Network Working Group
INTERNET-DRAFT
Obsoletes: draft-ietf-dhc-options-uap-00.txt

S. Drach
Sun Microsystems

September 1998
Expires March 1999

DHCP Option for User Authentication Protocol
<draft-ietf-dhc-options-uap-01.txt>

Status of this Memo

Abstract

This document defines a DHCP [1] option that contains a list of pointers to User Authentication Protocol servers that provide user authentication services for clients that conform to The Open Group Network Computing Client Technical Standard [2].

Introduction

The Open Group Network Computing Client Technical Standard, a product of The Open Group's Network Computing Working Group (NCWG), defines a network computing client user authentication facility named the User Authentication Protocol (UAP).

UAP provides two levels of authentication, basic and secure. Basic authentication uses the Basic Authentication mechanism defined in the HTTP 1.1 [3] specification. Secure authentication is simply basic authentication encapsulated in an SSLv3 [4] session.

In both cases, a UAP client needs to obtain the IP address and port of the UAP service. Additional path information may be required, depending on the implementation of the service. A URL [5] is an excellent mechanism for encapsulation of this information since many UAP servers will be implemented as components within legacy HTTP/SSL servers.

Most UAP clients have no local state and are configured when booted through DHCP. No existing DHCP option [6] has a data field that contains a URL. Option 72 contains a list of IP addresses for WWW servers, but it is not adequate since a port and/or path can not be specified. Hence there is a need for an option that contains a list of URLs.

User Authentication Protocol Option

This option specifies a list of URLs, each pointing to a user authentication service that is capable of processing authentication requests encapsulated in the User Authentication Protocol (UAP). UAP servers can accept either HTTP 1.1 or SSLv3 connections. If the list includes a URL that does not contain a port component, the normal default port is assumed (i.e., port 80 for http and port 443 for https). If the list includes a URL that does not contain a path component, the path /uap is assumed.

```
 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      |    Length     |   URL list
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Code TBD

Length The length of the data field (i.e., URL list) in bytes.

URL list A list of one or more URLs separated by the ASCII space character (0x20).

References

Droms, R., "Dynamic Host Configuration Protocol", RFC-2131, March 1997.

Technical Standard: Network Computing Client, The Open Group, Document Number C801, October 1998.

Fielding, R., Gettys, J., Mogul, J., Frystyk, H., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC-2068, January 1997.

Freier, A., Karlton, P., and P. Kocher, "The SSL Protocol, Version 3.0", Internet Draft, November 1996.

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

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

Security Considerations

DHCP currently provides no authentication or security mechanisms. Potential exposures to attack are discussed in section 7 of the DHCP protocol specification.

Author's Address

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

Phone: (650) 960-1300

EMail: drach@sun.com