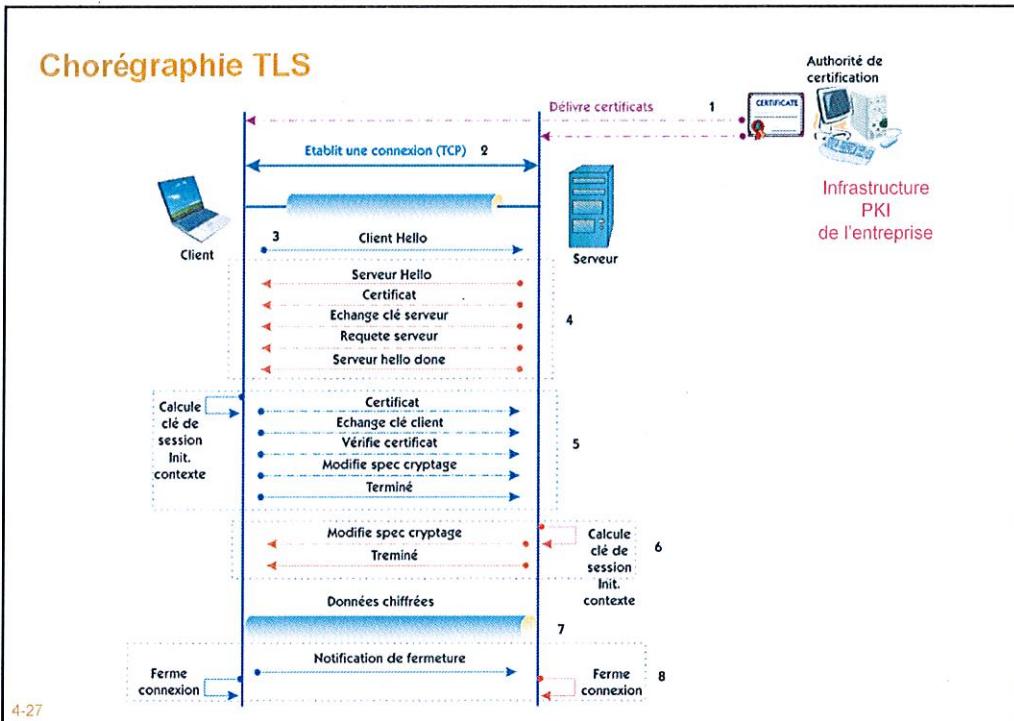
- À l'origine, destiné à des liaisons PPP, protocole SSLv1, complétée et remplacée par SSL 2.0
- Jusqu'en 2015 et 2016, version SSL 3.0 courante (créé en 1996), mais désormais obsolète.
- Aujourd'hui TLS 1.2 est nécessaire (1.3 en draft) – Paypal le rend obligatoire en juin 2017.

• Principe TLS

- Connexion et session
- La connexion est un canal créé pour la communication
- La session est gérée par un contexte de sécurité.
 - Identification de la session
 - Certificat du client
 - Méthode de compression
 - Méthode de chiffrement pour la clé de la session
 - Paramètres de l'algorithme MAC et la clé secrète maîtresse.
- TLS négociera en toute sécurité différents paramètres de session tout en maintenant la même connexion (TCP en général).
- La phase handshake établit une session. Les données pendant la phase de transfert sont cryptées par les clés de la session.
- TLS fournit également un contrôle d'intégrité.

- 4-26

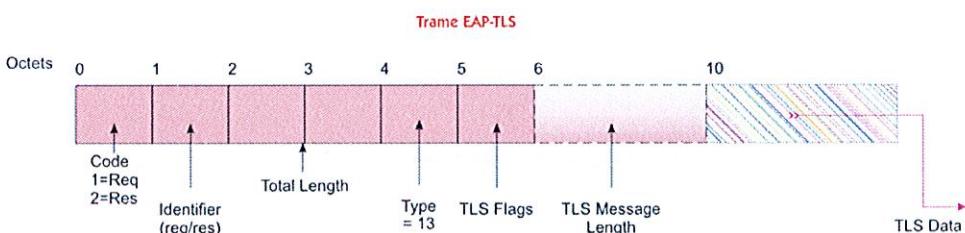
Chorégraphie TLS



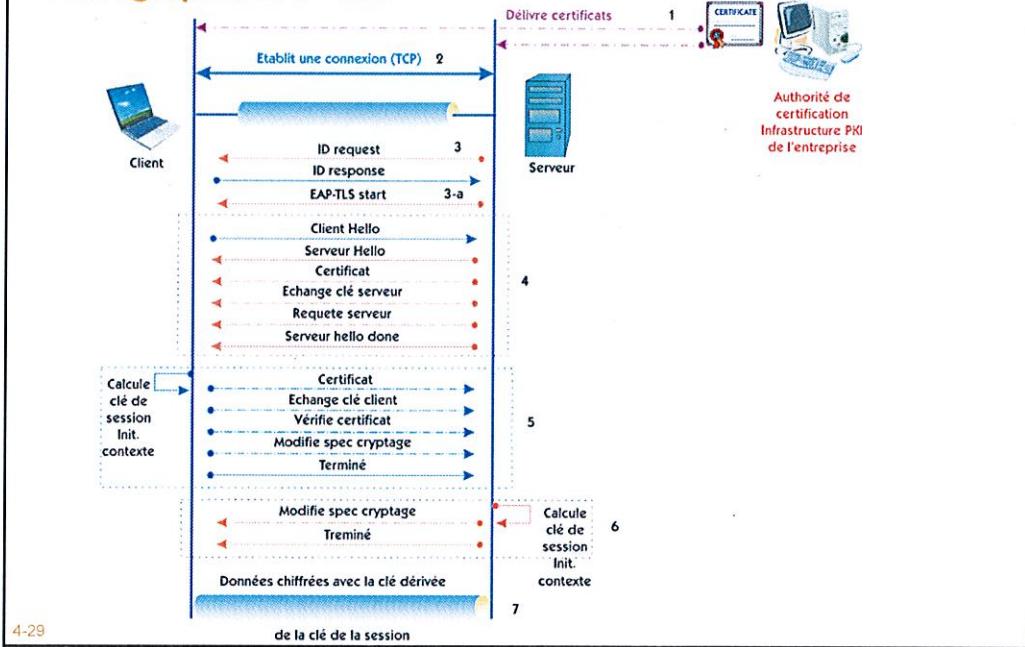
EAP-TLS

EAP-TLS (Transport Layer Security)

- Par rapport aux EAP précédents, rajoute plus de capacités comme l'authentification mutuelle
- Fournit une couche transport cryptée
- Offre la possibilité de changer de clés
- EAP-TLS est basé sur une infrastructure de certification gérant certificats et clés
- EAP-TLS utilise une partie de TLS.



