Protocoles d'accès réseau à distance - Quelle sécurité?

Constantin Yamkoudougou

28 décembre 2005

Table des matières

Glossaire

IP : Internet Protocol
IAB : Internet Architecture Board
TCP : Transport Control Protocol
UDP : User Datagramme Protocol
TACACS : Terminal Access Controller Access System
L2TP : Layer 2 Tunneling Protocol
PPTP Point to point Tunnelling Protocol
PPP Point to Point Protocol
PAP : Password Authentication Protocol
IPSec : IP Security
SSH : Secure Shell
SSL : Secure Socket Layer

1 Enjeu des protocoles d'accès réseau à distance

Avoir la possibilité d'utiliser à distance les ressources de son réseau local est devenu indispensable pour beaucoup d'entreprises. Un tel accès suppose le déploiement au sein de l'infrastructure locale de réseau d'équipements permettant d'authentifier, d'allouer les ressources selon le profil de l'utilisateur. Pour certaines entreprises spécialisées telles que les fournisseurs d'accès, comptabiliser le temps d'utilisation, la bande passante est indispensable pour adresser la facturation idoine à leurs client qui accèdent à un internet par le biais de leur réseau. La typologie des protocoles d'accès à distance est très variée. Elle va de protocoles de première génération tels que TELNET à des VPN légers tels que PPTP, L2TP qui sont des protocoles de niveau 2 et enfin des protocoles plus élaborés tels que IPSec, SSH.

Ces protocoles n'offrent pas tous le même niveau de sécurité. Certains n'offrent aucune sécurité.
Pour contrôler l'accès à distance et authentifier les utilsateurs, les protocoles les plus connus pour ce faire sont RADIUS qui possède les implémentations les plus anciennes, DIAMETER et TACACS.

2 sécurité du protocole RADIUS

Le protocole RADIUS (Remote Authentication Dial In User Services) est un protocole d'authentification et de gestion d'habilitation utilisé pour l'accès de réseau à distance. Il fonctionne selon une architecture de type client et serveur. Ce protocole est très utilisé par les fournisseurs d'accès Internet parce qu'il permet aussi d'assurer des fonctions de comptablité pour

les besoins de facturation. Le client RADIUS est typiquement un server d'accès qui reçoit les demandes et les paramètres de connexion des utilisateurs distants qu'il communique ensuite au serveur RADIUS. Le serveur vérifié ensuite ces informations dans une base de données ou dans un annuaire afin de prendre la décision d'autoriser ou de refuser l'accès demandé par le client. Ce processus peut être représenté par le schéma ci-dessous.

Ce protocole n'assure pas la confidentialité des échanges entre les postes utilisateurs et le client RADIUS, ce qui fait courir au demandeur d'accès un risque d'usurpation de son identité si d'aventure une tierse personne avait la possibilité d'écouter et d'enregistrer les données échangées (login et mot de passe).

3 sécurité de l'accès à distance par le protocole DIAMETER

La diffèrence essentielle entre protocole DIAMETER et RADIUS est que celui-ci utilise le protocole de transport TCP au lieu d'UDP

4 sécurité de l'accès réseau à distance par TELNET

TELNET est un protocole de connexion à distance de première génération écrit au début des années 80. Il permet à l'utilisateur de se connecter à distance sur une machine en utilisant un login et un mot de passe pour l'identification et l'authentification. L'utilisateur dispose alors ensuite d'un shell pour exécuter des commandes. Tout se passe comme s'il était connecté localement à la machine distante. On dit que TELNET est un protocole d'émulation de terminal. Les serveurs TELNET écoutent les requêtes sur le port TCP 53.

Malheusement, ce protocole n'offre que très peu de sécurité. En effet le login et le mot de passe sont transmis en clair sur Internet. Aujourd'hui, il est recommandé d'utiliser des protocoles plus élaborés tels que SSH qui offrent une meilleure sécurité que TELNET en vertu de la couche chiffrante SSL .

