Nomadisme réseau pour la communauté enseignement supérieur-recherche, projet ARREDU

Christian Claveleira
Comité Réseau des Universités
christian.claveleira@cru.fr

Vincent Carpier
Comité Réseau des Universités
vincent.carpier@cru.fr

Résumé

Si dans notre vie professionnelle quotidienne et, de plus en plus, à notre domicile, l'accès à des services réseau est devenu aussi banal qu'indispensable, on aimerait retrouver ces mêmes services au cours de déplacements chez des collègues plus ou moins lointains. Si l'accès physique aux réseaux d'établissement se simplifie avec la mise en place de réseaux sans fil de type 802.11x, il doit en même temps être soigneusement contrôlé par leurs propriétaires pour en maîtriser l'usage.
L'idéal serait de trouver sur tous les sites des établissements de notre communauté des accès réseau accessibles avec le même identifiant et le même protocole d'authentification que sur son lieu de travail.
C'est le but du projet ARREDU (Authentification Répartie Recherche EDUcation) et, plus largement, de son pendant européen le projet eduroam.
Il s'agit d'établir un réseau de confiance, basé sur le protocole RADIUS, permettant à n'importe quel membre d'une des institutions participantes de pouvoir s'authentifier sur le réseau de n'importe quelle autre pour obtenir une connectivité IP.

Après la présentation des technologies mises en oeuvre (802.1x, EAP, RADIUS,...) et celle du projet européen eduroam auquel participe ARREDU, le concept de relations de confiance, les aspects organisationnels et les problèmes de sécurité seront développés. Un coup d'oeil critique et prospectif conclura cette présentation.

Mots clefs

Nomadisme, RADIUS, 802.1x, EAP, Wi-Fi, ARREDU, eduroam

1 Introduction

Avec la démocratisation des accès sans fil dits Wi-Fi, qui n'a pas envie d'avoir, en déplacement professionnel, un accès à l'Internet dans des conditions aussi proches que possibles de celles de son lieu de travail ?

Mais quel administrateur de réseau d'établissement a envie d'offrir des accès anonymes ou d'ouvrir et fermer des comptes utilisateurs au gré des passages de visiteurs ?

Le projet ARREDU a pour ambition de permettre aux utilisateurs nomades de la communauté enseignement supérieur-recherche française d'utiliser les infrastructures réseau des établissements où ils sont de passage sans induire d'administration supplémentaire ni d'ouverture d'accès anonymes. Son intégration dans le projet *eduroam* permettra d'élargir cette possibilité aux établissements raccordés aux réseaux académiques européens. Les protocoles RADIUS, 802.1x et EAP sont les solution techniques retenues dans ces projets.

Cependant, la technologie actuelle pose un problème de sécurité car, sans précautions particulières, un réseau sans fil est très vulnérable, malgré le mécanisme initialement conçu pour y pallier : le WEP .

Pour assurer un bon niveau de sécurité et de service, des méthodes d'authentification sécurisées doivent être utilisées (TTLS, TLS, PEAP, basées sur EAP), les liaisons sans-fil doivent être chiffrées de façon fiable et des relations de confiance instaurées entre les participants au projet.

2 Les technologies au service du nomadisme

2.1 Généralités sur les accès sans fil de type 802.11

Communément appelée Wi-Fi, la norme 802.11 est une certification commerciale. Pour offrir un accès à un réseau sans fil, le seul mécanisme obligatoire pour le fonctionnement est le SSID (Service Set ID). Il n'est aucunement question de sécurité avec ce mécanisme et il faudra donc mettre en place au minimum le cryptage WEP « Wired Equivalent Privacy » pour les données en transit via le lien sans fil. Nous verrons plus loin que ce mécanisme est peu fiable pour la confidentialité, l'authentification, l'intégrité. Il tend à être remplacé par le protocole WPA « *Wi-Fi Protected Access* ».

2.2 RADIUS (*Remote Access Dial-In User Service*)

Introduction

Le protocole RADIUS est un protocole d'Authentification, d'Autorisation et d'Accounting (AAA), chargé de contrôler les accès d'un utilisateur au réseau.

L'origine du protocole RADIUS est l'authentification des utilisateurs vis à vis des fournisseurs d'accès à l'Internet (utilisant des connexions RTC). Il supporte nativement l'authentification PAP et CHAP via PPP et utilise désormais le port 1812/UDP (RADIUS), qui a remplacé le port initial 1645, et 1813/UDP pour l'accounting (radacct).

Voici la structure d'un paquet de données RADIUS :

Figure 2 : *Structure d'un paquet de données RADIUS*

La distinction du type de donnée est faite via le premier champ de l'entête du paquet (Code). Voici les neuf codes valides, dont quatre (en gras) servent à la phase d'authentification et d'autorisation :

- **1 Access-Request**
- **2 Access-Accept**
- **3 Access-Reject**
- 4 Accounting-Request
- 5 Accounting-Response
- **11 Access-Challenge**
- 12 Status-Server
- 13 Status-Client
- 255 Reserved

La section « *"authenticator"* » sert à contrôler l'intégrité du message. Ce champ est utilisé avec le secret partagé RADIUS pour chiffrer les mots de passe. Il y a deux types de valeurs, « *request* » et « *response* ». Les « *request-authenticator* » sont utilisées avec les paquets *Access-Request* et *Accounting-request*, tandis que les « *response-authenticator* » le sont avec les paquets *Access-Accept, Access-Reject* et *Access-Challenge*.

