

## Option DHCP pour le protocole d'authentification d'un utilisateur de groupe ouvert

### 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.

### Copyright

Copyright © "Internet society" (1999) – tous droits réservés.

### Résumé

Ce document définit une option du DHCP [1] qui contient une liste de pointeurs vers des serveurs d'authentification d'utilisateurs qui fournissent des services d'authentification d'utilisateur à des clients conforme au standard technique de client de réseau informatique ouvert [2].

### Introduction

Le standard technique d'un client réseau de groupe ouvert, un produit du groupe de travail sur les réseaux informatiques ouverts (NCWG Network Computing Working Group), définit une facilité pour l'authentification d'un utilisateur du réseau informatique nommée protocole d'authentification utilisateur (UAP User Authentication Protocol).

UAP fournit deux niveaux d'authentification, élémentaire et sûre. L'authentification élémentaire utilise le mécanisme d'authentification basique défini dans la spécification HTTP 1.1 [3]. L'authentification sûre est simplement une authentification élémentaire encapsulée dans une session SSLv3 [4].

Dans les deux cas, un client UAP a besoin d'obtenir l'adresse IP et le port du service UAP. L'information du chemin additionnel doit être demandée, selon l'implantation du service. Un URL [5] est un mécanisme excellent pour l'encapsulation de cette information puisque plusieurs serveurs UAP seront implantés comme composants à l'intérieur de serveurs HTTP/SSL.

La plupart des clients UAP ne possèdent pas d'état local et sont configurés lors du démarrage via DHCP. Aucune option DHCP existante [6] ne possède de champ de données pouvant contenir un URL. L'option 72 contient une liste d'adresses IP pour des serveurs WWW, mais n'est pas acceptable puisqu'un port et/ou chemin ne peut être spécifié. Ainsi il y a un besoin pour une option pouvant contenir une liste d'URLs.

## Option protocole d'authentification utilisateur

Cette option spécifie une liste d'URLs, chacune pointant vers un service d'authentification d'utilisateur capable de traiter les demandes d'authentification encapsulées dans le protocole d'authentification utilisateur (UAP). Les serveurs UAP peuvent accepter soit les connexions HTTP 1.1 soit SSLv3. Si la liste comprend un URL qui ne contient pas de numéro de port, le port par défaut est utilisé (c.-à-d., port 80 pour HTTP et port 443 pour HTTPS). Si la liste comprend un URL qui ne contient pas de chemin, le chemin /uap est utilisé.

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|      Code      |      Longueur      |      liste d'URL      |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

Code : 98

Longueur : La longueur du champ de données (c.-à-d., liste d'URL) en octets.

Liste d'URL : Une liste d'un ou plusieurs URL séparés par le caractère ASCII espace (0x20).

## Références

- [1] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.
- [2] Technical Standard: Network Computing Client, The Open Group, Document Number C801, October 1998.
- [3] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2068, January 1997.
- [4] Freier, A., Karlton, P., and P. Kocher, "The SSL Protocol, Version 3.0", Netscape Communications Corp., November 1996. Standards Information Base, The Open Group, [http://www.db.opengroup.org/sib.htm#SSL\\_3](http://www.db.opengroup.org/sib.htm#SSL_3).

[5] Berners-Lee, T., Masinter, L., and M. McCahill, "Uniform Resource Locators (URL)", RFC 1738, December 1994.

[6] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

## **Considérations sécuritaires**

DHCP ne fournit pas actuellement de mécanismes d'authentification ou de sécurité. L'exposition potentielle aux attaques sont discutées dans la section 7 des spécifications du protocole DHCP.

Le protocole d'authentification de l'utilisateur n'a aucun moyen de détecter si le client communique ou non avec un service d'authentification pirate que le client a contacté car il a reçu une option UAP contrefaite d'un service DHCP dont la sécurité a été compromise. De même, l'authentification sécurisée ne garantit pas contre ce type d'attaque. Cette exposition sécuritaire est mitigée par les suppositions environnementales renseignées dans le standard technique client réseau informatique.

## **Adresse de l'auteur**

Steve Drach  
Sun Microsystems, Inc.  
901 San Antonio Road  
Palo Alto, CA 94303

Phone: (650) 960-1300  
EMail: drach@sun.com