5 sécurité de l'accès à distance par le protocole PPTP

PPTP (Point to Point Tunneling Protocol) est une extension du protocole PPP (Point to Point Protocol) conçu à l'initiative de plusieurs opérateurs et éditeurs du marché des technologies dont Microsoft était le leader. Les architectures utilisant ce type de technologie sont organisées en trois tiers : Un client PPTP installé sur le poste client, un serveur d'accès (NAS : Network Access Server) appartenant à un réseau intermédiaire dont l'utilisateur se servira pour accéder au serveur PPTP qui est le serveur d'authentification du réseau mère de l'utilisateur. L'exemple le plus éloquent de réseau intermédaire est celui d'un fournisseur d'accès Internet. La communication entre le client et le serveur d'accès commence en utilisant le protocole PPP. L'authentification dans cette première phase se fait par login et mot de passe (Protocole PAP) ou par challenge (CHAP). Les paramètres d'authentification sont transmis en clair dans cette phase. La seconde phase est l'authentification entre le serveur PPTP et le serveur d'accès qui a recueilli préalablement les données d'authentification de l'utilisateur en vue de les présenter au serveur PPTP. Une fois que cette seconde phase d'authentification est réussie, un tunnel PPTP est mis en place entre le poste de l'utilisateur et le serveur PPTP. Les données dans ce tunnel peuvent être chiffrées pour en préserver la confidentialité. La RFC 2637 ne dit rien sur les algorithmes et les protocoles cryptographiques applicables à des données acheminées dans un tunnel PPTP. Microsoft [ref2] utilise par exemple l'algorithme de chiffrement à la volet RC4 de la société RSA dont de nombreuses cryptanalyses ont demontrées des vulnérablités tant au niveau des longueurs de clés (40 bits - 128 bits) que du vecteur d'initialisation.

6 sécurité de l'accès à distance par le protocole L2TP

La dernière génération de protocole s'apparentant à PPTP est L2TP qui est originellement une initiative de CISCO pour une extension du protocole L2F. Ce protocole possède les mêmes fonctionalités que PPTP sauf qu'il est conu pour tenir compte de la diversité des réseaux : ATM, frame relay, alors que PPTP est conçu uniquement pour IP. Ce protocole qui utilise le port UDP 1701 a été conçu dans la l'optique d'une implémentation hardware essentiellement. Il est compatible avec la plupart des serveurs d'authentification RADIUS, TACACS+

7 sécurité de l'accès à distance par le protocole TACACS

TACACS est un protocole qui a été originellement développé par un consortium d'industriels et ensuite adopté par l'IETF sous la référence RFC 1492. Il s'agit d'un protocole d'authentification centralisée par usage de base de données spécifiées le RFC 1492 et également ouvert à d'autres base de donnée telles que le fichier mot de passe d'un serveur UNIX par exemple.

CISCO a repris ce protocole pour lui ajouter de nouvelles fonctions telles que la possibilité d'utiliser des entités distinctes pour l'authentification, l'autorisation et la comptabilité et le support de protocoles sous-jacents tels que ARA, SLIP, PAP, KCHAP, enable et PPP. Le protocole a d'abord été rebaptisé XTACACS puis TACACS+ dans sa dernière version. Au niveau architecturale se protocole est comparable à DIAMETER Compte tenu de l'utilisation de TCP comme protocole de transport.

8 IPSEC toujours aussi utilisé

IPsec (IP security) est un protocole conçu pour assurer l'authenticité, la confidentialité et l'intégrité des données au niveau de la couche réseau. Il existe deux modes de sécurisation des données. le mode transport et le mode tunnel. Le mode transport assure la protection de la charge utile des paquets. Les informations de routage (adresse source et destination par exemple) sont connues. Dans le mode tunnel, le paquet à transmettre est entièrement chiffré et intégré dans une autre paquet. Aucune information sur le paquet n'est accessible lors de son transit sur Internet. Il s'agit du protocole le plus utilisé aujourd'hui pour la sécurité de l'accès réseau à distance même si on lui reproche de plus en plus sa lourdeur en matière de gestion de clés et d'infrastructure à déployer.

9 Références documentaires

ref1 :http ://www.schneier.com/paper-pptpv2.html
ref2 :http ://www.microsoft.com/ntserver/ProductInfo/faqs/PPTPfaq.asp#8
ref3http ://www.cisco.com/warp/public/614/7.html
http ://www.ietf.org/rfc/rfc1492.txt
Security + certification exam guide Gregory White Mc Graw Hill-Osborne
RFC 3127 authentication, authorization and accounting : protocol Evalation
RFC 3588 Diameter Base Protocol
Authentication, authorization and accounting charter (http ://www.ietf.org/html.charters/aaa-charter.html)
http ://www.jacco2.dds.nl/networking/freeswan-l2tp.html#ProsCons

http ://www.faqs.org/rfcs/rfc2661.html
http ://www.faqs.org/rfcs/rfc3193.html
http ://www.vpnc.org/vpn-standards.html
http ://www.ietf.org/html.charters/pppext-charter.html
http ://www.securityfocus.com/archive/105/339788
http ://www.cisco.com/warp/public/614/7.html
http ://www.ietf.org/rfc/rfc1492.txt