Internet Engineering Task Force (IETF)
Request for Comments: 6331
Obsoletes: 2831
Category: Informational
ISSN: 2070-1721

A. Melnikov
Isode Limited

July 2011

Moving DIGEST-MD5 to Historic

Abstract

This memo describes problems with the DIGEST-MD5 Simple Authentication and Security Layer (SASL) mechanism as specified in RFC 2831. It marks DIGEST-MD5 as OBSOLETE in the IANA Registry of SASL mechanisms and moves RFC 2831 to Historic status.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6331.

Copyright Notice

Table of Contents

1. Introduction and Overview

[RFC2831] defines how HTTP Digest Authentication [RFC2617] can be used as a Simple Authentication and Security Layer (SASL) [RFC4422] mechanism for any protocol that has a SASL profile. It was intended both as an improvement over CRAM-MD5 [RFC2195] and as a convenient way to support a single authentication mechanism for web, email, the Lightweight Directory Access Protocol (LDAP), and other protocols. While it can be argued that it is an improvement over CRAM-MD5, many implementors commented that the additional complexity of DIGEST-MD5 makes it difficult to implement fully and securely.

Below is an incomplete list of problems with the DIGEST-MD5 mechanism as specified in [RFC2831]:

1. The mechanism has too many options and modes. Some of them are not well described and are not widely implemented. For example, DIGEST-MD5 allows the "qop" directive to contain multiple values, but it also allows for multiple qop directives to be specified. The handling of multiple options is not specified, which results in minor interoperability problems. Some implementations amalgamate multiple qop values into one, while others treat multiple qops as an error. Another example is the use of an empty authorization identity. In SASL, an empty authorization identity means that the client is willing to authorize as the authentication identity. The document is not clear on whether

the authzid must be omitted or if it can be specified with an empty value to convey this. The requirement for backward compatibility with HTTP Digest means that the situation is even worse. For example, DIGEST-MD5 requires all usernames/passwords that can be entirely represented in the ISO-8859-1 charset to be down converted from UTF-8 [RFC3629] to ISO-8859-1 [ISO-8859-1]. Another example is the use of quoted strings. Handling of characters that need escaping is not properly described, and the DIGEST-MD5 document has no examples to demonstrate correct behavior.

2. The DIGEST-MD5 document uses ABNF from RFC 822 [RFC0822], which allows an extra construct and allows for "implied folding whitespace" to be inserted in many places. The difference from a more common ABNF defined in [RFC5234] is confusing for some implementors. As a result, many implementations do not accept folding whitespace in many places where it is allowed.

3. The DIGEST-MD5 document uses the concept of a "realm" to define a collection of accounts. A DIGEST-MD5 server can support one or more realms. The DIGEST-MD5 document does not provide any guidance on how realms should be named and, more importantly, how they can be entered in User Interfaces (UIs). As a result, many DIGEST-MD5 clients have confusing UIs, do not allow users to enter a realm, and/or do not allow users to pick one of the server-supported realms.

4. Use of username in the inner hash is problematic. The inner hash of DIGEST-MD5 is an MD5 hash of colon-separated username, realm, and password. Implementations may choose to store inner hashes instead of clear text passwords. This has some useful properties, such as protection from compromise of authentication databases containing the same username and password on other servers if a server with the username and password is compromised; however, this is rarely done in practice. First, the inner hash is not compatible with widely deployed Unix password databases, and second, changing the username would invalidate the inner hash.

5. Description of DES/3DES [DES] and RC4 security layers are inadequate to produce independently developed interoperable implementations. In the DES/3DES case, this is partly a problem with existing DES APIs.

6. DIGEST-MD5 outer hash (the value of the "response" directive) does not protect the whole authentication exchange, which makes the mechanism vulnerable to "man-in-the-middle" (MITM) attacks, such as modification of the list of supported qops or ciphers.

