SEC105 - Architectures et bonnes pratiques de la sécurité des réseaux, des systèmes, des données et des applications

PEI Millau – Concepteur Architecte Informatique (toutes spécialités)

Objectif : Comprendre le fonctionnement et les vulnérabilités, configurer, exploiter, superviser les exigences de sécurité de base pour accéder aux réseaux d'entreprise et protéger les accès aux actifs essentiels et support de l'entreprise :

Thème : Architectures et protocoles de sécurité pour les accès au SI

Contexte

Constat :

« Le système d'information est un patrimoine important très convoité par la concurrence, mais également par les personnes malveillantes. »

*Il est donc dans l'intérêt de tous d'assurer une gouvernance efficace des différents mécanismes permettant à un individu ou à un programme d'**accéder aux données de l'entreprise**.*

*C'est dans cette logique que nous allons nous focaliser sur les **systèmes de gestion d'identité**, qui permettent **l'identification, l'authentification** puis l'attribution ou non **des droits d'accès** à tout ou une partie de ces données ou ressources.*

Contexte

Pour évaluer le niveau de sécurité d'un bien informatique, nous faisons appel à des critères déjà introduits :

***La confidentialité** : Il s'agit de mettre en place des mécanismes pour ne pas divulguer un message d'un utilisateur, et donc le rendre inaccessible à tout attaquant ou espion potentiel. Seul l'auteur du message et les destinataires sont capables d'accéder à son contenu. La confidentialité est rendue possible par les mécanismes cryptographiques.*

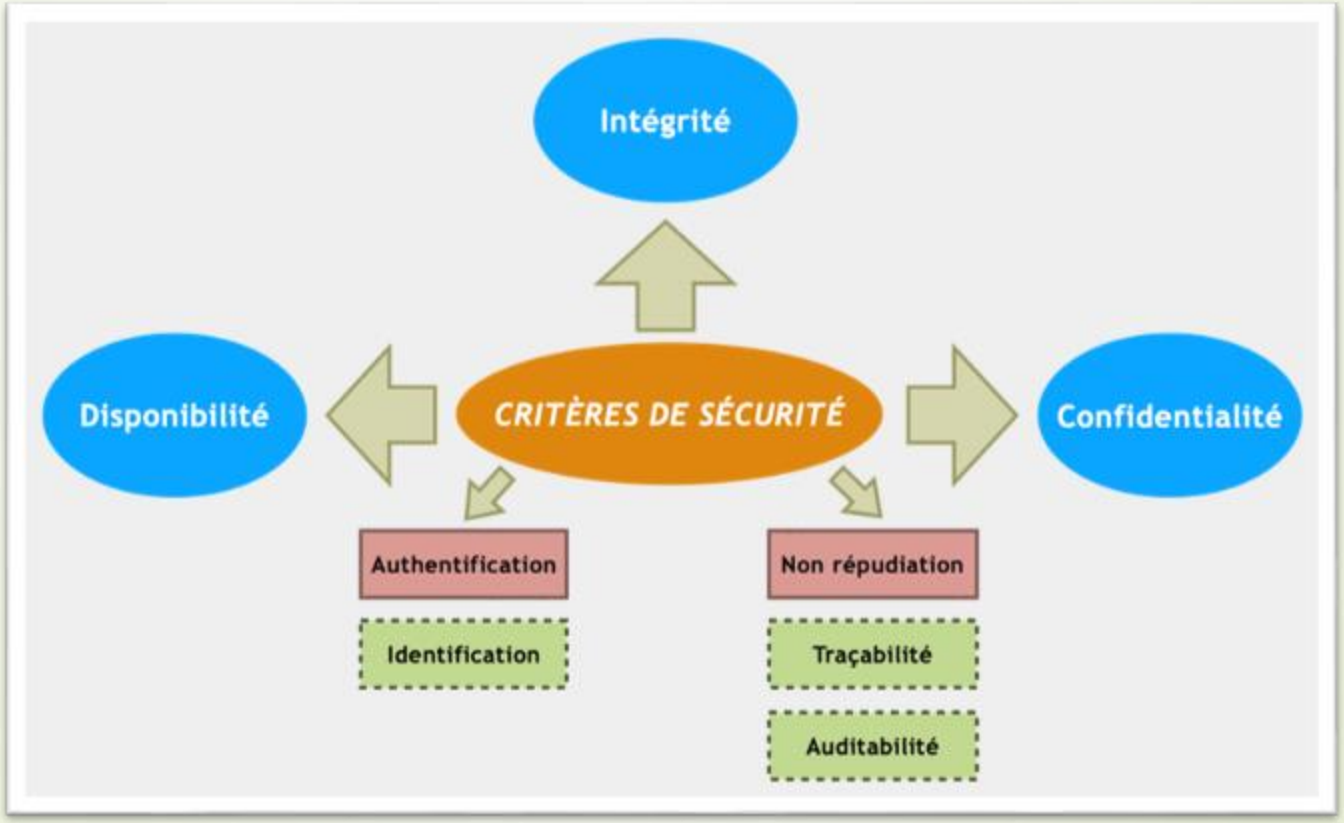
***L'intégrité** : Il s'agit de la garantie qu'un message n'a pas été altéré, de façon fortuite, illicite ou malveillante, au cours d'une transaction, entre le moment où il a été émis et le moment où il a été reçu. Pour assurer cette fonction, il existe des fonctions de hachage à sens unique qui permettent de calculer un haché d'une donnée.*