Chorégraphie EAP-TLS



EAP-TTLS

• EAP-Tunneled Transport Layer Security

- Extension d'EAP-TLS. L'authentification du client est étendue, après l'établissement du tunnel sécurisé pour le transport.
- L'authentification du client peut se faire par l'une des méthodes connues comme UN/PW, CHAP, MSCHAPv2. Ceci est encore appelé « authentification tunnélisée ».

• Version sécurisée et facile à gérer

- Ne nécessite de certificat que sur le serveur d'authentification
- Pas besoin de certificat client
 - Pas besoin de PKI
 - Beaucoup plus facile à déployer

PEAP

• PEAP (Protected EAP)

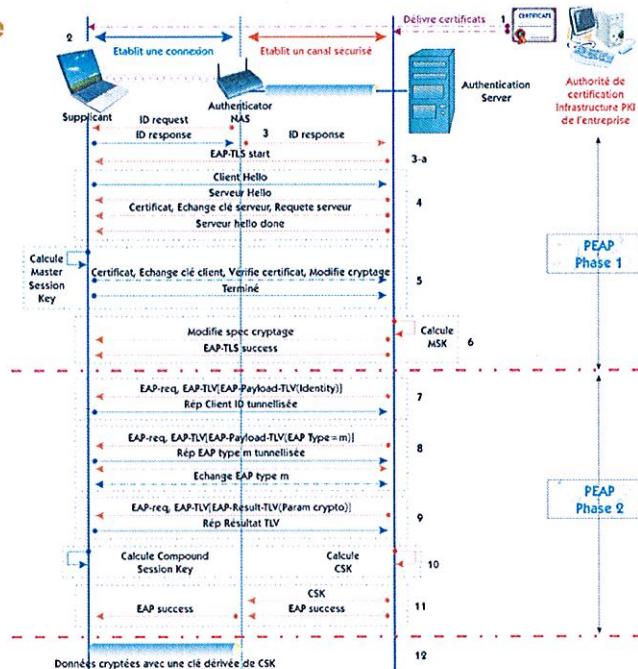
- De plusieurs manières, PEAP est considéré actuellement comme l'équivalent EAP-TLS pour le domaine sans fil.
- Draft de l'IETF, s'appuyant sur les drafts EAP génériques et le RFC 3579.
- L'une des faiblesses des différents EAP, est que les premières phases d'échange dans le domaine sans fil se font en clair (identités, certificats, clés).
- L'objectif de PEAP est de sécuriser ces échanges dans le domaine sans fil.

• Le protocole s'exécute en deux phases

- D'abord établir un tunnel sécurisé avec EAP-TLS
- Ensuite authentifier le client avec un processus EAP à l'intérieur du tunnel.
- Échange d'informations arbitraire à l'intérieur du tunnel.
- Calcul de la clé CSK (Compound Session Key)
- Chiffre les données avec une clé dérivée de la CSK

4-31

Chorégraphie PEAP



4-32

Phase 1

- Étapes 1 et 2
 - Identique à EAP-TLS. Délivrance de certificats
 - Établissement d'une connexion avec l'AP dans le domaine sans fil.
 - Canal sécurisé entre l'AP et le serveur EAP. Le standard ne précise pas la méthode.
- Étape 3
 - Échange d'identité par requête et réponse. Séquence de base EAP, en clair.
 - Ces informations sont d'ordre administrative du type quel serveur choisir, ou pour initialiser un autre contexte.
 - Un second échange d'ID sera effectué dans la seconde phase
 - 3-a : Démarrage EAP-TLS.
- Étapes 4, 5 et 6
 - EAP-TLS handshake protocol
 - Il en résulte, authentifications et établissement de la clé maîtresse de la session pour sécuriser un tunnel.

Fonctionnement PEAP

Phase 2

- EAP-TLV est utilisé pour tunneller les échanges EAP.
- Étapes 7
 - Échange d'ID EAP
- Étape 8
 - Le serveur EAP authentifie le client en utilisant un des mécanismes : MD5, CHAP, SIM, ...
 - Ces échanges sont protégés par le tunnel sécurisé, avec le mécanisme EAP-TLV.
- Étapes 9
 - Dernière étape avec la finalisation des paramètres de chiffrement entre serveur et client.
- Étape 10
 - Client et serveur vont calculer les clés dérivées pour la session.
 - RFC 3269. La CSK est la concaténation du MSK (64 octets) et du Extended MSK (64 octets).
- Étape 11
 - L'AP reçoit les résultats de l'authentification et les clés.
- Étape 12
 - Client et AP peuvent maintenant échanger des données chiffrées avec la clé résultante.

