Lemonade
Internet-Draft
Updates: 5092 (if approved)
Intended status: Standards Track
Expires: September 11, 2009

N. Cook
Cloudmark

March 10, 2009

Internet Message Access Protocol (IMAP) - URL Access Identifier Extension
draft-ncook-urlauth-accessid-02

Status of this Memo

Copyright Notice

Abstract

The existing IMAP URL specification (RFC 5092) lists several <access> identifiers and <access> identifier prefixes, that can be used to restrict access to URLAUTH-generated URLs. However, these identifiers do not provide facilities for new services such as streaming. This document proposes a set of new <access> identifiers as well as an IANA mechanism to register new <access> identifiers for future applications.

This document updates RFC 5092.

Table of Contents

1. Introduction

The IMAP URL specification [RFC5092] provides a way to carry authorization information in IMAP URLs. Several authorization <access> identifiers are specified in the document, which allow URLAUTH-authorized URLs to be used only by anonymous users, authenticated users, or message submission entities. However there is no mechanism defined to create new <access> identifiers, and overloading the existing mechanisms has security as well as administrative implications.

This document describes a new <access> identifier "stream", to be used by message streaming entities (as described in [STREAMING]), and defines an IANA registration template, which can be used to register new <access> identifiers for future applications. IANA definitions for the existing access identifiers and prefixes from RFC 5092 are also defined in this document - this document updates RFC 5092 and should be taken as the master in the event of any differences or discrepancies.

2. Conventions Used in this Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

In examples, "C:" and "S:" indicate lines sent by the client and server respectively. If a single "C:" or "S:" label applies to multiple lines, then some of the line breaks between those lines are for editorial clarity only and may not be part of the actual protocol exchange.

3. Additional Authorized Access Identifiers

3.1. Existing Access Identifiers

The IMAP URL specification, IMAPURL [RFC5092], specifies the following authorized <access> identifiers:

- "authuser" - Indicating that use of this URL is limited to authenticated IMAP sessions that are logged in as any non-anonymous user
- "anonymous" - Indicating that use of this URL is not restricted by session authorization identity

Additionally the following <access> identifier prefixes are defined:

- "submit+" - Followed by a userid, indicating that only a userid authorized as a message submission entity on behalf of the specified userid is permitted to use this URL

- "user+" - Followed by a userid, indicating that use of this URL is limited to IMAP sessions that are logged in as the specified userid

3.2. Requirement for Additional Access Identifiers

The existing <access> identifiers are suitable for user-based authorization, but only the "submit+" <access> identifier prefix is suitable for entities acting on behalf of a user. Generic support for external entities acting on behalf of users is required for new services such as streaming [STREAMING].

The "submit+" <access> identifier prefix is not suitable for use as a general mechanism to grant access to entities acting on behalf of users, for reasons that include:

- Security - The IMAP server maintains a list of submission server entities that are entitled to retrieve IMAP URLs specifying the "submit+" <ccess> identifier prefix. If this list is extended to include the set of all external entities that could act on behalf of users, then the attack surface would be increased.

- Administration - When URLAUTH-style IMAP URLs are presented to an IMAP server by entities acting on behalf of users, the server administrator has no way of determining the intended use of that URL from the server logs.

- Resourcing - Without a mechanism to distinguish between the application for which an IMAP URL is to be used, the IMAP server has no way to prioritize resources for particular applications. For example, the server could prioritize "submit+" URL fetch requests over other access identifiers.

3.3. Additional Access Identifier Specification

The previous section established that additional access identifiers are required to support applications, such as streaming [STREAMING], that require entities to retrieve URLAUTH URLs on behalf of users. This section describes the scope and meaning of any additional <access> identifiers that are created.

Additional <access> identifiers MUST take one of two forms (Section 4

gives the formal ABNF syntax):

- <access> identifier - The name of the application e.g. "stream"

- <access> identifier prefix - The name of the application e.g. "stream" followed by a "+" and then a userid. For example "stream+testuser".

In both cases, the semantics are the same as those for "submit+", i.e. the <access> identifier or <access> identifier prefix (which MUST be followed by a userid), indicates that only a userid authorized as an application entity for the specified application is permitted to use this URL. In the case of <access> identifier prefixes, the IMAP server SHALL NOT validate the specified userid but MUST validate that the IMAP session has an authorization identity that is authorized as an application entity for the specified application. The application entity itself MAY choose to perform validation on any specified userid before attempting to retrieve the URL.

