Avant-propos

Le réseau informatique de tout établissement ou de toute entreprise est le premier maillon d'une grande chaîne qu'un utilisateur rencontre dès qu'il veut bénéficier des services en ligne qui lui sont proposés localement ou à distance dans les méandres d'Internet. L'accès à un réseau est un service qui peut être convoité dans un but malveillant. Un pirate qui obtient la clé d'un réseau peut chercher à s'y introduire, compromettre des machines et s'en servir pour rebondir vers d'autres réseaux avec toutes les conséquences désagréables que cela implique.

Du point de vue de l'utilisateur, le fait de se connecter physiquement au réseau doit être une opération très simple, parce que c'est la première étape qu'il doit franchir, avant bien d'autres, pour accéder aux ressources dont il a besoin. Il convient donc de ne pas lui compliquer les procédures à outrance.

De son côté, le responsable du réseau a le souci de mettre en place des moyens de contrôle des accès, et pour cela, il doit résoudre une sorte de quadrature du cercle : simplicité pour l'utilisateur, fiabilité des mécanismes, niveau de sécurité élevé, le tout en utilisant le plus possible les standards disponibles.

Pour tendre vers cet objectif, il a à sa disposition toute une palette de protocoles d'authentification qu'il doit associer selon une formule optimale. Au cœur de celle-ci on trouve comme principal ingrédient le protocole Radius. Il est épaulé par une panoplie d'autres protocoles qui lui apportent les fonctions supplémentaires permettant d'augmenter et de graduer le niveau de sécurité en fonction des conditions liées à l'environnement local.

L'imbrication et l'interaction de ces protocoles sont à l'origine de la complexité interne des solutions d'authentification réseau. Comprendre ces environnements est une étape importante dans la maîtrise d'un tel dispositif. C'est l'objectif de ce livre.

À qui est destiné ce livre ?

Ce livre est destiné à tous les administrateurs de réseau qui s'intéressent aux solutions d'authentification autour des serveurs Radius, et plus particulièrement dans les réseaux locaux, filaires ou sans fil. Ils y trouveront la documentation nécessaire, qu'ils aient déjà commencé à déployer une solution ou s'ils s'apprêtent à le faire. Il leur sera présenté des explications théoriques dans lesquelles les mécanismes d'authentification seront décortiqués, ainsi que des exemples pratiques sur tous les aspects de la mise en œuvre, depuis le serveur Radius jusqu'au poste de travail, en passant par les équipements réseau.

Structure du livre

Les chapitres 1 à 6 constituent une première partie de description des principes fondamentaux.

La seconde partie, à partir du chapitre 7, correspond à la mise en œuvre des mécanismes étudiés dans la première partie.

Le **chapitre 1** pose les problèmes liés à l'authentification sur réseau local et définit le périmètre du contenu de ce livre.

Le **chapitre 2** passe en revue les divers matériels (au sens large) qui seront nécessaires pour mener à bien une authentification réseau.

Le **chapitre 3** s'intéresse aux critères que peut présenter un utilisateur ou un poste de travail pour être authentifié.

Le **chapitre 4** explique les principes généraux des protocoles Radius et 802.1X qui seront analysés dans les chapitres suivants.

Le **chapitre 5** détaille le protocole Radius.

Dans le **chapitre 6** nous verrons comment Radius a été étendu pour s'interfacer avec d'autres protocoles complémentaires (802.1X par exemple) et nous les détaillerons à leur tour.

Le **chapitre 7** est une introduction à FreeRadius, qui détaille les mécanismes qu'il met en jeu pour implémenter le protocole Radius.

Dans le **chapitre 8**, nous verrons, au travers d'exemples concrets, comment un serveur FreeRadius doit être mis en œuvre et comment les autres participants (équipements réseaux, postes de travail) de la chaîne d'authentification doivent être paramétrés.

Le **chapitre 9** est une continuation du précédent. Il y est décrit comment les postes de travail doivent être configurés pour utiliser le protocole 802.1X.

Le **chapitre 10** explique comment un serveur FreeRadius peut s'interfacer avec un domaine Windows ou LDAP pour stocker les informations dont il a besoin.

Le **chapitre 11** décrit quelques moyens d'analyse du trafic réseau lors de l'établissement d'une authentification.

Une liste de documents de spécifications (*Request For Comments*) liés aux protocoles étudiés pourra être trouvée dans l'**annexe A**.

Dans **l'annexe B**, on trouvera le texte de la RFC 2865, la principale référence du protocole Radius.

Remerciements

Mes premiers remerciements chaleureux vont à Stella Manning, ma compagne, qui m'a soutenu dans ce projet et qui, bien que profane en la matière, a patiemment relu tout le livre afin de me conseiller pour en améliorer le style et la syntaxe.

Philéas, qui a bien voulu rester sage dans le ventre de sa mère (précédemment citée) et qui a certainement déjà pu apprécier le monde numérique dans lequel il naîtra à peu près en même temps que cet ouvrage.

Roland Dirlewanger, directeur des systèmes d'information à la délégation régionale Aquitaine-Limousin du CNRS, qui a apporté son avis d'expert en matière de réseaux et de sécurité informatique.

Anne Facq, responsable du service informatique du Centre de Recherche Paul Pascal, et Laurent Facq, directeur technique de REAUMUR (REseau Aquitain des Utilisateurs en Milieu Universitaire et de Recherche) qui ont, en famille, décortiqué ce livre et apporté une critique constructive et précieuse.

Régis Devreese, responsable du service informatique du Laboratoire d'Étude de l'Intégration des Composants et Systèmes Électroniques pour les questions pointues qu'il m'a souvent posées et qui m'ont incité à approfondir mes connaissances dans le domaine de l'authentification.

Je remercie également Muriel Shan Sei Fan et Nat Makarevitch des éditions Eyrolles qui m'ont permis de publier ce livre et qui m'ont aidé à le composer.