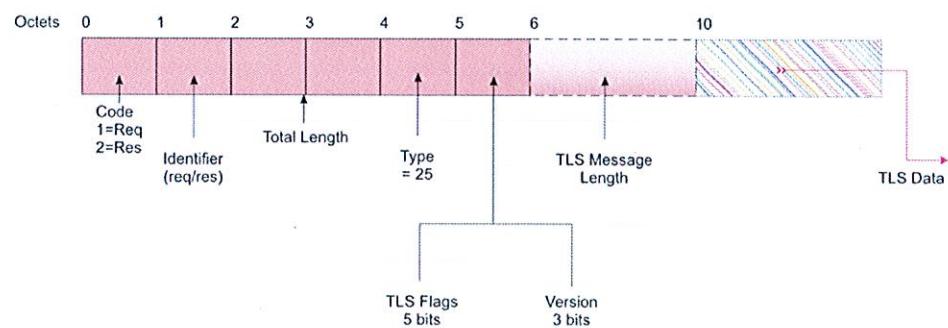
4-33

PEAP

Format des trames PEAP

- Semblables aux trames EAP-TLS avec champ type = 25

Trame PEAP



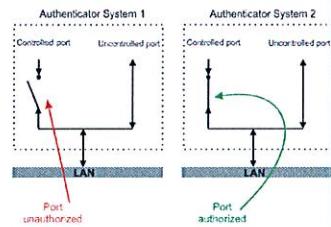
4-34

802.1x : Introduction et principes généraux

Modèle 802.1x

- Les différentes méthodes EAP ont été développé pour des liaisons à distance (dial-up).
- On ne peut pas arbitrairement sur un Lan, ouvrir une connexion TCP et démarrer EAP.
- C'est la raison d'être de 802.1x, qui va fournir un contexte, des machines d'état entre les différentes couches et le protocole EAP over Lan (EAPOL).
- 802.1x a été développé pour les réseaux filaires et étendus aux réseaux sans fil.
- 802.1x fournit la méthode d'accès et EAP complète avec les mécanismes d'authentification.
- Le standard est clair sur le point suivant : 802.1x fournit uniquement un cadre pour les échanges mais ne précise pas le contenu ou les bases de l'authentification.
- 802.1x commence avec le concept d'un port (physique) comme entrée unique du réseau pour un demandeur.
- Dans le domaine sans fil, l'association à un AP peut être considéré comme analogue à un port au sens 802.1x.
- Ce port physique va être divisé en deux ports logiques qui seront ouvert ou fermé.
 - Un port contrôlé est celui qui accorde l'accès au réseau après une authentification fructueuse. Le port contrôlé va offrir tous les services du réseau.
 - Un port non contrôlé va offrir uniquement les services administratifs minimum.
 - Les messages initiaux et les services d'authentification passent par le port non contrôlé.

4-35

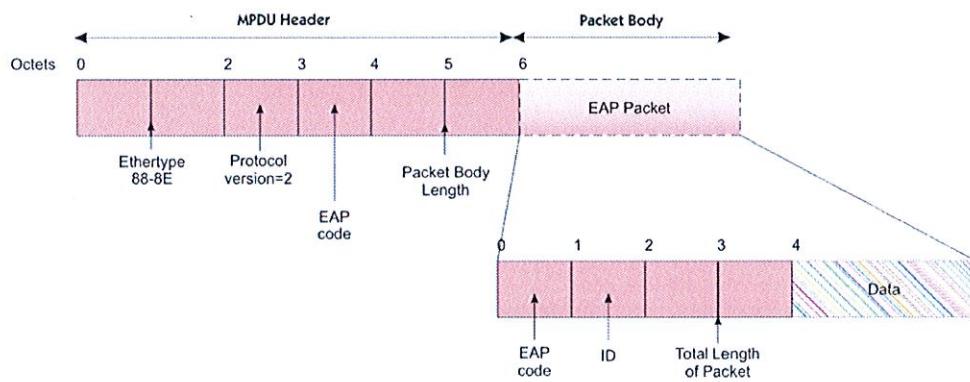


EAPOL

EAPOL

- La méthode pour transporter les paquets EAP entre demandeur et authentificateur par un service MAC sur un Lan (802.3).

Trame EAPOL _ MAC PDU pour Ethernet 802.3



4-36

Cisco LEAP (Lightweight EAP)

LEAP

- A été développé à l'époque où WEP présentait quelques faiblesses, et les protocoles de sécurité 802.11 n'étaient pas encore finalisés.
- LEAP utilise les messages 802.1x EAPOL pour authentifier le serveur.
- Le mécanisme d'authentification utilisé est UserName/PassWord, version MS-CHAP.
- Le serveur est un serveur RADIUS pour les clés de chiffrement.
- Le client se connecte au domaine Windows et à l'Active Directory Windows.
- Faiblesse contre des attaques par dictionnaire et man-in-the-middle.

● Serveur RADIUS local

● Gestion des utilisateurs

The screenshot shows the 'Local RADIUS Server - General Setup' page. Under 'Enable Authentication Protocols', 'EAP FAST' and 'EAP LEAP' are selected. In the 'Network Access Servers (AAA Clients)' section, a network access server is listed with IP 172.16.1.150 and shared secret '*****'. Below it, a user named 'Duc' is listed under 'Current Users' with a password field containing '*****'.

4-37

The screenshot shows three windows:
 1. 'Cisco LEAP (client) Profile Management' window: Set Security Options to 'WPA/WPA2/CCM' with EAP Type 'LEAP'. It includes fields for 'User Name' (Duc), 'Password' (*****), and 'Log on to' (Windows).
 2. 'Configure LEAP' dialog: Shows 'Always Resume the Secure Session' checked. Under 'User Name and Password Settings', 'Use Temporary User Name and Password' is selected. It also includes fields for 'User Name' (Duc), 'Password' (*****), 'Confirm Password' (*****), and 'Domain'.
 3. 'Cisco Aironet Desktop Utility - Current Profile: WPA' window: Displays connection details like 'Profile Name: WPA', 'Link Status: Authenticated', 'Wireless Mode: 2.4 GHz 11 Mbps', 'Server-Based Authentication: LEAP', 'IP Address: 172.16.1.52', and 'Signal Strength: Excellent'.
 Arrows indicate the flow from the client profile settings through the configuration dialog to the final connection status window.