Principe de fonctionnement

Le déroulement d'une authentification à l'aide de RADIUS est assez simple :

- Le client (*supplicant*) désirant obtenir une connexion réseau envoie une requête au « NAS » (*Network Access Server*), une borne d'accès dans le cas du Wi-Fi ;
- Le NAS achemine la demande au serveur RADIUS ;
- le serveur RADIUS est responsable de l'authentification de l'utilisateur. Suivant le protocole d'authentification défini par les administrateurs, soit toutes les informations nécessaires sont transmises, soit un complément d'information est demandé. Ensuite, le serveur RADIUS interroge la base de données des utilisateurs pour autoriser ou non l'accès au réseau.

proxy et domaine *("realm")*

Nous avons vu comment authentifier un utilisateur lorsqu'il désire se connecter à son réseau d'établissement de rattachement. Nous allons maintenant nous intéresser aux utilisateurs nomades.

Il faut trouver un moyen d'authentifier ces personnes sur des réseaux extérieurs en utilisant la base de données des utilisateurs de l'établissement de rattachement, ceci afin de ne pas devoir dupliquer « à l'infini » cette base.

Pour ces nomades, la mise en place de domaine (*"realm"*) est nécessaire. La syntaxe locale d'identification de l'utilisateur « *login* » devient « login@domaine ». L'information « domaine » va permettre de router la demande d'authentification vers le serveur RADIUS de l'établissement de rattachement de l'utilisateur.

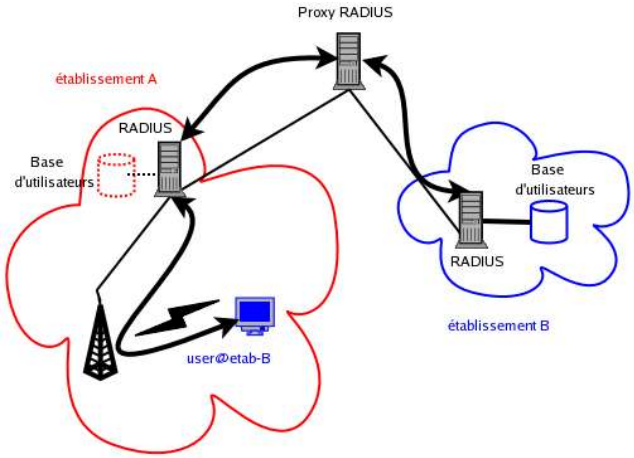

Figure 3 : *Echange des données avec la fonction proxy-RADIUS*

Pour mettre en place une telle infrastructure d'authentification, il faut déployer un ou plusieurs *proxy*. Le principe de fonctionnement est là aussi assez simple. Voici le déroulement d'une phase d'authentification d'un utilisateur de l'établissement A sur le réseau de l'établissement B :

- Le client désirant un accès au réseau d'un établissement visité contacte le NAS via le SSID diffusé ;
- Le NAS (une borne sans fil dans le cas de la figure 4) transmet la requête au serveur d'authentification local ;
- Ce dernier, à l'aide de la valeur du domaine (*"realm"*) fourni par l'utilisateur, va relayer la requête au *proxy* immédiatement supérieur ;
- Si besoin , ce *proxy* contactera également un autre *proxy*, sinon, c'est qu'il connaît le serveur RADIUS de l'établissement d'origine de cet utilisateur. Dans ce cas, il lui transmet la demande d'authentification.

- Le serveur RADIUS de l'établissement de rattachement va répondre à cette demande en suivant le même parcours.

Ce mode de fonctionnement permet l'authentification d'une personne nomade, en s'appuyant sur la base de données de son établissement d'origine. Les échanges entre les différents serveurs RADIUS et *proxy*-RADIUS sont protégés par des secrets partagés différents. Toutes ces connexions constituent un cercle de confiance.

Interfaçage avec la base de données des utilisateurs

Les différents serveurs RADIUS sont conçus pour interroger des bases d'utilisateurs de toutes sortes (LDAP, SQL, Fichiers ...). Le choix du serveur RADIUS peut être influencé par l'existence du connecteur avec votre type de base de données.

Sécurité

Les demandes d'authentification viennent du NAS (*routeur, serveur vpn, point d'accès, etc ...*), qui interroge le serveur RADIUS. Ces échanges entre le NAS et le serveur RADIUS sont protégés par un secret partagé. Pour sécuriser tous les échanges, il reste à sécuriser le lien entre le serveur RADIUS et la base de données des utilisateurs, par la mise en oeuvre de SASL, SSL/TLS, IPSec...

