Internet Engineering Task Force (IETF)
Request for Comments: 8143
Updates: 4642
Category: Standards Track
ISSN: 2070-1721

J. Elie

April 2017

Using Transport Layer Security (TLS) with Network News Transfer Protocol (NNTP)

Abstract

This document provides recommendations for improving the security of the Network News Transfer Protocol (NNTP) when using Transport Layer Security (TLS). It modernizes the NNTP usage of TLS to be consistent with TLS best current practices. This document updates RFC 4642.

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 7841.

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/rfc8143.

Table of Contents

1. Introduction

The Network News Transfer Protocol (NNTP) [RFC3977] has been using Transport Layer Security (TLS) [RFC5246] along with its precursor, Secure Sockets Layer (SSL), since at least the year 2000. The use of TLS in NNTP was formalized in [RFC4642], providing implementation recommendations at the same time. In order to address the evolving threat model on the Internet today, this document provides stronger recommendations regarding that use.

In particular, this document updates [RFC4642] by specifying that NNTP implementations and deployments MUST follow the best current practices documented in [BCP195], which currently consists of RFC 7525 ("Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)"). This includes stronger recommendations regarding SSL/TLS protocol versions, fallback to lower versions, TLS negotiation, TLS-level compression, TLS session resumption, cipher suites, public key lengths, forward secrecy, hostname validation, certificate verification, and other aspects of using TLS with NNTP.

1.1. Conventions Used in This Document

Any term not defined in this document has the same meaning as it does in [RFC4642] or the NNTP core specification [RFC3977].

When this document uses the term "implicit TLS", it refers to TLS negotiation immediately upon connection on a separate port.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [BCP14].

2. Updates/Changes to RFC 4642

This document updates [RFC4642] in the following aspects:

- NNTP implementations and deployments SHOULD disable TLS-level compression (Section 3.3 of RFC 7525 [BCP195]), thus no longer using TLS as a means to provide data compression (contrary to the Abstract and Section 2.2.2 of [RFC4642]).

- NNTP implementations and deployments SHOULD prefer implicit TLS, and therefore use strict TLS configuration (Section 3.2 of RFC 7525 [BCP195]). That is to say, they SHOULD use a port dedicated to NNTP over TLS and begin the TLS negotiation immediately upon connection (contrary to a dynamic upgrade from unencrypted to TLS-protected traffic via the use of the STARTTLS command, as Section 1 of [RFC4642] was encouraging). Implicit TLS is the preferred way of using TLS with NNTP for the same reasons, transposed to NNTP, as those given in Appendix A of [MUA-STS]. (Note that [MUA-STS] and [RFC4642] have one author in common.)

- NNTP implementations and deployments MUST NOT negotiate RC4 cipher suites ([RFC7465]); this is contrary to Section 5 of [RFC4642], which required them to implement the TLS_RSA_WITH_RC4_128_MD5 cipher suite so as to ensure that any two NNTP-compliant implementations can be configured to interoperate. This document removes that requirement, so that NNTP client and server implementations follow the recommendations given in Sections 4.2 and 4.2.1 of RFC 7525 [BCP195] instead. The mandatory-to-implement cipher suite or cipher suites depend on the TLS protocol version. For instance, when TLS 1.2 is used, the TLS_RSA_WITH_AES_128_CBC_SHA cipher suite MUST be implemented (Section 9 of [RFC5246]).

- All NNTP clients and any NNTP server that is known by multiple names MUST support the Server Name Indication (SNI) extension defined in Section 3 of [RFC6066], in conformance with Section 3.6 of RFC 7525 [BCP195]. It was only a "SHOULD" in Section 2.2.2 of [RFC4642].

- NNTP implementations and deployments MUST follow the rules and guidelines defined in [RFC6125] and [RFC5280] for hostname validation and certificate verification. Part of Section 5 of [RFC4642] is, therefore, rationalized in favor of following those two documents.

Appendix A of this document gives detailed changes with regard to the wording of [RFC4642].

3. Recommendations

The best current practices documented in [BCP195] apply here. Therefore, NNTP implementations and deployments compliant with this document are REQUIRED to comply with [BCP195] as well.

Instead of repeating those recommendations here, this document mostly provides supplementary information regarding secure implementation and deployment of NNTP technologies.

3.1. Compression

NNTP supports the use of the COMPRESS command, defined in Section 2.2 of [RFC8054], to compress data between an NNTP client and server. Although this NNTP extension might have slightly stronger security properties than TLS-level compression [RFC3749] (since NNTP compression can be activated after authentication has completed, thus reducing the chances that authentication credentials can be leaked via, for instance, a Compression Ratio Info-leak Made Easy (CRIME) attack, as described in Section 2.6 of [CRIME]), this document neither encourages nor discourages the use of the NNTP COMPRESS extension.

