                ESMTP and LMTP Transmission Types Registration

Status of this Memo

Copyright Notice

Abstract

   This registers seven new mail transmission types (ESMTPA, ESMTPS,
   ESMTPSA, LMTP, LMTPA, LMTPS, LMTPSA) for use in the "with" clause of
   a Received header in an Internet message.

1. IANA Considerations

   As directed by SMTP [2], IANA maintains a registry [7] of "WITH
   protocol types" for use in the "with" clause of the Received header
   in an Internet message. This registry presently includes SMTP [6],
   and ESMTP [2]. This specification updates the registry as follows:

   o The new keyword "ESMTPA" indicates the use of ESMTP when the SMTP
      AUTH [3] extension is also used and authentication is successfully
      achieved.

   o The new keyword "ESMTPS" indicates the use of ESMTP when STARTTLS
      [1] is also successfully negotiated to provide a strong transport
      encryption layer.

   o The new keyword "ESMTPSA" indicates the use of ESMTP when both
      STARTTLS and SMTP AUTH are successfully negotiated (the
      combination of ESMTPS and ESMTPA).

   o The new keyword "LMTP" indicates the use of LMTP [4].

o The new keyword "LMTPA" indicates the use of LMTP when the SMTP
   AUTH extension is also used and authentication is successfully
   achieved.

o The new keyword "LMTPS" indicates the use of LMTP when STARTTLS is
   also successfully negotiated to provide a strong transport
   encryption layer.

o The new keyword "LMTPSA" indicates the use of LMTP when both
   STARTTLS and SMTP AUTH are successfully negotiated (the
   combination of LSMTPS and LSMTPA).

o The references for the ESMTP and SMTP entries in the registry
   should be updated to the latest specification [2] since both RFC
   821 and RFC 1869 [5] are obsoleted by RFC 2821.

2. Implementation Experience

   The ESMTPA, ESMTPS and ESMTPSA keywords have been implemented in
   deployed email server software for several years and no problems have
   been reported with their use.

3. Security Considerations

   Use of these additional keywords provides trace information to
   indicate when various high-level security framing protocols are used
   for hop-to-hop transport of email without exposing details of the
   specifics of the security mechanism. This trace information provides
   an informal way to track the deployment of these mechanisms on the
   Internet and can assist after-the-fact diagnosis of email abuse.

   These keywords are not normally protected in transport which means
   they can be modified by an active attacker. They also do not
   indicate the specifics of the mechanism used, and therefore do not
   provide any real-world security assurance. They should not be used
   for mail filtering or relaying decisions except in very controlled
   environments. As they are both cryptic and hidden in trace headers
   used primarily to diagnose email problems, it is not expected they
   will mislead end users with a false sense of security. Information
   with a higher degree of reliability can be obtained by correlating
   the Received headers with the logs of the various Mail Transfer
   Agents through which the message passed.

   The trace information provided by these keywords and other parts of
   the Received header provide a significant benefit when doing after-
   the-fact diagnosis of email abuse or problems. Unfortunately, some
   people in a misguided attempt to hide information about their
   internal servers will strip Received headers of useful information

and reduce their ability to correct security abuses after they
happen. The result of such misguided efforts is usually a reduction
of the overall security of the systems.

4. References

4.1. Normative References

   [1] Hoffman, P., "SMTP Service Extension for Secure SMTP over
        Transport Layer Security", RFC 3207, February 2002.

   [2] Klensin, J., Ed., "Simple Mail Transfer Protocol", RFC 2821,
        April 2001.

   [3] Myers, J., "SMTP Service Extension for Authentication", RFC
        2554, March 1999.

   [4] Myers, J., "Local Mail Transfer Protocol", RFC 2033, October
        1996.

4.2. Informative References

   [5] Klensin, J., Freed, N., Rose, M., Stefferud, E., and D. Crocker,
        "SMTP Service Extensions", STD 10, RFC 1869, November 1995.

   [6] Postel, J., "Simple Mail Transfer Protocol", STD 10, RFC 821,
        August 1982.

4.3. URIs

   [7] <http://www.iana.org/assignments/mail-parameters>

Author's Address

   Chris Newman
   Sun Microsystems
   1050 Lakes Drive
   West Covina, CA 91790
   US

   EMail: chris.newman@sun.com

Full Copyright Statement

Intellectual Property

   The IETF takes no position regarding the validity or scope of any
   Intellectual Property Rights or other rights that might be claimed to
   pertain to the implementation or use of the technology described in
   this document or the extent to which any license under such rights
   might or might not be available; nor does it represent that it has
   made any independent effort to identify any such rights. Information
   on the procedures with respect to rights in RFC documents can be
   found in BCP 78 and BCP 79.

   Copies of IPR disclosures made to the IETF Secretariat and any
   assurances of licenses to be made available, or the result of an
   attempt made to obtain a general license or permission for the use of
   such proprietary rights by implementers or users of this
   specification can be obtained from the IETF on-line IPR repository at
   http://www.ietf.org/ipr.

   The IETF invites any interested party to bring to its attention any
   copyrights, patents or patent applications, or other proprietary
   rights that may cover technology that may be required to implement
   this standard. Please address the information to the IETF at ietf-
   ipr@ietf.org.

Acknowledgement