2.3 EAP : Extensible Authentification Protocol

Le but du protocole EAP est l'authentification d'un utilisateur sur un réseau non ouvert (obligation d'authentification). Dans un premier temps seul le trafic EAP est autorisé. La demande d'authentification se fait soit à l'initiative du client (*supplicant*) soit du point d'accès (*authenticator*). Les différentes méthodes d'authentification (OTP, TLS, SIM, AKA, PEAP, TLS, TTLS ...) utilisent ce protocole pour véhiculer leurs informations, y compris la clé WEP lorsque celle ci est utilisée. Dans un deuxième temps, en fonction de la réussite ou non de l'authentification le NAS laissera passer tout le trafic.

Déployé initialement sur les réseaux filaires, le protocole EAP est la pierre angulaire de la sécurisation des réseaux sans fil. Le seul point faible de ce protocole est sa vulnérabilité face aux attaques par déni de service.

2.4 Authentification : IEEE 802.1x

Le standard 802.1x définit les techniques d'encapsulation utilisées pour transporter les paquets EAP entre le client et le NAS (« *Network Access Server* »). Cette encapsulation est appelé *EAPoL* (« *EAP over LAN* »). Nous détaillerons plus loin le protocole EAP.

C'est la mise en place de 802.1x (et donc EAP) qui permet de mettre en place des solutions de sécurisation accrue telles que WPA et 802.11i.

Ce protocole d'authentification permet de bloquer le flux de données d'un utilisateur non authentifié, à l'exception du protocole EAP. Le NAS se comporte alors comme un interrupteur à deux positions, ouvert ou fermé. Dans le cas d'un réseau Wi-Fi, ce blocage est effectué par la borne d'accès elle même.

L'architecture 802.1x met en jeu trois entités fonctionnelles :

- le client 802.1x (*supplicant*) : la machine qui veut utiliser le réseau ;
- l'*"authenticator"* : il dispose de deux ports : autorisé et non autorisé. Tant que l'utilisateur n'est pas correctement authentifié, le trafic est bloqué, à l'exception du protocole EAP ;
- le serveur d'authentification : c'est la machine faisant fonctionner le processus responsable de l'authentification de l'utilisateur, généralement un serveur RADIUS (décrit plus loin dans cet article).

Le schéma ci-dessous décrit le déroulement d'une session d'authentification et les protocoles utilisés après authentification entre, d'un coté, le client 802.1x et la borne d'accès et, de l'autre coté, la borne et le serveur d'authentification (ici un serveur RADIUS) :

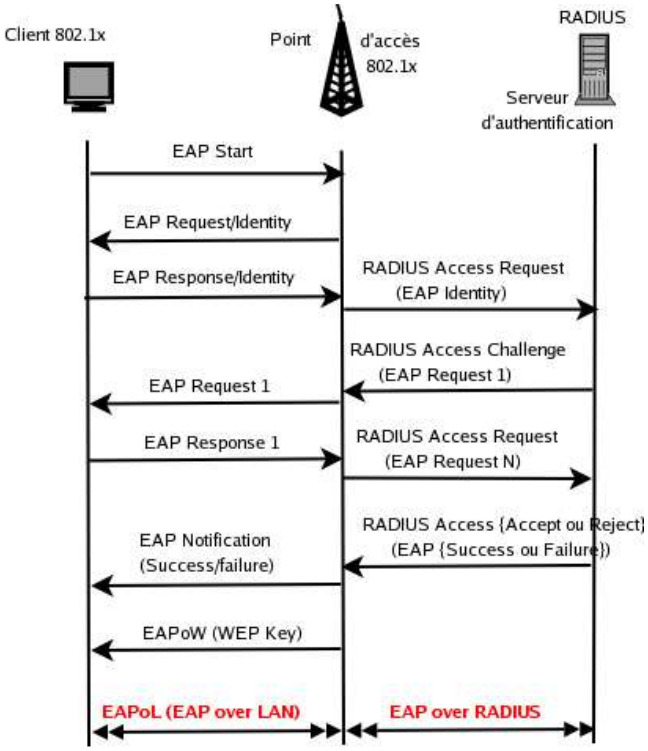

Figure 1 : D*iagramme de séquence d'une authentification 802.1x*

2.5 Sécurisation IEEE 802.11i

Les normes 802.11 et 802.1x ayant été conçues indépendamment, deux types d'attaques sont apparues possibles : « *MIM* » (*Man In the Middle*) et « *Hijacking* » (détournement de session).

L'attaque « *MIM* » exploite le fait que l'authentification cliente n'est pas mutuelle , une usurpation d'adresse client

permet de contourner les mécanismes d'authentification. L'attaque « *Hijacking* » (détournement de session) tire profit d'une faille de synchronisation dû aux manques d'authentification des trames de gestion.

A la mise en lumière de ces faiblesses du WEP, un groupe de travail de l'IEEE, a débuté en 2002 les travaux de la future norme 802.11i. Cette norme tardant à être finalisée, la « Wi-Fi Alliance » a publié une version allégée de 802.11i appellée WPA. Ce protocole, regroupant l'authentification 802.1x et TKIP, utilise la cryptologie RC4. Il introduit l'utilisation de clé dynamique et une ré-authentification périodique qui a grandement amélioré la sécurité. Le matériel d'ancienne génération (norme a et b) est compatible, moyennant une mise à jour du *firmware*.

