

Network Working Group  
Internet-Draft  
Expires: June 21, 2004

A. Melnikov  
Isode  
December 22, 2003

HTTP URL Scheme extension for authentication  
draft-melnikov-http-auth-url-00.txt

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on June 21, 2004.

Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

Abstract

"HTTPS" scheme gives an HTTP client a hint that it must establish a TLS protected channel before invoking an operation described by the URL. This document defines extension to both "HTTP" and "HTTPS" schemes that tells the client to perform Simple Authentication and Security Layer [[SASL](#)] authentication according to SASL in HTTP 1.1 [[HTTP-SASL](#)] before invoking an operation described by the HTTP URL.

---

Internet-Draft

HTTP AUTH URL

December 2003

## Table of Contents

<a href="#">1.</a>	Conventions Used in this Document . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Introduction and Overview . . . . .	<a href="#">4</a>
<a href="#">3.</a>	HTTP User Name and Authentication Mechanism . . . . .	<a href="#">6</a>
<a href="#">4.</a>	Security Considerations . . . . .	<a href="#">7</a>
<a href="#">5.</a>	Acknowledgements . . . . .	<a href="#">8</a>
<a href="#">6.</a>	Open Issues/ToDo . . . . .	<a href="#">9</a>
	Normative References . . . . .	<a href="#">10</a>
	Informative References . . . . .	<a href="#">11</a>
	Author's Address . . . . .	<a href="#">11</a>
	Full Copyright Statement . . . . .	<a href="#">12</a>

---

Internet-Draft

HTTP AUTH URL

December 2003

## 1. Conventions Used in this Document

The key words "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", and "MAY" in this document are to be interpreted as defined in "Key words for use in RFCs to Indicate Requirement Levels" [[KEYWORDS](#)].

## [2](#). Introduction and Overview

Introduction of SASL in HTTP 1.1 [[HTTP-SASL](#)] emphasizes a security problem that is already present in HTTP. Imagine that a client is willing to send some data to the server (e.g. POST or PUT request) and the server requires that the data is being protected with TLS or SASL security layer. The server may refuse to perform the operation and return an appropriate error code (e.g. Unauthorized), however the data was already sent in the clear to the server. One can argue that this is a client problem: if the client has sent the data in the clear, than the user didn't consider the data worth protecting. However, knowing what the client has sent to the server in a request might help an attacker to decipher the corresponding response from the server, even if it is encrypted. So, by protecting the request, it is possible to help protect the response.

"HTTPS" URL schema helps to avoid the issue by giving the client a hint that it must establish a TLS protected channel before invoking an operation described by the URL. This document defines extension to both "HTTP" and "HTTPS" schemes to achieve the same effect for SASL in HTTP. This section is replacing [section 3.2.2](#) from HTTP 1.1 [[RFC2616](#)].

The "http"/"https" schemes are used to locate network resources via the HTTP protocol. The scheme "http" means the HTTP protocol alone, while "https" means the HTTP protocol over TLS/SSL. This section defines the scheme-specific syntax and semantics for http URLs.

```

http_URL      = http_scheme "://" iserver [ abs_path [ "?" query ] ]

http_scheme   = "http:" | "https:"

iserver       = [iuserauth "@" ] hostport
               ;; See [BASIC-URL] for "hostport" definition

achar         = uchar / "&" / "=" / "~"
               ;; see [BASIC-URL] for "uchar" definition

enc_auth_type = 1*achar
               ;; encoded version of [SASL] "auth_type"

enc_user      = 1*achar
               ;; encoded version of [HTTP] "userid"

iauth         = ";AUTH=" ( "*" / enc_auth_type )

iuserauth     = enc_user [iauth] / [enc_user] iauth

```

```

hostport      = host [ ":" port ]
               ;; If the port is empty or not given, port 80 is
               ;; assumed for the 'http' scheme and port 443 for
               ;; 'https' scheme.

```

The semantics are that the identified resource is located at the server listening for TCP connections on that port of that host, and the Request-URI for the resource is `abs_path` ([section 5.1.2](#)). The use of IP addresses in URLs SHOULD be avoided whenever possible (see [RFC 1900](#) [24]). If the `abs_path` is not present in the URL, it MUST be given as `"/` when used as a Request-URI for a resource ([section 5.1.2](#)). If a proxy receives a host name which is not a fully qualified domain name, it MAY add its domain to the host name it received. If a proxy receives a fully qualified domain name, the proxy MUST NOT change the host name.

### 3. HTTP User Name and Authentication Mechanism

A user name and/or authentication mechanism may be supplied. They are used to construct Authorization header as described in SASL in HTTP 1.1 [[HTTP-SASL](#)] after making the connection to the HTTP server. If no user name and no authentication mechanism is supplied, no user authentication is performed.

An authentication mechanism can be expressed by adding ";AUTH=<enc\_auth\_type>" to the end of the user name. When such an <enc\_auth\_type> is indicated, the client SHOULD request appropriate credentials from that mechanism and use SASL authentication as described in SASL in HTTP 1.1 [[HTTP-SASL](#)]. If no user name is specified, one SHOULD be obtained from the mechanism or requested

from the user (for interactive clients) or from configuration database (for non-interactive client) as appropriate.