3.2. Protocol Versions and Security Preferences

NNTP implementations of news servers are encouraged to support options to configure 1) the minimal TLS protocol version to accept and 2) which cipher suites, signature algorithms, or groups (like elliptic curves) to use for incoming connections. Additional options can naturally also be supported. The goal is to enable administrators of news servers to easily and quickly strengthen security, if needed (for instance, by rejecting cipher suites considered unsafe with regard to local policy).

News clients may also support similar options, either configurable by the user or enforced by the news reader.

3.3. Server Name Indication

The TLS extension for Server Name Indication (SNI) defined in Section 3 of [RFC6066] MUST be implemented by all news clients. It also MUST be implemented by any news server that is known by multiple names. (Otherwise, it is not possible for a server with several hostnames to present the correct certificate to the client.)

3.4. Prevention of SSL Stripping

In order to help prevent SSL Stripping attacks (Section 2.1 of [RFC7457]), NNTP implementations and deployments MUST follow the recommendations provided in Section 3.2 of RFC 7525 [BCP195]. Notably, in case implicit TLS is not used, news clients SHOULD attempt to negotiate TLS even if the server does not advertise the STARTTLS capability label in response to the CAPABILITIES command (Section 2.1 of [RFC4642]).

3.5. Authenticated Connections

[RFC4642] already provides recommendations and requirements for certificate validation in the context of checking the client or the server's identity. Those requirements are strengthened by Appendix A.5 of this document.

Wherever possible, it is best to prefer certificate-based authentication (along with Simple Authentication and Security Layer (SASL) [RFC4422]), and ensure that:

- Clients authenticate servers.
- Servers authenticate clients.
- Servers authenticate other peer servers.

This document does not mandate certificate-based authentication, although such authentication is strongly preferred. As mentioned in Section 2.2.2 of [RFC4642], the AUTHINFO SASL command (Section 2.4 of [RFC4643]) with the EXTERNAL mechanism (Appendix A of [RFC4422]) MAY be used to authenticate a client once its TLS credentials have been successfully exchanged.

Given the pervasiveness of eavesdropping [RFC7258], even an encrypted but unauthenticated connection might be better than an unencrypted connection (this is similar to the "better-than-nothing security"

approach for IPsec [RFC5386], and in accordance with opportunistic security principles [RFC7435]). Encrypted but unauthenticated connections include connections negotiated using anonymous Diffie-Hellman mechanisms or using self-signed certificates, among others.

Note: when an NNTP server receives a Netnews article, it MAY add a <diag-match> (Section 3.1.5 of [RFC5536]), which appears as "!!" in the Path header field of that article, to indicate that it verified the identity of the client or peer server. This document encourages the construction of such Path header fields, as described in Section 3.2.1 of [RFC5537].

3.6. Human Factors

NNTP clients SHOULD provide ways for end users (and NNTP servers SHOULD provide ways for administrators) to complete at least the following tasks:

- Determine if a given incoming or outgoing connection is encrypted using a security layer (either using TLS or an SASL mechanism that negotiates a security layer).
- Be warned if the version of TLS used for encryption of a given stream is not secure enough.
- If authenticated encryption is used, determine how the connection was authenticated or verified.
- Be warned if the certificate offered by an NNTP server cannot be verified.
- Be warned if the cipher suite used to encrypt a connection is not secure enough.
- Be warned if the certificate changes for a given server.
- When a security layer is not already in place, be warned if a given server stops advertising the STARTTLS capability label in response to the CAPABILITIES command (Section 2.1 of [RFC4642]), whereas it advertised the STARTTLS capability label during any previous connection within a (possibly configurable) time frame. (Otherwise, a human might not see the warning the first time, and the warning would disappear immediately after that.)
- Be warned if a failure response to the STARTTLS command is received from the server, whereas the STARTTLS capability label was advertised.

Note that the last two tasks cannot occur when implicit TLS is used, and that the penultimate task helps prevent an attack known as "SSL Stripping" (Section 2.1 of [RFC7457]).

4. Security Considerations

Beyond the security considerations already described in [RFC4642], [RFC6125], and [BCP195], the following caveat is worth mentioning when not using implicit TLS: NNTP servers need to ensure that they are not vulnerable to the STARTTLS command injection vulnerability (Section 2.2 of [RFC7457]). Though this command MUST NOT be pipelined, an attacker could pipeline it. Therefore, NNTP servers MUST discard any NNTP command received between the use of STARTTLS and the end of TLS negotiation.