En 2004, la « *Wi-Fi Alliance »* complète le WPA avec la solution WPA2. Contrairement à la mise en oeuvre de la norme WPA, le matériel ne supportant pas la norme 802.11g ne peut pas mettre en oeuvre cette méthode de cryptologie, même avec un *upgrade* de *firmware*. En effet, le remplacement de la cryptologie RC4 par CCMP, qui utilise le chiffrement AES, ne peut fonctionner que s'il est nativement implémenté dans le NAS. Ceci est un frein à la mise en place de WPA2 pour les établissements ayant déjà déployé de nombreuses bornes d'accès de type 802.11a et/ou 802.11b.

Le fait que, dans cette dernière norme WPA2, chaque point d'accès joue le rôle d'un *"authenticator"* partageant un secret partagé avec le serveur RADIUS, assure l'intégrité, la confidentialité et l'authentification mutuelle. Cette technique est à ce jour la méthode de communication sans fil la plus sécurisée.

2.6 Méthodes d'authentification liées à EAP

Nous allons présenter brièvement les principales procédures d'authentification couramment utilisées via EAP.

EAP-LEAP Lightweight Extensible Authentication Protocol

C'est la première méthode proposé par Cisco, pour Windows. On calcule une empreinte MD4 issue du mot de passe + 5 octets nuls, on obtient 21 octets que l'on interprète sous la forme d'un 3DES. On chiffre un nombre aléatoire que l'on combine à la clef 3DES, le tout est utilisé pour une double authentification, de type CHAP, entre le *supplicant* et le serveur d'authentification, puis entre le serveur d'authentification et le point d'accès.

Cette méthode est fragile face à des attaques par dictionnaire sur mots de passe faibles.

EAP -PEAP Protected Extensible Authentication Protocol

Ce protocole est né d'une alliance entre Microsoft, Cisco et RSA.

Le processus d'authentification de PEAP consiste à établir un tunnel sécurisé TLS entre le client et le serveur d'authentification, en authentifiant le serveur RADIUS à l'aide d'un certificat. Ensuite, il est possible de choisir entre la méthode MS-CHAP(v2) ou TLS pour authentifier l'utilisateur. Quand la méthode PEAP est utilisée c'est souvent pour éviter d'utiliser les certificats client, il est donc logique que sur les deux méthodes proposées par PEAP, l'utilisation de login/password, via MS-CHAP, soit largement privilégiée.

EAP-TTLS Tunneled Transport Layer Security

Comme dans le cas de PEAP, la première phase est la création d'un canal TLS sécurisé entre le client et le serveur d'authentification. Ici l'utilisateur n'est pas authentifié par un certificat, il devra donc fournir un login/password.

Ce protocole d'authentification mutuelle très robuste n'oblige pas le déploiement de certificats client. Comme PEAP, TTLS utilise la cryptographie de TLS, mais utilise d'autres méthodes pour l'authentification de l'usager.

EAP-TLS (Transport Layer Security)

Dans le cas de la méthode EAP-TLS des certificats X509 sont utilisés pour l'authentification mutuelle du serveur RADIUS et de l'utilisateur. Il est donc nécessaire de déployer des certificats pour tous les utilisateurs de cette méthode.

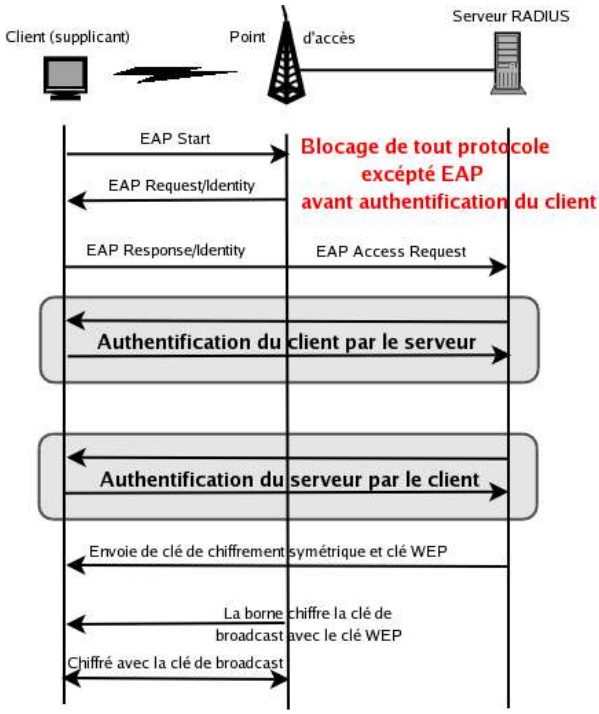

Figure 4 : *Authentification EAP-TLS*

Cette méthode est considérée comme la plus sécurisée et la plus robuste.
Le point faible de cette méthode est la protection de la clé privée, chiffrée par un mot de passe, qu'il est possible de sécuriser encore plus par la mise en place de carte à puce.

EAP-FAST Flexible Authentification via Secure Tunneling

Proposé initialement par Cisco à l'IETF pour remplacer LEAP, elle vise à résoudre le problème de sécurité sur les attaques par dictionnaire concernant les mots de passe faibles. Ce protocole est intégré dans tous les produits Aironet de Cisco, ainsi que dans le serveur VPN « Cisco Secure ACS ».