7. The following features are missing from DIGEST-MD5, making it insecure or unsuitable for use in protocols:

   A. Channel bindings [RFC5056].

   B. Hash agility (i.e., no easy way to replace the MD5 hash function with another one).

   C. Support for SASLPrep [RFC4013] or any other type of Unicode character normalization of usernames and passwords. The original DIGEST-MD5 document predates SASLPrep and does not recommend any Unicode character normalization.

8. The cryptographic primitives in DIGEST-MD5 are not up to today’s standards, in particular:

   A. The MD5 hash is sufficiently weak to make a brute force attack on DIGEST-MD5 easy with common hardware [RFC6151].

   B. The RC4 algorithm is prone to attack when used as the security layer without discarding the initial key stream output [RFC6229].

   C. The DES cipher for the security layer is considered insecure due to its small key space [RFC3766].

Note that most of the problems listed above are already present in the HTTP Digest authentication mechanism.

Because DIGEST-MD5 is defined as an extensible mechanism, it is possible to fix most of the problems listed above. However, this would increase implementation complexity of an already complex mechanism even further, so the effort is not worth the cost. In addition, an implementation of a "fixed" DIGEST-MD5 specification would likely either not interoperate with any existing implementation of [RFC2831] or would be vulnerable to various downgrade attacks.

Note that despite DIGEST-MD5 seeing some deployment on the Internet, this specification recommends obsoleting DIGEST-MD5 because DIGEST-MD5, as implemented, is not a reasonable candidate for further standardization and should be deprecated in favor of one or more new password-based mechanisms currently being designed.

The Salted Challenge Response Authentication Mechanism (SCRAM) family of SASL mechanisms [RFC5802] has been developed to provide similar features as DIGEST-MD5 but with a better design.

2. Security Considerations

Security issues are discussed throughout this document.

3. IANA Considerations

IANA has changed the "Intended usage" of the DIGEST-MD5 mechanism registration in the SASL mechanism registry to OBSOLETE. The SASL mechanism registry is specified in [RFC4422] and is currently available at:

http://www.iana.org/assignments/sasl-mechanisms

4. Acknowledgements

The author gratefully acknowledges the feedback provided by Chris Newman, Simon Josefsson, Kurt Zeilenga, Sean Turner, and Abhijit Menon-Sen. Various text was copied from other RFCs, in particular, from [RFC2831].

5. References

5.1. Normative References

[RFC2617] Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999.

[RFC2831] Leach, P. and C. Newman, "Using Digest Authentication as a SASL Mechanism", RFC 2831, May 2000.

5.2. Informative References

[DES] National Institute of Standards and Technology, "Data Encryption Standard (DES)", FIPS PUB 46-3, October 1999.

[ISO-8859-1] International Organization for Standardization, "Information technology - 8-bit single-byte coded graphic character sets - Part 1: Latin alphabet No. 1", ISO/IEC 8859-1, 1998.

[RFC0822] Crocker, D., "Standard for the format of ARPA Internet text messages", STD 11, RFC 822, August 1982.

[RFC2195] Klensin, J., Catoe, R., and P. Krumviede, "IMAP/POP AUTHorize Extension for Simple Challenge/Response", RFC 2195, September 1997.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, November 2003.

[RFC3766] Orman, H. and P. Hoffman, "Determining Strengths For Public Keys Used For Exchanging Symmetric Keys", BCP 86, RFC 3766, April 2004.

[RFC4013] Zeilenga, K., "SASLprep: Stringprep Profile for User Names and Passwords", RFC 4013, February 2005.

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

[RFC5056] Williams, N., "On the Use of Channel Bindings to Secure Channels", RFC 5056, November 2007.

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

[RFC5802] Newman, C., Menon-Sen, A., Melnikov, A., and N. Williams, "Salted Challenge Response Authentication Mechanism (SCRAM) SASL and GSS-API Mechanisms", RFC 5802, July 2010.

[RFC6151] Turner, S. and L. Chen, "Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms", RFC 6151, March 2011.

[RFC6229] Strombergson, J. and S. Josefsson, "Test Vectors for the Stream Cipher RC4", RFC 6229, May 2011.

Author’s Address

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

EMail: Alexey.Melnikov@isode.com
URI: http://www.melnikov.ca/