***La disponibilité** : L'objectif est de garantir l'accès à un service ou à une ressource à un instant précis, avec des temps de réponse attendus et de maintenir le bon fonctionnement de l'ensemble des services en production.*

*À ces trois piliers, nous pouvons bien entendu ajouter **la non-répudiation** et **l'imputabilité** qui sont des critères essentiels pour un système de gestion d'identité, qui nous amènent à généraliser ces deux aspects par leur finalité : **la traçabilité.***

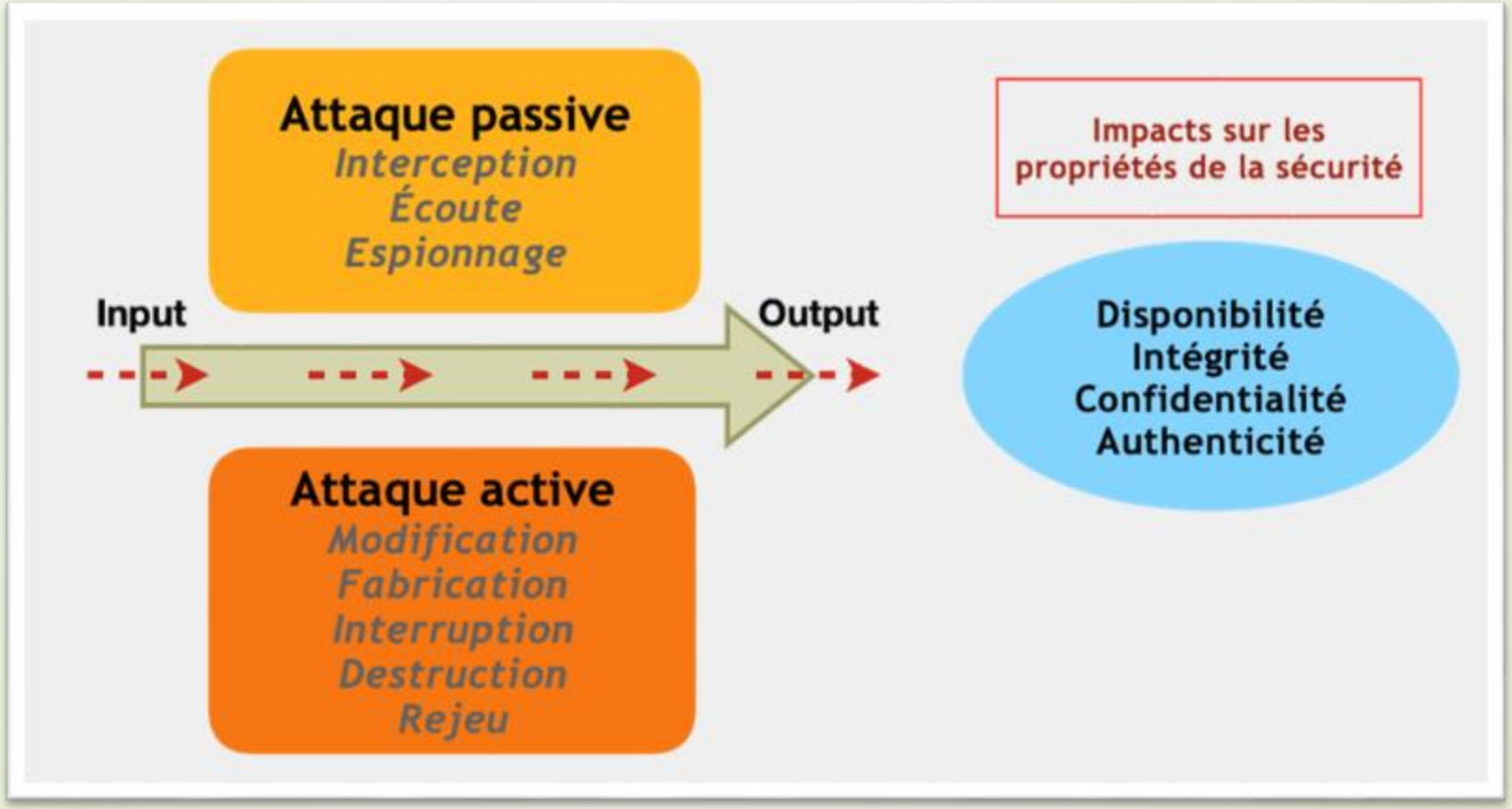
Contexte

Notre définition des critères de sécurité à appliquer à un système de gestion d'identités peut (et doit) être évalué sur ces quatre piliers :
***D**isponibilité. **C**onfidentialité. **I**ntégrité. **T**raçabilité.*



