Internet Engineering Task Force (IETF)
Request for Comments: 7817
Updates: 2595, 3207, 3501, 5804
Category: Standards Track
ISSN: 2070-1721

A. Melnikov
Isode Ltd

March 2016

Updated Transport Layer Security (TLS) Server Identity Check Procedure for Email-Related Protocols

Abstract

This document describes the Transport Layer Security (TLS) server identity verification procedure for SMTP Submission, IMAP, POP, and ManageSieve clients. It replaces Section 2.4 (Server Identity Check) of RFC 2595 and updates Section 4.1 (Processing After the STARTTLS Command) of RFC 3207, Section 11.1 (STARTTLS Security Considerations) of RFC 3501, and Section 2.2.1 (Server Identity Check) of RFC 5804.

Status of This Memo

This is an Internet Standards Track document.

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). Further information on Internet Standards is available in 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/rfc7817.

Table of Contents

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. Section 3 of this document replaces Section 2.4 of [RFC2595].

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

This document provides a consistent TLS server identity verification procedure across multiple email-related protocols. This should make it easier for Certification Authorities (CAs) 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: One of the domain names that the email client (an SMTP, IMAP, POP3, or ManageSieve client) associates with the target email server. For some identifier types, the identifier also includes an application service type. Reference identifiers are used for performing name checks on server certificates. (This term is formally defined in [RFC6125].)

CN-ID, DNS-ID, SRV-ID, and URI-ID are identifier types (see [RFC6125] for details). For convenience, their short definitions from [RFC6125] are listed below:

CN-ID: A Relative Distinguished Name (RDN) in the certificate subject field that contains one and only one attribute-type-and-value pair of type Common Name (CN), where the value matches the overall form of a domain name (informally, dot-separated, letter-digit-hyphen labels).

DNS-ID: A subjectAltName entry of type dNSName

SRV-ID: A subjectAltName entry of type otherName whose name form is SRVName

URI-ID: A subjectAltName entry of type uniformResourceIdentifier whose value includes both (i) a "scheme" and (ii) a "host" component (or its equivalent) that matches the "reg-name" rule (where the quoted terms represent the associated [RFC5234] productions from [RFC3986]).

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 identity (client’s reference identifiers) against the server’s identity as presented in the server Certificate message in order to prevent man-in-the-middle attacks. This check is only performed after the server certificate passes certification path validation as described in Section 6 of [RFC5280]. Matching is performed according to the rules specified in Section 6 of [RFC6125], including the relative order of matching of different identifier types, "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 domain portion of the user's 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 [RFC4033] [RFC4034] [RFC4035] validated lookup.

2. When using email service discovery procedure specified in [RFC6186], the client MUST also use the domain portion of the user's email address as another "reference identifier" to compare against an SRV-ID identifier in the server certificate.

The rules and guidelines defined in [RFC6125] apply to an email server certificate 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]. A list of SRV-ID types for email services is specified in [RFC6186]. For the ManageSieve protocol, the service name "sieve" is used.

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

4. For backward compatibility with deployed software, a 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 wildcards in identifiers presented by email servers. The "*" wildcard character MAY be used as the left-most name component of a 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. CAs MUST support issuance of server certificates with a DNS-ID identifier type (subjectAltName of dNSName type [RFC5280]). (Note that some DNS-IDs may refer to domain portions of email addresses, so they might not have corresponding A/AAAA DNS records.)

2. CAs MUST support issuance of server certificates with an SRV-ID identifier type (subjectAltName of SRVName type [RFC4985]) for each type of email service. See Section 4.1 for more discussion on what this means for CAs.

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

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

4.1. Notes on Handling of Delegated Email Services by Certification Authorities

[RFC6186] provides an easy way for organizations to autoconfigure email clients. It also allows for delegation of email services to an email hosting provider. When connecting to such delegated hosting service, an email client that attempts to verify TLS server identity needs to know that if it connects to "imap.hosting.example.net", such server is authorized to provide email access for an email such as alice@example.org. In absence of SRV-IDs, users of compliant email clients would be forced to manually confirm exceptions because the TLS server certificate verification procedures specified in this document would result in failure to match the TLS server certificate against the expected domain(s). One way to provide such authorization is for the TLS certificate for "imap.hosting.example.net" to include SRV-ID(s) (or a DNS-ID) for the "example.org" domain. Note that another way is for DNS Service Record (SRV) lookups to be protected by DNSSEC, but this solution depends on ubiquitous use of DNSSEC and availability of DNSSEC-aware APIs and thus is not discussed in this document. A future update to this document might rectify this.

