Network Working Group
Internet-Draft
Updates: 6120 (if approved)
Intended status: Standards Track
Expires: May 30, 2015

P. Saint-Andre
&yet
T. Alkemade

November 26, 2014

Use of Transport Layer Security (TLS) in the Extensible Messaging and Presence Protocol (XMPP) draft-ietf-uta-xmpp-04

Abstract

This document provides recommendations for the use of Transport Layer Security (TLS) in the Extensible Messaging and Presence Protocol (XMPP). This document updates RFC 6120.

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 May 30, 2015.

Copyright Notice

Table of Contents

1. Introduction

The Extensible Messaging and Presence Protocol (XMPP) [RFC6120] (along with its precursor, the so-called "Jabber protocol") has used Transport Layer Security (TLS) [RFC5246] (along with its precursor, Secure Sockets Layer or SSL) since 1999. Both [RFC6120] and its predecessor [RFC3920] provided recommendations regarding the use of TLS in XMPP. In order to address the evolving threat model on the Internet today, this document provides stronger recommendations.

> NOTE: Unless explicitly noted otherwise, all of the recommendations specified in [I-D.ietf-uta-tls-bcp] apply to XMPP. In the main, this document merely provides supplementary information; those who implement and deploy XMPP technologies are expected to follow the recommendations of [I-D.ietf-uta-tls-bcp].

This document updates [RFC6120].

2. Terminology

Various security-related terms are to be understood in the sense defined in [RFC4949].

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].

3. Recommendations

3.1. Support for TLS

Support for TLS (specifically, the XMPP profile of STARTTLS) is mandatory for XMPP implementations, as already specified in [RFC6120] and its predecessor [RFC3920].

The server (i.e., the XMPP receiving entity) to which a client or peer server (i.e., the XMPP initiating entity) connects might not offer a stream feature of <starttls xmlns='urn:ietf:params:xml:ns :xmpp-tls'/>. Although in general this stream feature indicates that the server supports XMPP 1.0 and therefore supports TLS, it is possible that this stream feature might be stripped out by an attacker (see Section 2.1 of [I-D.ietf-uta-tls-attacks]). Therefore, the initiating entity SHOULD proceed with the stream negotiation even if the receiving entity does not advertise support for TLS. Similarly, although a receiving entity SHOULD include the <required/> child element to indicate that negotiation of TLS is mandatory, an initiating entity MUST NOT depend on receiving the <required/> flag in determining whether TLS will be enforced for the stream.

3.2. Compression

XMPP supports an application-layer compression technology [XEP-0138]. Although this XMPP extension might have slightly stronger security properties than TLS-layer compression (since it is enabled after SASL authentication, as described in [XEP-0170]), this document neither encourages nor discourages use of XMPP-layer compression.

3.3. Session Resumption

In XMPP, TLS session resumption can be used in concert with the XMPP Stream Management extension; see [XEP-0198] for further details.

3.4. Authenticated Connections

Both the core XMPP specification [RFC6120] and the "CertID" specification [RFC6125] provide recommendations and requirements for certificate validation in the context of authenticated connections. This document does not supersede those specifications. Wherever possible, it is best to prefer authenticated connections (along with SASL [RFC4422]), as already stated in the core XMPP specification [RFC6120]. In particular, clients MUST authenticate servers. Because this document does not mandate that servers need to authenticate peer servers, unauthenticated server-to-server connections are allowed (consistent with current practice on the XMPP network).

This document does not modify the recommendations in [RFC6120] regarding the Subject Alternative Names (or other certificate details) that need to be supported for authentication of XMPP connections.

3.5. Unauthenticated Connections

Given the pervasiveness of passive eavesdropping, even an unauthenticated connection might be better than an unencrypted connection (this is similar to the "better than nothing security" approach for IPsec [RFC5386]). In particular, because of current deployment challenges for authenticated connections between XMPP servers (see [I-D.ietf-xmpp-dna] and [I-D.ietf-xmpp-posh] for details), it can be reasonable for XMPP server implementations to accept unauthenticated connections when the Server Dialback protocol [XEP-0220] is used for weak identity verification; this will at least enable encryption of server-to-server connections. Unauthenticated connections include connections negotiated using anonymous Diffie-Hellman algorithms or using self-signed certificates, among other scenarios.

3.6. Server Name Indication

Although there is no harm in supporting the TLS Server Name Indication (SNI) extension [RFC6066], this is not necessary since the same function is served in XMPP by the 'to' address of the initial stream header as explained in Section 4.7.2 of [RFC6120].