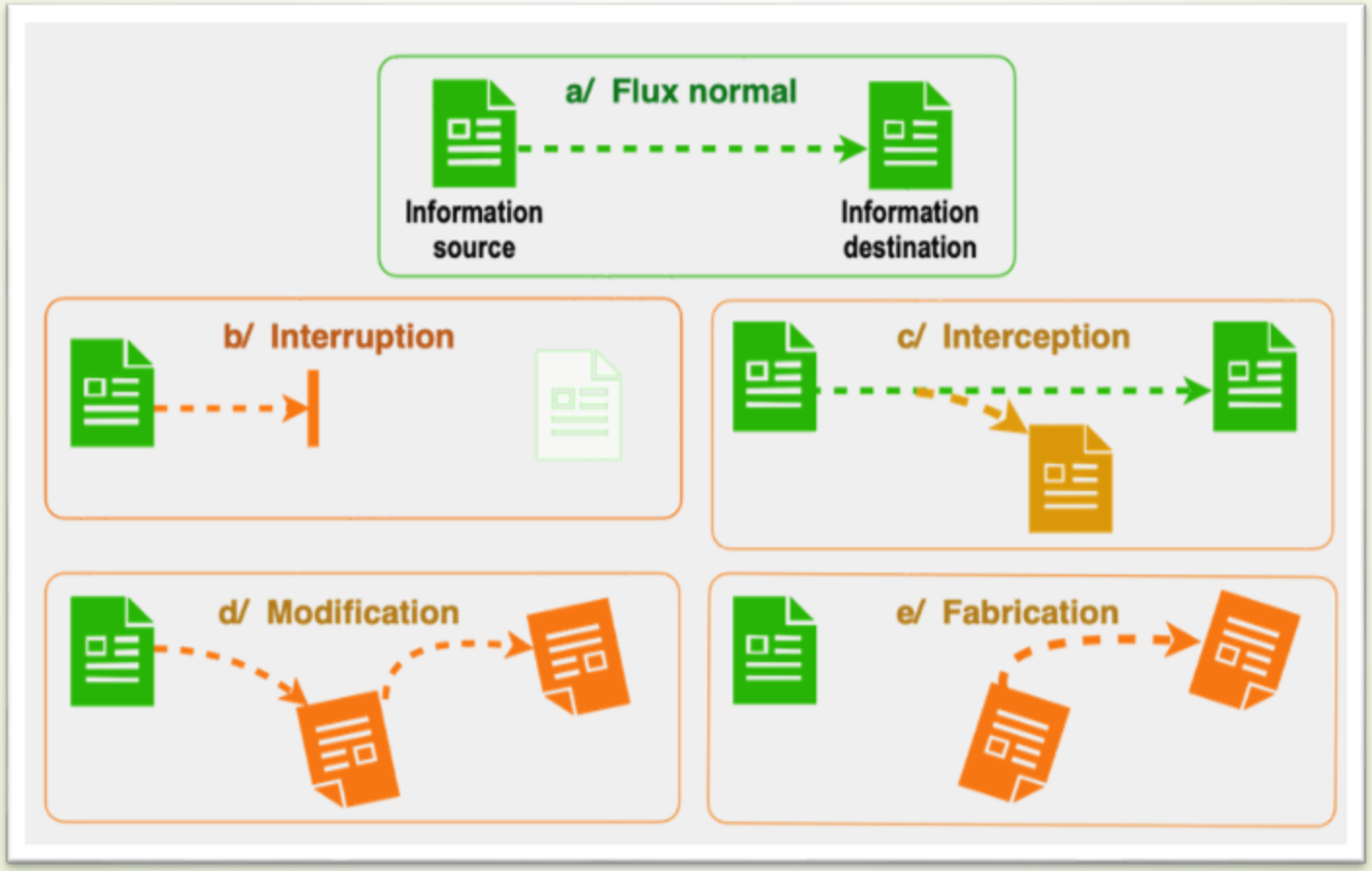
Contexte – Risques d'attaque

Une attaque consiste essentiellement à déjouer les mécanismes de sécurité d'un système d'information et à identifier les failles techniques et organisationnelles.



Contexte – Risques d'attaque

*Les attaques qui modifient les données sont dites **actives**, tandis que celles relevant de l'écoute sont dites **passives**.*



Contexte – Défauts de conception

Une méthode également très répandue pour d'attaquer, entre autres, aux systèmes de gestion d'identité est l'exploitation de failles de sécurité logicielles.