4-38

EAP-FAST

• EAP-FAST (Flexible Authentication via Secure Tunnelling)

- A été développé par Cisco et présenté à l'IETF en 2004 pour la standardisation du protocole.
- L'objectif est d'améliorer LEAP avec un meilleur chiffrement pour protéger les échanges challenge/réponse.
- EAP-FAST met en place un secret partagé entre le client et le serveur par un processus appelé Protected Access Credential (PAC).
- Le PAC consiste en une clé de 32 octets (PAC-Key), un champ opaque caché par le serveur et des informations PAC.
- Le PAC va mettre en place un tunnel pour l'authentification.

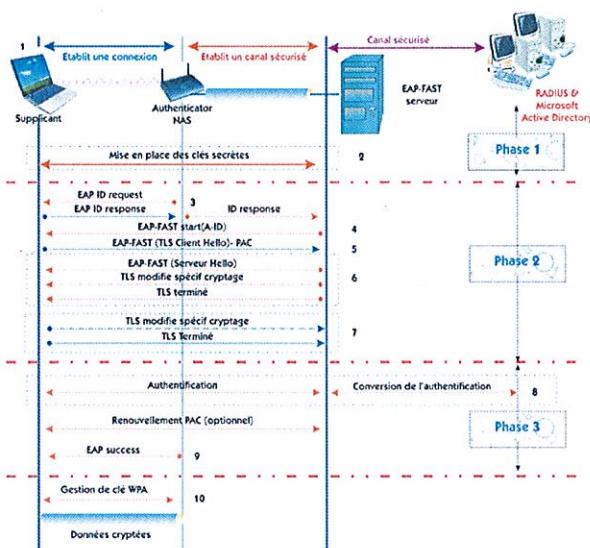
• EAP-FAST se fait en trois phases.

- Phase 1 : échange du secret partagé. Cette phase est indépendante des deux autres.
- Phase 2 : mise en place du tunnel avec PAC.
- Phase 3 : authentification.

4-39

Chorégraphie EAP-FAST

• EAP-FAST est une combinaison de multiples échanges.



4-40

Sécurité avancée

Authentification par adresses MAC

Autres menaces sur la sécurité

Authentification avancée



Chiffrement avancé

EAP et RADIUS

Menace sur WPA

Résumé du chapitre

4-41

Les standards 802.11

Une comparaison entre WEP, WPA et 802.11i

Caractéristiques	WEP	802.1x	WPA	802.11i (WPA2)
Identité	Machine (clé)	Utilisateur	Utilisateur	Utilisateur
Authentification	Clé partagé/EAP	UserN/Passw Certif PEAP	Usr/Pw - RADIUS PEAP	Usr/Pw - RADIUS PEAP
Intégrité	Integrity Check Value 32 Bits	ICV 32 Bits	Message Integrity Code 64 Bits	Counter with CBC-MAC (CCM)
Chiffrement	Clé statique	Clé par session	Rotation des clés TKIP	CCMP
Distribution des clés	Manuel, 1 fois	Clé par session après authentification	Rotation automatique	Rotation automatique
IV Vecteur d'Initialisation	Texte clair 24 Bits	Texte clair 24 Bits	IV étendu - 64 Bits sélection suivant séquences	non
Algorithme	RC4	RC4	RC4 AES - option	AES
Longueur de la clé	64/128 bits	64/128 bits	128 bits	128 bits
Infrastructure	ACL statique	RADIUS	RADIUS	RADIUS

4-42

Les standards 802.11

• Vulnérabilité des réseaux sans fil

- Comme nous l'avons souligné, les premiers standards 802.11 ont montré des faiblesses, en particulier WEP. (Attaque Fluhrer-Martin-Shamir en 2001)
- L'alliance Wi-Fi avait besoin de rassurer le grand public pour qu'on continue d'utiliser les produits Wi-Fi.
- Le groupe IEEE 802.11i a commencé ses travaux, mais les organismes de standardisation sont relativement lents.
- Cisco proposait sa propre version de sécurisation (CKIP – Cisco Key Integrity Protocol).
- L'alliance Wi-Fi a mis en place un sous-ensemble proposé comme le pré-standard 802.11i, baptisé WPA (Wi-Fi Protected Access), qui devient en 2003 un package proposé par les constructeurs.
- Le standard 802.11i, approuvé en juin 2004, rajoute de nouvelles méthodes de chiffrement et de protection des données.
- L'une des méthodes est de conserver la continuité avec le WEP, l'autre méthode est basée sur l'AES (Advanced Encryption Standard) et nécessite parfois, une mise à niveau du matériel.
- La Wi-Fi alliance a évolué vers le standard, rebaptisé WPA2.

4-43

WPA & WPA2

• WPA (Wi-Fi Protected Access)

- Développé par la Wi-Fi Alliance et l'IEEE
- Solution provisoire en avance sur les standards 802.11i
- Conçu pour fonctionner avec les équipements existants avec une mise à niveau du *firmware*.
- Certains équipement ne pourront pas suivre.

• WPA 2 est le nom donné pour la version conforme à 802.11i.

- Pour utiliser CCMP, une modification du matériel est nécessaire pour certains constructeurs.

• Ratification de 802.11i en juin 2004

- WPA 2 de la Wi-Fi Alliance pour se mettre en conformité avec 802.11i
- Gestion des clés
- Chiffrement
- Et mécanisme d'authentification

• Deux classes (WPA & WPA2):

- WPA 2 – Entreprise :
 - RADIUS
 - Authentification 802.1x et clé partagée
- WPA 2 – Personnel
 - Clé partagée

4-44

Le standard 802.11i

- ➲ Le but est d'apporter de nouveaux mécanismes de sécurité pour assurer la confidentialité et l'intégrité des messages.
 - On va incorporer l'algorithme d'authentification de port 802.1x.
- ➲ Les nouvelles caractéristiques comprendront :
 - Deux types de réseaux appelés Transition Security Network (TSN) et Robust Security Network (RSN).
 - Les méthodes de chiffrement et de contrôle d'intégrité : Temporary Key Integrity Protocol (TKIP) et Counter mode / CBC-MAC protocol (CCMP).
 - Mécanismes d'authentification EAP.
 - Gestion des clés avec des protocoles de handshake sécurisé sur 802.1x.

