Extended Authentication Protocol

(EAP)

Anaïs Gantet, Benoît Camredon

TLS-SEC 2019/2020

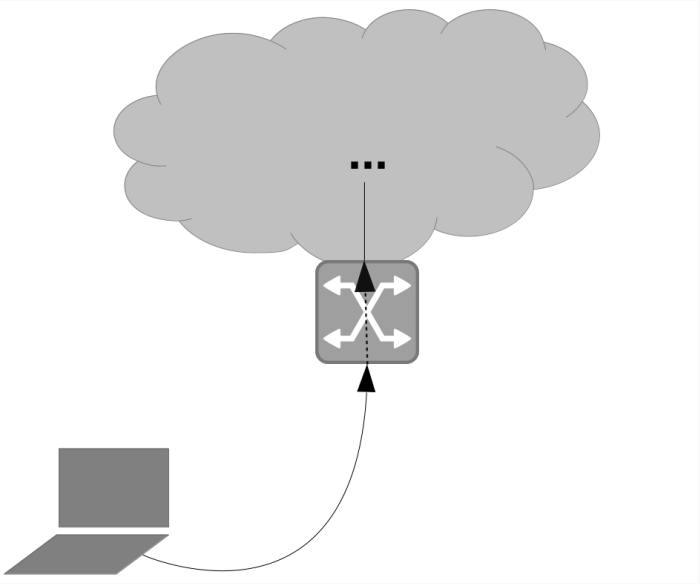
Introduction

Qu'est-ce qu'EAP ?

- EAP : Extended Authentication Protocol
- C'est un framework, pas un protocole
- Surcouche générique donnant accès à divers protocoles d'authentification
- Très utilisé pour gérer le contrôle d'accès à un réseau local

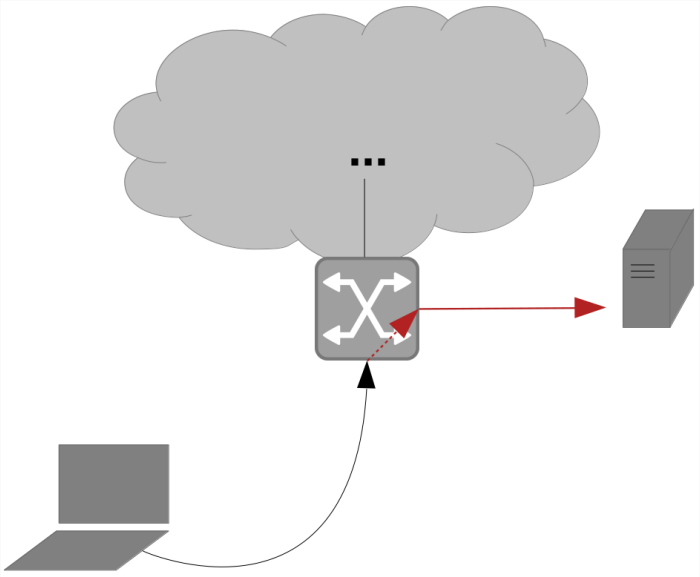
EAP et notion de contrôle d'accès

Sans EAP, il suffit de se brancher pour être connecter au réseau cible



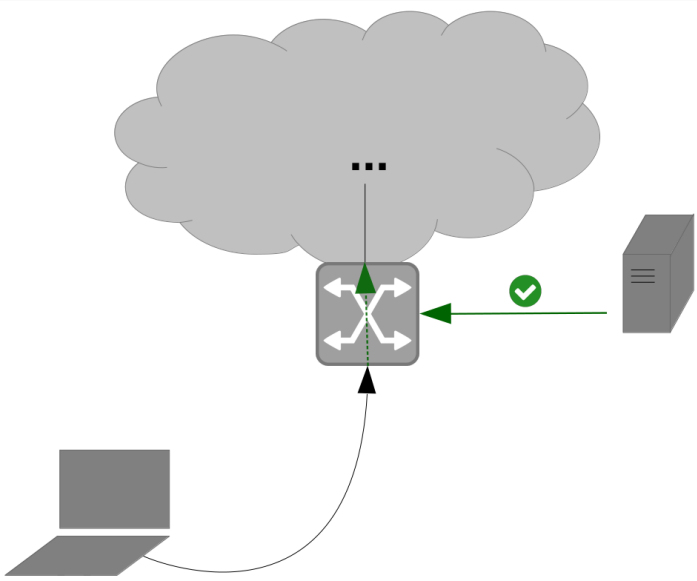
EAP et notion de contrôle d'accès

Avec EAP, le switch redirige la connexion vers un serveur d'authentification



EAP et notion de contrôle d'accès

Avec EAP, le switch n'accepte la connexion qu'après validation du serveur d'authentification