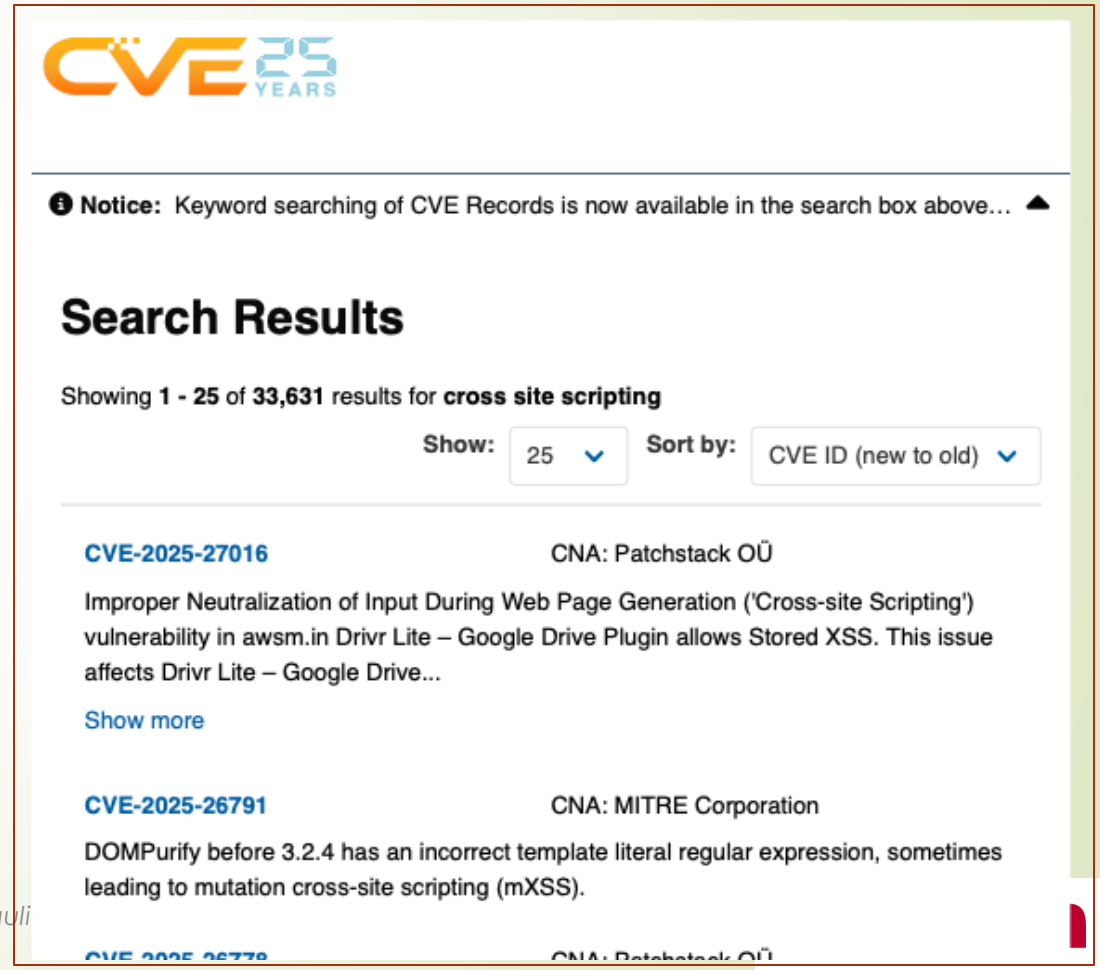
C'est ainsi qu'il est vivement conseillé d'intégrer à ses processus de sécurité une veille régulière des « CVE databases » (Common Vulnerabilities and Exposures).

CVE

Exemples de recherche :

Search CVE-2025-21401

Search Wazuh Server



Contexte – Défauts de conception - Exemple

*Prenons l'exemple de la faille « HeartBleed » d'OpenSSL qui signifie tout bonnement « Saignement du cœur » [**CVE**-2014-0160].*

En effet, il s'agit une vulnérabilité logicielle présente dans la bibliothèque de cryptographie open source OpenSSL à partir de mars 2012, qui permet à un « attaquant » de lire la mémoire d'un serveur ou d'un client (jusqu'à 64Ko de données) pour récupérer par exemple, les clés privées utilisées lors d'une communication avec le protocole Transport Layer Security (TLS).

Découverte en mars 2014 et rendue publique le 7 avril 2014, elle concerne de nombreux services Internet. Ainsi 17 % des serveurs web dits sécurisés, soit environ un demi-million de serveurs, auraient été touchés par la faille au moment de la découverte du bogue.

Notez que cette erreur est survenue au cours d'une correction d'un bug et d'améliorations de fonctionnalités d'OpenSSL dans un protocole "Heartbeat" (ce qui signifie battement de cœur).

Contexte – Répondre à ce risque

L'exploitation d'une vulnérabilité du système de gestion des identités fait peser un risque sur le processus métier d'une organisation, et des enjeux considérables sur leur système d'information, à la hauteur des habilitations allouées aux utilisateurs et des conséquences lourdes en cas d'usurpation d'identité.