The authorization granted by any <access> identifiers used as described above is self-describing, and so requires the IMAP server to provide an extensible mechanism for associating userids with new applications. For example, imagine a new application "foo" is created, which requires application entities to retrieve URLs on behalf of users. In this case, the IMAP server would need to provide a way to register a new application "foo", and to associate the set of userids to be used by those entities with the application "foo". Any attempt to retrieve URLs containing the <access> identifier "foo" would be checked for authorization against the list of userids associated with the application "foo".

Section 6 provides the template required to register new <access> identifiers or prefixes with IANA.

3.4. Defining an access identifier for Streaming

One application that makes use of URLAUTH-authorized URLs is that of streaming multimedia files received as internet messaging attachments. This application is described in [STREAMING].

See Section 6.2 for the IANA registration template for the "stream" <access> identifier.

4. Formal Syntax

The following syntax specification uses the Augmented Backus-Naur

Form (ABNF) notation as specified in [RFC5234].

Except as noted otherwise, all alphabetic characters are case-insensitive. The use of upper or lower case characters to define token strings is for editorial clarity only. Implementations MUST accept these strings in a case-insensitive fashion.

The ABNF specified below updates the formal syntax of <access> identifier as defined in IMAP URL [RFC5092].

```
application = 1*(ALPHA/DIGIT)

access      =/ application / (application "+" enc-user)
```

5. Acknowledgements

This document was inspired by discussions in the Lemonade Working Group.

6. IANA Considerations

IANA is requested to create a new registry for IMAP URLAUTH access identifiers and prefixes.

Access identifiers and prefixes MUST be specified in a standards track or IESG approved experimental RFC. This section gives the IANA registration entries for the existing access identifiers and prefixes from RFC 5092 as well as the entry for the "stream" application.

6.1. Access Identifier Registration Template

```
To: iana@iana.org
Subject: IMAP URL Access Identifier Registration

Type:          [Either "<access> identifier" or
                "<access> identifier prefix"]

Application:   [Name of the application, e.g. "stream"]

Description:   [A description of the application and its use
                of IMAP URLs]

RFC Number:    [Number of the RFC that the application was
                defined in ]

Contact:       [email and/or physical address to contact for
                additional information]
```

6.2. Stream Application Registration

```
To: iana@iana.org
Subject: IMAP URL Access Identifier Registration

Type:          <access> identifier

Application:   stream

Description:   Used by SIP Media Servers to retrieve
               attachments for streaming to email
               clients

RFC Number:    This RFC

Contact:       mailto:neil.cook@noware.co.uk
```

6.3. Submit Application Registration

To: iana@iana.org
Subject: IMAP URL Access Identifier Registration

Type: <access> identifier prefix

Application: submit

Description: Used by message submission entities to retrieve attachments to be included in submitted messages

RFC Number: This RFC

Contact: Lemonade WG mailto:lemonade@ietf.org

6.4. User Application Registration

To: iana@iana.org
Subject: IMAP URL Access Identifier Registration

Type: <access> identifier prefix

Application: user

Description: Used to restrict access to to IMAP sessions that are logged in as the specified userid

RFC Number: This RFC

Contact: Lemonade WG mailto:lemonade@ietf.org

6.5. Authuser Application Registration

To: iana@iana.org
Subject: IMAP URL Access Identifier Registration

Type: <access> identifier

Application: authuser

Description: Used to restrict access to to IMAP sessions that are logged in as any non-anonymous user of that IMAP server

RFC Number: This RFC

Contact: Lemonade WG mailto:lemonade@ietf.org

6.6. Anonymous Application Registration

To: iana@iana.org
Subject: IMAP URL Access Identifier Registration

Type: <access> identifier

Application: anonymous

Description: Indicates that use of this URL is not restricted by session authorization identity

RFC Number: This RFC

Contact: Lemonade WG mailto:lemonade@ietf.org

7. Security Considerations

The extension to <access> identifiers specified in this document provides a mechanism for extending the semantics of the "submit+" <access> prefix to arbitrary applications. The use of such additional <access> identifiers and prefixes is primarily for security purposes, i.e. to prevent the overloading of "submit+" as a generic mechanism to allow entities to retrieve IMAP URLs on behalf of userids. Other than this, the security implications are identical to those discussed in Section 10.1 of IMAPURL [RFC5092].

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5092] Melnikov, A. and C. Newman, "IMAP URL Scheme", RFC 5092, November 2007.

[RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

8.2. Informative References

[STREAMING] Cook, N., "Streaming Internet Messaging Attachments", draft-ietf-lemonade-streaming-10.txt (Work in Progress) , Dec 2008.

Author's Address

Neil L Cook
Cloudmark

Email: neil.cook@noware.co.uk