5. IANA Considerations

This document does not change the formal definition of the STARTTLS extension (Section 6 of [RFC4642]). Nonetheless, as implementations of the STARTTLS extension should follow this document, IANA has added reference to this document to the existing STARTTLS label in the "NNTP Capability Labels" registry contained in the "Network News Transfer Protocol (NNTP) Parameters" registry:

Label	Meaning	Reference
STARTTLS	Transport layer security	[RFC4642][RFC8143]

6. References

6.1. Normative References

[BCP14] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, <http://www.rfc-editor.org/info/bcp14>.

[BCP195] Sheffer, Y., Holz, R., and P. Saint-Andre, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", BCP 195, RFC 7525, May 2015, <https://www.rfc-editor.org/info/bcp195>.

[RFC3977] Feather, C., "Network News Transfer Protocol (NNTP)", RFC 3977, DOI 10.17487/RFC3977, October 2006, <http://www.rfc-editor.org/info/rfc3977>.

[RFC4422] Melnikov, A., Ed. and K. Zeilenga, Ed., "Simple Authentication and Security Layer (SASL)", RFC 4422, DOI 10.17487/RFC4422, June 2006, <http://www.rfc-editor.org/info/rfc4422>.

[RFC4642] Murchison, K., Vinocur, J., and C. Newman, "Using Transport Layer Security (TLS) with Network News Transfer Protocol (NNTP)", RFC 4642, DOI 10.17487/RFC4642, October 2006, <http://www.rfc-editor.org/info/rfc4642>.

[RFC4643] Vinocur, J. and K. Murchison, "Network News Transfer Protocol (NNTP) Extension for Authentication", RFC 4643, DOI 10.17487/RFC4643, October 2006, <http://www.rfc-editor.org/info/rfc4643>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <http://www.rfc-editor.org/info/rfc5246>.

[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>.

[RFC5536] Murchison, K., Ed., Lindsey, C., and D. Kohn, "Netnews Article Format", RFC 5536, DOI 10.17487/RFC5536, November 2009, <http://www.rfc-editor.org/info/rfc5536>.

[RFC5537] Allbery, R., Ed. and C. Lindsey, "Netnews Architecture and Protocols", RFC 5537, DOI 10.17487/RFC5537, November 2009, <http://www.rfc-editor.org/info/rfc5537>.

[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>.

6.2. Informative References

[CRIME] Rizzo, J. and T. Duong, "The CRIME Attack", Ekoparty Security Conference, 2012.

[MUA-STS] Moore, K. and C. Newman, "Mail User Agent Strict Transport Security (MUA-STS)", Work in Progress, draft-ietf-uta-email-deep-06, March 2017.

[PKI-CERT] Housley, R., Ford, W., Polk, T., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, DOI 10.17487/RFC3280, April 2002, <http://www.rfc-editor.org/info/rfc3280>.

[RFC3749] Hollenbeck, S., "Transport Layer Security Protocol Compression Methods", RFC 3749, DOI 10.17487/RFC3749, May 2004, <http://www.rfc-editor.org/info/rfc3749>.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <http://www.rfc-editor.org/info/rfc4301>.

[RFC5386] Williams, N. and M. Richardson, "Better-Than-Nothing Security: An Unauthenticated Mode of IPsec", RFC 5386, DOI 10.17487/RFC5386, November 2008, <http://www.rfc-editor.org/info/rfc5386>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <http://www.rfc-editor.org/info/rfc7258>.

[RFC7435] Dukhovni, V., "Opportunistic Security: Some Protection Most of the Time", RFC 7435, DOI 10.17487/RFC7435, December 2014, <http://www.rfc-editor.org/info/rfc7435>.

[RFC7457] Sheffer, Y., Holz, R., and P. Saint-Andre, "Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS)", RFC 7457, DOI 10.17487/RFC7457, February 2015, <http://www.rfc-editor.org/info/rfc7457>.

[RFC7465] Popov, A., "Prohibiting RC4 Cipher Suites", RFC 7465, DOI 10.17487/RFC7465, February 2015, <http://www.rfc-editor.org/info/rfc7465>.

[RFC7590] Saint-Andre, P. and T. Alkemade, "Use of Transport Layer Security (TLS) in the Extensible Messaging and Presence Protocol (XMPP)", RFC 7590, DOI 10.17487/RFC7590, June 2015, <http://www.rfc-editor.org/info/rfc7590>.

[RFC8054] Murchison, K. and J. Elie, "Network News Transfer Protocol (NNTP) Extension for Compression", RFC 8054, DOI 10.17487/RFC8054, January 2017, <http://www.rfc-editor.org/info/rfc8054>.

Appendix A. Detailed Changes to RFC 4642

This section lists the detailed changes that this document applies to [RFC4642].