Ce protocole authentifie le serveur à l'aide d'un certificat et, comme PEAP et EAP-TTLS, il authentifie le client en utilisant un couple login/password à travers un tunnel TLS.

Cette méthode a été conçue pour accélérer la ré-authentification d'un client qui passe d'une borne d'accès à une autre.

En effet TLS et PEAP requièrent de nombreux échanges pour récupérer toutes les informations nécessaires à l'authentification, ce qui peut prendre plusieurs secondes. Ceci peut être gênant dans l'utilisation de quelques services comme la voix sur IP. EAP-FAST utilise une clé partagée pour accélérer la ré-authentification 802.1X.

EAP-SIM Subscriber Identity Module

Protocole d'authentification utilisé pour compléter l'authentification des réseaux GSM dans les « *hotspots* » ou dans les zones à très forte densité de population. Les opérateurs de téléphonie peuvent utiliser cette méthode afin de proposer à leurs clients des connexions Wi-Fi et assurer aisément la facturation.

3 Eduroam

3.1 Introduction

En 2003 TERENA créa la « Task Force on Mobility » pour étudier les problèmes de sécurité liés aux réseaux sans fil et élaborer des recommandations pour mettre en place une solution internationale de nomadisme pour les utilisateurs des réseaux académiques de recherche (NREN). Cette solution devait leur permettre d'avoir un accès Internet sécurisé (avec ou sans fil) sur les campus des organismes académiques. Cette infrastructure a été appelée **eduroam** (pour Education Roaming).

3.2 Les buts

Offrir, aux utilisateurs nomades, des accès à l'Internet

- faciles et contrôlés,
- n'engendrant qu'un surcroît d'administration minimal pour les gestionnaires de réseaux,
- avec un niveau de sécurité comparable au réseau filaire,
- facilement déployable à grande échelle.

Trois solutions ont été étudiées :

- L'authentification Web avec *backend* RADIUS (Finlande) ;
- L'authentification via VPN (Allemagne, Suisse) ;
- L'authentification via 802.1x avec *backend* RADIUS (Pays bas).

Synthèse des caractéristiques de chacune :

- L'authentification Web avec *backend* RADIUS est facile à déployer à grande échelle, déjà utilisée mais pose des problèmes de sécurité ;
- VPN : méthode sûre, déjà déployée mais se prête mal à un déploiement à grande échelle ;
- Authentification basée sur 802.1x : sûre, facile à déployer à grande échelle, nouvelle (à l'époque).

Conclusion : comme WPA et 802.11i restent compatibles avec 802.1x, cette dernière solution, associée à une infrastructure RADIUS, a été retenue.

Une expérience de mise en oeuvre de mobilité inter-NREN a été entreprise et a évolué en un pilote trans-européen, appelé **eduroam**. Il met en oeuvre une hiérarchie de serveurs/*proxies* RADIUS dont le serveur racine est géré par TERENA.

3.3 État actuel

Au début de l'été 2005 18 pays, dont l'Australie, étaient raccordés, rassemblant plus de 350 établissements et organismes.

Figure 6 : *Carte des pays participants à* **eduroam** *(en vert ou foncé)*

Les rattachements se font par NREN représentant un pays après signature d'agrément avec TERENA.

4 ARREDU (Authentification Répartie Recherche ÉDUcation)

En 2004 des opérations d'incitation au déploiement de réseaux sans fil dans les universités sont lancées en parallèle de l'opération Micro Portable Étudiant. Ces opérations sont renouvelées en 2005 et accroissent d'autant l'intérêt d'accéder au réseau de façon fiable et simple.

Démarré fin 2004, le projet ARREDU a donc pour but de mettre en place une infrastructure d'authentification répartie basée sur le protocole RADIUS, entre les établissements de recherche et/ou d'enseignement supérieur raccordés à *RENATER*.

Cette infrastructure est appelée à s'intégrer au projet *eduroam* et à permettre d'offrir des accès réseau aux personnels (et, éventuellement, étudiants) des établissements participants en déplacement sur le site d'un autre participant. Ceci en utilisant leurs identifiants et mots de passe habituels avec une sécurité comparable à celle d'un accès filaire sur leur propre réseau.

Type d'accès visés : ce sont en priorité les accès sans fil dits Wi-Fi mais cela peut également s'appliquer aux accès filaires de type Ethernet.