A CA that receives a Certificate Signing Request containing multiple unrelated DNS-IDs and/or SRV-IDs (e.g., a DNS-ID of "example.org" and a DNS-ID of "example.com") needs to verify that the entity that supplied such Certificate Signing Request is authorized to provide email service for all requested domains.

The ability to issue certificates that contain an SRV-ID (or a DNS-ID for the domain part of email addresses) implies the ability to verify that entities requesting them are authorized to run email service for these SRV-IDs/DNS-IDs. In particular, CAs that can't verify such authorization (whether for a particular domain or in general) MUST NOT include such email SRV-IDs/DNS-IDs in certificates they issue. This document doesn't specify exact mechanism(s) that can be used to achieve this. However, a few special case recommendations are listed below.

A CA willing to sign a certificate containing a particular DNS-ID SHOULD also support signing a certificate containing one or more of the email SRV-IDs for the same domain because the SRV-ID effectively provides more restricted access to an email service for the domain (as opposed to unrestricted use of any services for the same domain, as specified by the DNS-ID).

A CA that also provides DNS service for a domain can use DNS information to validate SRV-IDs/DNS-IDs for the domain.

A CA that is also a Mail Service Provider for a hosted domain can use that knowledge to validate SRV-IDs/DNS-IDs for the domain.

5. Compliance Checklist for Mail Service Providers and Certificate Signing Request Generation Tools

Mail Service Providers and Certificate Signing Request generation tools:

1. MUST include the DNS-ID identifier type in Certificate Signing Requests for the host name(s) where the email server(s) are running. They SHOULD include the DNS-ID identifier type in Certificate Signing Requests for the domain portion of served email addresses.

2. MUST include the SRV-ID identifier type for each type of email service in Certificate Signing Requests if the email services provided are discoverable using DNS SRV as specified in [RFC6186].

3. SHOULD include the CN-ID identifier type 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 a CN-ID can be used).

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

5.1. Notes on Hosting Multiple Domains

A server that hosts multiple domains needs to do one of the following (or some combination thereof):

1. Use DNS SRV records to redirect each hosted email service to a fixed domain, deploy TLS certificate(s) for that single domain, and instruct users to configure their clients with appropriate pinning (unless the SRV records can always be obtained via DNSSEC). Some email clients come with preloaded lists of pinned certificates for some popular domains; this can avoid the need for manual confirmation.

2. Use a single TLS certificate that includes a complete list of all the domains it is serving.

3. Serve each domain on its own IP/port, using separate TLS certificates on each IP/port.

4. Use the Server Name Indication (SNI) TLS extension [RFC6066] to select the right certificate to return during TLS negotiation. Each domain has its own TLS certificate in this case.

Each of these deployment choices have their scaling disadvantages when the list of domains changes. Use of DNS SRV without an SRV-ID requires manual confirmation from users. While preloading pinned certificates avoids the need for manual confirmation, this information can get stale quickly or would require support for a new mechanism for distributing preloaded pinned certificates. A single certificate (the second choice) requires that when a domain is added, then a new Certificate Signing Request that includes a complete list of all the domains needs to be issued and passed to a CA in order to generate a new certificate. A separate IP/port can avoid regenerating the certificate but requires more transport layer resources. Use of TLS SNI requires each email client to use it.

Several Mail Service Providers host hundreds and even thousands of domains. This document, as well as its predecessors, RFCs 2595, 3207, 3501, and 5804, don’t address scaling issues caused by use of TLS in multi-tenanted environments. Further work is needed to address this issue, possibly using DNSSEC or something like PKIX over Secure HTTP (POSH) [RFC7711].

