Network Working Group
Request for Comments: 4959
Category: Standards Track

R. Siemborski
Google, Inc.
A. Gulbrandsen
Oryx Mail Systems GmbH

September 2007

IMAP Extension for Simple Authentication and Security Layer (SASL) Initial Client Response

Status of This Memo

Abstract

To date, the Internet Message Access Protocol (IMAP) has used a Simple Authentication and Security Layer (SASL) profile which always required at least one complete round trip for an authentication, as it did not support an initial client response argument. This additional round trip at the beginning of the session is undesirable, especially when round-trip costs are high.

This document defines an extension to IMAP which allows clients and servers to avoid this round trip by allowing an initial client response argument to the IMAP AUTHENTICATE command.

1. Introduction

The SASL initial client response extension is present in any IMAP [RFC3501] server implementation which returns "SASL-IR" as one of the supported capabilities in its CAPABILITY response.

Servers which support this extension will accept an optional initial client response with the AUTHENTICATE command for any SASL [RFC4422] mechanisms which support it.

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 [RFC2119].

In examples, "C:" and "S:" indicate lines sent by the client and server, respectively.

Formal syntax is defined by [RFC4234] as extended by [RFC3501].

3. IMAP Changes to the IMAP AUTHENTICATE Command

This extension adds an optional second argument to the AUTHENTICATE command that is defined in Section 6.2.2 of [RFC3501]. If this second argument is present, it represents the contents of the "initial client response" defined in Section 5.1 of [RFC4422].

As with any other client response, this initial client response MUST be encoded as defined in Section 4 of [RFC4648]. It also MUST be transmitted outside of a quoted string or literal. To send a zero-length initial response, the client MUST send a single pad character ("="). This indicates that the response is present, but is a zero-length string.

When decoding the BASE64 [RFC4648] data in the initial client response, decoding errors MUST be treated as IMAP [RFC3501] would handle them in any normal SASL client response. In particular, the server should check for any characters not explicitly allowed by the BASE64 alphabet, as well as any sequence of BASE64 characters that contains the pad character ('=') anywhere other than the end of the string (e.g., "=AAA" and "AAA=BBB" are not allowed).

If the client uses an initial response with a SASL mechanism that does not support an initial response, the server MUST reject the command with a tagged BAD response.

Note: support and use of the initial client response is optional for both clients and servers. Servers that implement this extension MUST support clients that omit the initial client response, and clients that implement this extension MUST NOT send an initial client response to servers that do not advertise the SASL-IR capability. In such a situation, clients MUST fall back to an IMAP [RFC3501] compatible mode.

If either the client or the server do not support the SASL-IR capability, a mechanism which uses an initial client response is negotiated using the challenge/response exchange described in [RFC3501], with an initial zero-length server challenge.

4. Examples

The following is an example authentication using the PLAIN (see [RFC4616]) SASL mechanism (under a TLS protection layer, see [RFC4346]) and an initial client response:

```
          ... client connects to server and negotiates a TLS
        protection layer ...
     C: C01 CAPABILITY
     S: * CAPABILITY IMAP4rev1 SASL-IR AUTH=PLAIN
     S: C01 OK Completed
     C: A01 AUTHENTICATE PLAIN dGVzdAB0ZXN0AHRlc3Q=
     S: A01 OK Success (tls protection)
```

Note that even when a server supports this extension, the following negotiation (which does not use the initial response) is still valid and MUST be supported by the server:

```
          ... client connects to server and negotiates a TLS
        protection layer ...
     C: C01 CAPABILITY
     S: * CAPABILITY IMAP4rev1 SASL-IR AUTH=PLAIN
     S: C01 OK Completed
     C: A01 AUTHENTICATE PLAIN
         (note that there is a space following the "+" in the
        following line)
     S: +
     C: dGVzdAB0ZXN0AHRlc3Q=
     S: A01 OK Success (tls protection)
```

The following is an example authentication using the SASL EXTERNAL mechanism (defined in [RFC4422]) under a TLS protection layer (see [RFC4346]) and an empty initial client response:

```
          ... client connects to server and negotiates a TLS
          protection layer ...
      C: C01 CAPABILITY
      S: * CAPABILITY IMAP4rev1 SASL-IR AUTH=PLAIN AUTH=EXTERNAL
      S: C01 OK Completed
      C: A01 AUTHENTICATE EXTERNAL =
      S: A01 OK Success (tls protection)
```

This is in contrast with the handling of such a situation when an initial response is omitted:

```
          ... client connects to server and negotiates a TLS protection
          layer ...
      C: C01 CAPABILITY
      S: * CAPABILITY IMAP4rev1 SASL-IR AUTH=PLAIN AUTH=EXTERNAL
      S: C01 OK Completed
      C: A01 AUTHENTICATE EXTERNAL
          (note that there is a space following the "+" in the
          following line)
      S: +
      C:
      S: A01 OK Success (tls protection)
```

5. IANA Considerations

The IANA has added SASL-IR to the IMAP4 Capabilities Registry.

6. Security Considerations

The extension defined in this document is subject to many of the Security Considerations defined in [RFC3501] and [RFC4422].

Server implementations MUST treat the omission of an initial client response from the AUTHENTICATE command as defined by [RFC3501] (as if this extension did not exist).

Although [RFC3501] has no express line length limitations, some implementations choose to enforce them anyway. Such implementations MUST be aware that the addition of the initial response parameter to AUTHENTICATE may increase the maximum line length that IMAP parsers may expect to support. Server implementations MUST be able to receive the largest possible initial client response that their supported mechanisms might receive.

7. Formal Syntax

The following syntax specification uses the Augmented Backus-Naur Form [RFC4234] notation. [RFC3501] defines the non-terminals capability, auth-type, and base64.

```
capability    =/ "SASL-IR"

authenticate  = "AUTHENTICATE" SP auth-type [SP (base64 / "=")]
                *(CRLF base64)
                ;;redefine AUTHENTICATE from [RFC3501]
```

8. Acknowledgments

The authors would like to acknowledge the contributions of Ken Murchison and Mark Crispin, along with the rest of the IMAPEXT Working Group for their assistance in reviewing this document.

Alexey Melnikov and Cyrus Daboo also had some early discussions about this extension.

9. References

9.1. Normative References

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

[RFC3501] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1", RFC 3501, March 2003.

[RFC4234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 4234, October 2005.

[RFC4422] Melnikov, A. and K. Zeilenga, "Simple Authentication and Security Layer (SASL)", RFC 4422, June 2006.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, October 2006.

9.2. Informative References

[RFC4616] Zeilenga, K., "The PLAIN Simple Authentication and Security Layer (SASL) Mechanism", RFC 4616, August 2006.

[RFC4346] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006.

Authors' Addresses

Robert Siemborski
Google, Inc.
1600 Ampitheatre Parkway
Mountain View, CA 94043

Phone: +1 650 623 6925
EMail: robsiemb@google.com

Arnt Gulbrandsen
Oryx Mail Systems GmbH
Schweppermannstr. 8
D-81671 Muenchen
Germany

EMail: arnt@oryx.com

Full Copyright Statement

Intellectual Property