4-45

Le standard 802.11i

- ➲ TKIP est un ensemble de mécanismes de chiffrement
 - Incluant un algorithme de modification des clés et un comptage de paquets, pour protéger les clés servant au chiffrement.
 - Il inclut également Michael, un algorithme de contrôle MIC (Message Integrity Check) qui, avec le compteur de paquets, évite le rejet et les modifications.
 - TKIP et Michael ont été conçus pour fonctionner sur des équipements en place, et donc de sécuriser les réseaux existants.
- ➲ CCMP est un algorithme basé sur AES pour le chiffrement et le contrôle d'intégrité.
 - CCMP est plus fort que TKIP et devrait être préféré, mais est incompatible avec les anciens équipements utilisant WEP.
 - Tous les constructeurs devront faire les mises à jours nécessaires pour être conformes au standard.
- ➲ Un RSN est un réseau qui n'autorise que les machines TKIP/Michael et CCMP.
- ➲ Un TSN supportera RSN et les machines pré-RSN utilisant WEP.
 - La faiblesse du TSN est que tous les broadcast doivent être envoyés avec le dénominateur commun le plus faible en terme de sécurité.
- ➲ La gestion de port 802.1x repose sur l'authentification EAP.
 - Les Master keys sont en place après l'authentification EAP, et les clés sont modifiées pendant la communication.

4-46

TKIP (Temporal Key Integrity Protocol)

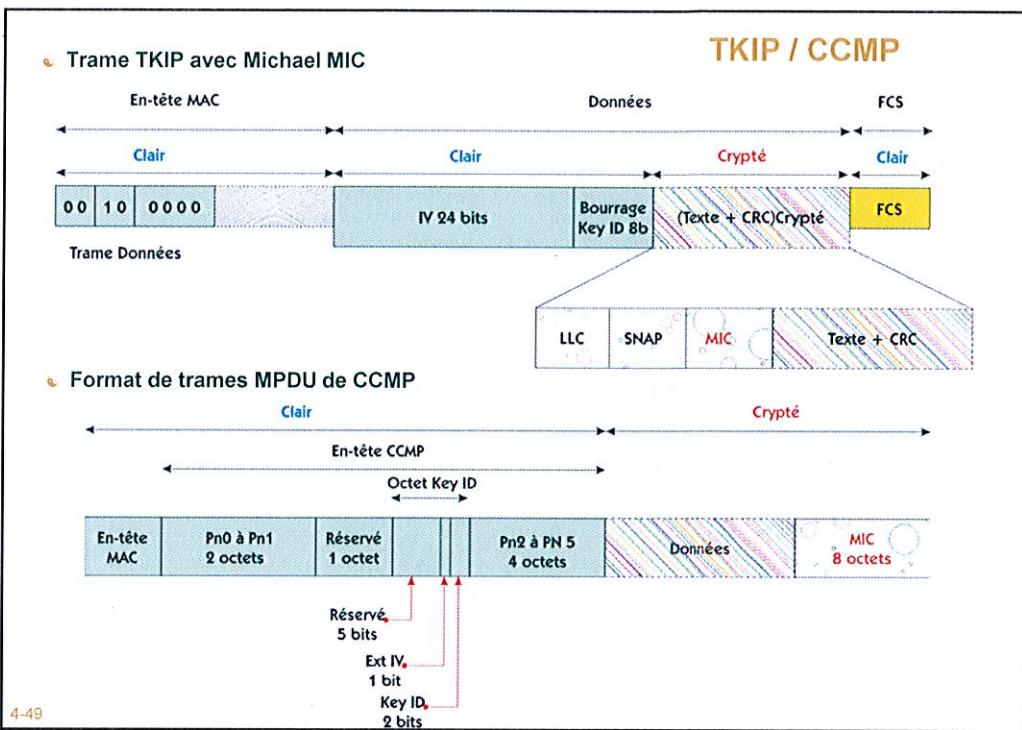
- Doit surmonter les faiblesses du chiffrement WEP et fonctionner avec les anciens équipements.
 - Trois protocoles : un contrôle d'intégrité crypté, un mélange des clés, et une amélioration du vecteur d'initialisation.
- Michael MIC
 - Une méthode de chiffrement du résultat du contrôle avec un mécanisme appelé Michael pour ne pas utiliser un mécanisme tel que SHA1, trop consommatrice de CPU.
- Le compteur TSC (TKIP Sequence Counter) est long de 48 bits, démarre à 0 et est incrémenté de 1 pour chaque paquet.
 - Le récepteur qui reçoit un paquet doit contrôler le TSC. S'il voit arriver un TSC inférieur ou égal au dernier reçu, il doit le jeter.
- L'algorithme de mixage des clés.
 - Pour la protection de la clé temporaire TEK (Temporal Encryption Key), l'algorithme de gestion des clés permet les modifications.
 - Le mixage démarre avec la TEK, combinée avec le TSC et l'adresse destinataire pour créer un germe WEP, utilisé avec le WEP. Comme le TSC change à chaque paquet, le germe WEP va changer aussi, cette modification n'inclut pas seulement les 24 bits de l'IV, mais également les 104 autres bits de la clé.

4-47

CCMP

- Counter mode/CBC-MAC Protocol
 - CBC-MAC : Cipher Block Chaining – Message Authentication Code
 - CCMP est le cœur de la portion RSN du réseau 802.11i.
 - CCMP est basé sur AES, l'état de l'art actuel des algorithmes de chiffrement, sans licence.
- CCMP va utiliser le mode Compteur pour la confidentialité et CBC-MAC pour l'intégrité.
 - CCMP choisit 128 bits pour la clé et la longueur du bloc.
 - CCMP prend un MIC de 8 octets avec un champ de 2 octets.
 - CCMP utilise un numéro de paquet (PN Packet Number), de 48 bits, assez semblable au TSC utilisé par TKIP.
 - La longueur de l'en-tête CCMP est de 8 octets. (4 de plus que VI WEP+ID clé).
 - Le bit Extended IV pour indiquer qu'il y a 4 octets de plus dans l'en-tête.
 - L'octet KeyID contient l'ID de la clé sur 2 bits.
 - CCMP coupe le PN en 2 parties. Les 2 octets de poids faible au début, et après l'octet KeyID, les 4 octets de poids fort du PN.