Méthode d'authentification : via 802.1x/EAP/RADIUS

Architecture :

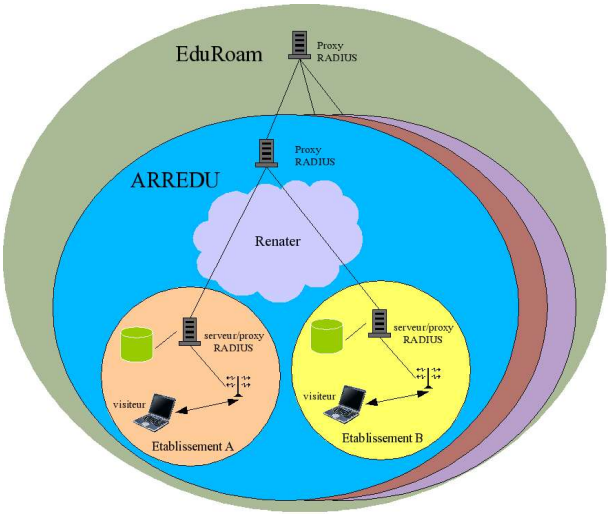

Figure 7 : *Architecture d'ARREDU, raccordement à eduroam*

Chaque établissement raccorde son ou ses serveurs RADIUS au serveur *proxy* national à qui il délègue toute demande d'authentification qui n'est pas de son ressort. Le serveur national remonte au serveur européen toutes les demandes ne concernant aucun des établissements français. Ces requêtes sont alors acheminées vers le bon pays puis l'établissement concerné. Les réponses suivent le chemin inverse.

4.1 Une question de confiance

Les utilisateurs nomades doivent avoir une qualité de service comparable en déplacement (en terme de sécurité et d'accès offerts) à celle de leur accès habituel dans leur établissement d'origine.

Pour cela ils doivent pouvoir faire confiance :

- au site visité (infrastructure réseau, configuration et administration réseau et équipements d'authentification),
- aux NRENs intermédiaires, en particulier *RENATER* et, par délégation, le CRU dans le cas d'ARREDU, pour la fiabilité et la sécurisation de leurs réseaux et des serveurs *proxy* RADIUS,
- à leur propre site, bien sûr.

D'autre part les sites visités doivent pouvoir faire confiance aux sites d'origine concernant la validité et la sécurisation de l'authentification ainsi que sur l'information de leurs utilisateurs (existence d'ARREDU, comment l'utiliser,...).

Pourquoi des engagements ?

Logiquement, pour justifier cette confiance, il faudrait que chaque participant s'engage à de bonnes pratiques auprès de tous les autres, soit N*(N-1) engagements, N ayant 3 chiffres (pour l'instant) dans le cas d'*eduroam* !

Pour formaliser ces relations de confiance sans signer des centaines d'engagements, chaque participant doit s'engager auprès de son réseau académique, *RENATER* en ce qui nous concerne, qui, à son tour s'engage auprès de TERENA.

Principaux engagements de RENATER auprès de TERENA :

- Les établissements participants doivent signer un engagement de "bonnes pratiques" (voir ci-dessous) ;
- Au moins un serveur national doit être mis en oeuvre, sécurisé et maintenu ;
- Le CERT doit être impliqué (connaissance de l'infrastructure, sécurisation des serveurs,...) ;
- De l'information sur le service et des résultats de surveillance doivent être disponibles ;
- Les établissements doivent "éduquer" leurs utilisateurs (cf ci-dessous).

Principaux engagements des établissements auprès de RENATER :

- Ils doivent offrir le service conformément aux recommandations du projet ;
- Ils doivent mettre en place et sécuriser convenablement un serveur/*proxy* d'authentification ;
- Ils doivent faire de l'information auprès des visiteurs sur l'existence du service ;
- Ils doivent former et informer leurs utilisateurs sur l'utilisation du service, le respect des règles d'utilisation des réseaux visités et sur la prise en charge d'éventuels problèmes techniques par l'établissement d'origine ;
- Ils doivent journaliser les résultats d'authentification.

4.2 Procédure d'adhésion à ARREDU/*eduroam*

La procédure qui devrait être mise en place d'ici à la fin de 2005 prévoit d'ajouter un nouveau "service mobilité", associé à une charte, dans les agréments *RENATER*. Un établissement désirant participer à ARREDU devra signer la nouvelle version de son agrément et communiquer le nom d'un correspondant. Il y aura alors création d'une entrée dans le système de gestion d'ARREDU que ce correspondant pourra renseigner (noms des domaines, serveurs, secrets partagés, compte de test,...). Une fois les renseignements requis fournis, le nouvel établissement sera ajouté à la configuration des serveurs *proxy* nationaux et pourra utiliser l'infrastructure ARREDU/*eduroam*.

4.3 Fonctionnement :

La cellule technique du CRU opère le service, au nom de *RENATER*, en mettant en oeuvre un serveur-*proxy* RADIUS gérant le domaine "fr" vis à vis de TERENA. Ce serveur est secouru par un serveur miroir géré par le CRC de Strasbourg. *RENATER* gère l'aspect administratif (agréments, engagement auprès de TERENA).

5 Aspects sécurité

L'utilisation d'accès réseau sans fil soumis à authentification, dans un environnement non maîtrisé, expose à plusieurs risques :

- Divulgation des éléments d'authentification de l'utilisateur (identifiant et mot de passe) :

  L'authentification étant traitée par le serveur du site d'origine, ces éléments traversent plusieurs équipements et réseaux avant d'y parvenir et sont donc tributaires de la sécurité de chacun d'eux (écoute, compromission d'équipement,...).

- Interception du trafic :

  Une fois l'accès obtenu, l'utilisateur peut accéder à divers services, applications et données plus ou moins sensibles or les réseaux sans fil sont très vulnérables à l'écoute du trafic (même en utilisant le WEP).

