Groupe de travail sur les réseaux
Requête pour Commentaires : 1994
Rend obsolète : 1334
Catégorie : Standard
Traduction : Yves lescop

W. Simpson
Daydreamer
Août 1996

Lycée la croix-rouge - Brest

Protocole d'Authentification en vue d'établir une liaison PPP (CHAP "Challenge Handshake Authentification Protocol")

Statut de ce document

Ce document spécifie un protocole standard d'Internet pour la communauté Internet, et ne sera éprouvé qu'après plusieurs discussions et suggestions. Merci de vous référer à l'édition courante du " Internet Official Protocol Standards " (STD1) pour l'état de standardisation et le statut de ce protocole. La distribution de ce document est illimitée.

Résumé

Le Protocole Point à Point (PPP) [1] fournit une méthode standard pour transporter des datagrammes multiprotocoles au-dessus de liens point à point.

Le PPP définit également un protocole extensible de contrôle de lien, qui permet la négociation d'un protocole d'authentification pour authentifier son pair avant de permettre à des protocoles de couche réseau de transmettre au-dessus du lien.

Ce document définit une méthode pour l'authentification sur PPP, qui utilise un challenge aléatoire, avec une réponse hachée cryptographiquement qui dépend du challenge et d'une clé secrète.

Table des matières

1 Introduction

Afin d'établir des transmissions au-dessus d'un lien point à point, chaque extrémité du lien PPP doit d'abord envoyer des paquets LCP pour configurer la liaison de données pendant la phase d'établissement du lien. Après que le lien ait été établi, PPP prévoit une phase facultative d'authentification avant de passer à la phase de protocole de couche Réseau.

Par défaut, l'authentification n'est pas obligatoire. Si l'authentification du lien est désirée, une implémentation DOIT indiquer l'option de configuration "Protocole d'authentification" pendant la phase d'établissement du lien.

Ces protocoles d'authentification sont destinés à être principalement utilisés par les machines et les routeurs qui se connectent à un serveur de réseau PPP par l'intermédiaire des circuits commutés ou des lignes téléphoniques, mais pourraient être aussi bien appliqués aux liens dédiés. Le serveur peut utiliser l'identification de la machine ou du routeur se connectant dans la sélection d'options pour des négociations de couche réseau.

Ce document définit un protocole d'authentification PPP. Les phases d'établissement et d'authentification du lien, et l'option de configuration de protocole d'authentification, sont définies dans le Protocole Point à Point (PPP) [1].

1.1 Spécification des obligations

Dans ce document, plusieurs mots sont employés pour signifier les obligations de la spécification. Ces mots sont souvent en majuscules.

"DOIT" Ce mot ou l'adjectif "OBLIGATOIRE" signifie que la définition est une nécessité absolue de cette spécification.

"NE DOIT PAS" Cette phrase signifie que la définition est absolument prohibée de cette spécification.

"DEVRAIT" Ce mot ou l'adjectif **"RECOMMANDÉ"** signifie qu'il peut exister des raisons valides dans des circonstances particulières pour ignorer cet item, mais les implications complètes devront être comprises et le cas soigneusement étudié avant de choisir un chemin différent.

"PEUT" Ce mot ou l'adjectif **"OPTIONNEL"** signifie que cet item est un élément d'un jeu de solutions alternatives autorisé. Une mise en place qui n'inclut pas cette option DOIT être préparée à interopérer avec une autre mise en place qui inclut l'option.

1.2 Terminologie

Ce document utilise fréquemment les termes suivants :

authentificateur
L'extrémité du lien exigeant l'authentification. L'authentificateur indique le protocole d'authentification à utiliser dans la "Demande-Configuration" pendant la phase d'établissement du lien.

Pair
L'autre extrémité du lien point à point ; l'extrémité qui est authentifiée par l'authentificateur.

Jeté silencieusement
Ceci signifie que l'implémentation jette le paquet sans traitement ultérieur. L'implémentation DEVRAIT fournir la capacité d'enregistrer l'erreur, y compris le contenu du paquet silencieusement jeté, et DEVRAIT enregistrer l'événement dans un compteur de statistiques.

2 CHAP - Protocole d'Authentification d'établissement de lien

Le protocole d'authentification d'établissement de lien (CHAP) est employé pour vérifier périodiquement l'identité du pair en utilisant un établissement à 3 voies. Ceci est fait sur l'établissement de lien initial, et PEUT être répété n'importe quand après que le lien ait été établi.