Pour répondre aux exigences de sécurité, les contre-mesures à implémenter dans un système de gestion des identités consistent à mettre en place des mécanismes d'authentification robustes.

Nous parlerons ici d'utiliser des protocoles permettant de mettre en œuvre une ***authentification forte****, basés sur des* ***standards*** *et reposant sur des* ***modèles reconnus****.*

Ce besoin intervient à tous les niveaux, ici nous aborderons les solutions de protection d'accès aux réseaux : les ***NAC*** *(**N**etwork **A**ccess **C**ontrol).*

Standard 802.1x - Une réponse ?

- *802.1X est un standard lié à la sécurité des réseaux informatiques, mis au point en 2001 par l'IEEE*
- *Il permet de contrôler l'accès aux équipements d'infrastructures réseau (et par ce biais, de relayer les informations liées aux dispositifs d'identification).*

Principe :

- *En s'appuyant sur le protocole **EAP*** pour le transport des informations d'identification en mode client/serveur, et sur un serveur d'authentification (tel que RADIUS, TACACS, CAS, etc.) le déploiement de l'IEEE 802.1X fournit une couche de sécurité pour l'utilisation des réseaux câblés et sans fil.*
- *Si un équipement réseau actif, tel qu'un commutateur réseau ou une borne Wi-Fi est compatible avec la norme IEEE 802.1X, il est possible de contrôler l'accès à chacun de ses ports (PAE :* Port Access Entity*).*
- *Indépendamment du type de connexion, chaque port se comporte alors comme une bascule à deux états : un état contrôlé en cas de succès d'identification et un état non contrôlé.*

* *EAP, Extensible Authentication Protocol*

Standard 802.1x – EAP ?

Extensible Authentication Protocol *ou* ***EAP*** *est un protocole de communication réseau embarquant de multiples méthodes d'authentification, pouvant être utilisé sur les liaisons point à point, les réseaux filaires et les réseaux sans fil tels que les réseaux Wi-Fi.*

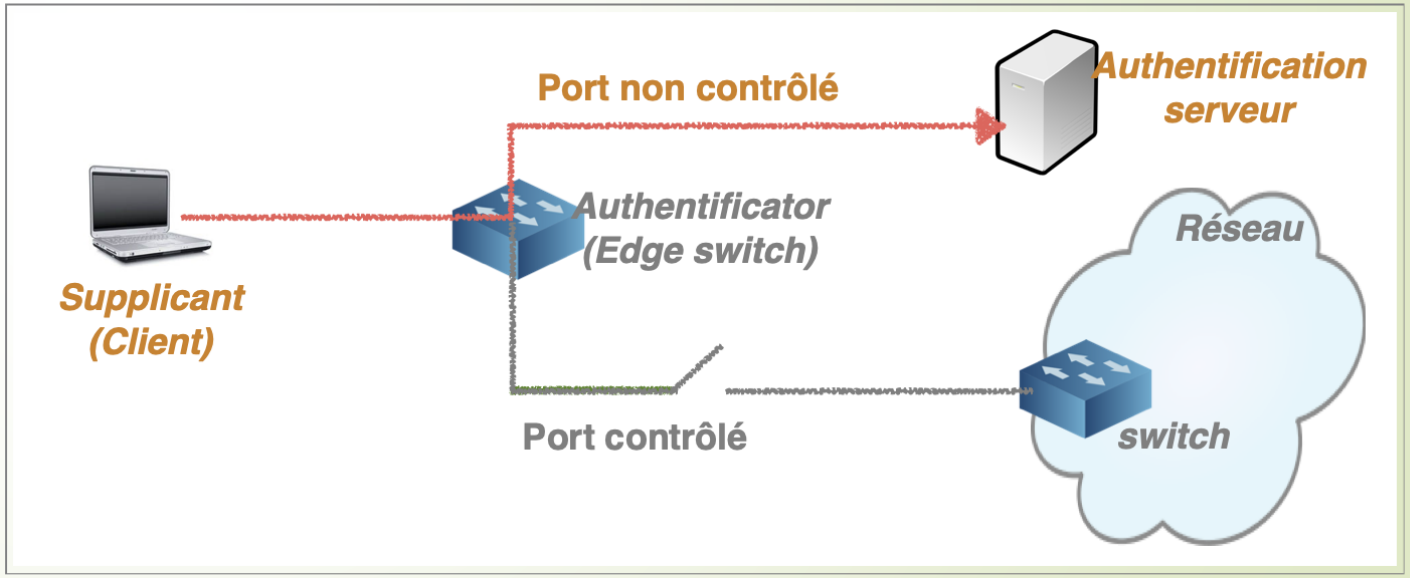
- *Le protocole EAP a été proposé en mars 1998 dans la RFC 2284 et proposé comme standard Internet auprès de l'IETF, initialement pour les connexions PPP afin d'autoriser ou interdire les accès à la couche réseau.*
- *En juin 2004, la RFC 3748 vient étendre le fonctionnement du protocole EAP aux réseaux définis dans le standard IEEE 802 :*
  - ***Réseaux filaires***
  - ***Réseaux Wi-Fi***
- *D'autres RFC ont été proposé pour EAP : RFC en octobre 2020 par exemple.*

Standard 802.1x – EAP ?