4-48



Gestion des clés

- L'un des problèmes majeurs de 802.11 est la distribution des clés.
 - Il est difficile pour l'administrateur de les générer et ensuite de les gérer.
 - La sécurité pourra être compromise en cas de perte de portable ou de carte réseau, les clés peuvent être compromises en cas de distribution massive, par Email, disquette ou CD.
- 802.11i introduit des schémas de gestion de clés qui permet une distribution indépendante du processus d'authentification.
 - 2 phases principales :
 - Mise en place de la clé principale (Master Key)
 - Échange de clé
 - La mise en place de la Master Key peut se faire soit par configuration manuelle, soit dynamiquement par 802.1x avec EAP.
 - Le terme échange de clé est utilisé dans la spécification, mais en fait, il s'agit d'une phase de négociation sans vraiment d'échange de la clé actuelle.

Gestion des clés

● Mise en place de la Master Key

- EAPOL est la méthode préférée pour mettre en place la Master Key.
- 802.1x est le protocole utilisé pour transporter les messages d'authentification EAPOL entre la station et le serveur d'authentification.
- Après la première phase d'authentification, le processus va générer une clé partagée entre le client et le serveur.
- Le serveur va transférer cette clé à l'AP via RADIUS. À ce moment, la Master Key est le secret partagé entre la station et l'AP, connu également sous le nom Pairwise Master Key (PMK).
- Notez que l'AP n'est pas impliqué dans ces négociations. C'est seulement à la fin du processus, après la dérivation de la PMK que l'AP reçoit cette dernière.
- Si l'administrateur n'utilise pas 802.1x, cette clé peut être configurée manuellement. C'est la Preshared Key (PSK) qui devient donc PMK.
- Deux types de clés dans 802.11i :
 - Pairwise key pour le trafic unicast PMK
 - Group key pour le multicast GMK
- La PMK peut avoir une durée de vie assez longue (plusieurs associations avec un AP)
- La GMK présente plus de risques et doit changer plus souvent (à chaque association-dissociation)

4-51

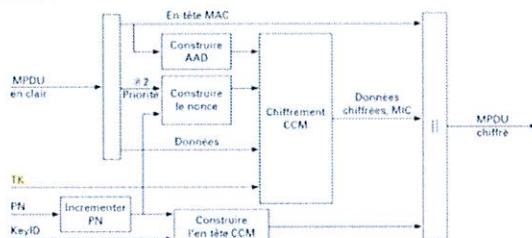
Gestion des clés

● Dérivation des clés suivantes à partir de la PMK

- De la PMK, le client et l'AP utilisent des fonctions pseudo-aléatoires pour calculer trois clés
- Il est d'abord calculé une clé intermédiaire appelée Pairwise Transient Key (PTK) clé fugace
 - 512 bits pour TKIP
 - 384 bits pour CCMP
- La PTK est ensuite découpée en trois clés
 - EAPOL Key Confirmation Key (EAPOL KCK) 128 bits
 - EAPOL Key Encryption Key (EAPOL KEK) 128 bits
 - Et la Temporal Key (TK), 256 bits pour TKIP et 128 bits pour CCMP.
 - Pour TKIP, la TK de 256 bits est ensuite subdivisée en TEK de 128 bits, la Michael Key de 64 bits pour le trafic authentificateur-station et la Michael Key pour le trafic station-authentificateur.
 - Pour CCMP, la TK devient la clé CCMP.

Le WEP nécessitait une puissance de calcul de l'ordre d'un i486 (équivalent à 1,2 million de transistors) et l'AES nécessite quant à lui la puissance de calcul d'un Pentium 150 (soit 3,1 millions) ... on comprend alors la nécessité de changement de matériel !

4-52



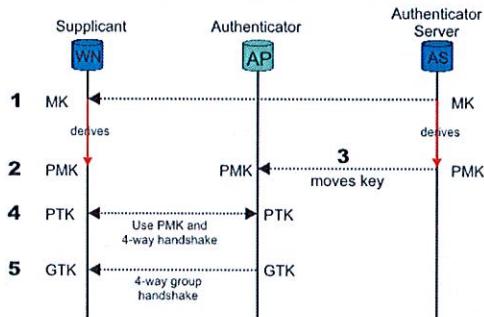
Gestion et découpage des clefs (chorégraphie) 1/2

- 1. Lorsque le Supplicant (WN) et le Serveur d'Authentification (AS) sont authentifiés, l'un des derniers messages envoyé par l'AS est la *Master Key* (MK).
- 2. La Station WN et l'AS dérivent une nouvelle clef, appellée *Pairwise Master Key*.
- 3. La PMK est alors transmise à l'AP
- 4. La PMK et un 4-way handshake sont alors utilisés pour calculer une *Pairwise Transient Key* (PTK). Cette clef est un ensemble de clefs :
 - Key Confirmation Key (KCK), sert à prouver la possession de la PMK.
 - Key Encryption Key (KEK) est utilisé pour distribuer la Group Transient Key (GTK).
 - La Temporal Key 1 & 2 (TK1/TK2) est utilisée pour le chiffrement.
- 5. La KEK et un 4-way group handshake sont alors utilisés pour envoyer la *Group Transient Key* (GTK) de l'AP vers la Station. Cette clef est une clef partagée par tous les supplicants connectés au même Authenticator, pour le multicast et le broadcast.