1. Après que la phase d'établissement de lien est achevée, l'authentificateur envoie un message "challenge" au pair.
2. Le pair répond avec une valeur calculée en utilisant une fonction de hachage à sens unique.
3. L'authentificateur vérifie la réponse avec son propre calcul de la valeur hachée prévue. Si les valeurs s'assortissent, l'authentification est reconnue ; autrement la connexion DEVRAIT être terminée.
4. A des intervalles aléatoires, l'authentificateur envoie un nouveau challenge au pair, et répète les étapes 1 à 3.

2.1 Avantages

CHAP assure la protection contre une attaque en play-back par le pair à travers l'utilisation d'un identificateur changeant incrémentalement et d'une valeur de challenge variable. L'utilisation des challenges répétés est destinée à limiter le temps d'exposition à n'importe quelle attaque simple. L'authentificateur est chargé du contrôle de la fréquence et de la synchronisation des challenges.

Cette méthode d'authentification dépend d'un "secret" connu seulement de l'authentificateur et du pair. Le secret n'est pas envoyé sur le lien.

Bien que l'authentification soit seulement à sens unique, par la négociation de CHAP dans les deux directions le même jeu secret peut facilement être utilisé pour une authentification mutuelle.

Puisque CHAP peut être employé pour authentifier beaucoup de systèmes différents, des champs d'identification peuvent être employés comme index pour localiser le secret approprié dans une grande table des secrets. Ceci rend également possible le support de plus d'une paire de nom/secret par système, et de changer le secret en service à tout moment pendant la session.

2.2 Inconvénients

CHAP exige que le secret soit disponible sous la forme de texte. Les bases de données de mots de passe chiffrés de manière irréversible généralement disponibles ne peuvent pas être utilisées.

Ce n'est pas pratique pour de grandes installations, puisque chaque secret possible est mis à jour aux deux extrémités du lien.

> Note de Mise en place : Pour éviter d'envoyer le secret au-dessus d'autres liens dans le réseau, il est recommandé que les valeurs de challenge et de réponse soient examinées sur un serveur central, plutôt que sur chaque serveur d'accès au réseau. Autrement, le secret

DEVRAIT être envoyé à de tels serveurs sous une forme chiffrée réversible. L'un ou l'autre cas exigent une relation de confiance, qui est hors de la portée de cette spécification.

2.3 Exigences de Conception

L'algorithme de CHAP exige que la longueur du secret DOIT être d'au moins 1 octet. Le secret DEVRAIT être au moins aussi grand et non devinable qu'un mot de passe bien choisi. Il est préférable que le secret soit au moins de la longueur de la valeur hachée pour l'algorithme de brouillage choisi (16 octets pour MD5). Ceci pour assurer un intervalle suffisamment étendu pour que le secret assure la protection contre des attaques par recherche exhaustive.

L'algorithme de hachage à sens unique est choisi de telle manière qu'il est infaisable par calcul de déterminer le secret à partir des valeurs connues de challenge et de réponse.

Chaque valeur de challenge DEVRAIT être unique, puisque la répétition d'une valeur de challenge en même temps que le même secret permettrait à un attaquant de répondre avec une réponse précédemment interceptée. Puisqu'on s'attend à ce que le même secret PUISSE être employé pour authentifier avec des serveurs dans des régions géographiques disparates, le challenge DEVRAIT montrer une unicité globale et temporelle.

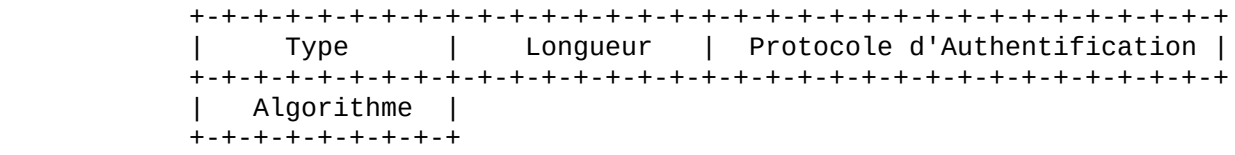
Chaque valeur de challenge DEVRAIT également être imprévisible, le moindre attaquant trompe un pair dans la réponse à un futur challenge prévu, et puis utilise la réponse pour se déguiser en tant que ce pair à un authentificateur.

Bien que les protocoles tels que CHAP soient incapables d’une protection contre des attaques d'écoute clandestine active en temps réel, la génération de challenges imprévisibles uniques peut protéger contre un éventail d'attaques actives.

Une discussion des sources d'unicité et probabilité de divergence est incluse dans l'option de configuration du Nombre Magique [1].