Trois acteurs principaux interviennent dans ce mécanisme :

- Le système à authentifier (supplicant ou client)
- Le point d'accès au réseau local (commutateur, borne Wi-Fi etc.)
- Le serveur d'authentification

Tant qu'il n'est pas authentifié, le client ne peut pas avoir accès au réseau, seuls les échanges liés au processus d'authentification sont relayés vers le serveur d'authentification par le point d'accès. Une fois authentifié, le point d'accès laisse passer le trafic lié au client.



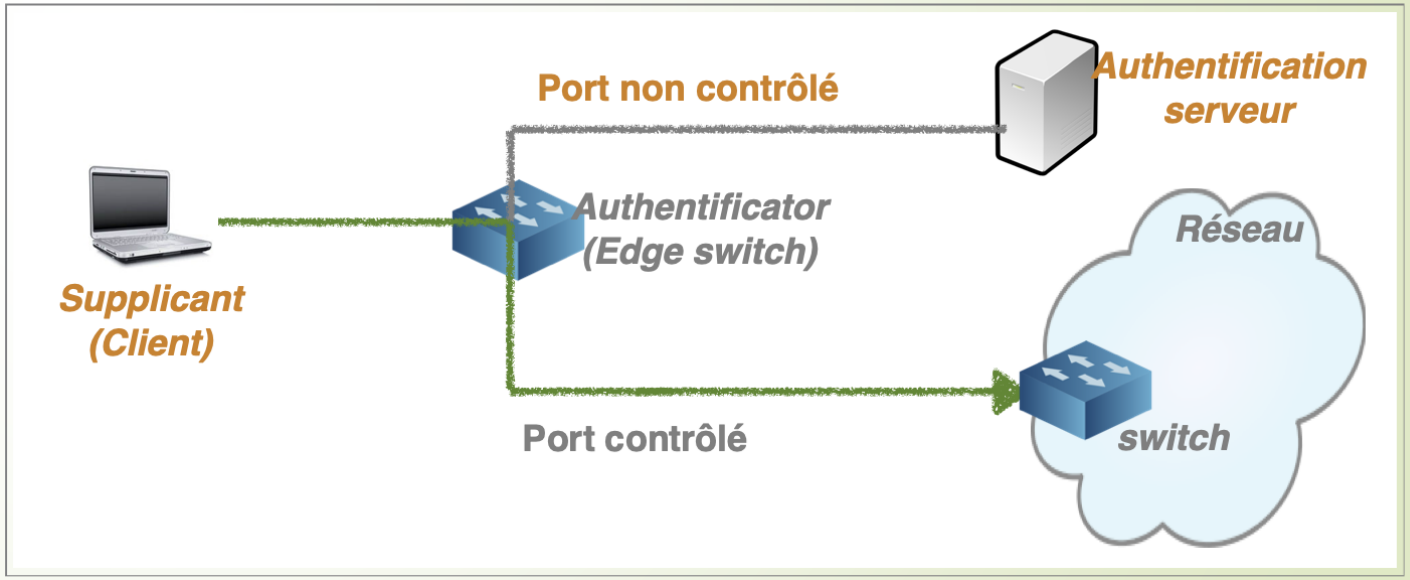
État : port non contrôlé

Standard 802.1x – EAP ?

Trois acteurs principaux interviennent dans ce mécanisme :

- Le système à authentifier (supplicant ou client)
- Le point d'accès au réseau local (commutateur, borne Wi-Fi etc.)
- Le serveur d'authentification

Tant qu'il n'est pas authentifié, le client ne peut pas avoir accès au réseau, seuls les échanges liés au processus d'authentification sont relayés vers le serveur d'authentification par le point d'accès. Une fois authentifié, le point d'accès laisse passer le trafic lié au client.



État : port contrôlé

AAA – Le concept

*L'**authentification** est un besoin bien défini aujourd'hui. Mais en parallèle de cette authentification, vient se greffer l'**autorisation**. Enfin, la notion d'**accounting** peut se rajouter aux deux précédentes.*

Ce sont les AAA ou triple A :

- **Authentication** (authentification)
- **Authorization** (autorisation)
- **Accounting** (rapports)

*Les protocoles de la triade **AAA** sont plébiscités par les opérateurs offrant des services de télécommunications à des utilisateurs. Ils peuvent ainsi facturer selon le temps de connexion ou selon la quantité d'information téléchargée.*

AAA – Le concept

AAA *est un modèle de sécurité implémenté dans certains routeurs Cisco mais que l'on peut également utiliser sur toute machine qui peut servir de NAS (Network Access Server), ou certains switches Alcatel.*

AAA est la base des protocoles de télécommunication ***Radius*** *et* ***Diameter*** *qui sont notamment utilisés dans les réseaux mobiles UMTS et LTE1 pour* ***authentifier et autoriser l'accès des terminaux mobiles au réseau****.*

Ils sont également présents dans de nombreuses solutions connues du marché, comme AWS IAM pour ne citer que lui.