3.7. Human Factors

It is strongly encouraged that XMPP clients provide ways for end users (and that XMPP servers provide ways for administrators) to complete the following tasks:

- Determine if a client-to-server or server-to-server connection is encrypted and authenticated.
- Determine the version of TLS used for a client-to-server or server-to-server connection.
- Inspect the certificate offered by an XMPP server.
- Determine the cipher suite used to encrypt a connection.
- Be warned if the certificate changes for a given server.

4. IANA Considerations

This document requests no actions of the IANA.

5. Security Considerations

The use of TLS can help limit the information available for correlation to the network and transport layer headers as opposed to the application layer. As typically deployed, XMPP technologies do not leave application-layer routing data (such as XMPP 'to' and 'from' addresses) at rest on intermediate systems, since there is only one hop between any two given XMPP servers. As a result, encrypting all hops (sending client to sender's server, sender's server to recipient's server, recipient's server to recipient's client) can help to limit the amount of "metadata" that might leak.

It is possible that XMPP servers themselves might be compromised. In that case, per-hop encryption would not protect XMPP communications, and even end-to-end encryption of (parts of) XMPP stanza payloads would leave addressing information and XMPP roster data in the clear. By the same token, it is possible that XMPP clients (or the end-user devices on which such clients are installed) could also be compromised, leaving users utterly at the mercy of an adversary.

This document and related actions to strengthen the security of the XMPP network are based on the assumption that XMPP servers and clients have not been subject to widespread compromise. If this assumption is valid, then ubiquitous use of per-hop TLS channel encryption and more significant deployment of end-to-end object encryption technologies will serve to protect XMPP communications to a measurable degree, compared to the alternatives.

6. References

6.1. Normative References

[I-D.ietf-uta-tls-bcp]
Sheffer, Y., Holz, R., and P. Saint-Andre, "Recommendations for Secure Use of TLS and DTLS", draft-ietf-uta-tls-bcp-07 (work in progress), November 2014.

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

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", RFC 4949, August 2007.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC6120] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 6120, March 2011.

[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.

6.2. Informative References

[I-D.ietf-uta-tls-attacks]
Sheffer, Y., Holz, R., and P. Saint-Andre, "Summarizing Current Attacks on TLS and DTLS", draft-ietf-uta-tls-attacks-05 (work in progress), October 2014.

[I-D.ietf-xmpp-dna]
Saint-Andre, P. and M. Miller, "Domain Name Associations (DNA) in the Extensible Messaging and Presence Protocol (XMPP)", draft-ietf-xmpp-dna-08 (work in progress), October 2014.

[I-D.ietf-xmpp-posh]
Miller, M. and P. Saint-Andre, "PKIX over Secure HTTP (POSH)", draft-ietf-xmpp-posh-02 (work in progress), October 2014.

[RFC3920] Saint-Andre, P., Ed., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 3920, October 2004.

[RFC4422] Melnikov, A. and K. Zeilenga, "Simple Authentication and Security Layer (SASL)", RFC 4422, June 2006.

[RFC5386] Williams, N. and M. Richardson, "Better-Than-Nothing Security: An Unauthenticated Mode of IPsec", RFC 5386, November 2008.

[RFC6066] Eastlake, D., "Transport Layer Security (TLS) Extensions: Extension Definitions", RFC 6066, January 2011.

[XEP-0138]
Hildebrand, J. and P. Saint-Andre, "Stream Compression", XSF XEP 0138, May 2009.

[XEP-0170]
Saint-Andre, P., "Recommended Order of Stream Feature Negotiation", XSF XEP 0170, January 2007.

[XEP-0198]
Karneges, J., Saint-Andre, P., Hildebrand, J., Forno, F., Cridland, D., and M. Wild, "Stream Management", XSF XEP 0198, June 2011.

[XEP-0220]
Miller, J., Saint-Andre, P., and P. Hancke, "Server Dialback", XSF XEP 0220, September 2013.

Appendix A. 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 B. Acknowledgements

The authors would like to thank the following individuals for their input: Dave Cridland, Philipp Hancke, Olle Johansson, Steve Kille, Tobias Markmann, Matt Miller, and Rene Treffer.

Authors' Addresses

Peter Saint-Andre
&yet

Email: peter@andyet.com
URI: https://andyet.com/

Thijs Alkemade

Email: me@thijsalkema.de