Groupe de travail Réseau
Request for Comments : 1929
Catégorie : Sur la voie de la normalisation

M. Leech, Bell-Northern Research Ltd
mars 1996
Traduction Claude Brière de L'Isle

Authentification par nom d'utilisateur/mot de passe pour SOCKS V5

Statut de ce mémoire
Le présent document spécifie un protocole en cours de normalisation de l'Internet pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Normes officielles des protocoles de l'Internet" (STD 1) pour connaître l'état de la normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

1. Introduction

La spécification du protocole pour SOCKS version 5 spécifie un cadre généralisé pour l'utilisation de protocoles d'authentification arbitraires dans l'établissement initial de connexion socks. Le présent document décrit un de ces protocoles, comme il entre dans la "sous négociation" de l'authentification de SOCKS version 5.

Note : Sauf mention contraire, les nombres décimaux qui apparaissent dans les diagrammes de format de paquet représentent la longueur du champ correspondant, en octets. Lorsque un certain octet doit prendre une valeur spécifique, la syntaxe X'hh' est utilisée pour noter la valeur du seul octet de ce champ. Quand le mot "variable" est utilisé, il indique que le champ correspondant a une longueur variable définie soit par un champ Longueur associé (un ou deux octets) soit par un champ Type de données.

2. Négociation initiale

Une fois que le serveur SOCKS V5 a commencé, et que le client a choisi un protocole d'authentification de nom d'utilisateur/mot de passe, la sous négociation de nom d'utilisateur/mot de passe commence. Cela commence par la production par le client d'une demande de nom d'utilisateur/mot de passe :

VER	ULEN	UNAME	PLEN	PASSWD
1	1	1 à 255	1	1 à 255

Le champ VER contient la version courante de la sous négociation, qui est X'01'.

Le champ ULEN contient la longueur du champ UNAME qui suit.

Le champ UNAME contient le nom d'utilisateur tel que connu du système d'exploitation source.

Le champ PLEN contient la longueur du champ PASSWD qui suit.

Le champ PASSWD contient l'association de mot de passe avec le UNAME donné.

Le serveur vérifie le UNAME et PASSWD fournis, et envoie la réponse suivante :

VER	STATUS
1	1

Un champ STATUS de X'00' indique le succès. Si le serveur retourne un état d'échec (une valeur de STATUS autre que X'00') il DOIT clore la connexion.

3. Considérations sur la sécurité

Le présent document décrit une sous négociation qui fournit des services d'authentification au protocole SOCKS. Comme la demande porte le mot de passe en clair, cette sous négociation n'est pas recommandée dans des environnements où le "reniflage" est possible et praticable.

4. Adresse de l'auteur

Marcus Leech
Bell-Northern Research Ltd
P.O. Box 3511, Station C
Ottawa, ON
CANADA K1Y 4H7

téléphone : +1 613 763 9145
mél : mleech@bnr.ca