AAA – Les implémentations

Plusieurs solutions existent sur le marché (propriétaires ou libres) supportant le protocole AAA, ici nous présenterons essentiellement les plus notables :

- **TACACS+ (*Terminal Access Controller Access-Control System Plus*) de CISCO.**

Il est le successeur de TACACS, initialement développé par IBM en 1984 pour assurer la communication distante des terminaux UNIX vers les serveurs d'authentification.

- **RADIUS (*Remote Authentication Dial-In User Service*)**

Initialement développé en 1991 par Livingston enterprise pour des serveurs d'accès au réseau pour du matériel uniquement équipé d'interfaces série ; il a fait ultérieurement l'objet d'une normalisation par l'IETF en juin 2000 dans deux RFC : RFC 2865 (RADIUS authentication) et RFC 2866 (RADIUS accounting).

- **Diameter**

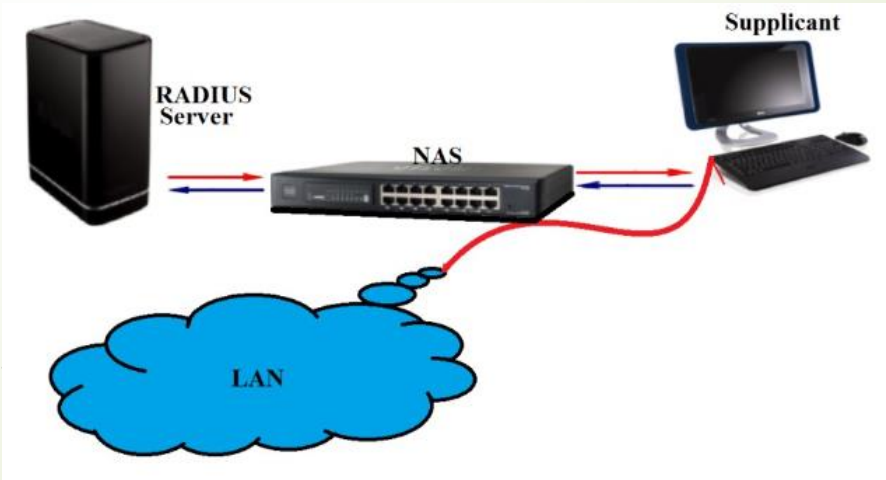
À l'origine, il est conçu pour faire de l'authentification, et succéder au protocole RADIUS (RFC 3588, étendu par RFC 5719, puis remplacés par RFC 6733).

Il est notamment utilisé dans le cœur des réseaux de téléphonie mobile 4G/LTE pour faire communiquer les différents équipements du cœur de réseau.

AAA – RADIUS : Architecture standard & Composants

Voici les composants principaux d'une architecture physique tripartie du standard RADIUS:

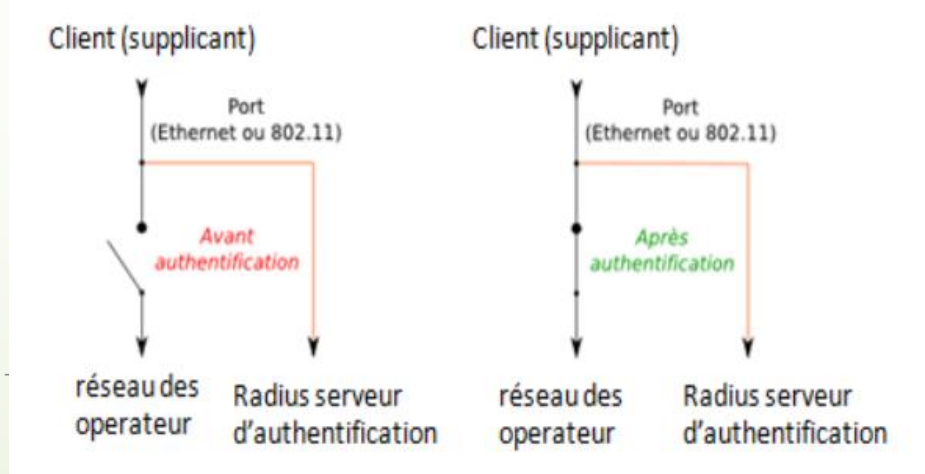
- **NAS** * **:** *équipement réseau appelé aussi client RADIUS, qui fait l'intermédiaire entre le serveur RADIUS et le terminal. Le NAS peut être une borne Wi-Fi ou un commutateur (Switch) qui implémente le protocole IEEE 802.1X et EAP, pour gérer les connexions et le transport des méthodes d'authentification.*
- **Supplicant** : *terminal de l'utilisateur*
- **RADIUS** : *serveur d'authentification. Ce dernier est généralement relié à une base d'identification (fichier, base de données, annuaire, etc.). Dans certains cas, le serveur RADIUS peut jouer le rôle d'un mandataire (proxy).*