3 Format d'Option de Configuration

Un récapitulatif du format d'option de configuration du Protocole d'Authentification pour négocier le protocole d'authentification d'établissement de lien est montré ci-dessous. Les champs sont transmis de gauche à droite.



Type : 3

Longueur : 5

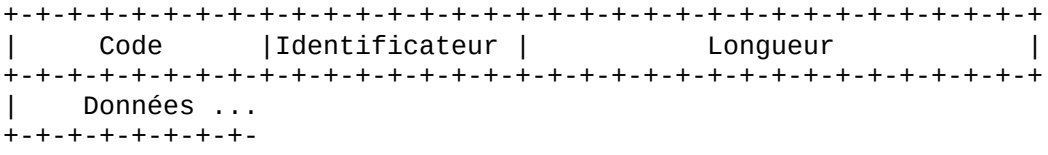
Protocole d'authentification : c223 (hexa) pour le protocole d'authentification d'établissement de lien (CHAP).

Algorithme : Le champ algorithme est d'un octet et indique la méthode d'authentification à utiliser. Des valeurs à jour sont indiquées dans le plus récent "nombres assignés" [2]. Il est exigé qu'une valeur soit implémentée :

5 CHAP avec MD5 [3]

4 Format du Paquet

Exactement un paquet de protocole d'authentification d'établissement de lien (CHAP) est encapsulé dans le champ information d'une trame de couche liaison de données PPP où le champ protocole indique le type en hexadécimal c223 (CHAP). Un récapitulatif du format de paquet CHAP est montré ci-dessous. Les champs sont transmis de gauche à droite.



Code : Le champ code est d'un octet et identifie le type de paquet CHAP. Des codes CHAP sont assignés comme suit :

1 Challenge
2 Réponse
3 Succès
4 Echec

Identificateur : Le champ identificateur est d'un octet et aide dans les assortiments des challenges, réponses et répliques.

Longueur : Le champ longueur est de deux octets et indique la longueur du paquet CHAP comprenant les champs code, identificateur, longueur et données. Les octets en dehors de l'intervalle du champ longueur devraient être traités en tant que remplissage de couche liaison de données et devraient être ignorés à la réception.

Données : Le champ information est de zéro octets ou plus. Le format du champ information est déterminé par le champ code.

4.1 Challenge et réponse

Description

Le paquet challenge est employé pour commencer le protocole d'authentification d'établissement de lien (CHAP). L'authentificateur DOIT transmettre un paquet CHAP avec le champ code positionné à 1 (Challenge). Des paquets "challenge" supplémentaires DOIVENT être envoyés jusqu'à ce qu'un paquet réponse valide soit reçu, ou qu'un compteur de relance facultatif expire.

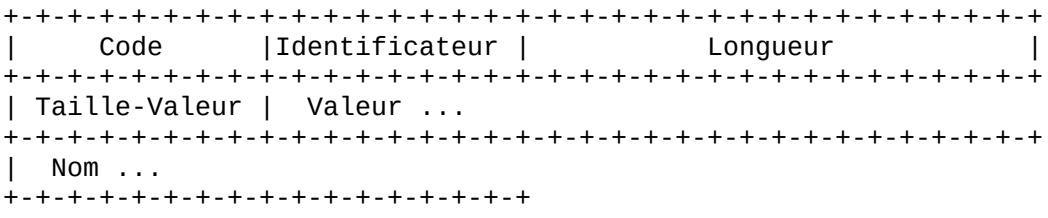
Un paquet "challenge" PEUT également être transmis à tout moment pendant la phase de protocole de couche Réseau pour s'assurer que la connexion n'a pas été altérée.

Le pair DEVRAIT attendre des paquets "challenge" pendant la phase d'authentification et la phase de protocole de couche Réseau. Toutes les fois qu'un paquet "challenge" est reçu, le pair DOIT transmettre un paquet CHAP avec le champ code réglé à 2 (réponse).

Toutes les fois qu'un paquet "réponse" est reçu, l'authentificateur compare la valeur de réponse à son propre calcul de la valeur prévue. En se basant sur cette comparaison, l'authentificateur DOIT envoyer un paquet "succès" ou "échec" (décrit ci-dessous).