- Leurres (faux serveurs) :

  Il est actuellement très facile de monter un point d'accès sans fil avec un simple PC portable ainsi qu'un pseudo-serveur d'authentification, induisant en erreur les utilisateurs. Il est alors facile d'intercepter leurs données d'authentification et, si le faux point d'accès offre un véritable accès, d'écouter le trafic, voire d'usurper des sessions ouvertes par l'utilisateur légitime.

Pour garantir la sécurité de la phase d'authentification (authentification mutuelle et protection des identifiants) il faut utiliser une méthode à base de tunnels SSL entre l'équipement de l'utilisateur (*supplicant*) et le serveur d'authentification sur le site d'origine. Les trois principales sont PEAP, TTLS et TLS. Cette sécurité dépend néanmoins en partie des utilisateurs qui ne doivent pas accepter "les yeux fermés" des certificats non reconnus mais ceci n'est pas propre à ces méthodes.

Ensuite, pour protéger le trafic, il faut utiliser un chiffrement à clé dynamique renouvelable basé sur WEP ou, mieux, sur WPA/WPA2.

Traçabilité

Les établissements sont censés savoir qui utilise leurs réseaux à tout moment, ne serait-ce que pour remonter à l'origine d'un problème ou d'un trafic douteux. Pour les accès via ARREDU la comptabilité RADIUS sera mise à profit, éventuellement croisée avec des journaux DHCP et/ou NAT, pour faire la relation entre une adresse IP et son utilisateur à un moment donné.

Le cas des portails-redirecteurs Web dits "captifs"

Ces portails posent généralement des problèmes de sécurité à plusieurs niveaux :

- Le lien radio n'étant pas protégé, le trafic des utilisateurs est "à la disposition" de tous ceux qui sont dans la zone de couverture du point d'accès ;
- De par l'absence de 802.1x, il n'y a pas de protection du contenu des requêtes RADIUS (s'ils s'appuient dessus). Il y a un risque de « craquage » si le flux RADIUS peut être intercepté à un endroit quelconque de la chaîne. Les mots de passe peuvent également être exposés par le simple fonctionnement en mode *debug* de l'un des serveurs RADIUS traversés. La compromission de la machine supportant le portail exposerait les données d'authentification des utilisateurs.
- Outre l'interception des données (éventuellement sensibles), des attaques de type MIM sont possibles ainsi que le vol de session (faux point d'accès, faux portail, faux serveur d'authentification...) pouvant révéler les données d'authentification des usagers ou usurper leurs sessions.

Pour ces raisons ce type d'accès ne peut être utilisé dans le cadre d'ARREDU/*eduroam* pour l'instant. Les établissements en ayant déployé pour d'autres utilisations devront veiller à ce qu'ils n'utilisent pas l'infrastructure ARREDU.

6 Authentification réseau et authentification applicative

L'infrastructure ARREDU/*eduroam* permet d'obtenir un accès réseau. Une fois authentifié, l'utilisateur devra probablement se ré-authentifier auprès du ou des services qu'il souhaite atteindre (ENT par exemple) avec probablement les mêmes éléments, ce qui peut être mal compris. Malheureusement, même si le « *back-end* » d'authentification final est le même (annuaire LDAP de l'établissement d'origine), il n'est pas possible, avec les mécanismes actuels, d'exporter une authentification réseau vers des applications (Web en particulier).

Mais le problème doit être relativisé car la plupart des clients 802.1x et des navigateurs Web permettent d'enregistrer des données d'authentification qu'ils peuvent transmettre sans intervention de l'utilisateur; ce qui pose d'ailleurs d'autres problèmes de sécurité.

La meilleure solution, du point de vue de l'utilisateur, est probablement l'utilisation de certificats X509 : authentification EAP/TLS pour le réseau et authentification SSL du client pour les applications : tout est transparent et la sécurité ne dépend que de la protection de la clé privée associée au certificat de l'utilisateur. Par contre c'est sans doute la plus lourde à déployer...

7 Limitations, problèmes, évolutions, *eduroam-NG*

L'architecture actuelle souffre de défauts :

- Pas de notion d'autorisation (accès si authentification sans autre considération) ce qui empêche, par exemple, de distinguer entre personnels et étudiants d'établissements d'enseignement ;
- Vulnérabilités à certaines attaques si l'on n'utilise pas de tunnel entre *supplicant* et serveur d'authentification ;
- Relative lourdeur de par l'absence de relation directe entre serveurs
- dépendance à une chaîne : en cas d'indisponibilité d'un service *proxy* national, non seulement les "ressortissants" à l'extérieur ne peuvent plus s'authentifier mais également les "étrangers" présents ;
- Modification statique de la chaîne (ajout/retrait de serveurs ou de domaines) avec une charge particulière d'administration sur les serveurs nationaux ;
- Problème de fiabilité de la comptabilité RADIUS ;
- Souhait de convergence entre authentification réseau et authentification applicative.

