Chapitre 1 : L'authentification

Le contrôle d'accès consiste à définir les accès au réseau et les services disponibles après identification. Le terme AAA est souvent utilisé pour désigner les facettes suivantes de la sécurité :

- Authentification (Authentication) : il s'agit de la vérification de l'identité d'un utilisateur.
- Autorisation (Authorization) : il s'agit des droits accordés à un utilisateur, tels que l'accès à une partie d'un réseau, à des fichiers, le droit d'écriture, etc.
- Comptabilité (Accounting) : il s'agit des informations récoltées pendant toute la durée de la session, après identification de l'utilisateur.

1. Principe d'authentification

Un service d'authentification repose sur deux composantes :

- L'identification dont le rôle est de définir les identités des utilisateurs.
- L'authentification permettant de vérifier les identités présumées des utilisateurs. Lorsqu'il existe une seule preuve de l'identité (mot de passe par exemple) on parle d'authentification simple. Lorsque l'authentification nécessite plusieurs facteurs, on parle alors d'authentification forte.

L'authentification permet de vérifier l'identité d'un utilisateur sur une des bases suivantes :

- un élément d'information que l'utilisateur connaît (mot de passe, « passphrase », etc.) ;
- un élément que l'utilisateur possède (carte à puce, clé de stockage, certificat) ;
- une caractéristique physique propre à l'utilisateur, on parle alors de biométrie (fond de rétine, empreinte digitale, ADN, etc.).

L'authentification intervient à différents niveaux dans les couches de protocoles du modèle Internet :

- au niveau applicatif : HTTP, FTP ;
- au niveau transport : SSL, SSH ;
- au niveau réseau : IPSEC ;
- au niveau transmission : PAP, CHAP.

2. Single Sign-On

L'objet du Single Sign-On, noté SSO, est de centraliser l'authentification afin de permettre à l'utilisateur d'accéder à toutes les ressources (machines, systèmes, réseaux) auxquels il est autorisé d'accéder, en s'étant identifié une seule fois sur le réseau. L'objectif du SSO est ainsi de propager l'information d'authentification aux différents services du réseau, voire aux autres réseaux et d'éviter ainsi à l'utilisateur de multiples identifications par mot de passe.

Toute la difficulté de l'exercice réside dans le niveau de confiance entre les entités d'une part et la mise en place d'une procédure de propagation commune à toutes les entités à fédérer.

3. Protocole PAP

Le protocole PAP (Password Authentication Protocol) est, comme son nom l'indique, un protocole d'authentification par mot de passe. Le protocole PAP a été originalement utilisé dans le cadre du protocole PPP

Le principe du protocole PAP consiste à envoyer l'identifiant et le mot de passe en clair à travers le réseau. Si le mot de passe correspond, alors l'accès est autorisé.

Ainsi, le protocole PAP n'est utilisé en pratique qu'à travers un réseau sécurisé.

4. Protocole CHAP

Le protocole CHAP (Challenge Handshake Authentication Protocol), défini par la RFC 1994, est un protocole d'authentification basé sur la résolution d'un défi (challenge), c'est-à-dire une séquence à chiffrer avec une clé et la comparaison de la séquence chiffrée ainsi envoyée.

Les étapes du défi sont les suivantes :

- un nombre aléatoire de 16 bits est envoyé au client par le serveur d'authentification, ainsi qu'un compteur incrémenté à chaque envoi ;
- la machine distante « hache » ce nombre, le compteur ainsi que sa clé secrète (le mot de passe) avec l'algorithme de hachage MD5 et le renvoie sur le réseau ;
- le serveur d'authentification compare le résultat transmis par la machine distante avec le calcul effectué localement avec la clé secrète associée à l'utilisateur ;
- si les deux résultats sont égaux, alors l'identification réussit, sinon elle échoue.

Le protocole CHAP améliore le protocole PAP dans la mesure où le mot de passe n'est plus transmis en clair sur le réseau.

5. Protocole MS-CHAP

Microsoft a mis au point une version spécifique de CHAP, baptisée MS-CHAP (Microsoft Challenge Handshake Authentication Protocol version 1, noté parfois MS-CHAP-v1), améliorant globalement la sécurité.En effet, le protocole CHAP implique que l'ensemble des mots de passe des utilisateurs soient stockés en clair sur le serveur, ce qui constitue une vulnérabilité potentielle.

Ainsi MS-CHAP propose une fonction de hachage propriétaire permettant de stocker un hash intermédiaire du mot de passe sur le serveur. Lorsque la machine distante répond au défi, elle doit ainsi préalablement hacher le mot de passe à l'aide de l'algorithme propriétaire.

Le protocole MS-CHAP-v1 souffre malheureusement de failles de sécurité liées à des faiblesses de la fonction de hachage propriétaire.