> Notes de Mise en place : Puisque le "succès" pourrait être détruit, l'authentificateur DOIT permettre la répétition des paquets de réponse pendant la phase de protocole de couche réseau après avoir fini la phase d'authentification. Pour empêcher la découverte des noms et des secrets alternatifs, tous les paquets de réponse reçus ayant l'identificateur courant du challenge DOIVENT renvoyer le même code de réponse que celui précédemment retourné pour ce challenge spécifique (la partie message PEUT être différente). Tous les paquets de réponse reçus pendant n'importe quelle autre phase DOIVENT être silencieusement jetés.
>
> Quand le paquet "échec" est perdu, et que l'authentificateur termine le lien, les "Demande-terminaison" et "ACK-Terminaison" LCP fournissent une indication alternative que l'authentification a échouée.

Un récapitulatif du format des paquets "Challenge" et "réponse" est montré ci-dessous. Les champs sont transmis de gauche à droite.



Code :

1 pour le challenge ;
2 pour la réponse.

Identificateur : Le champ identificateur est d'un octet. Le champ identificateur DOIT être changé chaque fois qu'un challenge est envoyé. L'identificateur de réponse DOIT être copié de la zone d'identificateur du challenge qui a causé la réponse.

Taille Valeur : Ce champ est d'un octet et indique la longueur du champ valeur.

Valeur : Le champ valeur est d'un ou plusieurs octets. L'octet le plus significatif est transmis d'abord.

La valeur du challenge est un flux variable d'octets. L'importance de l'unicité de la valeur du challenge de son rapport avec le secret est décrite ci-dessus. La valeur du challenge DOIT être changée chaque fois qu'un challenge est envoyé. La longueur de la valeur du challenge dépend de la méthode employée pour produire les octets, et est indépendante de l'algorithme de hachage utilisé.

La valeur de réponse est le hachage à sens unique calculé sur un flux d'octets comprenant l'identificateur, suivi (enchaîné avec) du "secret", suivi (enchaîné avec) de la valeur du challenge. La longueur de la valeur de réponse dépend de l'algorithme de hachage utilisé (16 octets pour MD5).

Nom : Le champ identification est d'un ou plusieurs octets représentant l'identification du système transmettant le paquet. Il n'y a aucune limitation sur la teneur de ce champ. Par exemple, elle PEUT contenir des chaînes de caractères ASCII ou des identificateurs globaux uniques en syntaxe ASN.1. Le nom ne devrait pas être NUL ou terminé par CR/LF. La taille est déterminée à partir du champ longueur.

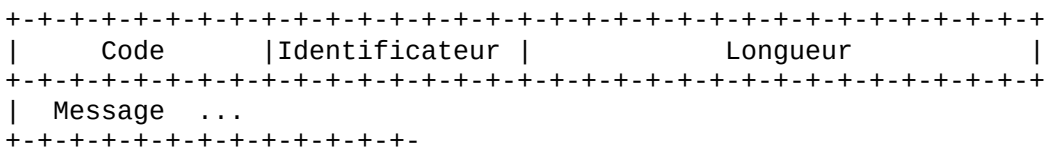
4.2 Succès et échec

Description

Si la valeur reçue dans une réponse est égale à la valeur prévue, alors l'implantation DOIT transmettre un paquet CHAP avec le champ code réglé à 3 (succès).

Si la valeur reçue dans une réponse n'est pas égale à la valeur prévue, alors l'implantation DOIT transmettre un paquet CHAP avec le champ code réglé à 4 (échec), et DEVRAIT agir pour rompre le lien.

Un récapitulatif du format des paquets "succès" et "échec" est montré ci-dessous. Les champs sont transmis de gauche à droite.



Code :
3 pour le succès ;
4 pour l'échec.

Identificateur : Le champ identificateur est d'un octet et aide dans les assortiments des demandes

et réponses. Le champ identificateur DOIT être copié du champ identificateur de la réponse qui a causé cette réponse.

Message : Le champ message est de zéro octets ou plus, et son contenu dépend de l'implantation. Il est destiné à être lisible par un humain, et NE DOIT PAS affecter l'exécution du protocole. Il est recommandé que le message contiennent les caractères ASCII affichables de 32 à 126 en décimal. Les mécanismes pour l'extension à d'autres jeux de caractères sont l'objet de recherche future. La taille est déterminée à partir du champ longueur.

Considérations Sécuritaires

Les problèmes de sécurités sont le sujet primaire de ce RFC.

L'interaction des protocoles d'authentification dans le PPP est fortement dépendant de l'implantation. Ceci est indiqué par l'utilisation de DEVRAIT dans tout le document.

Par exemple, lors de l'échec de l'authentification, quelques réalisations ne rompent pas le lien. Au lieu de cela, l’implantation limite le genre de trafic dans les protocoles de couche Réseau à un sous-ensemble filtré, ce qui permet en retour à l'utilisateur de mettre à jour les secrets ou d'envoyer un courrier à l'administrateur de réseau indiquant un problème.