La prochaine version d'*eduroam* (NG) devrait essayer de corriger tout ou partie de ces points. Plusieurs pistes sont explorées dans ce sens :

- Diameter : successeur/remplaçant de RADIUS censé corriger beaucoup de lacunes de RADIUS (transport d'attributs, fiabilité, support d'IPsec, négociation, découverte dynamique de serveurs, messages à l'initiative du serveur, remontée d'erreur,...) mais (très) peu implémenté ;
- RadSec : extensions de RADIUS, proposées par « Open System Consultant », apportant le transport TCP, le chiffrement TLS, l'authentification mutuelle par certificat,... ;
- DNSRoam : extension propriétaire inspirée de certaines caractéristiques de Diameter, qui permet de déterminer dynamiquement le serveur d'authentification via le DNS (sec).

Il est trop tôt pour juger de l'intérêt réel de ces différentes solutions mais aucune ne semble pouvoir pallier toutes les limitations de la solution actuelle.

Références

eduroam : http://www.eduroam.org/

ARREDU : http://www.cru.fr/nomadisme-sans-fil/arredu/

Trans-European Research and Education Networking Association : http://www.terena.nl/

Inventory of 802.1X-based solutions for inter-NRENs roaming : http://www.terena.nl/tech/task-forces/tf-mobility/Deliverables/delD/DelD_v1.2-f.pdf

"Inventory of VPN-based Solutions for Inter-NREN Roaming" : http://www.terena.nl/tech/task-forces/tf-mobility/Deliverables/delE/DeliEv4.4-np.pdf

"Inventory of web-based solution for inter-NREN roaming" : http://www.terena.nl/tech/task-forces/tf-mobility/Deliverables/delF/DelF-f.pdf

http://www.nantes-wireless.org/pages/wiki/index.php/802.1x

http://www.Cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1680_pp.htm

http://www.miscmag.com/articles/index.php3?page=713

RFC2865 : Remote Authentication Dial In User Service (RADIUS)

RFC2866 : RADIUS Accounting

RFC 2867 : RADIUS Accounting Modifications for Tunnel Protocol Support

RFC 2868 : RADIUS Attributes for Tunnel Protocol Support

RFC2869 : RADIUS Extensions

Bibliographie

[1] Guy Pujolle. Sécurité Wi-Fi. Editions Eyrolles, 2004

[2] Aurélien Géron. Wi-Fi Déploiement et Sécurité. Editions Dunod, 2004

[3] Jonathan Hassel. RADIUS. Editions O'Reilly, 2003

Glossaire

AAA : Authentication Autorisation Accounting

AES : Advanced Encryption Standard – Algorithme de chiffrement symétrique, rapide et sûr, utilisé par WPA2

AKA : Authentication and Key Agreement - Authentification utilisant les cartes à puce SIM dans les réseaux UMTS

CBC : Cypher Bloc Chaining

CCMP : Counter-mode with CBC-MAC Protocol – Protocole d'utilisation d'un algorithme de chiffrement par blocs, utilisé par 802.11i (WPA2)

CERT : Computer Emergency Response Team – Structure de diffusion d'informations et de coordination dans le domaine de la sécurité informatique

CHAP : Challenge Handshake Authentication Protocol – RFC 1994

CRU : Comité Réseaux des Universités

EAPoL : EAP over LAN – Échange de paquets EAP sur un réseau local

ENT : Environement Numérique de Travail

IEEE : Institute of Electrical and Electronics Engineers – Organisme de normalisation américain

IETF : Internet Engineering Task Force – Organisme élaborant les RFC, devenant généralement des standards pour l'internet

LDAP : Lightweight Directory Access Protocol - Protocole d'accès à un annuaire, inspiré de X500

MIM : Man In the Middle – Attaque consistant à s'intercaler entre deux éléments d'un réseaux

MS-CHAP : Extension Microsoft de Challenge Handshake Authentication Protocol – Suite aux problémes de sécurité de la version 1, c'est la version 2 qui est utilisée - RFC 2759

NAS : Network Access Server – Contrôle d'accès au réseau dans l'architecture RADIUS

NREN : National Research and Education Network - Réseau académique national

OTP : One Time Password – Mot de passe à usage unique

PAP : Password Authentication Protocol – Protocole d'authentification par mot de passe - RFC1334

PPP : Point to Point Protocol – Protocole de transport de paquet d'un noeud à un autre - RFC1661

RC4 : Rivest Chipher 4 – Algorithme de chiffrement par flots

RENATER : Réseau National de Télécommunications pour la Technologie, l'Enseignement et la Recherche

RFC : Request For Comment – Document faisant souvent office de standard pour l'internet

RTC : Réseau Téléphonique Commuté

SIM : Subscriber Identity module – Authentification de l'utilisateur sur un réseau GSM

SQL : Structured Query Language – language de contrôle de données

SSID : Service Set ID - Identifiant réseau

SSL : Secure Socket Layout – Mécanismes de sécurisation de communications TCP

TERENA : Trans-European Research and Education Networking Association – Association de développement et d'expérimentation des projets innovateurs pour la communauté éducation-recherche européenne.

TKIP : Temporal Key Integrity Protocol – Protocole de communications pour la protection et l'authentification des données, utilisée dans 802.11i

VPN : Virtual Private Network