* *NAS, Network Access Server*

AAA – RADIUS : Architecture standard & Composants

- *L'architecture logique de RADIUS se base sur le standard 802.1x, mis en place par l'IEEE en juin 2001 et le protocole EAP (Extensible Authentication Protocol).*
- *Le standard 802.1X permet de valider une autorisation d'accès à un réseau après authentification d'un Supplicant, indépendamment du réseau physique utilisé.*
- *Le NAS qui implémente le protocole 802.1X autorise en cas de succès l'accès physique au service réseau.*
- *En effet, les ports du NAS (Le commutateur dans la figure précédente) sont configurés d'une façon logique. Avant d'être complètement ouverts, ils ne laissent passer qu'un seul type de trafic particulier vers le serveur. Il contrôle une ressource disponible au niveau du port physique réseau, nommé PAE (Port Access Entity).*



AAA – RADIUS : Fonctionnement

Le fonctionnement de RADIUS est basé sur un scénario proche de celui-ci :

- *Un utilisateur envoie une requête au NAS afin d'autoriser une connexion à distance ;*
- *Le NAS achemine la demande au serveur RADIUS ;*
- *Le serveur RADIUS consulte la base de données d'identification afin de connaître le type de scénario d'identification demandé pour l'utilisateur. Soit le scénario actuel convient, soit une autre méthode d'identification est demandée à l'utilisateur. Le serveur RADIUS retourne ainsi une des trois réponses suivantes :*
  - ***ACCEPT** : l'identification a réussi ;*
  - ***REJECT** : l'identification a échoué ;*
  - ***CHALLENGE** : le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur et propose un « défi » (en anglais « challenge ») ;*
- *À la suite de cette phase dite d'authentification, débute une phase d'autorisation où le serveur retourne les autorisations de l'utilisateur.*

AAA – RADIUS : Intérêts

- *Permet d'authentifier les machines/utilisateurs pour l'accès au réseau local*
- *Utilisable en filaire et sans-fil*
- *Permet de placer les machines dans des sous-réseaux virtuels*
- *Plusieurs moyens d'authentification*
- *Initialiser les algorithmes de chiffrement des communications (WPA) : Les communications Wi-Fi peuvent être ainsi sécurisées*
- *Radius est un élément actif du réseau, pas seulement une base de données. Grâce aux modules ou attributs programmables.*
- *Interfaçage avec des logiciels de portails captifs*
- *Authentification distante par redirection de requêtes (proxy)*
- *Utilisable par d'autres types de serveurs (VPN)*

* WPA, Wi-Fi Protected Access

AAA – RADIUS : Limites

- *RADIUS a été conçu pour des identifications par modem, sur des liaisons lentes et peu sûres :*
  - *c'est la raison du choix du protocole UDP.*
  - *ce choix technique d'un protocole non agressif conduit à des échanges laborieux basés sur des temporisations de réémission, des échanges d'accusés-réceptions.*
  - *En conséquence, appliqué à nos réseaux actuels, il est amené à engendrer des lenteurs, voir des échecs de connexion.*
- *RADIUS base son identification sur le seul principe du couple user/mot de passe :*
  - *parfaitement adapté à l'époque (1996),*
  - *cette notion a dû être adaptée.*
  - *Exemple : pour l'identification des terminaux mobiles par leur numéro IMEI ou par leur numéro d'appel (Calling-Station-ID en Radius) sans mot de passe (alors que la RFC interdit le mot de passe vide !).*

AAA – RADIUS : Limites

- *RADIUS assure un transport en clair, seul le mot de passe est chiffré par hachage :*
  - *la sécurité toute relative du protocole repose sur le seul **secret partagé** et impose la sécurisation des échanges entre le client et le serveur par sécurité physique ou VPN.*
- *RADIUS limite les attributs :*
  - *gérés sous forme de chaîne "Pascal" avec un octet en entête donnant la longueur, à 255 octets, ce qui était cohérent avec la notion de nom/mot de passe,*
  - *mais inadapté à toute tentative d'introduction de la biométrie (fond d'œil, empreinte digitale) de cryptographie (certificat).*
- *RADIUS n'assure pas de mécanismes d'identification du serveur :*
  - *se faire passer pour un serveur est un excellent moyen de récolter des noms et mots de passe.*

*Tous ces points ont été pris en compte dans **Diameter**, qui permet ainsi de bénéficier d'un protocole d'authentification forte plus adapté aux évolutions du numérique.*

AAA – En bref !

AAA = **A**uthentication **A**uthorization **A**ccounting

- ***A**uthentication : Tu es qui ?*
- ***A**uthorization : Tu as le droit de faire quoi ?*
- ***A**ccounting : Qu'as-tu fait ?*