Network Working Group
Internet-Draft
Updates: 2595, 3207 (if approved)
Intended status: Standards Track
Expires: March 15, 2015

A. Melnikov
Isode Ltd

September 11, 2014

Updated TLS Server Identity Check Procedure for Email Related Protocols

draft-ietf-uta-email-tls-certs-00

Abstract

This document describes TLS server identity verification procedure for SMTP Submission, IMAP, POP and ManageSieve clients. It replaces Section 2.4 of RFC 2595.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on March 15, 2015.

Table of Contents

1. Introduction

This document describes the updated TLS server identity verification procedure for SMTP Submission [RFC4409] [RFC3207], IMAP [RFC3501], POP [RFC1939] and ManageSieve [RFC5804] clients. It replaces Section 2.4 of RFC 2595.

Note that this document doesn't apply to use of TLS in MTA-to-MTA SMTP.

The main goal of the document is to provide consistent TLS server identity verification procedure across multiple email related protocols. This should make it easier for Certificate Authorities and ISPs to deploy TLS for email use, and would enable email client developers to write more secure code.

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].

3. Email Server Certificate Verification Rules

During a TLS negotiation, an email client (i.e., an SMTP, IMAP, POP3 or ManageSieve client) MUST check its understanding of the server hostname against the server's identity as presented in the server Certificate message, in order to prevent man-in-the-middle attacks. Matching is performed according to the rules specified in Section 6 of [RFC6125], including "certificate pinning" and the procedure on failure to match. The following inputs are used by the verification procedure used in [RFC6125]:

1. The client MUST use the server hostname it used to open the connection as the value to compare against the server name as

expressed in the server certificate (the reference identity). The client MUST NOT use any form of the server hostname derived from an insecure remote source (e.g., insecure DNS lookup). CNAME canonicalization is not done.

The rules and guidelines defined in [RFC6125] apply to an email server certificates, with the following supplemental rules:

1. Support for the DNS-ID identifier type (subjectAltName of dNSName type [RFC5280]) is REQUIRED in Email client software implementations. Certification authorities that issue Email-specific certificates MUST support the DNS-ID identifier type. Service providers SHOULD include the DNS-ID identifier type in Certificate Signing Requests.

2. Support for the SRV-ID identifier type (subjectAltName of SRVName type [RFC4985]) is REQUIRED for email client software implementations. Certification authorities that issue email-specific certificates MUST support the SRV-ID identifier type. Service providers SHOULD include the SRV-ID identifier type in Certificate Signing Requests. List of SRV-ID types for email services is specified in [RFC6186]. For ManageSieve the value "sieve" is used.

3. URI-ID identifier type (subjectAltName of uniformResourceIdentifier type [RFC5280]) MUST NOT be used by clients for server verification.

4. For backward compatibility with deployed software CN-ID identifier type (CN attribute from the subject name, see [RFC6125]) MAY be used for server identity verification.

5. Email protocols allow use of certain wilcards in identifiers presented by email servers. The "*" wildcard character MAY be used as the left-most name component of DNS-ID or CN-ID in the certificate. For example, a DNS-ID of *.example.com would match a.example.com, foo.example.com, etc. but would not match example.com. Note that the wildcard character MUST NOT be used as a fragment of the left-most name component (e.g., *oo.example.com, f*o.example.com, or foo*.example.com).

4. Examples

Consider an IMAP-accessible email server which supports both IMAP and IMAPS (IMAP-over-TLS) at the host "mail.example.net" servicing email addresses of the form "user@example.net" and discoverable via DNS SRV lookups on the application service name of "example.net". A certificate for this service needs to include SRV-IDs of

"_imap.example.net" and "_imaps.example.net" (see [RFC6186]) along with DNS-IDs of "example.net" and "mail.example.net". It might also include CN-IDs of "example.net" and "mail.example.net" for backward compatibility with deployed infrastructure.

Consider an SMTP Submission server at the host "submit.example.net" servicing email addresses of the form "user@example.net" and discoverable via DNS SRV lookups on the application service name of "example.net". A certificate for this service needs to include SRV-IDs of "_submission.example.net" (see [RFC6186]) along with DNS-IDs of "example.net" and "submit.example.net". It might also include CN-IDs of "example.net" and "submit.example.net" for backward compatibility with deployed infrastructure.

5. IANA Considerations

This document doesn't require any action from IANA.

6. Security Considerations

The goal of this document is to improve interoperability and thus security of email clients wishing to access email servers over TLS protected email protocols, by specifying a consistent set of rules that email service providers, email client writers and certificate authorities can use when creating server certificates.

7. References

7.1. Normative References

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

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, October 2008.

[RFC4409] Gellens, R. and J. Klensin, "Message Submission for Mail", RFC 4409, April 2006.

[RFC3207] Hoffman, P., "SMTP Service Extension for Secure SMTP over Transport Layer Security", RFC 3207, February 2002.

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

[RFC1939] Myers, J. and M. Rose, "Post Office Protocol - Version 3", STD 53, RFC 1939, May 1996.

[RFC5804] Melnikov, A. and T. Martin, "A Protocol for Remotely Managing Sieve Scripts", RFC 5804, July 2010.

[RFC6125] Saint-Andre, P. and J. Hodges, "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)", RFC 6125, March 2011.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

[RFC4985] Santesson, S., "Internet X.509 Public Key Infrastructure Subject Alternative Name for Expression of Service Name", RFC 4985, August 2007.

7.2. Informative References

[RFC2595] Newman, C., "Using TLS with IMAP, POP3 and ACAP", RFC 2595, June 1999.

[RFC6186] Daboo, C., "Use of SRV Records for Locating Email Submission/Access Services", RFC 6186, March 2011.

Appendix A. Acknowledgements

Thank you to Chris Newman for comments on this document.

The editor of this document copied lots of text from RFC 2595 and RFC 6125, so the hard work of editors of these document is appreciated.

Author's Address

Alexey Melnikov
Isode Ltd
14 Castle Mews
Hampton, Middlesex TW12 2NP
UK

EMail: Alexey.Melnikov@isode.com