Network Working Group
Internet-Draft
Updates: 2595, 3207, 3501, 5804 (if
approved)
Intended status: Standards Track
Expires: March 23, 2016

A. Melnikov
Isode Ltd

September 20, 2015

Updated TLS Server Identity Check Procedure for Email Related Protocols

draft-ietf-uta-email-tls-certs-05

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, updates Section 4.1 of RFC 3207, updates Section 11.1 of RFC 3501, updates Section 2.2.1 of RFC 5804.

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 23, 2016.

Copyright Notice

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 2
2. Conventions Used in This Document 3
3. Email Server Certificate Verification Rules 3
4. Compliance Checklist for Certification Authorities 4
5. Compliance Checklist for Mail Service Providers and Certificate Signing Request generation tools 4
6. Examples 5
7. IANA Considerations 6
8. Security Considerations 6
9. References 6
  9.1. Normative References 6
  9.2. Informative References 7
Appendix A. Acknowledgements 9
Appendix B. Changes since draft-ietf-uta-email-tls-certs-00 . . 9
Author's Address 9

1. Introduction

Use of TLS by SMTP Submission, IMAP, POP and ManageSieve clients is described in [RFC3207], [RFC3501], [RFC2595] and [RFC5804] respectively. Each of the documents describes slightly different rules for server certificate identity verification (or doesn't define any rules at all). In reality, email client and server developers implement many of these protocols at the same time, so it would be good to define modern and consistent rules for verifying email server identities using TLS.

This document describes the updated TLS server identity verification procedure for SMTP Submission [RFC6409] [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 Certification 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].

The following terms or concepts are used through the document:

reference identifier: (as defined in [RFC6125]) One of the domain names associated by the email (i.e., an SMTP, IMAP, POP3 or ManageSieve) client with the destination email server and optionally an application service type for performing name checks on the server certificate. When name checks are applicable, at least one of the reference identifiers MUST match an [RFC6125] DNS-ID or SRV-ID (or if none are present the [RFC6125] CN-ID) of the server certificate.

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. For DNS-ID and CN-ID identifier types the client MUST use one or more of the following as "reference identifiers": (a) the right hand side of the email address, (b) the hostname it used to open the connection (without CNAME canonicalization). The client MAY also use (c) a value securely derived from (a) or (b), such as using "secure" DNSSEC validated lookup.

2. When using email service discovery procedure specified in [RFC6186] the client MUST also use the right hand side of the email address as another "reference identifier" to compare against SRV-ID identifier in the server certificate.

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.

2. Support for the SRV-ID identifier type (subjectAltName of SRVName type [RFC4985]) is REQUIRED for email client software implementations that support [RFC6186]. List of SRV-ID types for email services is specified in [RFC6186]. For the ManageSieve protocol the service name "sieve" is used.

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

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. Compliance Checklist for Certification Authorities

1. CA MUST support issuance of server certificates with DNS-ID identifier type (subjectAltName of dNSName type [RFC5280]).

2. CA MUST support issuance of server certificates with SRV-ID identifier type (subjectAltName of SRVName type [RFC4985]) for each type of email service.

3. For backward compatibility with deployed client base, CA MUST support issuance of server certificates with CN-ID identifier type (CN attribute from the subject name, see [RFC6125]).

4. CA MAY allow "*" (wildcard) as the left-most name component of DNS-ID or CN-ID in server certificates it issues.

5. Compliance Checklist for Mail Service Providers and Certificate Signing Request generation tools

1. SHOULD include the DNS-ID identifier type (subjectAltName of dNSName type [RFC5280]) in Certificate Signing Requests for both the right hand side of served email addresses, as well as for the host name where the email server(s) are running.

2. If the email services provided are discoverable using DNS SRV as specified in [RFC6186], the Mail Service Provider MUST include the SRV-ID identifier type (subjectAltName of SRVName type [RFC4985]) for each type of email service in Certificate Signing Requests.

3. SHOULD include CN-ID identifier type (CN attribute from the subject name, see [RFC6125]) for the host name where the email server(s) is running in Certificate Signing Requests for backward compatibility with deployed email clients. (Note, a certificate can only include a single CN-ID, so if a mail service is running on multiple hosts, either each host has to use different certificate with its own CN-ID, a single certificate with multiple DNS-IDs, or a single certificate with wildcard in CN-ID can be used).

4. MAY include "*" (wildcard) as the left-most name component of DNS-ID or CN-ID in Certificate Signing Requests.

6. 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". A certificate for this service needs to include DNS-IDs of "example.net" (because it is the right hand side of emails) and "mail.example.net" (this is what a user of this server enters manually, if not using [RFC6186]). It might also include CN-IDs of "mail.example.net" for backward compatibility with deployed infrastructure.