5.1.MS-CHAP-v2

La version 2 du protocole MS-CHAP a été définie en janvier 2000 dans la RFC 2759. Cette nouvelle version du protocole définit une méthode dite « d'authentification mutuelle », permettant au serveur d'authentification et à la machine distante de vérifier leurs identités respectives. Le processus d'authentification mutuelle de MS-CHAP-v2 fonctionne de la manière suivante :

- Le serveur d'authentification envoie à l'utilisateur distant une demande de vérification composée d'un identifiant de session ainsi que d'une chaîne aléatoire.
- Le client distant répond avec :
  - son nom d'utilisateur,
  - un haché contenant la chaîne arbitraire fournie par le serveur d'authentification, l'identifiant de session ainsi que son mot de passe,

- une chaîne aléatoire.
- Le serveur d'authentification vérifie la réponse de l'utilisateur distant et renvoie à son tour les éléments suivants :
- la notification de succès ou d'échec de l'authentification,
- une réponse chiffrée sur la base de la chaîne aléatoire fournie par le client distant, la réponse chiffrée fournie et le mot de passe de l'utilisateur distant.
- Le client distant vérifie enfin à son tour la réponse et, en cas de réussite, établit la connexion.

Le protocole MS-CHAP-v2 a été cassé et des outils (chapcrack) de déchiffrement du mot de passe à partir d'écoute du réseau ont été rendus publics en 2012.

6. Protocole EAP

Le protocole EAP est une extension du protocole PPP, un protocole utilisé pour les connexions à Internet à distance (généralement via un modem RTC classique) et permettant notamment l'identification des utilisateurs sur le réseau. Contrairement à PPP, le protocole EAP permet d'utiliser différentes méthodes d'identification et son principe de fonctionnement rend très souple l'utilisation de différents systèmes d'authentification.

EAP possède plusieurs méthodes d'authentification, dont les plus connues sont : EAP-MD5 (Message Digest 5) ; EAP-PEAP ; EAP-TLS ; EAP-TTLS.

7. Protocole RADIUS

Le protocole RADIUS (Remote Authentication Dial-In User Service), mis au point initialement par Livingston, est un protocole d'authentification standard, défini par un certain nombre de RFC.

Le fonctionnement de RADIUS est basé sur un système client/serveur chargé de définir les accès d'utilisateurs distants à un réseau.

Il s'agit du protocole de prédilection des fournisseurs d'accès à Internet car il est relativement standard et propose des fonctionnalités de comptabilité permettant aux FAI de facturer précisément leurs clients.

Le protocole RADIUS repose principalement sur un serveur (le serveur RADIUS), relié à une base d'identification (base de données, annuaire LDAP, etc.) et un client RADIUS, appelé NAS (Network Access Server), faisant office d'intermédiaire entre l'utilisateur final et le serveur. L'ensemble des transactions entre le client RADIUS et le serveur RADIUS est chiffré et authentifié grâce à un secret partagé.

À savoir

Le serveur RADIUS peut faire office de proxy, c'est-à-dire transmettre les requêtes du client à d'autres serveurs RADIUS.

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.