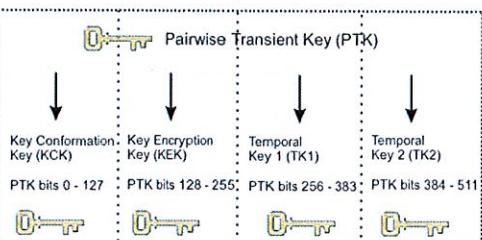
4-53

Gestion et découpage des clefs (chorégraphie) 2/2

Chorégraphie d'échange et calcul des clefs



Découpage et calcul des clefs



4-54

Sécurité avancée

Authentification par adresses MAC

Autres menaces sur la sécurité

Authentification avancée

Chiffrement avancé



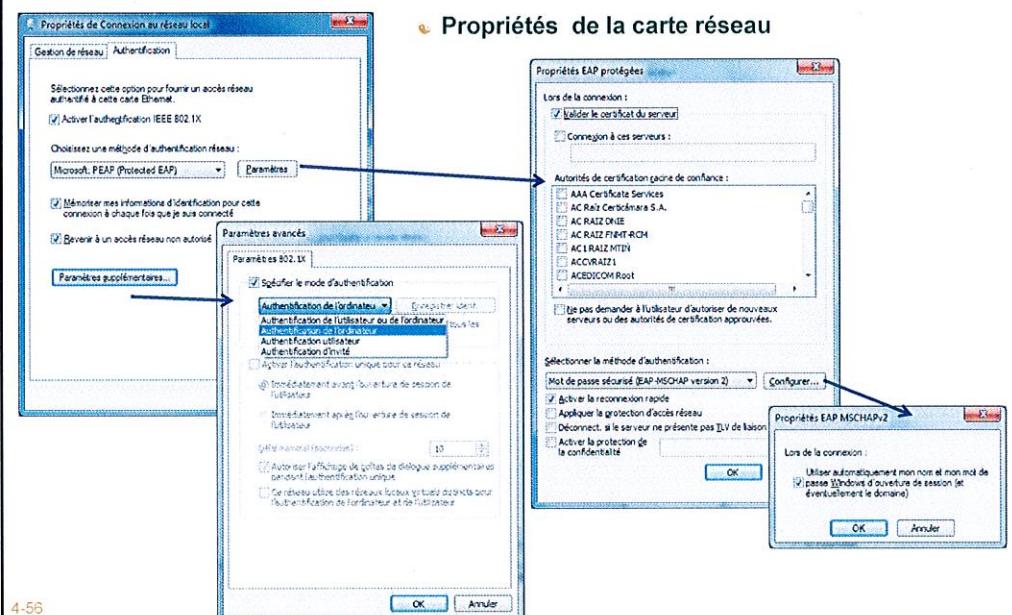
EAP et RADIUS

Menace sur WPA

Résumé du chapitre

4-55

Configuration EAP / RADIUS (Supplicant)



4-56

Configuration client RADIUS (AP Cisco)

The screenshot shows two windows from the Cisco ICS Series AP Security interface:

- SSID Properties (Top Window):** Shows the current SSID list with 'INTERNET' selected. It includes fields for SSID, VLAN, Interface (selected as 'Radio 0/0 11G'), and Network ID.
- Backup RADIUS Server (Bottom Window):** Shows the 'Corporate Servers' section with 'RADIUS' selected. It lists 'Server' (IP address 192.168.51) and 'Shared Secret' (*****). Below it is the 'Default Server Priorities' section.

Annotations:

- A callout points to the 'Authentification' dropdown in the 'Client Authentication Settings' section of the top window, with the text: "Sur l'AP, pour le SSID, définition de l'authentification".
- A callout points to the 'RADIUS' entry in the 'Corporate Servers' list of the bottom window, with the text: "Précision du serveur RADIUS".

4-57

Configuration serveur RADIUS (Microsoft NPS)

The screenshot shows the Microsoft NPS Management console with the following windows open:

- Radii Stratégies (Main Window):** Displays a list of RADIUS strategies. One strategy is selected: 'Accès VTN - Utilisateur Internet Public'. It shows conditions like 'Type de port NAS: Wireless Client/Wireless IEEE 802.11' and 'Groupes Windows: INTERNET\Ordinateurs du domaine'.
- Stratégie d'accès (Left Panel):** Shows the parameters for the selected strategy, including 'Parallèles: Les paramètres suivants sont appliqués' and 'Conditions: Si les conditions suivantes sont évaluées'.
- Stratégies d'accès (Right Panel):** Shows a list of other RADIUS strategies, such as 'Accès VTN', 'Accès Réseau Intérieur - Ordinateur Internet Public', 'Authentification par MAC', and 'Utilisateurs Internet (Non utilisés)'.

Annotations:

- A callout points to the 'Accès VTN - Utilisateur Internet Public' strategy in the main window, with the text: "Sur le serveur RADIUS, définition des clients (AP, switchs)".

4-58

Sécurité avancée

Authentification par adresses MAC

Autres menaces sur la sécurité

Authentification avancée

Chiffrement avancé

EAP et RADIUS



Menace sur WPA

Résumé du chapitre

4-59

Faillle WPA (Bulletin CERTFR-2017-ALE-014 du 16 octobre 2017)

- ➲ Plusieurs vulnérabilités ont été découvertes dans WPA/WPA2. Il est possible lors de l'établissement d'une session de communication utilisant le protocole WPA/WPA2 d'interférer sur le **mécanisme en quatre temps** visant à assurer la confidentialité des échanges. Lors de cette phase d'initialisation, un utilisateur malveillant interceptant les communications entre un client et un point d'accès Wi-fi, peut amener le client à **réutiliser des paramètres** entrant en compte dans le chiffrement des données échangées. Cela peut permettre à un attaquant de provoquer une atteinte à la **confidentialité ou à l'intégrité des données**.
- ➲ Par ailleurs, l'implémentation du protocole dans les logiciels **wpa_supplicant** rend l'exploitation de la vulnérabilité particulièrement aisée. Dans ces conditions il est notamment possible de rejouer des paquets réseau, d'injecter du contenu vers un client connecté en Wi-Fi et d'accéder à des communications confidentielles.
- ➲ Si tous les clients utilisant WPA/WPA2 sont vulnérables à cette attaque, **les objets connectés, les appareils sous Linux et Android** sont particulièrement sensibles de par l'utilisation native de **wpa_supplicant** *

* wpa_supplicant est un package multi-plateforme qui permet le support de WEP, WPA et WPA2.

