Independent Submission
Internet-Draft
Updates: 4642 (if approved)
Intended status: Standards Track
Expires: January 24, 2017

J. Elie

July 23, 2016

Use of Transport Layer Security (TLS) in the Network News Transfer Protocol (NNTP) draft-elie-nntp-tls-recommendations-00

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. If approved, this document updates RFC 4642.

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 January 24, 2017.

Copyright Notice

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 or SSL) since at least year 2000. The use of TLS in NNTP was formalized in [RFC4642], providing at the same time implementation recommendations. 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 the "Recommendations for Secure Use of TLS and DTLS" [RFC7525]. This includes stronger recommendations regarding SSL/TLS protocol versions, fallback to lower versions, strict TLS, TLS-level compression, TLS session resumption, cipher suites, public key lengths, forward secrecy, and other aspects of using TLS with NNTP.

Notably, this document updates [RFC4642] in the following aspects:

- NNTP implementations and deployments SHOULD disable TLS-level compression (Section 3.3 of [RFC7525]), thus no longer using TLS

  as a means to provide data compression (contrary to Abstract and Section 2.2.2 of [RFC4642]).

- NNTP implementations and deployments SHOULD prefer strict TLS configuration (Section 3.2 of [RFC7525]), that is to say they SHOULD use TCP port 563 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). For the same reasons as those given in Appendix A of [MUA-STS] transposed to NNTP, strict TLS is the preferred way of using TLS with NNTP.

- NNTP implementations and deployments MUST NOT negotiate RC4 cipher suites ([RFC7465]) contrary to Section 5 of [RFC4642] that 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 of Section 4.2.1 of [RFC7525] instead.

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].

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 [RFC2119].

1.2. Author's Note

Please write the first letter of "Elie" and the penultimate letter of "allee" with an acute accent wherever possible -- they are respectively U+00C9 ("É" in XML) and U+00E9 ("é" in XML).

2. Recommendations

The best current practices documented in the "Recommendations for Secure Use of TLS and DTLS" [RFC7525] are included here by reference. Instead of repeating those recommendations here, this document mostly provides supplementary information regarding secure implementation and deployment of NNTP technologies.

2.1. Compression

NNTP supports the use of the COMPRESS command, defined in Section 2.2 of [NNTP-COMPRESS], 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 CRIME attack, as described in Section 2.6 of [CRIME]), this document neither encourages nor discourages use of NNTP COMPRESS extension.

2.2. Protocol Versions and Cipher Suites

NNTP implementations are encouraged to support options to configure the minimal TLS protocol version to accept, and the cipher suites not to accept. Additional options can naturally also be supported. The goal is to enable news administrators to easily and quickly strengthen security, if need be.

2.3. Authenticated Connections

[RFC4642] already provides recommendations and requirements for certificate validation in the context of checking the client or the server's identity.

Wherever possible, it is best to prefer certificate-based authentication (along with 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]). Encrypted but unauthenticated connections include connections negotiated using anonymous

Diffie-Hellman mechanisms or using self-signed certificates, among others.

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].

2.4. Human Factors

It is strongly encouraged that NNTP clients provide ways for end users (and that NNTP servers provide ways for administrators) to complete 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).

- Determine the version of TLS used for encryption of a given stream.

- If authenticated encryption is used, determine how the connection was authenticated or verified.
- Inspect the certificate offered by an NNTP server.
- Determine the cipher suite used to encrypt a connection.
- Be warned if the certificate changes for a given server.
- Be warned if a given server stops advertising the STARTTLS capability label in response to the CAPABILITIES command (of course when a security layer is not already in place) whereas it advertised the STARTTLS capability label during the previous connection.
- 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 strict TLS is used.

3. Security Considerations

Beyond the security considerations already described in [RFC4642] and [RFC7525], the author wishes to add the following caveat when not using strict TLS.

NNTP servers need ensure that they are not vulnerable to the STARTTLS command injection vulnerability (CERT vulnerability ID #555316). 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.

4. IANA Considerations

This document has no actions for IANA.

5. References

5.1. 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>.

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

[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>.

5.2. 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)", July 2016.

[NNTP-COMPRESS] Murchison, K. and J. Elie, "Network News Transfer Protocol (NNTP) Extension for Compression", June 2016.

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

[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>.

[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>.

[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>.

[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>.

[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>.

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

[RFC7525] 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, DOI 10.17487/RFC7525, May 2015, <http://www.rfc-editor.org/info/rfc7525>.

[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>.

Appendix A. Changes to RFC 4642

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

The second sentence in the Abstract of [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 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 use of strict TLS on a separate port is the preferred way of using TLS with NNTP.
>
> As some existing implementations negotiate TLS via a dynamic upgrade from unencrypted to TLS-protected traffic during an NNTP session, this specification formalizes the STARTTLS command in use for that purpose. However, as already mentioned above, implementations SHOULD use strict TLS on a separate port.

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.

The third paragraph in Section 5 of [RFC4642] is removed. Consequently, NNTP no longer requires to implement any cipher suites, other than those prescribed by TLS [RFC5246] and Section 4.2.1 of [RFC7525].

Appendix B. Implementation Notes

Some governments enforce legislation prohibiting the export of strong cryptographic technologies. Nothing in this document ought to be taken as advice to violate such prohibitions.

Appendix C. Acknowledgements

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

Appendix D. Issues to Address

- Should the paragraph starting with "Servers MUST be able to understand backwards-compatible TLS Client Hello messages" in Section 2.2.2 of [RFC4642] be modernized with current TLS practices? (And which ones?)

- Should the paragraphs in Section 5 of [RFC4642] dealing with how the client checks the server hostname and the binding between the identity of servers and the public keys presented be modernized? (Obsolete them in favour of RFC 6125 for instance?)

- Section 3.2 of [RFC7525] applied to NNTP adds the following requirement: a client SHOULD attempt to negotiate TLS even if the STARTTLS capability label is not advertised by the news server. The goal is to help prevent SSL Stripping. Yet, an attacker who can strip STARTTLS from the capability list could easily ensure that 502 is answered to that command. So, should we all the same keep that requirement for NNTP? (I would suggest not to keep it.)

- Regarding peering between mode-switching news servers, should something specific be added? (e.g., as strict TLS is the preferred way to negotiate TLS, innfeed would connect to port 563 of a news server, and innd would also listen on port 563. Or should we ask the registration of a new port for that purpose, NNSP over TLS, like port 433 already dedicated to NNSP? Or should we recommend the use of stunnel with TCP wrappers, or an equivalent mechanism, in case using a separate port is not possible?)

Author's Address

Julien Elie

10 allee Clovis
Noisy-le-Grand 93160
France

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