Il n'y a aucune disposition pour des relances d'une authentification échouée. Cependant, la machine d'état LCP peut renégocier le protocole d'authentification à tout moment, permettant de ce fait une nouvelle tentative. Il est recommandé que tous les compteurs employés pour l'échec d'authentification ne soient remis à l'état initial qu'après l'authentification réussie, ou l'arrêt ultérieur du lien échoué.

Il n'y a aucune obligation que l'authentification soit en duplex ou que le même protocole soit utilisé dans les deux directions. Il est parfaitement acceptable que différents protocoles soient utilisés dans chaque direction. Ceci, naturellement, dépendra des protocoles spécifiques négociés.

Le secret NE DEVRAIT PAS être le même dans les deux directions. Ceci permet à un attaquant de rejouer le challenge du pair, de recevoir la réponse calculée, et d'utiliser cette réponse pour s'authentifier.

Dans la pratique, en dedans ou lié à chaque serveur PPP, il y a une base de données qui associe les noms "utilisateur" avec l'information d'authentification ("secrets"). On ne prévoit pas qu'un utilisateur nommé particulier soit authentifié par des méthodes multiples. Ceci rendrait l'utilisateur vulnérable aux attaques qui négocient la méthode la moins sûre parmi un ensemble (tel que le PAP plutôt que le CHAP). Si le même secret était utilisé, le PAP indiquerait le secret à utiliser plus tard avec le CHAP.

Au lieu de cela, pour chaque nom d'utilisateur il devrait y avoir l'indication d’une seule méthode employée pour authentifier ce nom d'utilisateur. Si un utilisateur doit se servir de différentes méthodes d'authentification sous différentes circonstances, alors des noms distincts d'utilisateur

DEVRAIENT donc être utilisés, chacun identifiant une seule méthode d'authentification.

Les mots de passe et autres secrets devraient être enregistrés aux extrémités respectives de telle sorte que l'accès à ceux-ci soit aussi limité que possible. Dans le meilleur des cas, les secrets devraient seulement être accessibles au processus exigeant l'accès afin d'accomplir l'authentification.

Les secrets devraient être distribués avec un mécanisme qui limite le nombre d'entités qui manipulent (et prennent ainsi connaissance de) le secret. Dans le meilleur des cas, aucune personne non autorisée ne devrait jamais prendre connaissance des secrets. Un tel mécanisme est en dehors du champ de cette spécification.

Remerciements

David Kaufman, Heinrich franc, et Karl Auerbach ont utilisé un challenge pour l'établissement d'un lien au SDC en concevant un des protocoles pour un réseau "sécurisé" au milieu des années 70. Tom Bearson a construit un produit prototype Sytek ("Poloneous"?) sur la notion de challenge-réponse dans le "timeframe 1982-83". Une autre variante est documentée dans divers manuels d'IBM SNA. Encore une autre variante a été mise en application par Karl Auerbach dans le "Telebit NetBlazer circa 1991".

Kim Toms et Barney Wolff ont fournis des critiques utiles des versions précédentes de ce document.

Remerciements spéciaux à Dave Balenson, Steve Crocker, James Galvin, et Steve Kent, pour leurs explications et suggestions étendues. Maintenant, si seulement nous pouvions les mettre d'accord les uns avec les autres.

Références

[1] Simpson, W., Editor, "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, DayDreamer, July 1994.

[2] Reynolds, J., and J. Postel, "Assigned Numbers", STD 2, RFC 1700, USC/Information Sciences Institute, October 1994.

[3] Rivest, R., and S. Dusse, "The MD5 Message-Digest Algorithm", MIT Laboratory for Computer Science and RSA Data Security Inc., RFC 1321, April 1992.

Contacts

Les commentaires devraient être soumis à la liste de diffusion ietf-ppp@merit.edu.

Ce document a été passé en revue par le groupe de travail du protocole Point à Point du "Internet Engineering Task Force" (IETF). Le groupe de travail peut être contacté par l'intermédiaire du siège actuel :

Karl Fox
Ascend Communications
3518 Riverside Drive, Suite 101
Columbus, Ohio 43221

karl@MorningStar.com
karl@Ascend.com

Des questions au sujet de cette note peuvent également être dirigées vers :

William Allen Simpson
DayDreamer
Computer Systems Consulting Services
1384 Fontaine
Madison Heights, Michigan 48071

wsimpson@UMich.edu
wsimpson@GreenDragon.com (préféré)