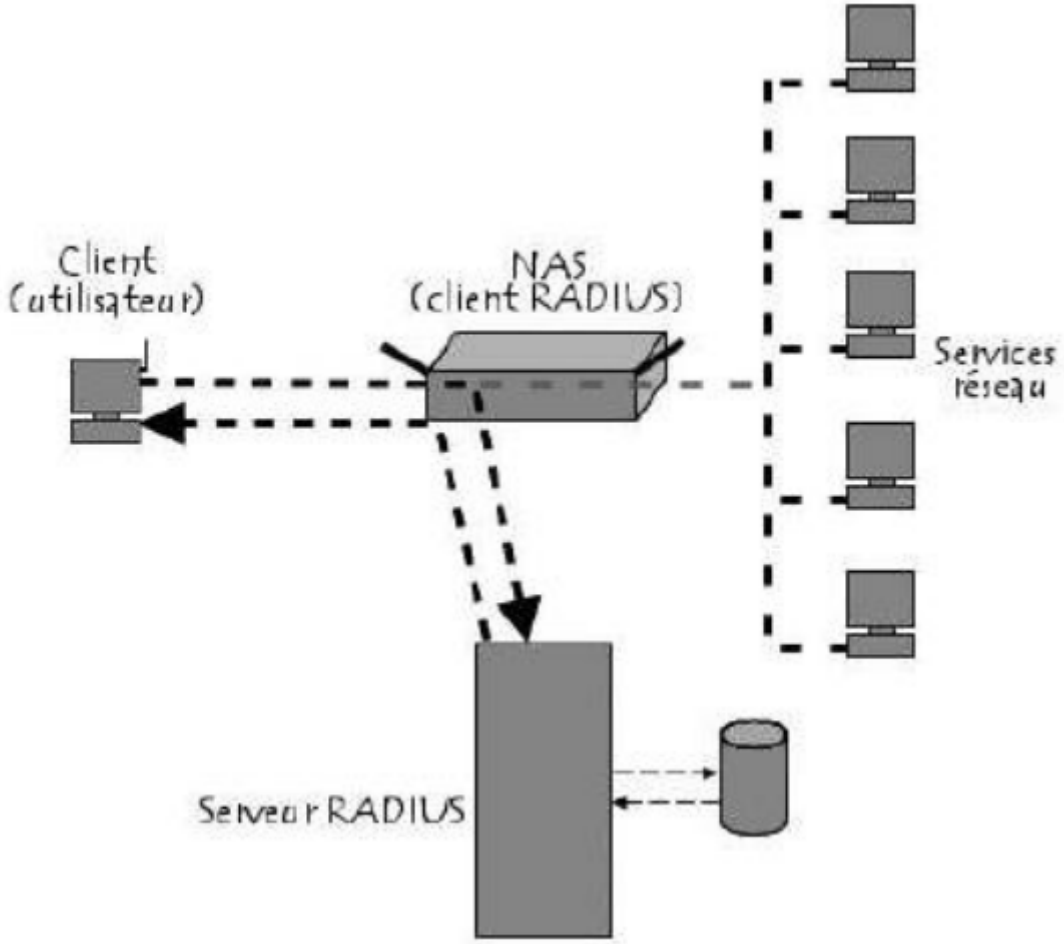
Soit le scénario actuel convient, soit une autre méthode d'identification est demandée à l'utilisateur.

Le serveur RADIUS retourne ainsi une des quatre réponses suivantes :

- ACCEPT : l'identification a réussi ;
- REJECT : l'identification a échoué ;
- CHALLENGE : le serveur RADIUS souhaite des informa-tions supplémentaires de la part de l'utilisateur et propose un défi (challenge) ;
- CHANGE PASSWORD : le serveur RADIUS demande à l'utilisateur un nouveau mot de passe.

À la suite de cette phase dite d'authentification, débute une phase d'autorisation où le serveur retourne les autorisations de l'utilisateur.

Le schéma suivant récapitule les éléments entrant en jeu dans un système utilisant un serveur RADIUS.



8. Protocole Kerberos

Le protocole Kerberos est issu du projet « Athena » du MIT, mené par Miller et Neuman. La version 5 du protocole Kerberos a été normalisée par l'IETF dans les RFC 1510 (septembre 1993) et 1964 (juin 1996). Le nom « Kerberos » provient de la mythologie grecque et correspond au nom du chien (en français « Cerbère ») protégeant l'accès aux portes d'Hadès.

L'objet de Kerberos est la mise en place de serveurs d'authentification (AS, Authentication Server), permettant d'identifier des utilisateurs distants, et des serveurs de délivrement de tickets de service (TGS, Ticket Granting System), permettant de les autoriser à accéder à des services réseau. Les clients peuvent aussi bien être des utilisateurs que des machines. La plupart du temps, les deux types de services sont regroupés sur un même serveur, appelé centre de distribution des clés (KDC, Key Distribution Center).

8.1.Principe de fonctionnement

Le protocole Kerberos repose sur un système de cryptographie à base de clés secrètes (clés symétriques ou clés privées), avec l'algorithme DES. Kerberos partage avec chaque client du réseau une clé secrète faisant office de preuve d'identité. Le principe de fonctionnement de Kerberos repose sur la notion de tickets :

- Afin d'obtenir l'autorisation d'accès à un service, un utilisateur distant doit envoyer son identifiant au serveur d'authentification.
- Le serveur d'authentification vérifie que l'identifiant existe et envoie un ticket initial au client distant, chiffré avec la clé associée au client.

Le ticket initial contient :

- une clé de session, faisant office de mot de passe temporaire pour chiffrer les communications suivantes ;
- un ticket d'accès au service de délivrement de ticket.

- Le client distant déchiffre le ticket initial avec sa clé et obtient ainsi un ticket et une clé de session.

Grâce à son ticket et sa clé de session, le client distant peut envoyer une requête chiffrée au service de délivrement de ticket, afin de demander l'accès à un service. Par ailleurs, Kerberos propose un système d'authentification mutuelle permettant au client et au serveur de s'identifier réciproquement. L'authentification proposée par le serveur Kerberos a une durée limitée dans le temps, ce qui permet d'éviter à un pirate de continuer d'avoir accès aux ressources : on parle ainsi d'antirejeu.