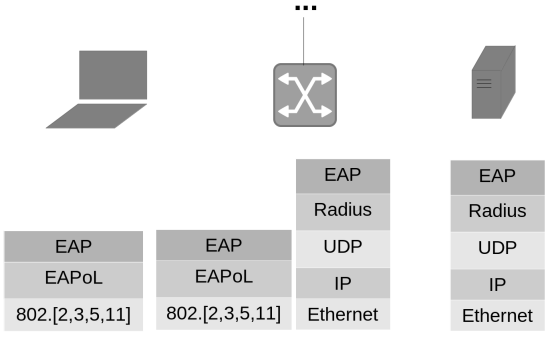


3 composants

- Le *supplicant* : machine qui demande l'accès au réseau
- L'*authenticator* : en général le switch ou le point d'accès en frontal du réseau
- L'*authentication server* : serveur qui connait les utilisateurs et renseigne l'*authenticator* s'il peut accepter la connexion

A noter

- Intelligence d'authentification déportée sur un serveur à part

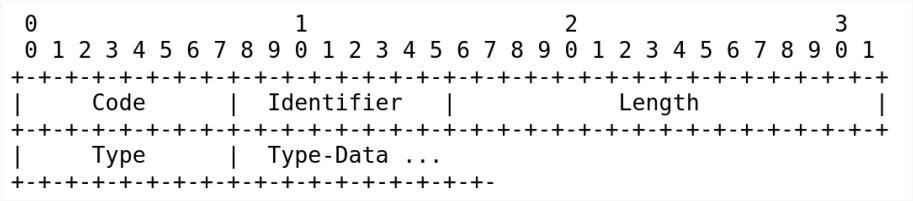


Quelques standards

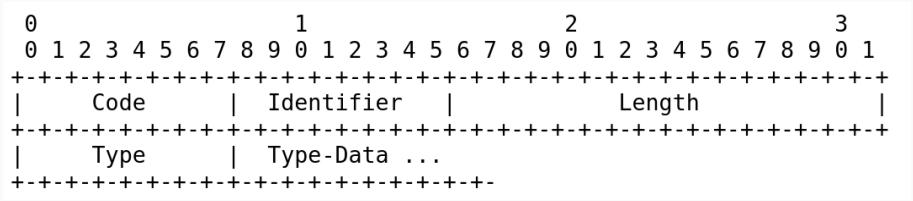
- RFC 1334 : PPP Authentication Protocols (dont PAP)
- RFC 1994 : CHAP (PPP Challenge Handshake Authentication Protocol)
- RFC 2433 : MS CHAP (Microsoft CHAP)
- RFC 2759 : MS CHAP v2
- RFC 3579 : RADIUS (Remote Authentication Dial-In User Service) Support For EAP
- **RFC 3748 : Extensible Authentication Protocol (EAP)**
- RFC 4186 : EAP-SIM (GSM Subscriber Identity Modules)
- RFC 4851 : EAP-FAST (Flexible Authentication via Secure Tunneling)
- RFC 4764 : EAP-PSK (Pre-Shared Key)
- RFC 4793 : EAP-POTP (Protected One-Time Password Protocol)
- RFC 5106 : EAP-IKEv2 (Internet Key Exchange)
- RFC 5181 : EAP-TTLSv0 (Tunneled Transport Layer Security)
- RFC 5216 : EAP-TLS (Transport Layer Security)
- RFC 5247 : EAP key management framwork
- RFC 5448 : EAP-AKA (Authentication and Key Agreement)
- RFC 5931 : EAP-pwd (Shared password)
- RFC 6124 : EAP-EKE (Encrypted Key Exchange)
- RFC 8146 : Support for Salted Password Databases to EAP-pwd
- etc.