4-60

Site web **spécialement dédié à KRACK Attacks** : <https://www.krackattacks.com/>

Solution : patcher les systèmes

- Le CERT-FR recommande plusieurs mesures afin de limiter l'impact de cette vulnérabilité :

- mettre à jour régulièrement tout système se connectant au réseau Wi-Fi (Systèmes industriels, objets connectés, ordiphones, postes clients, répéteurs Wi-Fi), en s'appuyant sur la liste des systèmes affectés ci-dessous ;
<https://www.kb.cert.org/vuls/byvendor?searchview&Query=FIELD+Reference=2285>
- privilégier les protections de type TLS ou VPN pour assurer l'intégrité et la confidentialité des données échangées sur les réseaux Wi-Fi ;
- configurer les équipements Wi-Fi pour imposer l'utilisation de WPA2 (et non pas WPA) et AES-CCMP (et non pas TKIP) ; cette recommandation ne permet pas de se prémunir contre une potentielle écoute d'une communication mais empêche le vol de la clé de session Wi-Fi ;
- désactiver ou filtrer le trafic multicast ; ce type de trafic rendant les systèmes Microsoft et Apple vulnérables ;
- faire un inventaire et une analyse de risque des systèmes utilisant un réseau Wi-Fi, notamment des systèmes cités plus haut, afin de désactiver si possible le service Wi-Fi.

- Le CERT-FR, dans le cadre de cette alerte, rappelle les bonnes pratiques suivantes :

- assurer une veille des publications des correctifs de sécurité des composants cités *supra* ;
- sensibiliser les utilisateurs, notamment ceux particulièrement ciblés et manipulant des informations sensibles, aux risques liés à l'utilisation du réseau Wi-Fi (public ou non)

4-61

Réaction des fournisseurs et éditeurs de logiciels

- Annonce de la faille de sécurité KRACK faite fin aout aux éditeurs, et rendue publique le 16 octobre 2017 bien que soumise le 19 Mai 2017

CVE-2017-13080 | Windows Wireless WPA Group Key Reinstallation Vulnerability

Security Vulnerability

Published: 10/16/2017 | Last Updated: 10/19/2017
MITRE CVE ID: CVE-2017-13080

A spoofing vulnerability exists in the Windows implementation of wireless networking. An attacker who successfully exploited this vulnerability could potentially replay broadcast and/or multicast traffic to hosts on a WPA or WPA 2 protected wireless network.

Multiple conditions would need to be met in order for an attacker to exploit the vulnerability – the attacker would need to be within the physical proximity of the targeted user, and the user's computer would need to have wireless networking enabled. The attacker would then need to execute a man-in-the-middle (MitM) attack to intercept traffic between the target computer and wireless access point.

The security update addresses the vulnerability by changing how Windows verifies wireless group key handshakes.

Exploitability Assessment

The following table provides an exploitability assessment for this vulnerability at the time of original publication.

Publicly Disclosed	Exploited	Latest Software Release	Older Software Release
No	No	2 - Exploitation Less Likely	2 - Exploitation Less Likely

Affected Products

The following software versions or editions are affected. Versions or editions that are not listed are either past their support life cycle or are not affected. To determine the support life cycle for your software version or edition, see the Microsoft Support Lifecycle.

Product	Platform	Article	Download	Impact	Severity	Supersedence
Windows 10 for 32-bit Systems		4042895	Security Update	Spoofing	Important	4038781
Windows 10 for x64-based Systems		4042895	Security Update	Spoofing	Important	4038781

← www.kb.cert.org/vuls/byvendor?searchview&Query=FIELD+Reference=2285

Vendor Information for VU#228519

Wi-Fi Protected Access (WPA) handshake traffic can be manipulated to induce nonce and session key reuse

Vendor	Status	Date Notified	Date Updated
Aerohive	Affected	30 Aug 2017	17 Oct 2017
Apple	Affected	28 Aug 2017	23 Oct 2017
Arch Linux	Affected	28 Aug 2017	17 Oct 2017
Aruba Networks	Affected	28 Aug 2017	09 Oct 2017
AsusTek Computer Inc.	Affected	28 Aug 2017	19 Oct 2017
Broadcom	Affected	30 Aug 2017	17 Oct 2017
CentOS	Affected	28 Aug 2017	23 Oct 2017
Cisco	Affected	28 Aug 2017	16 Oct 2017
D-Link Systems, Inc.	Affected	28 Aug 2017	20 Oct 2017
dd-wrt	Affected	-	23 Oct 2017
Debian GNU/Linux	Affected	28 Aug 2017	17 Oct 2017
Microchip Technology	Affected	28 Aug 2017	17 Oct 2017
Microsoft Corporation	Affected	28 Aug 2017	15 Oct 2017

KRACK =

key reinstallation attacks
« attaques de clé de réinitialisation »

4-62

Sécurité avancée

Authentification par adresses MAC

Autres menaces sur la sécurité

Authentification avancée

Chiffrement avancé

EAP et RADIUS

Menace sur WPA



Résumé du chapitre

4-63

Résumé du chapitre

● Dans ce chapitre, nous avons

- Configuré le filtrage par adresses MAC
- Analysé d'autres menaces sur la sécurité
- Vu des protocoles d'authentification et de chiffrement avancés : 802.1X, TKIP, CCMP, EAP et WPA
- Etudié le mécanisme d'authentification EAP avec RADIUS
- Vu la faille récente de la norme WPA (octobre 2017)

4-64