6. Examples

Consider an IMAP-accessible email server that supports both IMAP and IMAP-over-TLS (IMAPS) 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 domain portion of emails) and "mail.example.net" (this is what a user of this server enters manually if not using [RFC6186]). It might also include a CN-ID of "mail.example.net" for backward compatibility with deployed infrastructure.

Consider the IMAP-accessible email server from the previous paragraph that is additionally discoverable via DNS SRV lookups in domain "example.net" (using DNS SRV records "_imap._tcp.example.net" and "_imaps._tcp.example.net"). In addition to the 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 the IMAP-accessible email server from the first paragraph that is running on a host also known as "mycompany.example.com". In addition to the DNS-ID identity types specified above, a certificate for this service also needs to include a DNS-ID of "mycompany.example.com" (this is what a user of this server enters manually if not using [RFC6186]). It might also include a CN-ID of "mycompany.example.com" instead of the CN-ID "mail.example.net" for backward compatibility with deployed infrastructure. (This is so, because a certificate can only include a single CN-ID)

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" (using DNS SRV record "_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 a CN-ID 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 a CN-ID of "mail.example.net" for backward compatibility with deployed infrastructure.

7. Operational Considerations

Section 5 covers operational considerations (in particular, use of DNS SRV for autoconfiguration) related to generating TLS certificates for email servers so that they can be successfully verified by email clients. Additionally, Section 5.1 talks about operational considerations related to hosting multiple domains.

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 CAs can use when creating server certificates.

The 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 that are verified by the client or trusted local resolver). Future work in this area might benefit from integration with DNS-Based Authentication of Named Entities (DANE) [RFC6698], but it is not covered by this document.

9. References

9.1. Normative References

[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>.

[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>.

[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>.

[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>.

[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>.

[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>.

[RFC6066] Eastlake 3rd, D., "Transport Layer Security (TLS) Extensions: Extension Definitions", RFC 6066, DOI 10.17487/RFC6066, January 2011, <http://www.rfc-editor.org/info/rfc6066>.

[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>.

[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>.

[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>.

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>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <http://www.rfc-editor.org/info/rfc3986>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <http://www.rfc-editor.org/info/rfc4033>.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, DOI 10.17487/RFC4034, March 2005, <http://www.rfc-editor.org/info/rfc4034>.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005, <http://www.rfc-editor.org/info/rfc4035>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <http://www.rfc-editor.org/info/rfc5234>.

[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>.

[RFC7711] Miller, M. and P. Saint-Andre, "PKIX over Secure HTTP (POSH)", RFC 7711, DOI 10.17487/RFC7711, November 2015, <http://www.rfc-editor.org/info/rfc7711>.

Appendix A. Changes to RFCs 2595, 3207, 3501, and 5804

This section lists detailed changes this document applies to RFCs 2595, 3207, 3501, and 5804.

The entire Section 2.4 of RFC 2595 is replaced with the following text:

> During the TLS negotiation, the client checks its understanding of the server identity against the provided server's identity as specified in Section 3 of [RFC7817].

The 3rd paragraph (and its subparagraphs) in Section 11.1 of RFC 3501 is replaced with the following text:

> During the TLS negotiation, the IMAP client checks its understanding of the server identity against the provided server's identity as specified in Section 3 of [RFC7817].

The 3rd paragraph (and its subparagraphs) in Section 4.1 of RFC 3207 is replaced with the following text:

> During the TLS negotiation, the Submission client checks its understanding of the server identity against the provided server's identity as specified in Section 3 of [RFC7817].

Sections 2.2.1 and 2.2.1.1 of RFC 5804 are replaced with the following text:

> During the TLS negotiation, the ManageSieve client checks its understanding of the server identity against the server's identity as specified in Section 3 of [RFC7817]. When the reference identity is an IP address, the iPAddress subjectAltName SHOULD be used by the client for comparison. The comparison is performed as described in Section 2.2.1.2 of RFC 5804.

Acknowledgements

Thank you to Chris Newman, Viktor Dukhovni, Sean Turner, Russ Housley, Alessandro Vesely, Harald Alvestrand, and John Levine for comments on this document.

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

Author's Address

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

EMail: Alexey.Melnikov@isode.com