A.1. Related to TLS-Level Compression

The second sentence in the Abstract in [RFC4642] is replaced with the following text:

> The primary goal is to provide encryption for single-link confidentiality purposes, but data integrity, and (optional) certificate-based peer entity authentication are also possible.

The second sentence of the first paragraph in Section 2.2.2 of [RFC4642] is replaced with the following text:

> The STARTTLS command is usually used to initiate session security, although it can also be used for client and/or server certificate authentication.

A.2. Related to Implicit TLS

The third and fourth paragraphs in Section 1 of [RFC4642] are replaced with the following text:

> TCP port 563 is dedicated to NNTP over TLS, and registered in the IANA Service Name and Transport Protocol Port Number Registry for that usage. NNTP implementations using TCP port 563 begin the TLS negotiation immediately upon connection and then continue with the initial steps of an NNTP session. This immediate TLS negotiation on a separate port (referred to in this document as "implicit TLS") is the preferred way of using TLS with NNTP.
>
> If a host wishes to offer separate servers for transit and reading clients (Section 3.4.1 of [NNTP]), TCP port 563 SHOULD be used for implicit TLS with the reading server, and an unused port of its choice different than TCP port 433 SHOULD be used for implicit TLS with the transit server. The ports used for implicit TLS should be clearly communicated to the clients, and specifically that no plaintext communication occurs before the TLS session is negotiated.
>
> As some existing implementations negotiate TLS via a dynamic upgrade from unencrypted to TLS-protected traffic during an NNTP session on well-known TCP ports 119 or 433, this specification

> formalizes the STARTTLS command in use for that purpose. However, as already mentioned above, implementations SHOULD use implicit TLS on a separate port.
>
> Note: a common alternative to protect NNTP exchanges with transit servers that do not implement TLS is the use of IPsec with encryption [RFC4301].

An additional informative reference to [RFC4301] is, therefore, added to Section 7.2 of [RFC4642].

A.3. Related to RC4 Cipher Suites

The third paragraph in Section 5 of [RFC4642] is removed. Consequently, NNTP no longer requires the implementation of any cipher suites, other than those prescribed by TLS (Section 9 of [RFC5246]), and Sections 4.2 and 4.2.1 of RFC 7525 [BCP195].

A.4. Related to Server Name Indication

The last two sentences of the seventh paragraph in Section 2.2.2 of [RFC4642] are removed. Section 3.6 of RFC 7525 [BCP195] applies.

A.5. Related to Certificate Verification

The text between "During the TLS negotiation" and "identity bindings)." in Section 5 of [RFC4642] is replaced with the following text:

> During TLS negotiation, the client MUST verify the server's identity in order to prevent man-in-the-middle attacks. The client MUST follow the rules and guidelines defined in [RFC6125], where the reference identifier MUST be the server hostname that the client used to open the connection, and that is also specified in the TLS "server_name" extension [RFC6066]. The following NNTP-specific consideration applies: DNS domain names in server certificates MAY contain the wildcard character "*" as the complete leftmost label within the identifier.
>
> If the match fails, the client MUST follow the recommendations in Section 6.6 of [RFC6125] regarding certificate pinning and fallback.
>
> Beyond server identity checking, clients also MUST apply the procedures specified in [RFC5280] for general certificate validation (e.g., certificate integrity, signing, and path validation).

Additional normative references to [RFC5280] (replacing [PKI-CERT], which it obsoletes), [RFC6066], and [RFC6125] are, therefore, added to Section 7.1 of [RFC4642].

A.6. Related to Other Obsolete Wording

The first two sentences of the seventh paragraph in Section 2.2.2 of [RFC4642] are removed. There is no special requirement for NNTP with regard to TLS Client Hello messages. Section 7.4.1.2 and Appendix E of [RFC5246] apply.

Acknowledgments

This document draws heavily on ideas in [RFC7590] by Peter Saint-Andre and Thijs Alkemade; a large portion of this text was borrowed from that specification.

The author would like to thank the following individuals for contributing their ideas and support for writing this specification: Stephane Bortzmeyer, Ben Campbell, Viktor Dukhovni, Stephen Farrell, Sabahattin Gucukoglu, Richard Kettlewell, Jouni Korhonen, Mirja Kuehlewind, David Eric Mandelberg, Matija Nalis, Chris Newman, and Peter Saint-Andre.

Special thanks to Michael Baeuerle, for shepherding this document, and to the Responsible Area Director, Alexey Melnikov, for sponsoring it. They both significantly helped to increase its quality.

Author’s Address

Julien Elie
10 allee Clovis
Noisy-le-Grand 93160
France

Email: julien@trigofacile.com
URI: http://www.trigofacile.com/