The string ";AUTH=\*" indicates that the client SHOULD select an appropriate authentication mechanism. It MAY use any SASL mechanism listed in the response to the OPTIONS request containing "Authorization: SASL" header (see [section 4.3.1.2](#) of SASL in HTTP 1.1 [[HTTP-SASL](#)]). If no user name is specified and no appropriate authentication mechanisms are available, the client SHOULD fall back to using unauthenticated HTTP connection. This allows a URL which grants read-write access to authorized users, and read-only anonymous access to other users.

If a user name is included with no authentication mechanism, then ";AUTH=\*" is assumed.

A program interpreting HTTP URLs MAY cache open connections to an HTTP server for later re-use. If a URL contains a user name, only connections authenticated as that user may be re-used. If a URL does not contain a user name or authentication mechanism, then only an anonymous connection may be re-used. If a URL contains an authentication mechanism without a user name, then any non- anonymous connection may be re-used.

Note that if unsafe or reserved characters such as " " or ";" are present in the user name or authentication mechanism, they MUST be encoded as described in [RFC 1738](#) [BASIC-URL].

#### [4.](#) Security Considerations

Since URLs can easily come from untrusted sources, care must be taken when resolving a URL which requires or requests any sort of authentication. If authentication credentials are supplied to the wrong server, it may compromise the security of the user's account. The program resolving the URL should make sure it meets at least one

of the following criteria in this case:

1. The URL comes from a trusted source, such as a referral server which the client has validated and trusts according to site policy. Note that user entry of the URL may or may not count as a trusted source, depending on the experience level of the user and site policy.
2. Explicit local site policy permits the client to connect to the server in the URL. For example, if the client knows the site domain name, site policy may dictate that any hostname ending in that domain is trusted.
3. The user confirms that connecting to that domain name with the specified credentials and/or mechanism is permitted.
4. A mechanism is used which validates the server before passing potentially compromising client credentials.
5. An authentication mechanism is used which will not reveal information to the server which could be used to compromise future connections.

URLs which do not include a user name must be treated with extra care, since they are more likely to compromise the user's primary account. A URL containing ";AUTH=\*" must also be treated with extra care since it might fall back on a weaker security mechanism. Finally, clients are discouraged from using a plain text password as a fallback with ";AUTH=\*" unless the connection has strong encryption (e.g. a key length of greater than 56 bits).



## 5. Acknowledgements

When writing this document some text was borrowed from [RFC 2192](#) ("IMAP URL Scheme") by Chris Newman.

---

Internet-Draft

HTTP AUTH URL

December 2003

## [6.](#) Open Issues/ToDo

1. Add support for ";REALM=<realm>"?
2. Add support for Basic/Digest authentication? This can be done by using ";AUTH=Basic" and ";AUTH=DIGEST" respectively, as currently there is no name conflict with any existing SASL mechanisms
3. Should I update/add IANA registration for HTTP/HTTPS?
4. Should I update rules for HTTP URL comparison?
5. Should I add an informative section describing how major deployed clients/servers handle the extension?

---

Internet-Draft

HTTP AUTH URL

December 2003

## Normative References

- [HTTP-SASL] Nystrom, M. and A. Melnikov, "SASL in HTTP/1.1", [draft-nystrom-http-sasl](#) (work in progress), December 2003.
- [KEYWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", March 1997.
- [RFC1738] Berners-Lee, T., Masinter, L. and M. McCahill, "Uniform Resource Locators (URL)", [RFC 1738](#), December 1994.
- [RFC2616] Fielding, R., Gettys, J., Mogul, J., Nielsen, H., Masinter, L., Leach, P. and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", [RFC 2616](#), June 1999.
- [RFC2818] Rescorla, E., "HTTP Over TLS", [RFC 2818](#), May 2000.
- [SASL] Myers, J., "Simple Authentication and Security Layer (SASL)", [RFC 2222](#), October 1997.
- [SASL[2]] Melnikov, A., "Simple Authentication and Security Layer (SASL)", [draft-ietf-sasl-rfc2222bis](#) (work in progress), October 2003.

---

Internet-Draft

HTTP AUTH URL

December 2003

## Informative References

- [RFC2817] Khare, R. and S. Lawrence, "Upgrading to TLS Within HTTP/1.1", [RFC 2817](#), May 2000.
- [UTF8] Yergeau, F., "UTF-8, a transformation format of ISO 10646", [RFC 2279](#), January 1998.

## Author's Address

Alexey Melnikov  
Isode Limited  
5 Castle Business Village  
36 Station Road  
Hampton, Middlesex TW12 2BX  
UK

EMail: [Alexey.Melnikov@isode.com](mailto:Alexey.Melnikov@isode.com)

URI: <http://www.melnikov.ca/>

Internet-Draft

HTTP AUTH URL

December 2003

#### Full Copyright Statement

Copyright (C) The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an

"AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

#### Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.