Fonctionnement

EAP : Format des messages



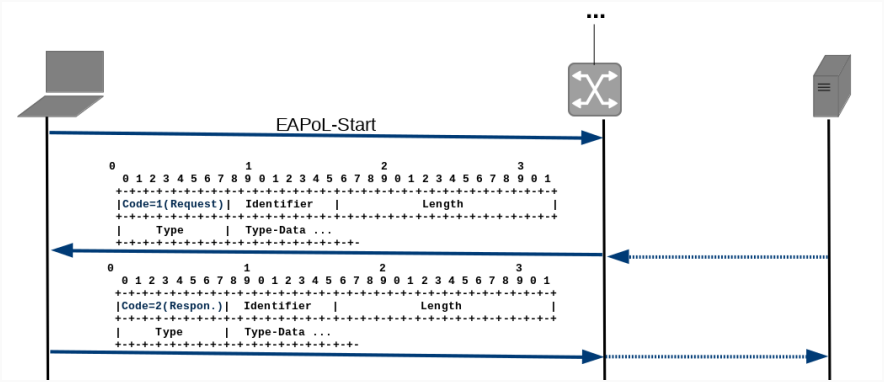
EAP : Format des messages



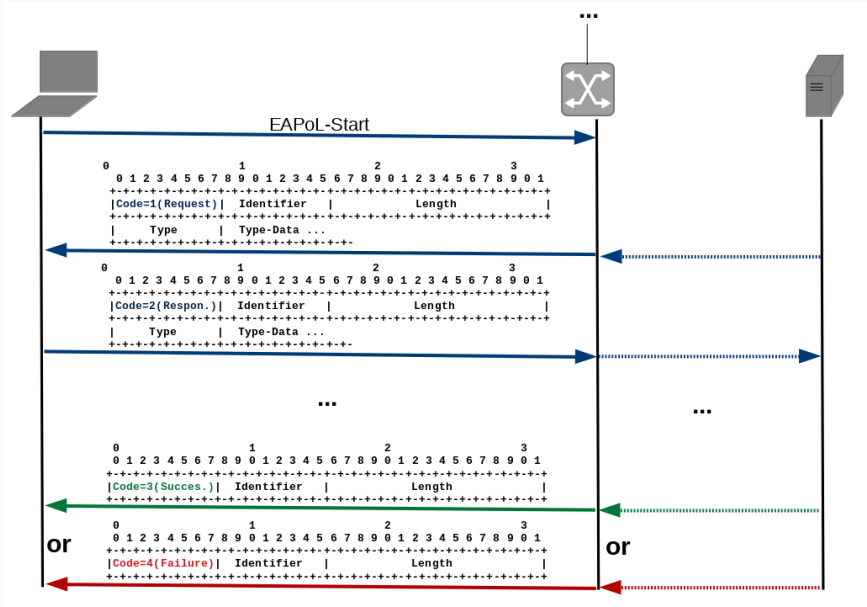
- Code
  - 1 : Request
  - 2 : Response
  - 3 : Success
  - 4 : Failure
- Identifier
  - Numéro dédié pour 1 communication EAP
- Length
  - Taille totale du paquet EAP

- Type (pour les paquets Request/Response)
  - 1: Identity
  - 4: MD5-Challenge
  - 6: Generic Token Card (GTC)
  - 13: EAP-TLS
  - 21: EAP-TTLS
  - 43: EAP-FAST
  - etc.

EAP : Echanges entre le supplicant et l'authenticator



EAP : Echanges entre le supplicant et l'authenticator



EAP : Méthodes d'authentification

- EAP-MD5
  - Authentification basée sur un mot de passe
  - Utilise un MD5 (mot de passe, challenge)
  - Aucune authentification du serveur
- EAP-PSK
  - Authentification basée sur une clé (symétrique) partagée à long terme entre le supplicant et le server (AES-128)
- EAP-TLS
  - Authenfication basée sur les certificats
  - Utilise les échanges TLS (avec échange et vérification de certificats)
- EAP-TTLS
  - Etape 1 : Etablissement d'un canal de communication sécurisé (avec TLS)
  - Etape 2 : Echanges et vérification d'authentification (par mot de passe par exemple) à travers le canal ouvert
- EAP-FAST
  - Etape 1 : Etablissement d'un canal de communication sécurisé (avec TLS)
  - Etape 2 : Echanges de messages TLV (type:length:values) à travers le canal ouvert
- LEAP
  - Protocole Cisco propriétaire
- EAP-PEAP
  - Ressemble à TTLS mais fait par Microsoft, RSA Security et Cisco Systems

Attaques EAP

EAP : faiblesses ?...

Attaques sur la méthode d'authentification

- EAP-MD5 : vulnérable aux attaques par dictionnaire hors-ligne (données : trafic client / contrôleur)
- EAP-TTLS/EAP-PEAP : vulnérable aux attaques dictionnaire en ligne (??)

Attaques sur la session en cours

- Pas de protection de session
- Validation par adresse MAC une fois authentifiée
- Possibilité de spoofing d'adresse MAC et de vol de session

Attaques de man-in-the-middle

- Surtout possible avec les réseaux non-filaires
- Possibilité d'usurpation du SSID d'un AP (attaquant se fait passer pour l'authenticator)

EAP : faiblesses ?...

Attaques sur la méthode d'authentification

- EAP-MD5 : vulnérable aux attaques par dictionnaire hors-ligne (données : trafic client / contrôleur)
- EAP-TTLS/EAP-PEAP : vulnérable aux attaques dictionnaire en ligne (??)

Attaques sur la session en cours

- Pas de protection de session
- Validation par adresse MAC une fois authentifiée
- Possibilité de spoofing d'adresse MAC et de vol de session

Attaques de man-in-the-middle

- Surtout possible avec les réseaux non-filaires
- Possibilité d'usurpation du SSID d'un AP (attaquant se fait passer pour l'authenticator)

A retenir

- Utiliser en priorité EAP-TLS, EAP-PEAP ou EAP-TTLS
- Une fois authentifié, mettre en place un canal de communication chiffré