Consider the IMAP-accessible email server from the previous paragraph which is additionally discoverable via DNS SRV lookups in domain "example.net" (DNS SRV records "_imap._tcp.example.net" and "_imaps._tcp.example.net"). In addition to DNS-ID/CN-ID identity types specified above, a certificate for this service also needs to include SRV-IDs of "_imap.example.net" (when STARTTLS is used on the IMAP port) and "_imaps.example.net" (when TLS is used on IMAPS port). See [RFC6186] for more details. (Note that unlike DNS SRV there is no "_tcp" component in SRV-IDs).

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 in domain "example.net" (DNS SRV records "_submission._tcp.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

"submit.example.net" for backward compatibility with deployed infrastructure.

Consider a host "mail.example.net" servicing email addresses of the form "user@example.net" and discoverable via DNS SRV lookups in domain "example.net", which runs SMTP Submission, IMAPS and POP3S (POP3-over-TLS) and ManageSieve services. Each of the servers can use their own certificate specific to their service (see examples above). Alternatively they can all share a single certificate that would include SRV-IDs of "_submission.example.net", "_imaps.example.net", "_pop3s.example.net" and "_sieve.example.net" along with DNS-IDs of "example.net" and "mail.example.net". It might also include CN-IDs of "mail.example.net" for backward compatibility with deployed infrastructure.

7. IANA Considerations

This document doesn't require any action from IANA.

8. 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 Certification Authorities can use when creating server certificates.

TLS Server Identity Check for Email relies on use of trustworthy DNS hostnames when constructing "reference identifiers" that are checked against an email server certificate. Such trustworthy names are either entered manually (for example if they are advertised on a Mail Service Provider's website), explicitly confirmed by the user (e.g. if they are a target of a DNS SRV lookup) or derived using a secure third party service (e.g. DNSSEC-protected SRV records which are verified by the client or trusted local resolver). Future work in this area might benefit from integration with DANE [RFC6698], but it is not covered by this document.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC6409] Gellens, R. and J. Klensin, "Message Submission for Mail", STD 72, RFC 6409, DOI 10.17487/RFC6409, November 2011, <http://www.rfc-editor.org/info/rfc6409>.

[RFC3207] Hoffman, P., "SMTP Service Extension for Secure SMTP over Transport Layer Security", RFC 3207, DOI 10.17487/RFC3207, February 2002, <http://www.rfc-editor.org/info/rfc3207>.

[RFC3501] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1", RFC 3501, DOI 10.17487/RFC3501, March 2003, <http://www.rfc-editor.org/info/rfc3501>.

[RFC1939] Myers, J. and M. Rose, "Post Office Protocol - Version 3", STD 53, RFC 1939, DOI 10.17487/RFC1939, May 1996, <http://www.rfc-editor.org/info/rfc1939>.

[RFC5804] Melnikov, A., Ed. and T. Martin, "A Protocol for Remotely Managing Sieve Scripts", RFC 5804, DOI 10.17487/RFC5804, July 2010, <http://www.rfc-editor.org/info/rfc5804>.

[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, DOI 10.17487/RFC6125, March 2011, <http://www.rfc-editor.org/info/rfc6125>.

[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, DOI 10.17487/RFC5280, May 2008, <http://www.rfc-editor.org/info/rfc5280>.

[RFC4985] Santesson, S., "Internet X.509 Public Key Infrastructure Subject Alternative Name for Expression of Service Name", RFC 4985, DOI 10.17487/RFC4985, August 2007, <http://www.rfc-editor.org/info/rfc4985>.

[RFC6186] Daboo, C., "Use of SRV Records for Locating Email Submission/Access Services", RFC 6186, DOI 10.17487/RFC6186, March 2011, <http://www.rfc-editor.org/info/rfc6186>.

9.2. Informative References

[RFC2595] Newman, C., "Using TLS with IMAP, POP3 and ACAP", RFC 2595, DOI 10.17487/RFC2595, June 1999, <http://www.rfc-editor.org/info/rfc2595>.

[RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, DOI 10.17487/RFC6698, August 2012, <http://www.rfc-editor.org/info/rfc6698>.

Appendix A. Acknowledgements

Thank you to Chris Newman, Viktor Dukhovni and Sean Turner 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.

Appendix B. Changes since draft-ietf-uta-email-tls-certs-00

[[Note to RFC Editor: Please delete this section before publication]]

Added another example, clarified that subjectAltName and DNS SRV are using slightly different syntax.

As any certificate can only include one CN-ID, corrected examples.

Split rules to talk seperately about requirements on MUAs, CAs and MSPs/CSR generation tools.

Updated Introduction section.

Author's Address

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

EMail: Alexey.Melnikov@isode.com